RC-I 2024-2025	TRABALHO DE LABORATÓRIO	Número:	4
CAMADA DE APLICAÇÃO		Data:	
Ferramentas de Rede, E-mail (SMTP, POP3)		Prazo:	

1. Introdução

O objectivo deste laboratório é utilizar o ambiente multi-nó (servidores, rede) criado no Laboratório #2 e #3 e realizar experiência com algumas ferramentas de rede, tais como o `ifconfig`, `ping`, `traceroute`, `whois` e `nmap` bem como examinar os protocolos de E-mail **SMTP** e **POP3**.

2. Multi-nó com Vagrant

Para começar, vá na pasta de projecto de rede, copia a pasta multinode e renomeie a pasta copiada para `multinode-email`. Faça download do ficheiro `RCI2025-Lab4-support_files.zip` e descompacte o conteúdo para a pasta `multinode-email`.

O ficheiro `bootstrap_client.sh` será criado.

Na pasta `multinode-email` edite o `Vagrantfile` no bloco que define a VM "`client`" para incluir a linha de provisionamento "shell" da seguinte forma:

```
config.vm.define "client" do |client_config|
  ....
  client_config.vm.provider "virtualbox" do |vb|
      ....
  end # of vb
  client_config.vm.provision "shell", path: "bootstrap_client.sh"
end # of client_config
```

Para garantir actualização e aprimoramento adequados para ambientes Vagrant usando o provedor Virtualbox, inicie o sistema com o comando:

```
$ vagrant up --provision
```

Inicie uma conexão ssh com a máquina:

```
$ vagrant ssh client
```

3. Experiências com as ferramentas de rede

Esses experimentos são válidos para todos os sistemas (Windows, Mac e Linux) se tiverem as ferramentas necessárias instaladas. Utilizaremos a VM "`client`" para executar os experimentos.

3.1. ifconfig

Nesta secção, listaremos e analisaremos as interfaces de rede em nosso sistema. Primeiro, utilize o comando `man` para saber um pouco mais sobre `ifconfig`.

```
vagrant@client:~$ man ifconfig
```

Ao emitir o comando ifconfig, obteremos uma lista detalhada das interfaces de rede actualmente activas da máquina. Ao dar um nome à interface como argumento, os detalhes dessa interface específica serão exibidos.

```
vagrant@client:~$ ifconfig eth1
```

O comando `ifconfig` também é usado para gerir essas interfaces, e assim podemos habilitar e desabilitar interfaces com os parâmetros do comando e definir essas interfaces para o modo promíscuo (permitindo "espionar" ou "inundar" todos os pacotes que passam nessa interface).

3.2. ping

Utilizará `ping` para tentar obter respostas de outros hosts. Tente acessar `www.wustl.edu` e descubra qual é o endereço IP.

```
vagrant@client:~$ ping www.wustl.edu
```

Utilize o comando `man` para `ping` para conhecer melhor as opções e o uso do comando. Por exemplo, o flag `-t` ttl é usado para definir o IP Time to Live (TTL), que representa o número de saltos que o pacote IP tem permissão para atravessar. Tente descobrir quantos saltos são necessários para o `ping` atingir o host com o endereço IP `193.136.128.169`.

```
vagrant@client:~$ ping -t 2 193.136.128.169
```

