Relatório

INSTITUTO POLITÉCNICO DE BEJA
ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Gestão de equipamento activo de rede

Trabalho realizado por:

Tiago Conceição Nº 11903
Tiago Maques Nº 11904
Paulo Martins Nº 11918

Índice

Índice de ilustrações

Introdução

Este projecto foi proposto pelo professor Armando Ventura, na disciplina de Gestão e Equipamento Activo de Rede. Pretende-se com a realização deste projecto a implementação de casos práticos realizados nas aulas com equipamentos Cisco, nomeadamente no que consiste à instalação, configuração, actualização e monitorização de *switches* e *routers* Cisco. Para a realização do projecto, a partida vai ser necessário o *software* GNS3 e VirtualBox.

Vamos abordar neste projecto os seguintes temas:

- Utilização do TFTP para gestão de configurações de Routers Cisco

- Acesso à configuração de Routers Cisco remotamente

- Instalação e actualização do sistema operativo IOS em Routers Cisco

- Procedimento de recuperação de passwords em equipamento Cisco

- Gestão de redes baseada em SNMP

Quanto ao endereçamento dos equipamentos, vai ser utilizada a gama de endereços de IP 172.16.0.0/12, sendo esta gama fornecida pelo docente da disciplina.
Esperamos não encontrar grandes dificuldades na realização deste projecto, visto que tivemos aulas teóricas e práticas relacionadas com a matéria do projecto em si.

Topologia

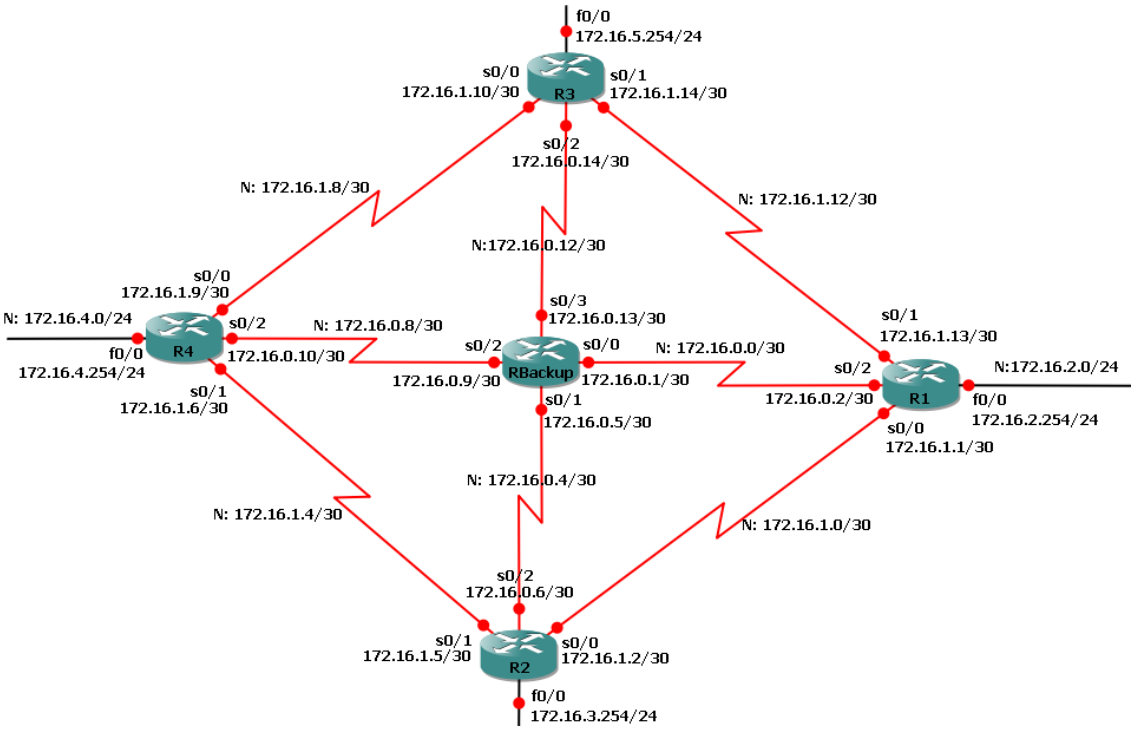

Ilustração 1 (Topologia)

