Estudo de caso de topologia de arquitetura de redes

Pedro Henrique Bufulin de Almeida[1], **Leonardo Ferreira Essia**[1], **Iury Resende Shirabiyoshi**[2]

[1]Ciência da Computação – Universidade Federal do Uberlândia (UFU)

[2]Engenharia Mecatrônica – Universidade Federal do Uberlândia (UFU)

Resumo. *Este trabalho tem como objetivo principal a familiarização dos estudantes autores com as features disponibilizadas pelo software GNS3 (Graphical Network Simulator-3). Tal aplicação fornece uma interface gráfica e vários outros recursos para a simulação de simples a complexas redes de computadores, podendo incluir tanto dispositivos virtuais como reais. Com isso, os estudantes têm a oportunidade também de realizar a experimentação e implementação das mais variadas configurações e protocolos de comunicação vistos nas aulas teóricas da disciplina de Arquitetura de Redes TCP/IP.*

1. Introdução

Ao longo das aulas da disciplina de Arquitetura de Redes TCP/IP os estudantes tiveram a oportunidade de aprofundar seus conhecimentos a respeito das camadas de Enlace, Rede e Transporte no contexto da comunicação entre sistemas em uma rede de computadores. Porém, além dos conteúdos teóricos, ao tratar da camada de Rede houve também a chance de cada aluno simular os mais variados ambientes de rede em aulas práticas de laboratório. Isso inclui o uso de diversos sistemas virtuais (como comutadores, roteadores e hosts) e configuração e teste de diferentes protocolos de comunicação (como roteamento estático, RIP, OSPF etc) entre hosts.

Todavia, diferentemente das aulas práticas, em que cada uma delas focava na configuração de um protocolo específico, este trabalho trata da simulação de uma topologia de rede mais complexa. Tal rede inclui diferentes redes locais/AS (Autonomous Systems), cada um com um tipo de protocolo de roteamento configurado, além da comunicação por tunelamento IPv6-in-IPv4 entre redes que usam diferentes versões de Internet Protocol.

A seguir serão descritos em mais detalhes as técnicas, a metodologia e os passos usados no desenvolvimento e configuração dessa topologia de rede mais complexa supramencionada. Isso inclui a descrição dos conceitos e protocolos explorados, além da demonstração dos elementos virtuais presentes na rede, com suas interfaces e endereços no contexto. Também são apresentados os comandos utilizados pelos estudantes nos consoles dos roteadores virtuais para habilitar diferentes protocolos de roteamento (RIP e OSPF), além de NAT (Network Address Translation) e DNS (Domain Namee System).

2. Protocolos e técnicas presentes na topologia desenvolvida

Ao longo da configuração dos elementos da topologia de rede desenvolvida, foram considerados os protocolos de roteamento RIP e OSPF para comunicação inter-AS, os quais serão melhor explicados a seguir. Ademais, também foi configurada a simulação da técnica NAT e do mecanismo DNS em um dos roteadores.

2.1. RIP (Routing Information Protocol)

O protocolo RIP é baseado no algoritmo de roteamento DV (Distance Vector), o qual usa a equação de Bellman-Ford para montar a tabela de custo de repasse entre os roteadores. O algoritmo em si é assíncrono, iterativo e distribuído: de tempos em tempos (no caso do RIP a cada 30 segundos) cada nó da rede envia uma atualização de suas estimativas de custo para os nós vizinhos. Então, se um vizinho recebe uma nova estimativa, ele atualiza suas próprias estimativas (usando a equação de BF) e as propaga para seus próprios vizinhos. Mais especificamente, além desse algoritmo, o RIP utiliza também da técnica de ”poisoned reverse” para evitar iterações contínuas desnecessárias quando algum enlace aumenta de custo. [Malkin 1998]

