Pequeno guia de bolso de referencia sobre

Comandos "Cisco IOS"

Para ligar à consola de um router ligue a mesma a uma porta COM de um PC e utilize o comando **`minicom`** para dialogar com a consola. Para parametrizar inicialmente o router pode usar o comando **`setup`**.

Para alterar a configuração corrente dê a seguinte sequencia de comandos:

```
configure terminal          (configuração a partir do terminal)
comandos de alteração da configuração
^Z                          (para sair e terminar)
```

Se pretender abortar a configuração também pode sair por ^**C** ao invés de por ^**Z**. No entanto, algumas das alterações foram imediatamente tomadas em consideração pelo sistema.

Sempre que alterar a configuração corrente não se esqueça de a guardar no ficheiro de configuração através do comando: **`write memory`**

Este comando copia a configuração activa em memória para o file system do router.
O mesmo efeito pode ser obtido por:

```
copy running-config nvram:startup-config
```

Para ver os file systems do router e listar os ficheiros use, por exemplo, os comandos:

```
show file systems
dir nvram:
dir flash:
show nvram:
```

Se quiser colocar o router no estado inicial, dê os comandos:

```
delete nvram:startup-config
reload
```

Idem mas mais radical:

```
erase nvram:
reload
```

Para guardar a configuração num host remoto dar o comando (o endereço IP é um exemplo):

```
copy running-config scp://userName@192.168.110.2/rt-so-confg.txt
```

Para carregar a configuração a partir de um host remoto dar o comando (o endereço IP é um exemplo):

```
copy scp:// userName@192.168.110.2/rt-so-confg.txt running-config
```

Também se pode realizar as mesmas operações com o apoio de um servidor tftp através dos comandos (o endereço IP é um exemplo):

```
copy running-config tftp://192.168.100.20/rt-so-confg.txt
copy tftp://192.168.100.20/rt-so-confg.txt running-config
```

Para configurar uma chave RSA e activar implicitamente um servidor SSH no router:

```
config term
      crypto key generate rsa (seguir restante diálogo)
^Z
```

Exemplos de comandos úteis para ver a configuração corrente e o estado das interfaces:

```
show int
sh int summary
sh ip int brief
sh int
sh int interface-name
sh int counters
show int fast 0/x  (em que x é o número da interface)
show running-config
show startup-config (a gravada)
```

Comandos globais úteis:

```
ip subnet-zero    (para não desperdiçar endereços)
ip classless      (actualmente é por defeito)


ip host sudoeste 192.168.200.1
ip host sul 192.168.200.2
ip host sudeste 192.168.200.3
ip host centro 192.168.200.4
ip host noroeste 192.168.200.5
ip host norte 192.168.200.6
ip host nordeste 192.168.200.7

.........
service password-encryption   (cifrar passwords na config)
hostname RT-SO          (nome do router)
enable secret  YY       (qual o enable secret / password )
enable password XX
username crc password crc (definição de um utilizador local)
no ip source-route      (ignorar as opções IP source routing)
ip domain-name name      (1 ou mais)
ip domain-name di.fct.unl.pt
ip name-server ip-address
ip name-server 193.136.122.1
no ip http server (não activar servidor de http)
no ip secure-http server (não activar servidor de https)
no ip bootp server (não activar servidor de bootp)
no cdp run (não activar o Cisco Discovery Protocol)
ip route    0.0.0.0  192.168.190.1 (exemplo de default route)
```

```
Exemplo de definição de uma ACL)
no access-list 190
access-list 190 permit ip 192.168.0.0  0.0.255.255 any log
access-list 190 deny   ip any any log
(Exemplo de definição de um banner de login)

banner motd □

**********************************************************
*                                                        *
*          You are connected to a private system         *
*           Any violations will be logged                *
*                    [ sudoeste ]                        *
*                                                        *
**********************************************************
□

line vty 0 15
      access-class 190 in (associar uma ACL aos logins)
      password 7  VVVVV (exigir password por defeito)

ntp server ip-address (1 ou mais)
ntp server  193.136.122.1  (servidor NTP)
```

Para configurar um servidor DHCP:

```
! parametrização do dhcp (ver a documentação)
! exemplo quando a rede local é a 192.168.100.0
ip dhcp excluded-address 192.168.110.1 192.168.110.3
ip dhcp pool 0
      network 192.168.110.0 255.255.255.0
      default-router 192.168.110.1
      dns-server 193.136.122.1
```

