Universidade do Minho

Virtualização de Redes

Trabalho Prático Nº 3

Anycast Communication in SDN

André Vieira A78322

João Freitas A74814

João Mendes A71862

July 8, 2020

Índice

Índice de Imagens

Acrónimos

GNS3 gns3

SDN Redes Definidas por Software

OpenflowManager openflow

OpendayLight openday

OpenVSwitch OVS

Anycast any

Unicast uni

Spanning Tree Protocol stp

Chapter 1

Introdução

Neste relatório iremos expor o processo de desenvolvimento do trabalho prático nº3 da Unidade Curricular de Virtualização de Redes. Este trabalho teve como objetivo aprofundar os conhecimentos relativos ao uso de *GNS3* como ferramenta de gestão de redes criando uma topologia de rede.

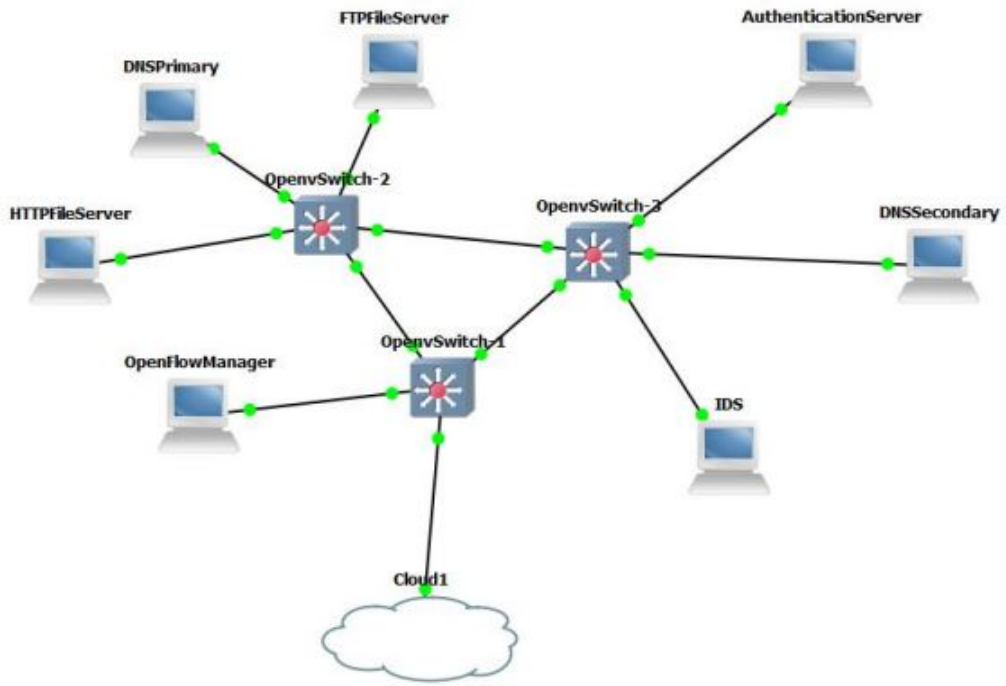

Figure 1.1: Topologia Base

Também aprofundamos os conhecimentos do *OpenflowManager* bem como a implementação das regras de monitorização dos flows dentro da nossa rede.

De seguida irão ser apresentados os conceitos teóricos referentes ao trabalho realizado, seguida da solução criada e a implementação da mesma. Finalizando com a conclusão do trabalho.

Chapter 2

Conceitos Teóricos

2.1 Redes SDN

SDN é um conceito da separação física do plano de controlo da rede, do plano de encaminhamento. Os nós de redes (*switches*) são programados por uma entidade central (*controller*) através de um protocolo bem definido (OpenFlow). Os *switches* fazem o encaminhamento de acordo com as tabelas (*flow tables*) que são preenchidas pelo *controller*.

Benefícios das redes *SDN*:

- Arquitetura é totalmente independente dos fabricantes: O controlador *SDN* gere qualquer dispositivo de rede, independentemente do fabricante, desde que esteja habilitado com o OpenFlow.
- Simplicidade na conceção e operação de rede: É possível desenvolver ferramentas para automatizar muitas tarefas que são feitas atualmente de forma manual.
- Maior fiabilidade e segurança: A automação reduz a probabilidade de falha de configuração ou inconsistência de políticas.
- Melhora a experiência de utilização.

2.2 OpenFlow Protocol

OpenFlow é um protocolo de comunicação, que nasceu de uma tese de doutoramento de um estudante, da Universidade de Stanford, Martin Casado, considerado um dos primeiros padrões da *SDN* que permite aos controladores de rede determinarem o caminho dos pacotes de rede ao longo de uma rede de *switches*.