Nesse protocolo, caso nenhum anúncio seja recebido num intervalo de 180 segundos, seu nó relacionado é considerado ”morto” e esta informação de falha rapidamente se propaga pela rede. Vale também mencionar tais anúncios são enviados pelo protocolo de comunicação de camada de transporte UDP, um protocolo não orientado a conexão e que preza pelo ”melhor esforço” no envio de dados. [Kurose and Ross 2006]

2.2. OSPF (Open Shorstest Path First)

Já o roteamento OSPF é um dos protocolos mais empregados, sendo desenvolvido justamente para substituir o RIP, que apresentou algumas limitações para operar em redes com muitos nós. Nesse caso, cada nó da rede contém informações sobre todos os enlaces/links da mesma e, caso haja mudança no valor de custo de algum caminho, o protocolo usa do algoritmo de Estado do Enlace (Dijkstra) para propagar as atualizações na topologia. Outras diferenças relevantes nesse tipo de roteamento são o fato de que podem existir múltiplos caminhos de mesmo custo e que as mensagens de anúncio são enviadas diretamente por protocolo IP (camada de rede) por ”pacotes OSPF”. [Moy 1998]

2.3. NAT (Network Address Translation)

O NAT é um esquema pelo qual uma rede local (por exemplo uma rede doméstica) usa de apenas um endereço IP para comunicar com o ”mundo exterior”, ou seja, apenas um endereço IP é utilizado para alcançar todos os dispositivos dessa rede. Isso é possível devido ao uso de uma tabla hash de tradução de endereços e portas para eencaminhar devidamente os datagramas quando os mesmos passam pelo roteador que implementa o NAT.

Essa técnica foi desenvolvida inicialmente como uma solução alternativa à possível falta de endereços no contexto IPv4, porém, mesmo com a posterior vinda do IPv6, ainda possui algumas vantagens: caso haja alguma mudança de disposição interna dos nós da rede local, a mesma não precisa comunicar elas para o mundo exterior; além de haver uma camada de segurança a mais, já que o ”mundo exterior” não sabe os reais endereços IP dos hosts finais.

2.4. DNS (Domain Name System)

O DNS é basicamente um sistema de gestão de nomes de domínios relacionados aos seus devidos endereços IP. Nesse esquema tem-se uma arquitetura de cliente-servidor que, assim como o RIP, também usa do protocolo UDP para a devida comunicação lógica entre os processos de resolução de nomes (o servidor resolve nomes para endereços).

Há pelo menos uma dezena de ”servidores DNS raiz” espalhados pelo mundo, essenciais para o devido funcionamento da Internet. Isso porque, para os usuário humanos, é muito mais realista e natural procurar por recursos online buscando pelos seus nomes/domínios do que acessando diretamente seus números de endereço IP.

2.5. Tunelamento IPv6-in-IPv4

Por fim, vale comentar também da técnica de tunelamento que foi utilizada para habilitar a comunicação entre hosts que utilizam de diferentes versões do Internet Protocol na topologia. Como redes IPv4 e IPv6 não são diretamente compatíveis entre si, pode-se utilizar esse método ”tunneling” no qual um pacote IPv6 é encapsulado num pacote IPv4. Com isso fica possível, por exemplo, ”ilhas” IPv6 mantendo suas redes intrmediárias em IPv4, sem a necessidade de alterar qualquer configuração de roteamento já utilizada pela infraestrutura.

3. Metodologia

Foi implementada no software de simulação GNS3 a seguinte topologia de rede ilustrada na figura 1.