3.3. traceroute

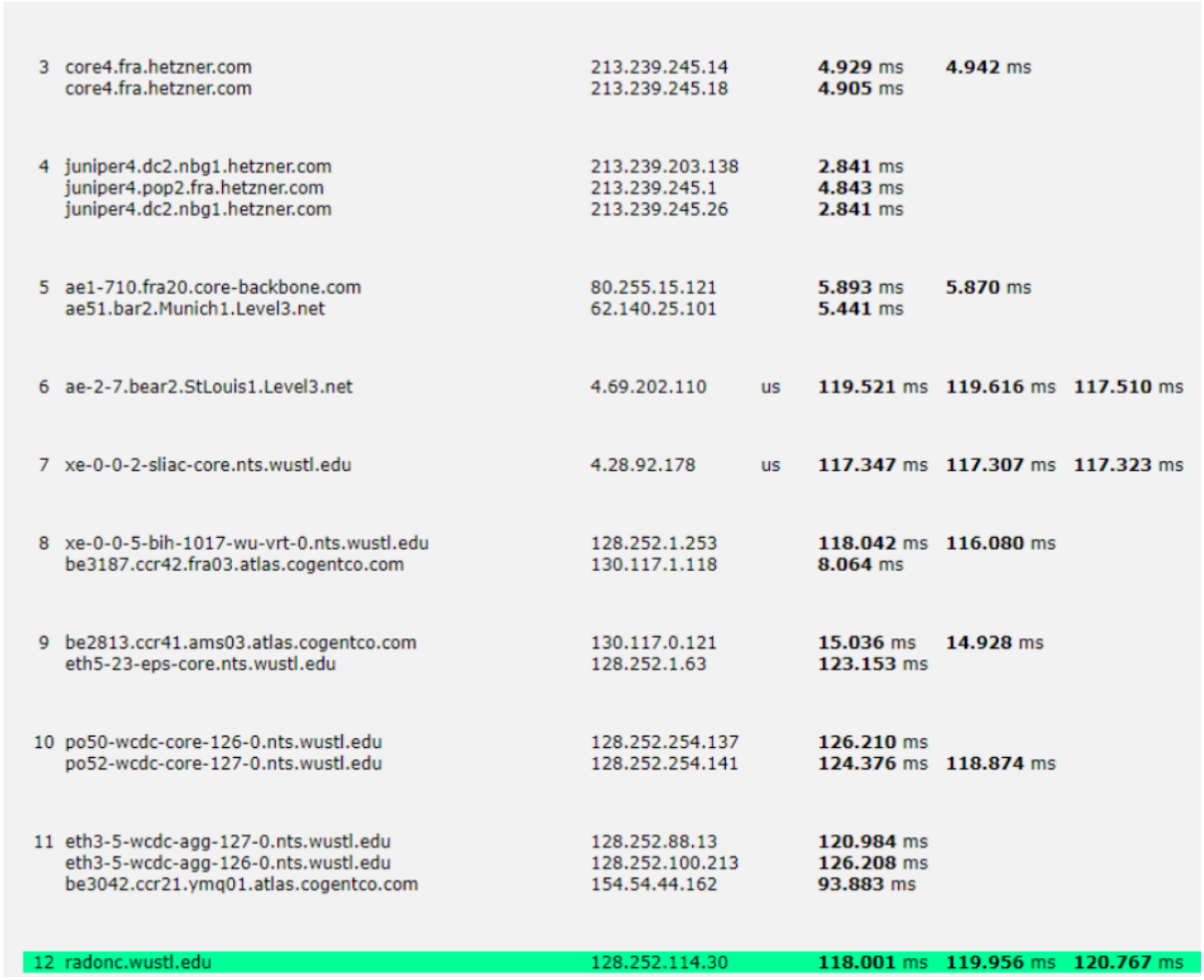
Esta ferramenta `traceroute`, ou equivalentes como `tracepath`, são utilizadas como uma ferramenta de diagnóstico de rede para apresentar a rota (caminho) até o destino e medir os atrasos de trânsito de pacotes pela rede (a Internet).

Utilize o comando `man` para aprender mais sobre `traceroute` e utilize esta ferramenta para rastrear o caminho para `www.wustl.edu`, conforme exemplificado:

```
vagrant@client:~$ man traceroute
```

```
vagrant@client:~$ traceroute www.wustl.edu
```

Podemos emular a ferramenta `traceroute` usando `ping` com valores incrementais para o parâmetro TTL. Há também uma implementação Web desta ferramenta (Figura 1). Vá para `http://ping.eu/traceroute` e tente rastrear a rota para o mesmo host. Compare as saídas de ambas as implementações desta ferramenta.



3	core4.fra.hetzner.com core4.fra.hetzner.com	213.239.245.14 213.239.245.18		**4.929** ms **4.905** ms	**4.942** ms	
4	juniper4.dc2.nbg1.hetzner.com juniper4.pop2.fra.hetzner.com juniper4.dc2.nbg1.hetzner.com	213.239.203.138 213.239.245.1 213.239.245.26		**2.841** ms **4.843** ms **2.841** ms		
5	ae1-710.fra20.core-backbone.com ae51.bar2.Munich1.Level3.net	80.255.15.121 62.140.25.101		**5.893** ms **5.441** ms	**5.870** ms	
6	ae-2-7.bear2.StLouis1.Level3.net	4.69.202.110	us	**119.521** ms	**119.616** ms	**117.510** ms
7	xe-0-0-2-sliac-core.nts.wustl.edu	4.28.92.178	us	**117.347** ms	**117.307** ms	**117.323** ms
8	xe-0-0-5-bih-1017-wu-vrt-0.nts.wustl.edu be3187.ccr42.fra03.atlas.cogentco.com	128.252.1.253 130.117.1.118		**118.042** ms **8.064** ms	**116.080** ms	
9	be2813.ccr41.ams03.atlas.cogentco.com eth5-23-eps-core.nts.wustl.edu	130.117.0.121 128.252.1.63		**15.036** ms **123.153** ms	**14.928** ms	
10	po50-wcdc-core-126-0.nts.wustl.edu po52-wcdc-core-127-0.nts.wustl.edu	128.252.254.137 128.252.254.141		**126.210** ms **124.376** ms	**118.874** ms	
11	eth3-5-wcdc-agg-127-0.nts.wustl.edu eth3-5-wcdc-agg-126-0.nts.wustl.edu be3042.ccr21.ymq01.atlas.cogentco.com	128.252.88.13 128.252.100.213 154.54.44.162		**120.984** ms **126.208** ms **93.883** ms		
12	radonc.wustl.edu	128.252.114.30		**118.001** ms	**119.956** ms	**120.767** ms