Este protocolo permite, também, a administração remota de tabelas de encaminhamento de pacotes de um *switch* da camada de rede (*layer 3*) por adicionar, modificar e remover regras e ações de correspondência de pacotes.

Chapter 3

Implementação

3.1 Topologia

Para a resolução deste trabalho decidimos desenvolver a seguinte topologia tendo como base a topologia colocada na introdução, sendo que, tiveram que ser feitas diversas alterações, nomeadamente, nas ligações entre os *OpenVSwitch* para evitar loops.

NOTA:Posteriormente vai ser mencionado o comando ***ovs-vsctl set Bridge br0 stp_ enable=true*** *que evita este problema.*

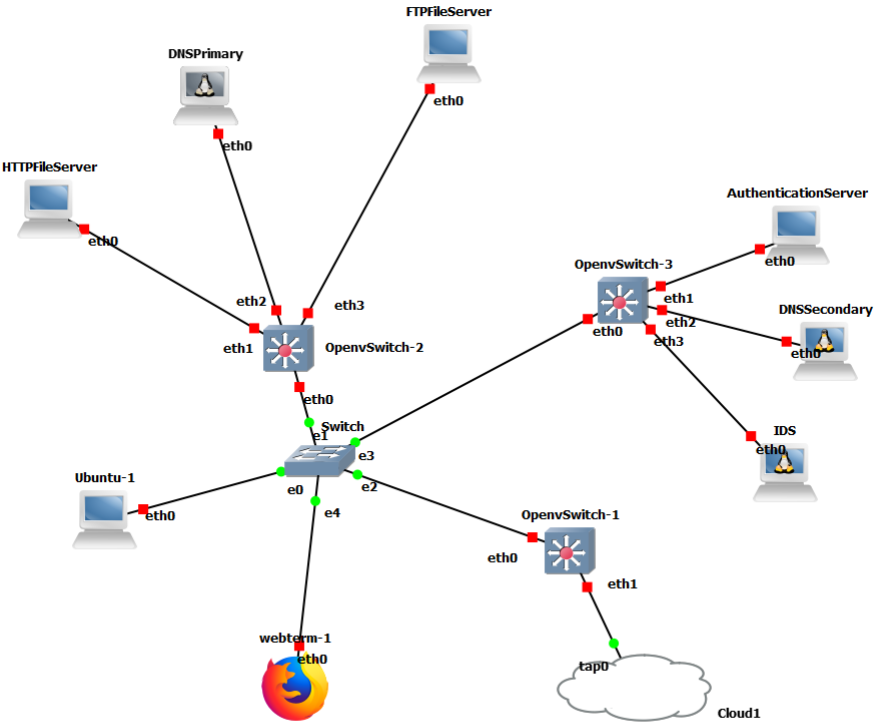

Figure 3.1: Topologia da rede

3.2 Configuração

Todos os end-devices desta rede têm dois endereços, um *Unicast* na gama *192.168.3.0/24* e um *Anycast* na gama *10.1.1.0/24*.

- **OpenFlowManager**-*Unicast*-*192.168.3.2*|*Anycast* *10.1.1.2*
- **HTTPFileServer**-*Unicast*-*192.168.3.3*|*Anycast* *10.1.1.3*
- **DNSPrimary**-*Unicast*-*192.168.3.4*|*Anycast* *10.1.1.4*
- **FTPFileServer**-*Unicast*-*192.168.3.5*|*Anycast* *10.1.1.5*
- **AuthenticationServer**-*Unicast*-*192.168.3.6*|*Anycast* *10.1.1.6*
- **DNSSecondary**-*Unicast*-*192.168.3.7*|*Anycast* *10.1.1.7*
- **IDS**-*Unicast*-*192.168.3.8*|*Anycast* *10.1.1.8*

De seguida, instalou-se *OpendayLight* e a *OpenflowManager* app no nó **OpenFlowManager** e foram atribuídos os seguintes endereços para a interface **eth0** de todos os *OpenVSwitch*.

- **OpenvSwitch-1**-*192.168.3.201*
- **OpenvSwitch-2**-*192.168.3.202*
- **OpenvSwitch-3**-*192.168.3.203*

Posteriormente, é necessário que o *OpenflowManager* conheça os *OpenVSwitch* da topologia, para tal foram executados os seguintes comandos para definir um end-device como controller e ligar a funcionalidade *Spanning Tree Protocol*, respetivamente.

```
ovs-vsctl set-controller br0 tcp:192.168.3.2:6633
ovs-vsctl set Bridge br0 stp_enable=true
```

Para comprovamos que está tudo connectado utilizaou-se o comando *ovs-vsctl list controller*.