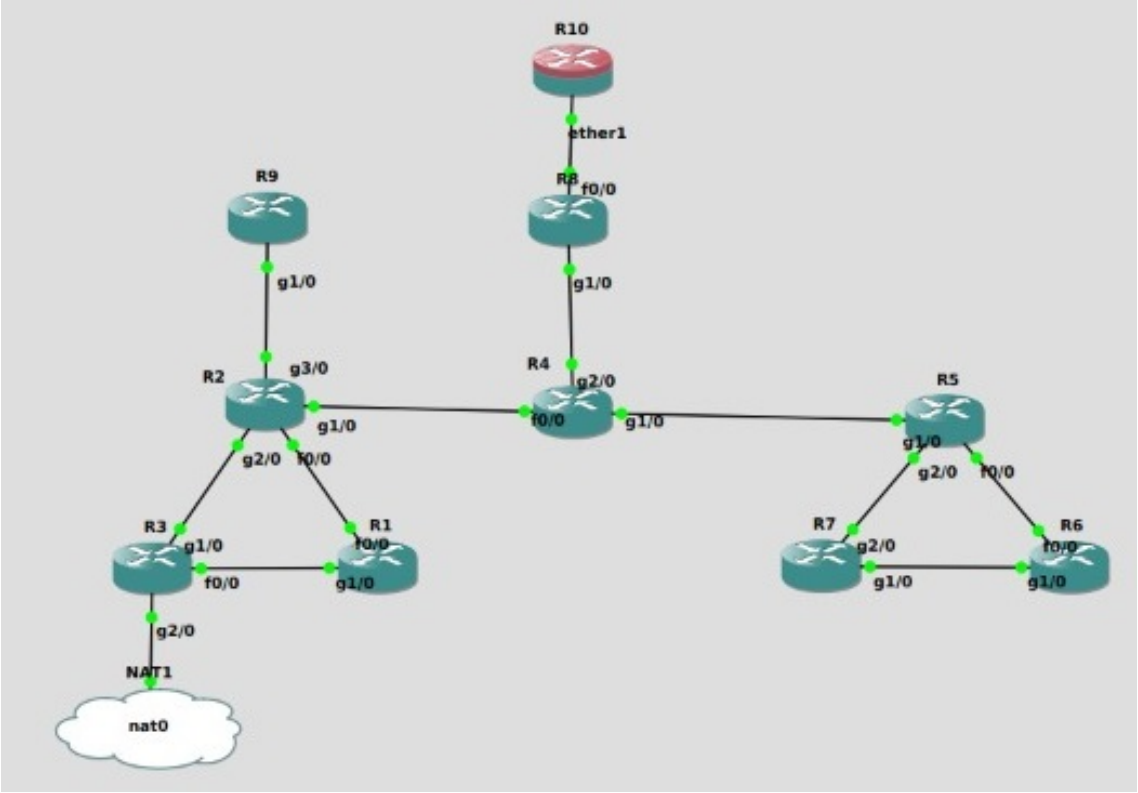

Figure 1. Topologia de rede desenvolvida no software GNS3

Como pode ser observado, foram utilizados 10 rotadores (9 Cisco e 1 Mikrotik), interconectados de modo serem geradas 11 redes (cada interface tem seu próprio IP, de acordo com a tabela que será apresentada).

Além das configurações básicas de inicialização de cada roteador, relativas a determinação de interfaces e endereçamento, foram também configurados diferentes protocolos de roteamento para diferentes grupos de roteadores. O grupo de roteadores R1,

R2, R3, R4, R8 e R9 implementam o roteamento RIP, enquanto o grupo R4 (apenas sua interface relativa a rede 192.168.5.0/30), R5, R6 e R7 implementam o OSPF.

Foi também configurado o esquema NAT em uma das interfaces do roteador R3, o qual também foi escolhido para ser configurado como o DNS server da topologia. Quanto à aplicação da técnica de tunelamento, essa foi configurada na comunicação entre uma das interfaces de R8 com o roteador R9.

