

# Serviços de Rede 1 –

## **Aula 11 - Práticas**

2019-2020

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática



# Pre – Requisitos -Exercício 1

- Ter instalada e a funcionar a topologia da aula anterior.
- No Moodle está o ficheiro de configuração do Squid.



## Exercício 1 – Squid configuração avançada

# Exercício

- Retire a versão do squid que está a correr em caso de erro. Gere um erro (por exemplo acesso a [www.sr1.pt](http://www.sr1.pt)) e veja se surge esse nome.

Erro no nome: o nome do domínio não existe.

Isso significa que o cache não conseguiu resolver o nome do host apresentado na URL. Verifique se o endereço está correto.

O administrador do cache é [webmaster](#).

---

Gerado terça-feira, 19 de maio de 2020 13:25:47 GMT por SRV\_SR1 (squid / 3.5.28)

O seguinte erro foi encontrado ao tentar recuperar o URL: <http://www.sr1.pt/>

**Incapaz de determinar o endereço IP através do nome do host "www.sr1.pt"**

O servidor DNS retornou:

Name Error: The domain name does not exist.

Isso significa que o cache não conseguiu resolver o nome do host apresentado na URL. Verifique se o endereço está correto.

Envie um mail para [webmaster](#).

---

Generated Tue, 26 May 2020 14:00:54 GMT by SRV\_SR1 (squid)

# Exercício

- Na acl que criou na aula passada mude o seu nome para extern. Faça um restart aos serviços do squid e veja o que acontece. Deve estar sem acesso à rede.
- Pela janela do terminal identifique qual a linha em que está a ocorrer o erro.
- Faça a correção do erro e verifique que está tudo a correr como tinha configurado.
- Ainda na janela do terminal identifique qual é a versão do SQUID que está a utilizar.
- Veja os seus ficheiros de logs... Devem ter crescido de forma muito significativa. Apague os logs dos acessos.



## Sem Internet

Existe um problema com o servidor proxy ou o endereço está incorreto.

Experimente:

- Contactar o gestor do sistema
- [Verificar o endereço proxy](#)
- [Executar o Diagnóstico de rede do Windows](#)

ERR\_PROXY\_CONNECTION\_FAILED

Detalhes

# Exercício

- Em `squid/var/cache` crie uma nova diretoria chamada SR1. Esta diretoria servirá para guardar os ficheiros da função de cache do seu servidor.
- Deve ativar a função cache com as seguintes características:
  - Diretoria `/var/cache/sr1`
  - Tipo – USF
  - 512MB de espaço, 128 diretórios e 256 subdiretórios
- Proceda à criação desta função.
- Valide na diretoria SR1 que foram criadas todas as pastas conforme estava definido no comando.

*How To*

- Um dos itens mais importantes do arquivo de configuração squid.conf são as listas de controle de acesso, ou ACLs.
- É possível criar ACLs com padrões diferentes de restrição e de acesso como, por exemplo, liberação e/ou bloqueio de acesso à internet para um determinado computador, rede de computadores ou sites indesejados. Temos assim:
  - **ACLs de origem:** são as regras que definem os IPs que poderão ter acesso ou restrição às regras definidas;
  - **ACLs de destino:** definem qual destino poderá ser ou não acessível. O controle pode ser por site, para uma rede ou fazendo uso de expressões regulares;
  - **ACLs de horário:** permitem liberar ou bloquear o acesso de acordo com horários definidos nas regras;
  - **ACLs utilizando blacklist:** permite controlar de forma granular o bloqueio de acessos através de palavras específicas;
  - **ACLs utilizando whitelist:** permite controlar de forma granular a liberação de domínios que contenham palavras da blacklist.



- O comando é:

**acl** [*nome*] [*tipo*] [*argumento*]

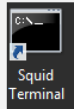
- Onde:
  - *nome* – é o nome da ACL
  - *tipo* – é o tipo de acl que vai ser criada (ver os tipos possíveis no slide seguinte)
  - *argumento* – opções que podem ser adicionadas

|               |  |
|---------------|--|
| src           | Filtro que define a origem dos hosts ou rede que será considerada na ACL |
| time          | Filtro por hora e dia da semana  |
| urlpath_regex | Filtro complementar de uma URL (\.gif, \.jpg).                           |
| url_regex     | Filtro de uma string na URL  |
| dstdomain     | Filtro por dominio   |
| proxy_auth    | Filtro por utilizadores autenticados                                     |
| arp           | Filtro por MAC address   |
| maxconn       | Filtro por conexões  |
| proto         | Filtro por protocolos  |
| port          | Filtro por portas de serviço   |