Figura 1: Saída parcial da versão web do traceroute

3.4. whois

Outra ferramenta interessante é o `whois`, uma ferramenta que nos permite obter conteúdo informativo sobre entidades na Internet.

Dado um endereço IP ou um Nome de Domínio, podemos obter algumas informações executando o seguinte (exemplo):

```
vagrant@client:~$ whois 193.136.128.169
```

Também pode encontrar uma implementação web do `whois` em `http://ping.eu/ns-whois/`

3.5. nmap

`nmap` ("Network Mapper") é uma ferramenta para descoberta de rede e auditoria de segurança. O `nmap` usa pacotes IP brutos de maneiras peculiares para determinar quais hosts estão disponíveis na rede, quais serviços (nome da aplicação e versão) esses hosts estão a oferecer, quais sistemas operativos (e versões de SO) estão a executar, que tipo de filtros de pacotes/firewalls estão em uso

e dezenas de outras características. O `nmap` é a base para a maioria das enumerações de segurança durante os estágios iniciais de um teste de penetração.

Por exemplo, o comando `ping` a seguir verifica a rede, listando as máquinas que respondem ao ping:

```
vagrant@client:~$ nmap -sP 192.168.1.0/24
```

Este outro comando escaneia todas as portas TCP reservadas na máquina `scanme.nmap.org`. A opção `-v` habilita o modo verbose:

```
vagrant@client:~$ nmap -v scanme.nmap.org
```

Agora conhece novas ferramentas para explorar redes, mais especificamente, a Internet.

4. Experiência E-mail

Nestes experimentos brincaremos com os protocolos de e-mail Simple Mail Transfer Protocol (SMTP) e Post Office Protocol (POP3), ilustrados na Figura 2.

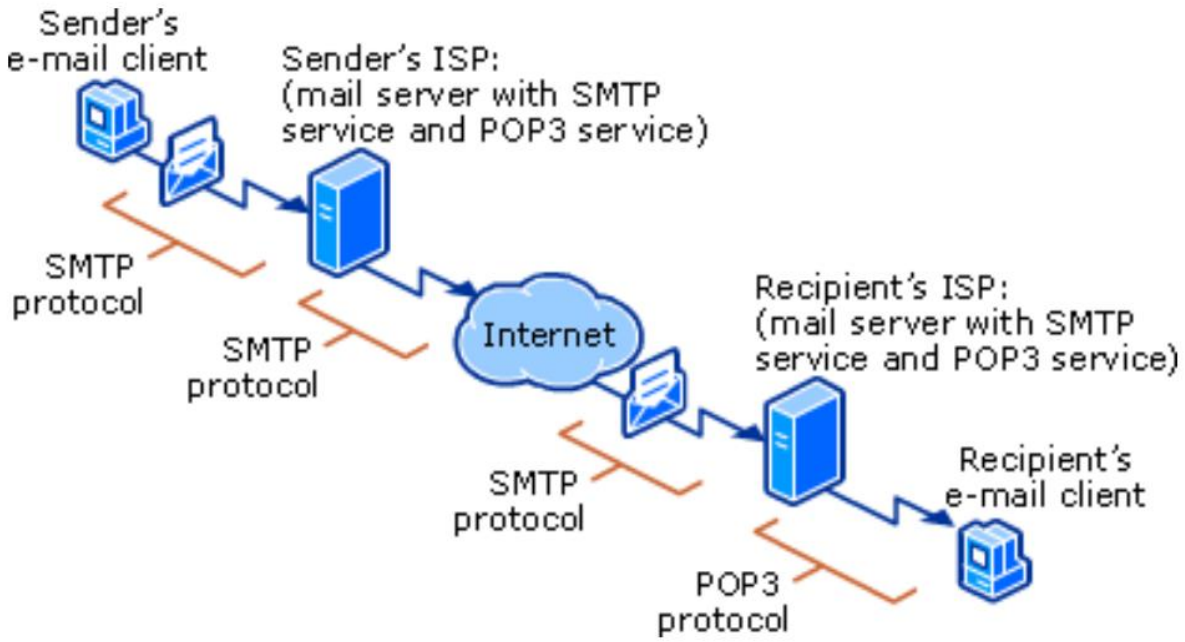


Figura 2: Funcionamento típico dos protocolos de e-mail SMTP e POP3.