A seguir é apresentada a tabela contendo uma relação com as interfaces e endereçamentos usados para cada roteador da topologia:

Hostname	Interface	CIDR	Máscara	iOS
R1	f0/0	192.168.1.1/30	255.255.255.252	Cisco
	g1/0	192.168.2.1/30	255.255.255.252	Cisco
R2	f0/0	192.168.1.2/30	255.255.255.252	Cisco
	g1/0	192.168.4.1/30	255.255.255.252	Cisco
	g2/0	192.168.3.1/30	255.255.255.252	Cisco
	g3/0	192.168.9.2/30	255.255.255.252	Cisco
R3	f0/0	192.168.2.2/30	255.255.255.252	Cisco
	g1/0	192.168.3.2/30	255.255.255.252	Cisco
	g2/0	gerado por dhcp	255.255.255.252	Cisco
R4	f0/0	192.168.4.2/30	255.255.255.252	Cisco
	g1/0	192.168.5.1/30	255.255.255.252	Cisco
	g2/0	192.168.8.2/30	255.255.255.252	Cisco
R5	g1/0	192.168.5.2/30	255.255.255.252	Cisco
	f0/0	192.168.6.1/30	255.255.255.252	Cisco
	g2/0	192.168.11.1/30	255.255.255.252	Cisco
R6	f0/0	192.168.6.2/30	255.255.255.252	Cisco
	g1/0	192.168.7.1/30	255.255.255.252	Cisco
R7	g1/0	192.168.7.2/30	255.255.255.252	Cisco
	g2/0	192.168.11.2/30	255.255.255.252	Cisco
R8	g1/0	192.168.8.1/30	255.255.255.252	Cisco
	f0/0	192.168.10.2/30	255.255.255.252	Cisco
R9	g1/0	192.168.9.1/30	255.255.255.252	Cisco
R10	ether1	192.168.10.1/30	255.255.255.252	Mikrotik

Table 1. Relação de roteadores, interfaces e endereços

Quanto aos comandos utilizados nos terminais de cada virtual router, pode-se subdividí-los de acordo com o seguinte esquema:

3.1. Comandos de configuração para cada roteador

Abaixo, os comandos que usamos para implementar o protocolo IP em cada roteador.

```
> R1
# configure terminal
```

```
# interface fastEthernet 0/0
# ip address 192.168.1.1 255.255.255.252
# no shutdown
# exit
# interface gigabitEthernet 1/0
# ip address 192.168.2.1 255.255.255.252
# no shutdown
# exit
# exit
# wr

> R2
# configure terminal
# interface fastEthernet 0/0
# ip address 192.168.1.2 255.255.255.252
# no shutdown
# exit
# interface gigabitEthernet 1/0
# ip address 192.168.4.1 255.255.255.252
# no shutdown
# exit
# interface gigabitEthernet 2/0
# ip address 192.168.3.1 255.255.255.252
# no shutdown
# exit
# interface gigabitEthernet 3/0
# ip address 192.168.9.2 255.255.255.252
# no shutdown
# exit
# exit
# wr

> R3
# configure terminal
# interface fastEthernet 0/0
# ip address 192.168.2.2 255.255.255.252
# no shutdown
# exit
# interface gigabitEthernet 1/0
# ip address 192.168.3.2 255.255.255.252
# no shutdown
# exit
# exit
# wr

> R4
```

```
# configure terminal
# interface fastEthernet 0/0
# ip address 192.168.4.2 255.255.255.252
# no shutdown
# exit
# interface gigabitEthernet 1/0
# ip address 192.168.5.1 255.255.255.252
# no shutdown
# interface gigabitEthernet 2/0
# ip address 192.168.8.2 255.255.255.252
# no shutdown
# exit
# exit
# wr

> R5
# configure terminal
# interface gigabitEthernet 1/0
# ip address 192.168.5.2 255.255.255.252
# no shutdown
# exit
# interface fastEthernet 0/0
# ip address 192.168.6.1 255.255.255.252
# no shutdown
# exit
# interface gigabitEthernet 2/0
# ip address 192.168.10.1 255.255.255.252
# no shutdown
# exit
# exit
# wr

> R6
# configure terminal
# interface fastEthernet 0/0
# ip address 192.168.6.2 255.255.255.252
# no shutdown
# exit
# interface gigabitEthernet 1/0
# ip address 192.168.7.1 255.255.255.252
# no shutdown
# exit
# exit
# wr

> R7
```

```
# configure terminal
# interface gigabitEthernet 1/0
# ip address 192.168.7.2 255.255.255.252
# no shutdown
# exit

> R7
# configure terminal
# interface gigabitEthernet 1/0
# ip address 192.168.7.2 255.255.255.252
# no shutdown
# exit
# interface gigabitEthernet 2/0
# ip address 192.168.10.2 255.255.255.252
# no shutdown
# exit
# exit
# wr

> R8
# configure terminal
# interface gigabitEthernet 1/0
# ip address 192.168.8.1 255.255.255.252
# interface f0/0
# ip address 192.168.10.2 255.255.255.252
# no shutdown
# exit

> R9
# configure terminal
# interface gigabitEthernet 1/0
# ip address 192.168.9.1 255.255.255.252
# no shutdown
# exit
```