Figure 3.2: OpenvSwitch ligado a um controller

Pode-se agora aceder ás páginas de configuração do *OpendayLight* e *OpenflowManager* através dos seguintes endereços.

- *OpendayLight-192.168.3.2:8181/index.html*
- *OpenflowManager-192.168.3.2:9000*

Ao executar o comando *ping* do **HTTPFileServer** para todos os outros nós da rede, consegue-se obter a topologia inteira nessas páginas.

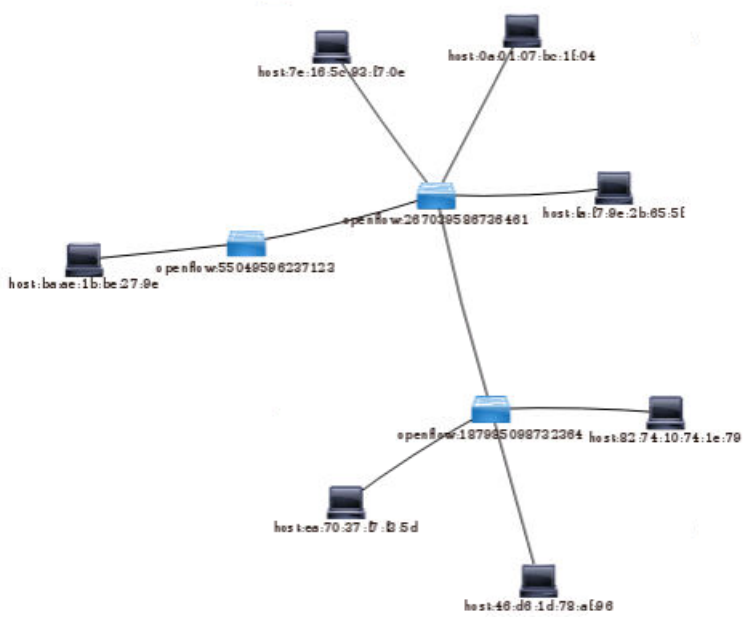

Figure 3.3: Representação da topologia dentro do *OpendayLight*

3.3 Regras OpenDaylight

Por fim foram definidas as diversas regras para cada *flow* e cada *OpenVSwitch* de acordo com os requisitos do enunciado.

3.3.1 Permitir *Anycast* DNS interno

Para permitir *Anycast* DNS interno é necessário definir 2 regras, uma que permita *flows Anycast*, com fonte e destino na gama *10.1.1.0/24*, do tipo **DNS**, na porta 53, e outra que bloqueie todas as restantes.
Estas regras irão ser implementadas nos três *OpenVSwitch*.

```
ovs-ofctl add-flow br0 table=0,priority=1001,dl_type=0x0800,nw_proto=6,
nw_src=10.1.1.0/24,nw_dst=10.1.1.0/24,tp_dst=53,actions=normal
```

```
ovs-ofctl add-flow br0 table=0,priority=1000,dl_type=0x0800,nw_proto=6,
nw_src=10.1.1.0/24,nw_dst=10.1.1.0/24,actions=drop
```

3.3.2 Bloquear *Unicast* externo

Para bloquear *Unicast* externo basta bloquear todos os flows com origem na porta dois do *OpenVSwitch* 1 com endereço de destino na gama *192.168.3.0/24*.

```
ovs-ofctl add-flow br0 table=0,priority=1000,dl_type=0x0800,nw_proto=6,in_port=2,
nw_dst=192.168.3.0/24,actions=drop
```

3.3.3 Reencaminhar flows da porta 80 para AuthenticationServer

Para reencaminhar os flows da porta 80 é necessário adicionar a seguinte regra em todos os *OpenVSwitch*.

```
ovs-ofctl add-flow br0 table=1,priority=999,dl_type=0x0800,nw_proto=6,tp_dst=80,
actions=mod_nw_dst:192.168.3.6
```

O endereço fornecido em *mod_nw_dst* é o endereço do **AuthenticationServer**.