- Através das ACLs são definidos os tipos controlo que desejamos fazer. Porém, ainda nessa etapa, os pedidos não são tratados, sendo necessário configurar o comando *http\_access*.
- Uma vez que as ACLs de origem e destino foram criadas, é necessário definir o que será liberado (*allow*) e/ou o que será bloqueado (*deny*), com o comando:

*http\_access [allow/denny] [nome da ACL]*

- Como a configuração do SQUID é feita no ficheiro squid.conf por vezes não é fácil diagnosticar um erro. Uma hipótese é o comando *squid -k parse* na **janela de terminal** do squid e analisar os erros.



```
C:\Squid>  
C:\Squid>  
C:\Squid>squid -k parse
```

- Pode saber os comandos que tem disponíveis, deve utilizar o comando squid - v.

- **cache.log**

- Este arquivo contém mensagens informativas, formatadas para o ser humano, sobre a operação do Squid. O nome do arquivo é definido pelo comando `cache_log`. Em condições normais, o ficheiro aumenta cerca de 10 a 100 KB por dia.

- **access.log**

- Este arquivo contém uma entrada para todas as transações HTTP e (opcionalmente) ICP feitas pelos clientes do Squid. O nome do arquivo é definido pelo comando `cache_access_log`. Em condições normais o ficheiro cresce a uma taxa de 100-200 bytes por transação.

- Para ativar a função de cache deve utilizar o comando:
  - **cache\_dir** *[tipo] [caminho] [tamanho em disco] [número de diretórios] [número de subdiretórios]*
- Deve ainda definir o espaço em memória que vai utilizar para a cache, utilizando o comando
  - **cache\_mem** *[valor]*
- Deve depois correr o comando `squid -k parse` na **janela de terminal** do squid e analisar os possíveis erros.
- Depois deve correr o comando `squid -z` para que o programa crie na diretoria definida para a cache as swap dir. Só necessita de o fazer na primeira vez que está a ativar a função de cache.

- Pode validar no ficheiro de logs a criação destas diretorias.

```

cache - Notepad
File Edit Format View Help
/var/cache/sr1/112020/05/26 19:04:43 kid1| Making directories in /var/cache/sr1/122020/05/26 19:04:43 kid1| Making directories in
/var/cache/sr1/132020/05/26 19:04:43 kid1| Making directories in /var/cache/sr1/142020/05/26 19:04:43 kid1| Making directories in
/var/cache/sr1/152020/05/26 19:04:44 kid1| Making directories in /var/cache/sr1/162020/05/26 19:04:44 kid1| Making directories in
/var/cache/sr1/172020/05/26 19:04:44 kid1| Making directories in /var/cache/sr1/182020/05/26 19:04:44 kid1| Making directories in
/var/cache/sr1/192020/05/26 19:04:44 kid1| Making directories in /var/cache/sr1/1A2020/05/26 19:04:44 kid1| Making directories in
/var/cache/sr1/1B2020/05/26 19:04:44 kid1| Making directories in /var/cache/sr1/1C2020/05/26 19:04:44 kid1| Making directories in
/var/cache/sr1/1D2020/05/26 19:04:44 kid1| Making directories in /var/cache/sr1/1E2020/05/26 19:04:44 kid1| Making directories in
/var/cache/sr1/1F2020/05/26 19:04:44 kid1| Making directories in /var/cache/sr1/202020/05/26 19:04:44 kid1| Making directories in
/var/cache/sr1/212020/05/26 19:04:45 kid1| Making directories in /var/cache/sr1/222020/05/26 19:04:45 kid1| Making directories in
/var/cache/sr1/232020/05/26 19:04:45 kid1| Making directories in /var/cache/sr1/242020/05/26 19:04:45 kid1| Making directories in
/var/cache/sr1/252020/05/26 19:04:45 kid1| Making directories in /var/cache/sr1/262020/05/26 19:04:45 kid1| Making directories in
/var/cache/sr1/272020/05/26 19:04:45 kid1| Making directories in /var/cache/sr1/282020/05/26 19:04:45 kid1| Making directories in
/var/cache/sr1/292020/05/26 19:04:45 kid1| Making directories in /var/cache/sr1/2A2020/05/26 19:04:45 kid1| Making directories in
/var/cache/sr1/2B2020/05/26 19:04:45 kid1| Making directories in /var/cache/sr1/2C2020/05/26 19:04:46 kid1| Making directories in
/var/cache/sr1/2D2020/05/26 19:04:46 kid1| Making directories in /var/cache/sr1/2E2020/05/26 19:04:46 kid1| Making directories in
/var/cache/sr1/2F2020/05/26 19:04:46 kid1| Making directories in /var/cache/sr1/302020/05/26 19:04:46 kid1| Making directories in
/var/cache/sr1/312020/05/26 19:04:46 kid1| Making directories in /var/cache/sr1/322020/05/26 19:04:46 kid1| Making directories in
/var/cache/sr1/332020/05/26 19:04:46 kid1| Making directories in /var/cache/sr1/342020/05/26 19:04:46 kid1| Making directories in
/var/cache/sr1/352020/05/26 19:04:46 kid1| Making directories in /var/cache/sr1/362020/05/26 19:04:46 kid1| Making directories in
/var/cache/sr1/372020/05/26 19:04:47 kid1| Making directories in /var/cache/sr1/382020/05/26 19:04:47 kid1| Making directories in
/var/cache/sr1/392020/05/26 19:04:47 kid1| Making directories in /var/cache/sr1/3A2020/05/26 19:04:47 kid1| Making directories in