Configuração do Mikrotik

```
[admin@MikroTik] > /routing/ ospf instance/ add name=default
```

Configuração do RIP:

```
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
```

```
R2(config)#router rip
R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.3.0
R2(config-router)#network 192.168.9.0

R3(config)#router rip
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0

R4(config)#router rip
R4(config-router)#network 192.168.4.0
R4(config-router)#network 192.168.8.0

R8(config)#router rip
R8(config-router)#network 192.168.8.0

R9(config)#router rip
R9(config-router)#network 192.168.9.0
```

Configuração dda distribuição do RIP pelo OSPF:

```
R4(config)#router rip
R4(config-router)#passive-interface g1/0
R4(config-router)#passive-interface g2/0
R4(config-router)#default-metric 10
R4(config-router)#redistribute ospf 1
R4(config-router)#distribute-list 10 out ospf 1

R4(config)#router ospf 1
R4(config-router)#redistribute rip subnets
R4(config-router)#distribute-list 11 out rip
```

4. Resultados e troubleshooting

As técnicas e protocolos configurados em cada um dos roteadores relacionados na tabela 1 funcionam considerando toda a topologia de rede e não apenas o contexto de hosts e redes isoladas. Por exemplo, pode-se considerar a seguinte a verificação de comunicação entre os roteadores R8 e R9, a qual ocorre por meio da simulação da técnica de tunelamento.

Pode-se verificar que nesse cenário ideal de simulação todos os pacotes foram entregues com sucesso.

Já com a built-in feature ”show ip” no console de cada roteador Cisco simulado, podemos também verificar que cada roteador teve suas interfaces configuradas de acordo

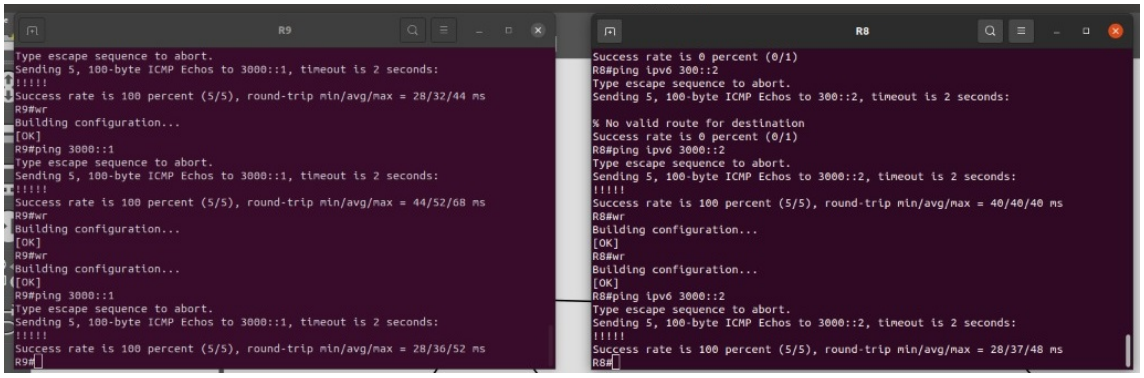

Figure 2. Verificação de tunneling desenvolvida no software GNS3

com a Tabela 1. Por exemplo, para os roteadores R4, R5, R6 e R7, os quais se comunicam entre si pelo roteamento OSPF, pode-se verificar:

Figure 3. Verificação de interfaces que implementam o roteamento OSPF no software GNS3

Quanto ao roteador de diferente sistema (Mikrotik) simulado R10, também podemos usar uma built-in feature semelhante para verificar que está ocorrendo a devida comunicação entre esse nó e o roteador R8 de diferente sistema (Cisco). Conforme é ilustrado na figura abaixo, todos os pacotes são entregues na comunicação entre eles.

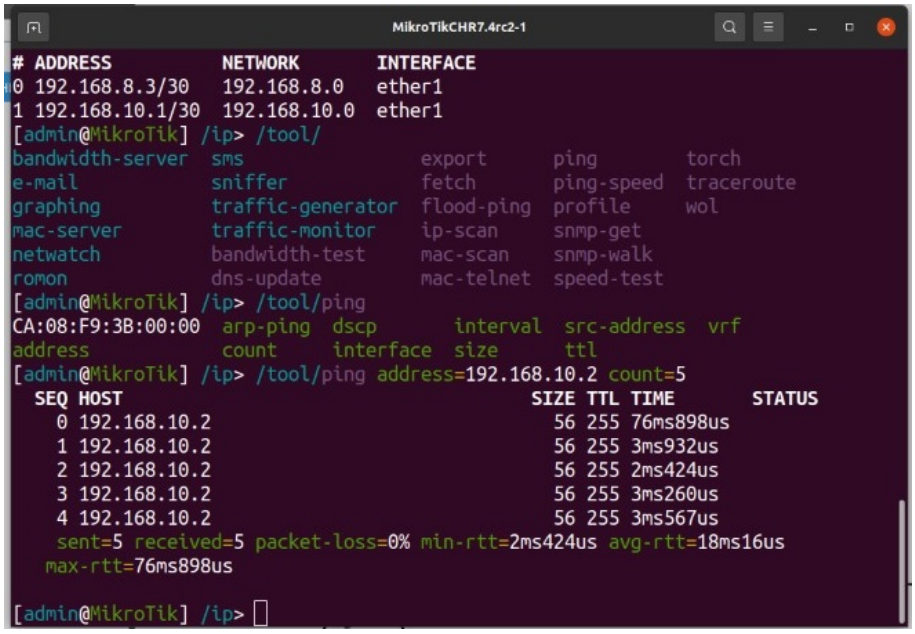

Figure 4. Verificação da comunicação entre roteadores de diferentes modelos

Na topologia desenvolvida neste estudo, os roteadores R1, R2, R3, R8, R9 estão alcançando uns aos outros pelo RIP, enquanto os roteadores R5, R6, R7 pelo OSPF. Nisso, o roteador R4 faz a distribuição, para que todos consigam se comunicar.