3.3.4 Reencaminhar flows da porta 81 para HTTPFileServer

Comportamento semelhante à regra anterior, sendo que agora as flows da porta 81 são reencaminhados para o **HTTPFileServer**.

```
ovs-ofctl add-flow br0 table=1,priority=999,dl_type=0x0800,nw_proto=6,tp_dst=81,
actions=mod_nw_dst:192.168.3.3
```

3.3.5 Reencaminhar flows FTP para FTPFileServer

Mais uma vez tem um comportamento semelhante ás duas regras anteriores, sendo que, mais uma vez, a porta muda para 21 e o destino para o **FTPFileServer**.

```
ovs-ofctl add-flow br0 table=1,priority=999,dl_type=0x0800,nw_proto=6,tp_dst=21,
actions=mod_nw_dst:192.168.3.5
```

3.3.6 DNS queries internas para DNSSecondary

Para esta regra é necessário implementar as seguintes flows:

```
ovs-ofctl add-flow br0 table=1,priority=950,dl_type=0x0800,nw_proto=6,
nw_src=10.1.1.0/24,tp_dst=53,actions=mod_nw_dst:192.168.3.7
```

```
ovs-ofctl add-flow br0 table=1,priority=950,dl_type=0x0800,nw_proto=6,
nw_src=192.168.3.0/24,tp_dst=53,actions=mod_nw_dst:192.168.3.7
```

A primeira envolve as **DNS** queries *Anycast* enquanto a segunda é para os *Unicast*.

3.3.7 DNS queries externas DNSPrimary

Para esta regra basta implementar a seguinte flow:

```
ovs-ofctl add-flow br0 table=1,priority=900,dl_type=0x0800,nw_proto=6,tp_dst=53,
actions=mod_nw_dst:192.168.3.4
```

3.3.8 Duplicar mensagens para IDS

Por fim temos a seguinte flow que tem como objetivo duplicar todas as mensagens válidas para o **IDS**.

```
ovs-ofctl add-flow br0 table=0,priority=800,dl_type=0x0800,nw_proto=6,
actions=normal,mod_nw_dst:192.168.3.8
```

3.3.9 Resultados

Infelizmente, foi nos impossível testar estas regras visto que as ações não eram adicionadas ás flows independentemente do comando exprimentado.

```
/ # ovs-ofctl add-flow br0 table=1,priority=999,dl_type=0x0800,nw_proto=6,tp_dst=80,actions=mod_nw_dst:192.168.3.6
```

Figure 3.4: Adição de regra

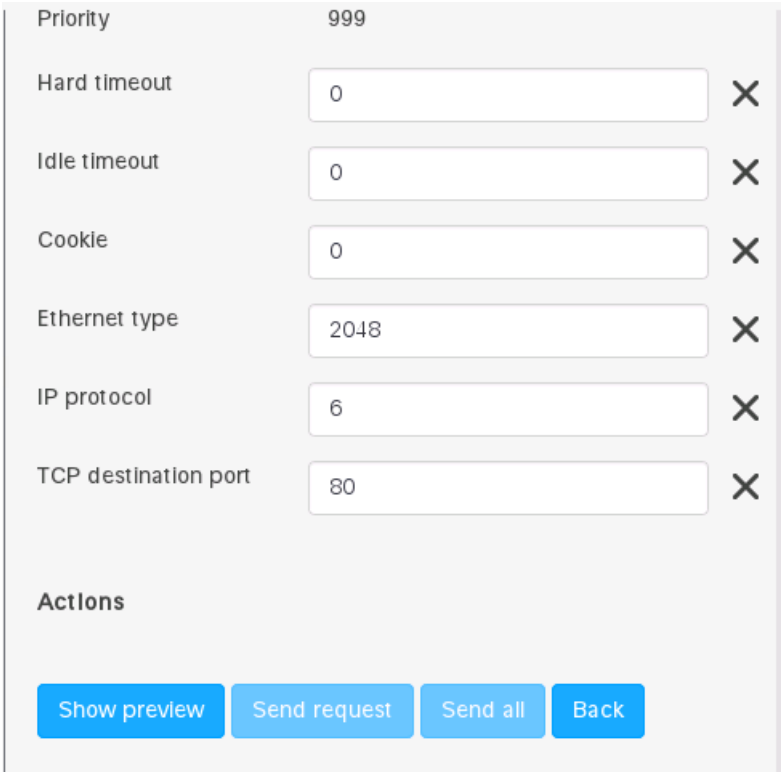

Figure 3.5: Resultado da regra

Chapter 4

Conclusão

Durante toda a resolução deste trabalho o grupo deparou-se com diversos problemas relacionados com a utilização do *OpendayLight* e *OpenflowManager*, cujas resoluções nos ocuparam demasiado tempo. Como tal, o tempo foi limitado para a fase final (implementação das regras do *OpenflowManager*), sendo que apareceu-nos um novo obstáculo.

Todavia, com este trabalho prático, o grupo conseguiu aprofundar os conhecimentos sobre o *GNS3* e *OpendayLight*, tendo um aproveitamento positivo mesmo com todos os obstáculos que foram encontrados durante a resolução do problema.

Em suma, o grupo está satisfeito com o trabalho realizado apesar de não o ter completado totalmente, pois sente-se capaz de conseguir utilizar as ferramentas no futuro se for necessário.