```

- Ou validar a sua criação com o explorador do Windows.

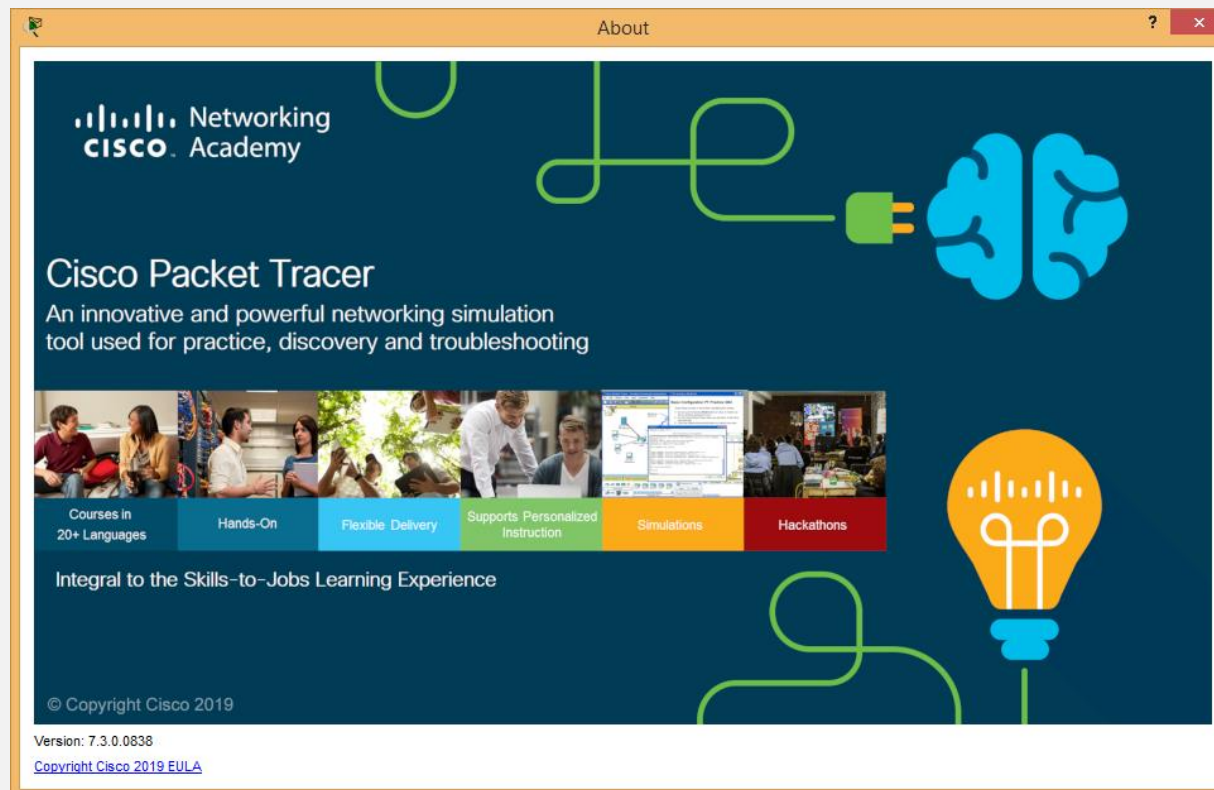
File Explorer view of the directory structure:

This PC > Local Disk (C:) > Squid > var > cache > sr1

| Name | Date modified    | Type        | Size |
|------|------------------|-------------|------|
| 00   | 26/05/2020 19:04 | File folder |      |
| 0A   | 26/05/2020 19:04 | File folder |      |
| 0B   | 26/05/2020 19:04 | File folder |      |
| 0C   | 26/05/2020 19:04 | File folder |      |
| 0D   | 26/05/2020 19:04 | File folder |      |
| 0E   | 26/05/2020 19:04 | File folder |      |
| 0F   | 26/05/2020 19:04 | File folder |      |
| 01   | 26/05/2020 19:04 | File folder |      |
| 1A   | 26/05/2020 19:04 | File folder |      |
| 1B   | 26/05/2020 19:04 | File folder |      |
| 1C   | 26/05/2020 19:04 | File folder |      |
| 1D   | 26/05/2020 19:04 | File folder |      |

# Pre – Requisitos -Exercício 2

- Ter instalado o *Cisco Packet Tracer* versão 7.3.0



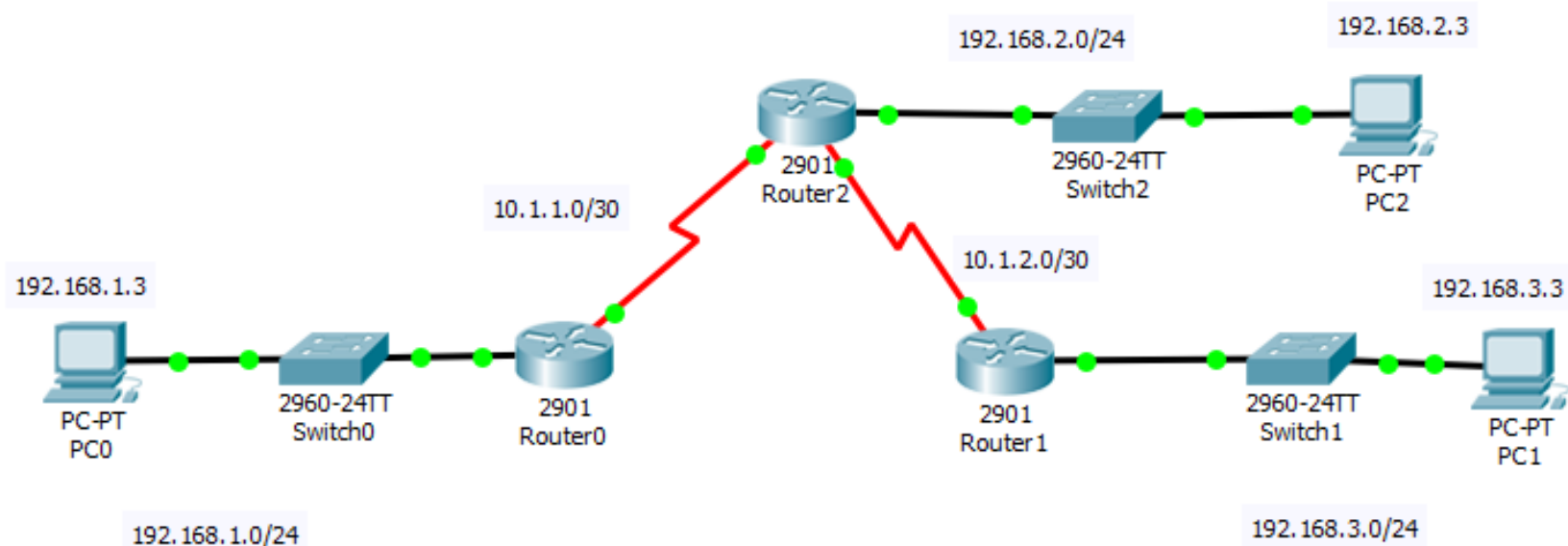
## Exercício 1 – VPN com túnel GRE em ambiente Cisco



# Exercício

A empresa SR1.SA necessita de ligar a rede da sede (192.168.1.0) à rede da delegação (192.168.3.0) utilizando a ligação de telecomunicações já instalada.