Dispositivo	Interface	IP/Máscara	Rede	Gateway
R1	S0/0	172.16.1.1/30	172.16.1.0/30	
	S0/1	172.16.1.13/30	172.16.1.12/30	
	S0/2	172.16.0.2/30	172.16.0.0/30	
	F0/0	172.16.2.254/24	172.16.2.0/24	
R2	S0/0	172.16.1.2/30	172.16.1.0/30	
	S0/1	172.16.1.5/30	172.16.1.4/30	
	S0/2	172.16.0.6/30	172.16.1.4/30	
	F0/0	172.16.3.254/24	172.16.3.0/24	
R3	S0/0	172.16.1.10/30	172.16.1.8/30	
	S0/1	172.16.1.14/30	172.16.1.12/30	
	S0/2	172.16.0.13/30	172.16.0.12/30	
	F0/0	172.16.5.254/24	172.16.5.0/24	
R4	S0/0	172.16.1.9/30	172.16.1.8/30	
	S0/1	172.16.1.6/30	172.16.1.4/30	
	S0/2	172.16.0.10/30	172.16.1.8/30	
	F0/0	172.16.4.254/24	172.16.4.0/24	
RBackup	S0/0	172.16.0.1/30	172.16.0.0/30	
	S0/1	172.16.0.5/30	172.16.0.4/30	
	S0/2	172.16.0.9/30	172.16.0.8/30	
	S0/3	172.16.0.13/30	172.16.0.12/30	
ISP → R1	NIC	172.16.2.1/24	172.16.2.0/24	172.16.2.254/24
WebServer → R2	E2	172.16.3.1/24	172.16.3.0/24	172.16.3.254/24

GoldenServer → R4	E2	172.16.4.1/24	172.16.4.0/24	172.16.4.254/24
Monitorização → R4	E2	172.16.4.2/24	172.16.4.0/24	172.16.4.254/24
Utilizador → R3	E2	DHCP	172.16.5.0/24	172.16.5.254/24
Utilizador2 → R3	E2	DHCP	172.16.5.0/24	172.16.5.254/24

Esta topologia é constituída por 5 Routers C2621 (R1, R2, R3, R4 e RBackup), uma Cloud (ISP) e 5 dispositivos/máquinas virtuais (WebServer, GoldenServer, Monitorização, Utilizador e Utilizador2). Estes equipamentos usam um endereçamento VLSM da gama 172.16.0.0, estando assim, reservado alguns endereços:

- **Ligação entre *routers*:** 172.16.1.0/30
- **Ligação entre *routers,* linha backup:** 172.16.0.0/30
- **Interfaces FastEthernet:** 172.16.2.0/24, 172.16.3.0/24, 172.16.4.0/24, 172.16.5.0/24

Todos os *routers* estão a utilizar a imagem IOS "**c2600-ipbasek9-mz.124-8.bin**".
Todos os servidores/computadores estão a utilizar o Windows XP como sistema operativo.
Todo o *software* usado foi instalado com as definições e portas por defeito.

Segurança e acessos

Equipamento/Protocolo	User(s)	Password(s)
Routers, modo enable		cisco
Acesso SSH	admin	cisco
Acesso Telnet		cisco
Web Server (172.16.3.1)		
TFTP (172.16.4.1:69)		
FTP (172.16.4.1:21)	backups	cisco
SNMP Web (172.16.4.2:80)	admin	cisco

Todas as *passwords* são iguais de modo a facilitar o utilizador a utilizar esta topologia.

Nenhum dispositivo da rede 172.16.5.0/24 pode aceder ao telnet dos *routers*.