4.1. Conectar a um servidor SMTP

SMTP é o protocolo universalmente utilizado para transferência de e-mail. Para nosso experimento SMTP, utilizaremos um servidor de teste SMTP externo fornecido para fins de estudo, o "`smtp.mailtrap.io`". Tente a seguinte interação (observe que as credenciais de utilizador a serem usadas são aquelas no exemplo), onde suas entradas são representadas com a cor laranja:

```
vagrant@client:~$ telnet smtp.mailtrap.io 2525
Trying 54.85.222.127...
Connected to mailtrap.io.
Escape character is '^] '.
220 mailtrap.io ESMTP ready
EHLO smtp.mailtrap.io
250 - mailtrap.io
250 - SIZE 5242880
250 - PIPELINING
250 - ENHANCEDSTATUSCODES
250 - 8BITMIME
250 - DSN
250 - AUTH PLAIN LOGIN CRAM-MD5
250 STARTTLS
AUTH LOGIN
```

```
334 VXNlcm5hbWU6
ZTM5OTNkZDg1ZWVhNDU=
334 UGFzc3dvcmQ6
MDU1ODgxNTAxOTQ4YWY=
235 2.0.0 OK
MAIL FROM: <from@smtp.mailtrap.io>
250 2.1.0 Ok
RCPT TO: <to@smtp.mailtrap.io>
250 2.1.0 Ok
DATA
354 Go ahead
To: to@smtp.mailtrap.io
From: from@smtp.mailtrap.io
Subject: Hello world!
This is the test message...
.
250 2.0.0 Ok: queued
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

4.2. Experimentos POP3

POP3 é um protocolo padrão da Internet de camada de aplicação de cliente de acesso a e-mail usado por clientes de e-mail locais para recuperar e-mails de um servidor remoto por meio de uma conexão TCP/IP. Apesar desse protocolo ser cada vez menos usado, ele é simples e é um dos mais adequados para ilustrar os mecanismos utilizados no serviço de e-mail. Tente a seguinte interação (note que as credenciais de utilizador a serem usadas são aquelas do exemplo), onde suas entradas são representadas com a cor laranja.

```
vagrant@client:~$ telnet smtp.mailtrap.io 1100
Trying 54.85.222.127...
Connected to mailtrap.io.
Escape character is '^] '.
+OK POP3 ready
USER e3993dd85eea45
+OK
PASS 055881501948af
+OK maildrop locked and ready
STAT
+OK 0 0
LIST
+OK 0 messages (0 octets )
.
QUIT
+OK Bye
```

```
Connection closed by foreign host.
```

5. Finalização da experiência

Para parar as Máquinas Virtuais e verificar o estado global de todos os ambientes Vagrant activos no sistema, podemos emitir os seguintes comandos:

```
$ vagrant halt
```

```
$ vagrant global-status
```

Confirme se o status das VMs é 'powered off'. Para evitar que essas máquinas instanciadas usem recursos. Depos de apresentar ao docente e escrever o seu memorando, pode destruí-las, pois podem ser recriadas com o comando simples vagrant up. Confirme se não há VMs listadas.

```
$ vagrant destroy
```

```
$ vagrant global-status
```

6. Envio dos resultados das experiências

As experiências que executar neste LAB produzirão resultados que precisa relatar ou dos quais será questionado sobre a execução. Para relatar os resultados que alcançou, proceda da seguinte forma:

6.1. Procedimento geral

Devia enviar via email um memorando contendo as respostas das questões a serem disponibilizadas e todo o material requerido para aferir a execução do laboratório (screen-shots, saída de linha de comando, código desenvolvido, etc.).

6.2. Procedimento específico

Para esta Tarefa LAB, fornecerá resultados do uso das Ferramentas de Rede, bem como da interação com SMTP e POP3. Além disso, algumas capturas de tela também são necessárias, como segue:

1. Envie o Vagrantfile modificado;
2. Captura de tela do comando `ifconfig` com informações sobre a interface ethernet com o endereçamento privado, na máquina cliente;
3. Captura de tela dos resultados do segundo comando `nmap`;
4. Copie da janela Terminal o texto resultante da interação com o servidor SMTP, para enviar;
5. Captura de tela do analisador de pacote, mostrando os pacotes trocados com a interação via POP3 com o servidor de e-mail;

Bom trabalho!