Numa primeira fase a empresa deseja que essa ligação seja feita sobre um túnel GRE. Considere a seguinte topologia:



# Exercício

- Faça a topologia indicada na imagem anterior. Grave a simulação como VPN\_GRE.
- Coloque os endereços IP dos diferentes equipamentos de forma fixa e de acordo com as redes indicadas na imagem.
- Garanta que o PC0 e o PC1 conseguem ter conectividade para o PC2.
- Crie uma VPN entre os Routers 0 e 1 baseado num túnel GRE. O IP do túnel será a rede 50.50.50.0/24.
- Faça o *tracert* do PC0 para o PC1 e vice-versa.

```
C:\>tracert 192.168.3.3

Tracing route to 192.168.3.3 over a maximum of 30 hops:

  1  2 ms    0 ms    0 ms    192.168.1.254
  2  14 ms   12 ms   15 ms   50.50.50.2
  3  12 ms   13 ms   14 ms   192.168.3.3

Trace complete.
```

```
C:\>tracert 192.168.1.3

Tracing route to 192.168.1.3 over a maximum of 30 hops:

  1   1 ms    2 ms    0 ms    192.168.3.254
  2  14 ms   14 ms   14 ms   50.50.50.1
  3  16 ms   12 ms   11 ms   192.168.1.3

Trace complete.
```

*How To*


- É possível que tenha de ativar *Security Technology Package* license em alguns routers. Para isso:
  - Faça **show version** em modo *Enable*:

| Technology | Technology-package<br>Current | Technology-package<br>Type | Technology-package<br>Next reboot |
|------------|-------------------------------|----------------------------|-----------------------------------|
| ipbase     | ipbasek9                      | Permanent                  | ipbasek9                          |
| security   | None                          | None                       | None                              |
| uc         | None                          | None                       | None                              |
| data       | None                          | None                       | None                              |

É necessário

- Pode não estar instalada a licença.
- Entre em modo de configuração e faça:

*license boot module cXXXX technology-package securityk9*



| Technology | Technology-package<br>Current | Type      | Technology-package<br>Next reboot |
|------------|-------------------------------|-----------|-----------------------------------|
| appxk9     | None                          | None      | None                              |
| uck9       | None                          | None      | None                              |
| securityk9 | securityk9                    | Permanent | securityk9                        |
| ipbase     | ipbasek9                      | Permanent | ipbasek9                          |
| security   | securityk9                    | Permanent | securityk9                        |
| ipbase     | ipbasek9                      | Permanent | ipbasek9                          |

cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.  
Processor board ID FLM232010G0

Não é necessário

- Grave a configuração.
- Faça *reload*.
- Faça *show version* e já deve ter ativada *Security Technology Package license*.

```
Technology Package License Information for Module:'c2900'
```