Access Lists

Negar Ping para o host Monitorização

Configuração no R4:

```
ip access-list extended NO_PING_TO_MONITOR
 deny icmp host 172.16.4.2 any echo
 end
```

Devido à imagem do *router* não suportar o uso de access-lists/access-group nas portas FastEthernet ou Serial não foi possível implementar esta regra, mas numa situação real esta regra iria impedir qualquer ping para esta máquina (172.16.4.2).

Negar Telnet aos utilizadores comuns

Configuração base em todos os routers:

```
! Access list para bloquear o uso do telenet por parte dos PCs dos utilizadores
ip access-list standard NO_TELNET_5_NETWORK
 deny 172.16.5.0 0.0.0.255 log
 permit any
 exit
! Configuração telnet
line vty 0 15
 ! Atribui a access list a ligações telnet
 access-class NO_TELNET_5_NETWORK in
 password cisco
 login
 exit
```

Gestão remota de equipamentos

Inicialmente foi configurado o SSH v2 em vez do Telnet, mas como era necessário gerar uma nova chave RSA usando o crypto cada vez que se reiniciasse o *router,* dessa forma foi aplicada a gestão via telnet.

SSH (Antes)	Telnet (Actual)
! Gerar chave RSA crypto key generate rsa 1024 **! Configuração do SSH** ip ssh time-out 60 ip ssh authentication-retries 2 ip ssh version 2 **! Criação de um utilizador para o SSH** username admin priv 15 secret cisco **! Usar o novo modelo de utilizador** aaa new-model **! Desactiva o uso do telnet e obriga o SSH** line vty 0 15 transport input ssh exit end	**! Activa o telnet** line vty 0 15 password cisco login **! Nega o acesso da rede 172.16.5.0/24** access-class NO_TELNET_5_NETWORK in exit end

Nota: Tanto o Telnet como o SSH deita a ligação do *router* de origem e destino a baixo, deixando a rede indisponível por um grande momento. Esta situação não acontece quando o *router* em questão é o próprio ou o da mesma rede.

Configurações comuns

Foram utilizadas as seguintes configurações em todos os *routers*:

```
! Password do modo privilegiado
enable secret cisco
no ip domain lookup
ip domain name gear.pt
! Activa o protocol SNMP e manda as mensagens para o servidor.
snmp-server community public rw
snmp-server host 172.16.4.2 version 2c public
snmp-server enable traps
!
! Access list para bloquear o uso do telenet por parte dos PCs dos utilizadores
!
ip access-list standard NO_TELNET_5_NETWORK
 deny 172.16.5.0 0.0.0.255 log
 permit any
 exit
!
! Configuração telnet
!
line vty 0 15
 ! Atribui a access list a ligações telnet
 access-class NO_TELNET_5_NETWORK in
 password cisco
 login
 exit
!
end
```

R1

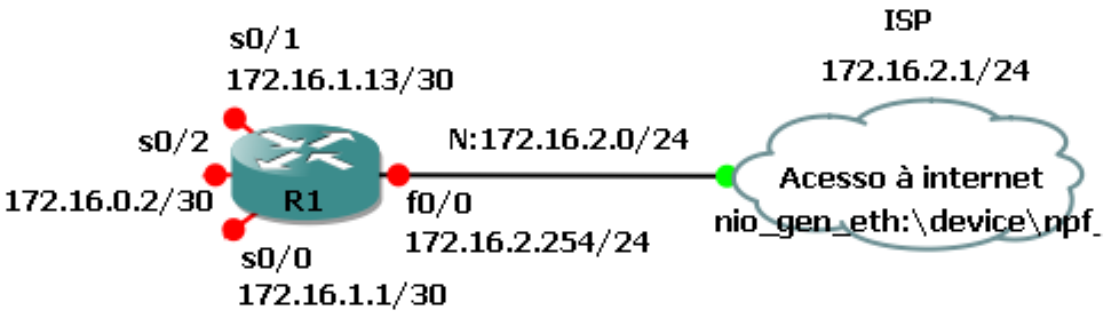

Ilustração 2 (Rede R1)