Para configurar uma interface de um router usar por exemplo alguns dos comandos (dependentes alguns deles do tipo de interface):

```
config term
int fast 0/1
      description Rede local da bancada
      ip address XXXXXX YYYYY (endereço IP e máscara)
      speed 10          (interfaces ethernet)
      speed 100         (interfaces ethernet)
      speed auto        (melhor ainda)
      duplex full       (interfaces ethernet)
      duplex half       (interfaces ethernet)
      duplex auto       (melhor ainda)
      shutdown          (desactivar a interface)
      no shutdown       (activar a interface)
^Z
```

Os comandos mais relevantes para "proteger as interfaces" são:

```
  no ip redirects
  no ip unreacheables
  no ip proxy-arp
  no cdp enable
```

Os comandos mais relevantes para interfaces série são:

```
config term
int serial 0/1
      description ligação a uma bancada remota
      ip address XXXXXX YYYYY (endereço IP e máscara)
      physical layer sync
      encapsulation hdlc
      clock rate 128000     ! só no lado da ficha macho
^Z
```

Exemplos de parametrização de interfaces dos Ciscos

```
interface Loopback1
 description This router - router sul
 ip address 192.168.200.2 255.255.255.255
!
interface FastEthernet0/1
 description Connection to students.di.fct.unl.pt
 ip address 10.200.0.34 255.255.248.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nat outside
 no cdp enable
!
!
interface FastEthernet0/0
 description My local network
 ip address 192.168.110.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nat inside
 no cdp enable
!
interface Serial0/0
 description Connection to sudoeste (exemplo)
 ip address 192.168.201.254 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 clockrate 2000000
 ip nat inside
 no cdp enable
!
interface Serial0/1
 description Connection to Centro (exemplo)
 ip address 192.168.205.1 255.255.255.0
 .......
!
interface Serial0/2
 description Connection to norte (exemplo)
 ip address 192.168.204.1 255.255.255.0
 no ip directed-broadcast
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 clockrate 128000 ! so' de um dos lados do cabo RS232
 ip nat inside
 no cdp enable
```

Routing RIP

```
ip routing
no router rip
router rip
  version 2
  redistribute connected
  redistribute static
  [ passive-interface FastEthernet0/0 ]
  [ passive-interface FastEthernet0/1 ]
  ! manipulação dos pesos dos anúncios – ver lista adiante
  [ offset-list 30 out 5 serial 0/1]
                              access-list 30 permit 0.0.0.0  0.0.0.0
  network 192.168.100.0
  network 192.168.101.0
  network 192.168.102.0
  network 192.168.103.0
       etc.
  ...
  network 0.0.0.0
...
```

Routing OSPF

```
no router rip
router ospf 10
network 192.168.0.0 0.0.255.255 area 0
network 10.200.0.0 0.0.255.255 area 0
[ default-information originate metric 30 metric-type 1 ]
    ! se quizermos que uma default route seja propagada
end
```

Rotas

```
ip route network mask next-hop [ distância ]
ip route 0.0.0.0   0.0.0.0   192.168.1.254
   ! uma rota específica para a default route
ip route 0.0.0.0   0.0.0.0   null0  ! anunciar uma default route
      quando não se tem uma
```

Distribuição de carga quando existem vários caminhos para o destino à mesma distância:

```
no ip-route-cache  ! para cada pacote e destino recalcula-se a
      rota e faz-se distribuição round-robin
ip route-cache ! a distribuição round-robin só é feita para cada
      destino
```

estas directivas devem ser associadas às interfaces relevantes.

Tradução de endereços via NAT

```
interface serial 0/1
  description connection to the inside network
  ip address ….
  ip nat inside ! a tradução de endereços é executada à entrada

interface serial 0/2
  description connection to the ISP
  ip address ….
  ip nat outside ! a tradução de endereços é executada à saída

ip nat translation timeout 1800  ! 30 minutos
ip nat inside source-list 1 interface serial 0/2 overload
access-list 1 permit 192.168.0.0    0.0.255.255
access-list 1 deny any
```

Aspectos de segurança, auditoria e controlo de acessos

```
service password-encryption   (cifrar passwords na config)
enable secret  YY       (qual o enable secret / password )
enable password XX
username crc password XXX (definição de um utilizador local)
service timestamps debug datetime msec (debug com timestamps
relacionadas com o relógio e em miisegundos)
service timestamps log datetime msec (logging com timestamps
relacionadas com o relógio e em miisegundos)
service timestamps debug uptime (idem com timestamps em termso de
uptime e sem milisegundos)
service timestamps log uptime
!
logging buffered 4096 debugging
logging trap debugging
logging facility local5
logging 192.168.101.1

username crc password  XXXXX
username status nopassword noescape
username status autocommand show ip interface brief
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common

line vty 0 15
exec-timeout 5 0
password xxxx
login local
transport preferred none
transport input telnet ssh
transport output none
access-class 190 in

access-list 190 permit tcp 192.168.100.0 0.0.0.255 any log
```

```
access-list 190 deny ip any any log

logging trap debugging
logging facility local5
logging ip address 192.168.1.13


banner login x
.....

x

banner motd x
.....

x
```