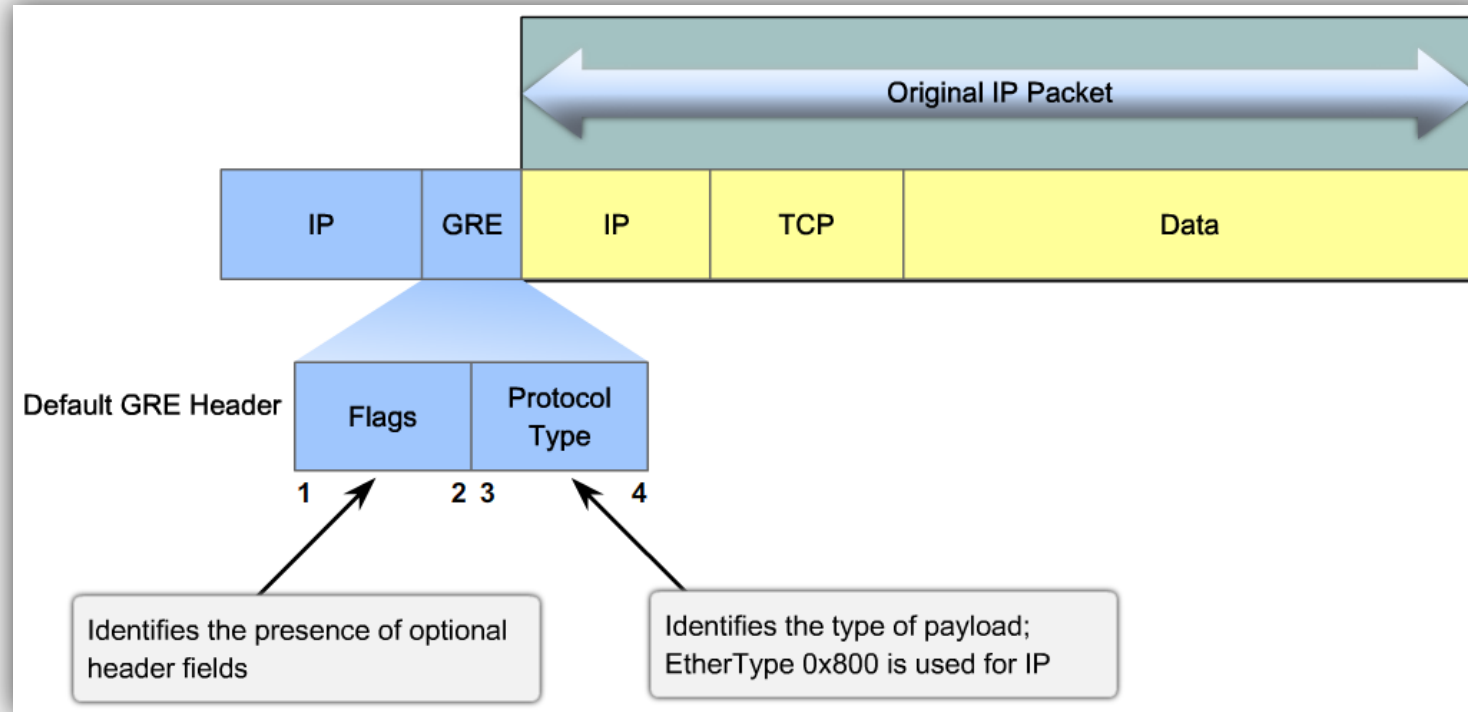
| Technology | Technology-package<br>Current | Type       | Technology-package<br>Next reboot |
|------------|-------------------------------|------------|-----------------------------------|
| ipbase     | ipbasek9                      | Permanent  | ipbasek9                          |
| security   | securityk9                    | Evaluation | securityk9                        |
| uc         | None                          | None       | None                              |
| data       | None                          | None       | None                              |

# Tunneling

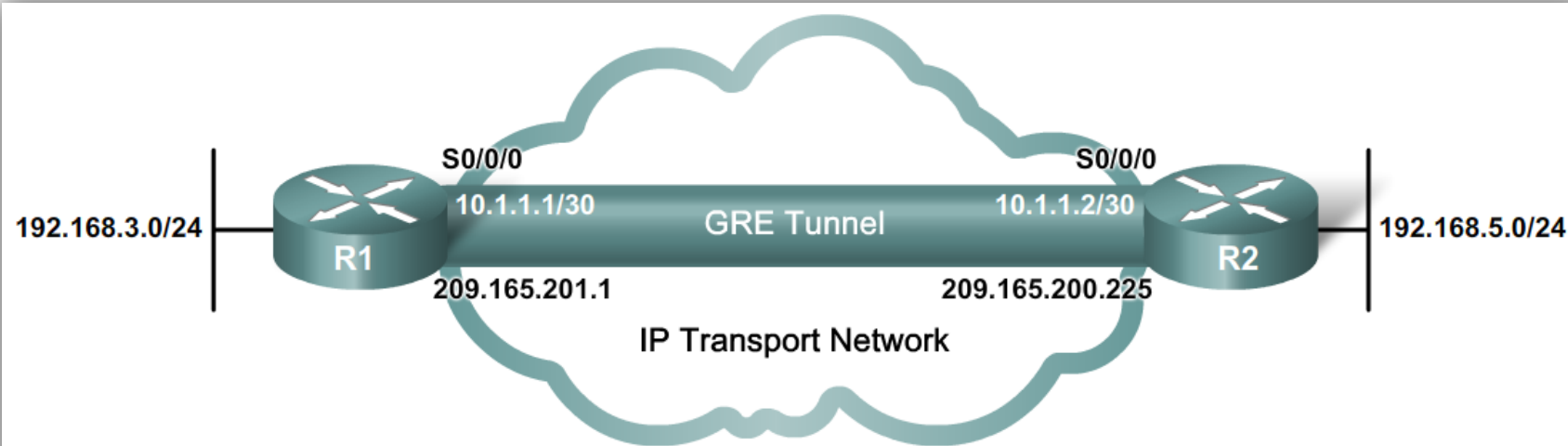
- Para que um túnel seja estabelecido é necessário que o servidor e o cliente utilizem o mesmo protocolo.
- Para o estabelecimento do túnel, são necessárias duas fases:
  - **Estabelecimento do túnel**
    - Negociação de variáveis, endereço, encriptação e compressão.
  - **Transmissão**
    - Encapsulamento e encriptação.
    - Envio.
    - Desencapsulamento e desencriptação.