Dispositivo	Interface	IP/Máscara	Rede	Gateway
R1	S0/0	172.16.1.1/30	172.16.1.0/30	
	S0/1	172.16.1.13/30	172.16.1.12/30	
	S0/2	172.16.0.2/30	172.16.0.0/30	
	F0/0	172.16.2.254/24	172.16.2.0/24	
ISP → R1	NIC	172.16.2.1/24	172.16.2.0/24	172.16.2.254/24

O *router* "**R1**" está ligado directamente ao **ISP**, sendo este que fornece internet. Este *router* fornece ainda IPs à rede 172.16.5.0/24 via **DHCP**, reservando a gama de IPs 172.16.5.1 até 172.16.5.9 para servidores ou outros dispositivos de IPs fixos.

```
! Exclui os IPs 172.16.5.1 até 172.16.5.9
ip dhcp excluded-address 172.16.5.1 172.16.5.9
! Cria uma pool de DHCP e define a rede a atribuir o DHCP
ip dhcp pool R3-F0/0
 network 172.16.5.0 255.255.255.0
 default-router 172.16.5.254
 end
```

A nuvem (ISP), foi criada a partir de uma internet loopback criada no próprio PC, a seguir partilhamos a ligação de internet com essa interface, não foi possível obter ligação à internet dentro dos *routers* do GNS3 mesmo este pingando para a interface 172.16.2.1.

Ver configurações do router em anexo, R1.cfg[a1].

R2

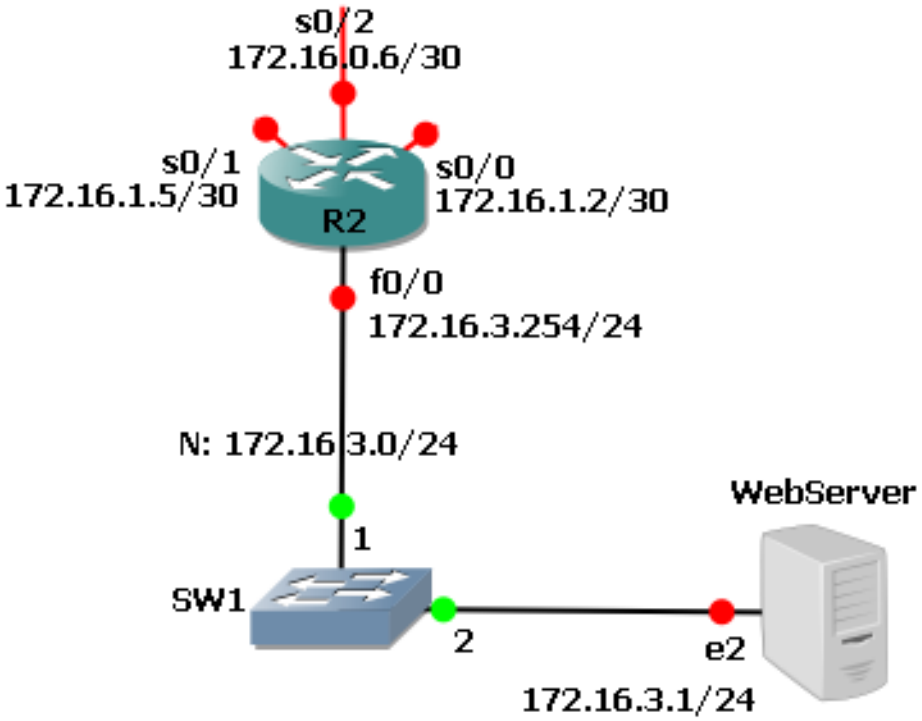

Ilustração 3 (Rede R2)

Dispositivo	Interface	IP/Máscara	Rede	Gateway
R2	S0/0	172.16.1.2/30	172.16.1.0/30	
	S0/1	172.16.1.5/30	172.16.1.4/30	
	S0/2	172.16.0.6/30	172.16.1.4/30	
	F0/0	172.16.3.254/24	172.16.3.0/24	
WebServer → R2	E2	172.16.3.1/24	172.16.3.0/24	172.16.3.254/24

O *router* "**R2**", serve apenas para o WebServer, que foi configurado com o IP 172.16.3.1/24, este pode ser acedido via HTTP pelo mesmo IP. Foi utilizado o software "**WAMP Server**[3]" que contém o Apache, MySQL e PHP de modo a poder servir pedidos de http.