Túneis GRE (Generic Routing Encapsulation IP Tunneling)

```
interface tunnel0
ip address 1.1.1.2  255.255.255.0
tunnel source Ethernet0/1
tunnel destination 192.168.3.2

interface Ethernet0/1
ip address 192.168.4.2  255.255.255.0

ip route 0.0.0.0   0.0.0.0   192.168.3.2
ip route 10.10.10.0  255.255.255.0  tunnel


interface tunnel0
ip address 1.1.1.1  255.255.255.0
tunnel source FastEthernet0/1
tunnel destination 192.168.4.2

interface FastEthernet0/1
ip address 192.168.3.2  255.255.255.0
```

IP multicasting pim sparse or dense mode

```
! para ver o que se passa com o IGMP
show ip igmp groups
show ip igmp interface
debug ip igmp

! global em cada router para usar pim em modo sparse
ip multicast routing
ip pim bidir-enable
ip pim rp-address 192.168.200.1

interface Ethernet0
```

```
      ip pim sparse-mode
! em todas as interfaces em que vai haver multicasting
! arranca o IGMP nesta interface

! idem para dense-mode
interface Ethernet0
      ip pim dense-mode
! em todas as interfaces em que vai haver multicasting
! arranca o IGMP nesta interface
! neste caso o único comando global é o "ip multicast routing"

! para analisar o estado do routing multicasting
show ip mroute
show ip mroute summary
show ip mroute count
show ip pim neighbor
show ip pim interface
```

Ferramentas Cisco de diagnóstico do multicasting

Traces the path from a source to a destination in a multicast tree:

```
mtrace source [ destination ] [ group-ip-address ]
```

Verifies multicast neighbors and shows multicast neighbor router information:

```
mrinfo [ hostname | address ] [ source-address | interface ]
```

Shows IP multicast paths:

```
mstat source [ destination ] [ group-ip address ]
```

Pings an IP multicast group:

```
ping group-ip-address
```

IP multicasting pim sparse mode

```
interface Ethernet0
      ip pim sparse-mode
! em todas as interfaces em que vai haver multicasting

! global em cada router
ip multicast routing
ip pim bidir-enable
ip pim rp-address 192.168.200.1
```

QoS com variantes

```
interface serial 0/1
! para ficar com a politica fifo
no fair-queue
! para ficar com a politica wfq
```

```
fair-queue
! para ficar com uma politica class based weigthed fair
! queeing
! service-policy output policy-map-name
! service-policy intput policy-map-name
service-policy output teste

! para analisar o estado das filas no router
show queuing
! para analisar o estado das filas numa interface
show queue serial 0/1

! introdução de WRED - Weigthed Random Early Discard
! WRED toma em consideração o campo TOS do cabeçalho IP
interface serial 0/0
    random-detect
    hold-queue 200 out
! A interface tem uma fila de espera de 200 pacotes e não de 40
! como por defeito

! Strict Priority Queuing no IOS da Cisco — low, medium, high
interface Serial0/0
    priority-group 1

priority-list 1 protocol ip medium udp domain
! dns por udp
priority-list 1 protocol ip low tcp ftp
! ftp por tcp
priority-list 1 protocol ip low tcp ftp-data
! ...

! custum queueing
interface Serial0/0
    custom-queue-list 1
!
queue-list 1 protocol ip 1 tcp www
queue-list 1 protocol ip 2 udp domain
queue-list 1 default 3
queue-list 1 queue 1 byte-count 7500
queue-list 1 queue 2 byte-count 500
queue-list 1 queue 3 byte-count 2000
! ...


! para definir uma classe de tráfego
! class-map ( match-all | match-any | empty ) class-map-name
class-map rtp
    description matches all rtp traffic
    match access-group acl-number
    ou match protocol protocol-name
! se vários protocolos, usar por exemplo match-any e a definição
! dos vários protocolos

! para definir uma política
! policy-map policy-map-name
policy-map teste
    description politica de teste de RTP e TCP
```

```
class rtp
      bandwidth percent 50
class tcp
      bandwidth percent 20
class class-default
      fair-queue
```