# GRE - Generic Routing Encapsulation

- Os pacotes IP são encapsulados num pacote GRE
  - *Implica um* payload adicional de, pelo menos, 24 bytes



# GRE - Configuração



```
R1(config)# interface tunnel 0
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# tunnel source serial 0/0/0
R1(config-if)# tunnel destination 209.165.200.225
R1(config-if)# tunnel mode gre ip
R1(config-if)#
```

```
R2(config)# interface tunnel 0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
R2(config-if)# tunnel source serial 0/0/0
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# tunnel mode gre ip
R2(config-if)#
```

GRE tunnel is up and the protocol is up if:

- Tunnel source and destination are configured
- Tunnel destination is in routing table
- GRE keepalives are received (if used)
- GRE is the default tunnel mode

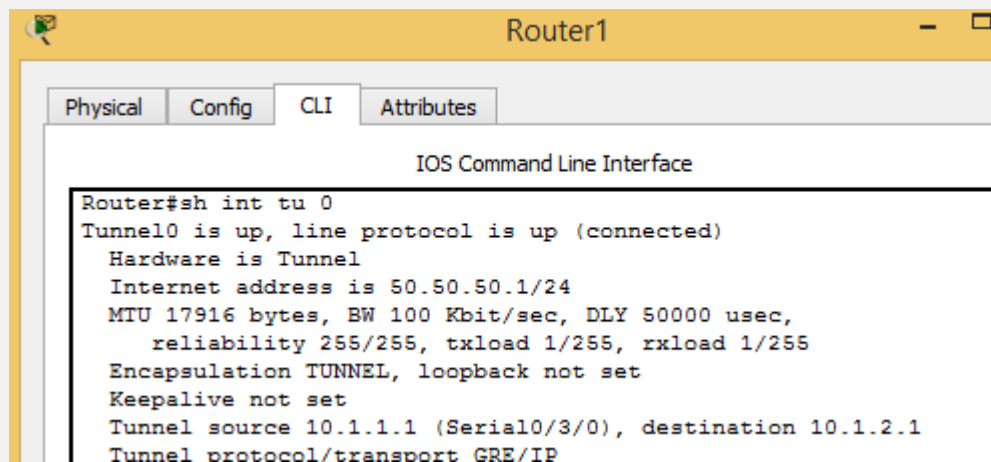


# GRE - Configuração

- Não se esqueça de fazer as rotas necessárias.

```
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/3/0
L    10.1.1.1/32 is directly connected, Serial0/3/0
S    10.1.2.0/30 is directly connected, Serial0/3/0
50.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    50.50.50.0/24 is directly connected, Tunnel0
L    50.50.50.1/32 is directly connected, Tunnel0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.254/32 is directly connected,
GigabitEthernet0/0
S    192.168.2.0/24 is directly connected, Serial0/3/0
S    192.168.3.0/24 [1/0] via 50.50.50.2
```

- Deve verificar se a sua interface está *up*



# Dúvidas



# Referências

---

- <https://www.devmedia.com.br/implementacao-de-um-proxy-web-com-squid-revista-infra-magazine-8/26302> - acessado em Maio de 2020
- <https://ipccisco.com/gre-tunnel-configuration-with-packet-tracer/> - acessado em Maio de 2020
- Cisco Networking Academy – Packet Tracer – Configuring VPNs