Ver configurações do router em anexo, R2.cfg[a2].

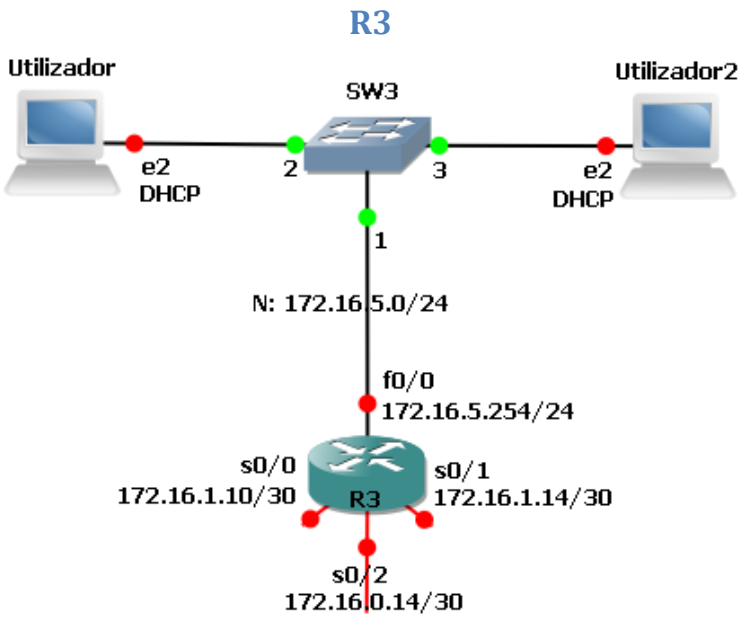

Ilustração 4 (Rede R3)

Dispositivo	Interface	IP/Máscara	Rede	Gateway
R3	S0/0	172.16.1.10/30	172.16.1.8/30	
	S0/1	172.16.1.14/30	172.16.1.12/30	
	S0/2	172.16.0.13/30	172.16.0.12/30	
	F0/0	172.16.5.254/24	172.16.5.0/24	
Utilizador → R3	E2	DHCP	172.16.5.0/24	172.16.5.254/24
Utilizador 2 → R3	E2	DHCP	172.16.5.0/24	172.16.5.254/24

O *router* "**R3**" gere toda a rede dos utilizadores comuns, estes obtêm o IP por DHCP que é fornecido pelo "**R1**". A rede 172.16.5.0/24 não pode aceder aos equipamentos por Telnet.