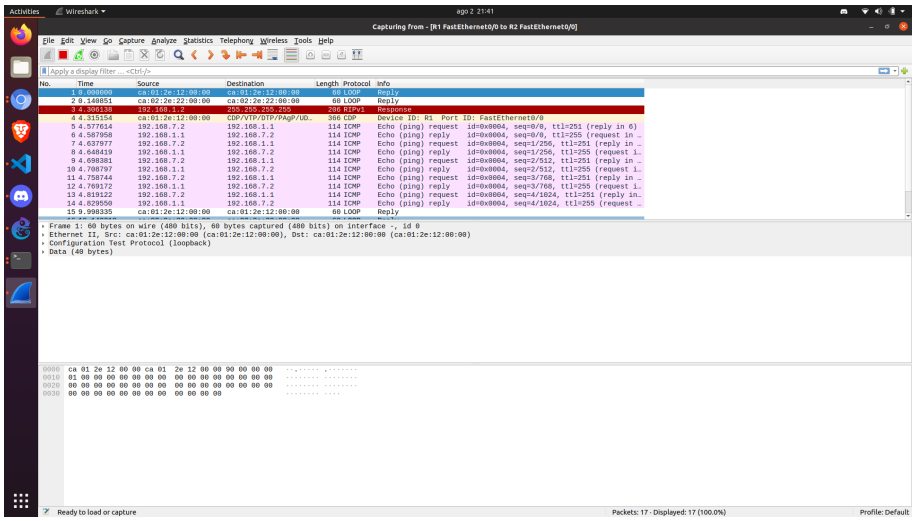

Figure 5. confirmação do ping de uma interface no roteador R7 para uma interface no roteador R1

À partir do R3 é possível se conectar com um NAT e ter acesso a internet.

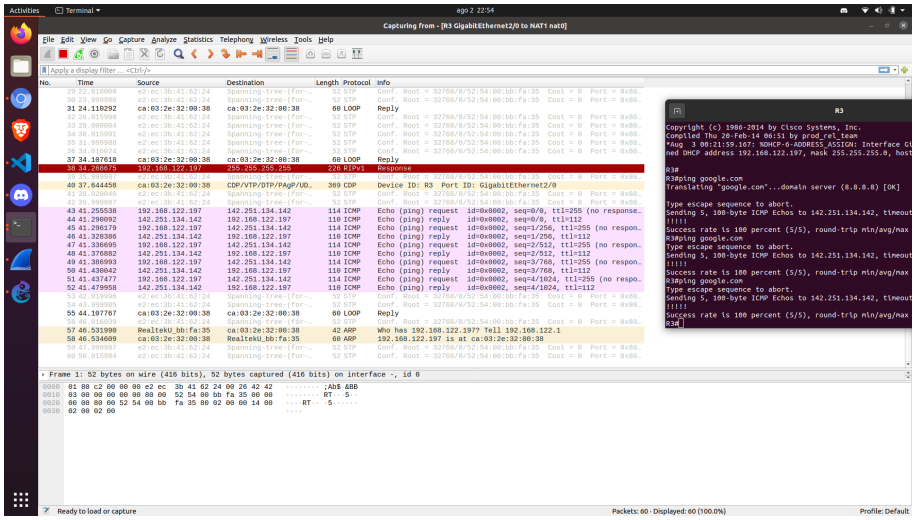

Figure 6. ping à partir do R3 em google.com

5. Conclusão

Com o desenvolvimento deste trabalho, foi possível verificar, em uma mesma topologia, roteadores trocando com sucesso pacotes mesmo implementando diferentes roteamentos (RIP e OSPF) ou diferentes sistemas (Mikrotik e Cisco), além de roteadores IPv6 se comunicando mesmo ilhados por uma região que trabalha em IPv4. Tudo isso enquanto também foram configurados serviços NAT e DNS em um dos nós da rede.

Em suma, os alunos tiveram a chance de implementar diferentes protocolos e técnicas de comunicação simultaneamente numa mesma topologia mais complexa. Essa topologia resultante serviu para o melhor entendimento do funcionamento de uma rede mais próxima daquelas ”reais” que milhões de usuários utilizam diariamente. Tais redes, por sua vez, também implementam harmonicamente os mais variados tipos de protocolos de roteamento e técnicas de comunicação entre hospedeiros e processos de aplicações.

6. Referências

References

Kurose, J. F. and Ross, K. W. (2006). Redes de computadores e a internet. *São Paulo: Person*, 28.

Malkin, G. (1998). Rfc2453: Rip version 2.

Moy, J. (1998). Rfc2328: Ospf version 2.