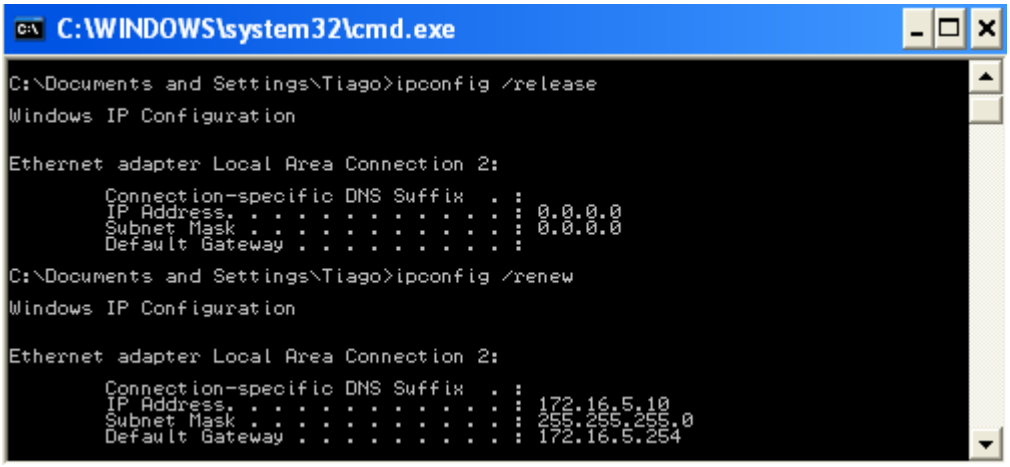

Ilustração 5 (Utilizador a obter IP por DHCP)

Ver configurações do router em anexo, R3.cfg[a3].

R4

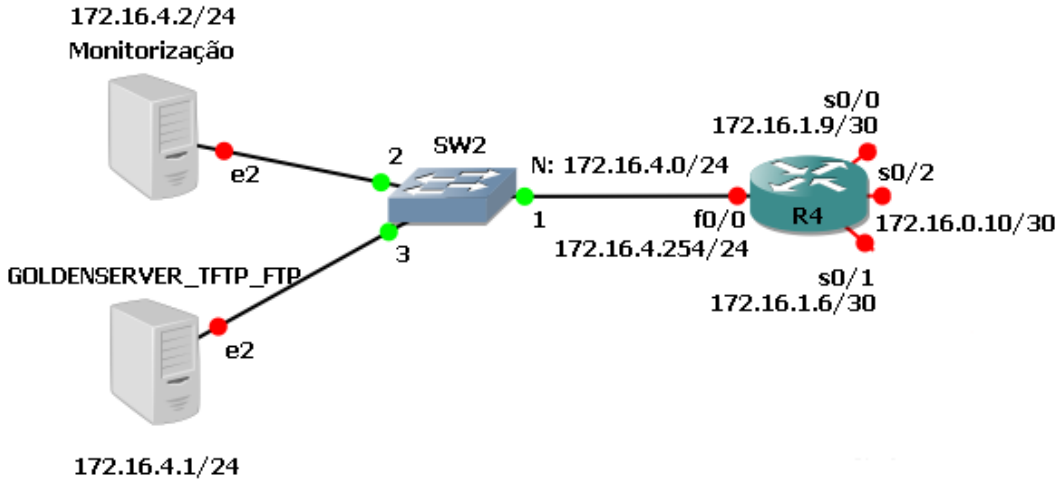

Ilustração 6 (Rede R4)

Dispositivo	Interface	IP/Máscara	Rede	Gateway
R4	S0/0	172.16.1.9/30	172.16.1.8/30	
	S0/1	172.16.1.6/30	172.16.1.4/30	
	S0/2	172.16.0.10/30	172.16.1.8/30	
	F0/0	172.16.4.254/24	172.16.4.0/24	
GoldenServer → R4	E2	172.16.4.1/24	172.16.4.0/24	172.16.4.254/24
Monitorização → R4	E2	172.16.4.2/24	172.16.4.0/24	172.16.4.254/24

O *router* "**R4**" gere os servidores de TFTP, FTP e Monitorização SNMP. Foram utilizados os seguintes *softwares*:

- **TFTP:** "TFTP Server" – Solarwinds[4]
- **FTP :** "FileZilla Server"[5]
- **Monitorização SNMP:** "Kiwi Syslog" – Solarwinds[6]

Para fazer um backup da configuração de qualquer router basta correr o comando: "*copy running-config tftp:172.16.4.1*"

Para aceder ao FTP podemos utilizar os PCs com o FileZilla cliente ou usar os *backups* do router para fazer *upload* para FTP, como imagens de IOS.

Para a monitorização SNMP versão 2c foi necessário configurar todos os *routers* com os seguintes comandos:

```
! Cria uma chave com permissão de leitura e escrita, define o host e activa todas as traps.
snmp-server community public rw
snmp-server host 172.16.4.2 version 2c public
snmp-server enable traps
```

Podemos ter acesso aos logs do Kiwi Syslog a partir do *browser*: **172.16.4.2**

Ver configurações do router em anexo, R4.cfg[a4].

RBackup

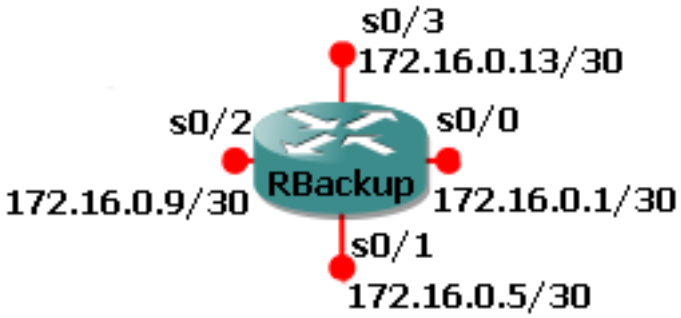

Ilustração 7 (Rede RBackup)

Dispositivo	Interface	IP/Máscara	Rede	Gateway
RBackup	S0/0	172.16.0.1/30	172.16.0.0/30	
	S0/1	172.16.0.5/30	172.16.0.4/30	
	S0/2	172.16.0.9/30	172.16.0.8/30	
	S0/3	172.16.0.13/30	172.16.0.12/30	

O *router* "**RBackup**" está ligado directamente a todos os routers (R1, R2, R3 e R4) com o único objectivo de garantir a ligação entre 2 pontos que estejam indisponíveis por outras rotas. Todas as rotas do RBackup estão configuradas como secundárias com uma distância administrativa de 150 usando o protocolo "**EIGRP**" com o processo **10**.

Neste caso se por exemplo o **R1** quiser comunicar com o **R4** e ambos os *routers* **R2** e **R3** estiverem indisponíveis a rota passará pelo **RBackup**.

```
! Configuração do protocolo de encaminhamento EIGRP do router
router eigrp 10
  passive-interface FastEthernet0/0
  passive-interface FastEthernet0/1
  network 172.16.0.0 0.0.0.3
  network 172.16.0.4 0.0.0.3
  network 172.16.0.8 0.0.0.3
  network 172.16.0.12 0.0.0.3
  distance eigrp 150 150
  no auto-summary
end
```

Ver configurações do router em anexo, RBackup.cfg[a5].

Conclusão

Concluindo este projecto, podemos citar que tivemos alguma dificuldade para a sua realização. Visto que tivemos alguns problemas, os quais ainda residem, da parte do próprio programa (GNS3), este bloqueava constantemente, por norma reiniciávamos o programa em questão e ficava resolvido por uns meros 5 minutos. Visto que esta era a única opção para realizar o trabalho, tivemos que trabalhar com o mesmo programa.

Como citamos no relatório tanto o Telnet, o SSH, e o WebServer deita a ligação do *router* de origem e destino abaixo, deixando a rede indisponível por um grande período de tempo. Este problema ainda reside.

Digamos que foi um projecto interessante, onde aplicamos muitos dos conhecimentos adquiridos nas aulas. As dificuldades sentidas na realização do mesmo, foram superadas com pesquisas e apoio do professor e colegas da turma. O projecto em si foi muito enriquecedor na matéria.

Bibliografia

[1] GNS3, http://www.gns3.net/

[2] VLSM (CIDR) Subnet Calculator, http://www.vlsm-calc.net/

[3] WAMP Server, http://www.wampserver.com/en/

[4] TFTP Server, http://www.solarwinds.com/products/freetools/free_tftp_server.aspx

[5] FTP Server, http://filezilla-project.org/

[6] Kiwi Syslog Server, http://www.kiwisyslog.com/kiwi-syslog-server-overview/

Conhecimentos adquiridos nas aulas.

Anexos

- **[a1]** R1.cfg
- **[a2]** R2.cfg
- **[a3]** R3.cfg
- **[a4]** R4.cfg
- **[a5]** RBackup.cfg