Segurança de Dispositivos de Rede
CCNA Security Ch.2: Securing Network Devices

Objectivos:

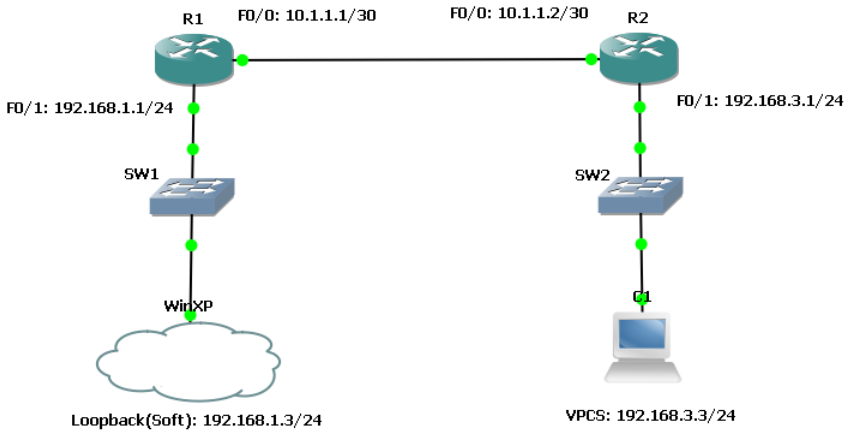
1. Proteger a instalação física e o acesso administrativo (CLI/SDM)
2. Programar perfis administrativos distintos de acesso ao CLI
3. Programar serviços básicos de gestão e monitorização (syslog, SNMP, SSH, and NTP)
4. Auditoria de segurança a routers baseada em SDM
5. Explorar as funcionalidades *auto-secure* e *One-Step Lockdown* do SDM

Tópicos

1. Cenário 1
2. Cenário 2
3. Enquadramento normativo
4. Segurança ao nível dos acessos
5. Configuração de perfis administrativos
6. Segurança e monitorização
7. AutoSecure

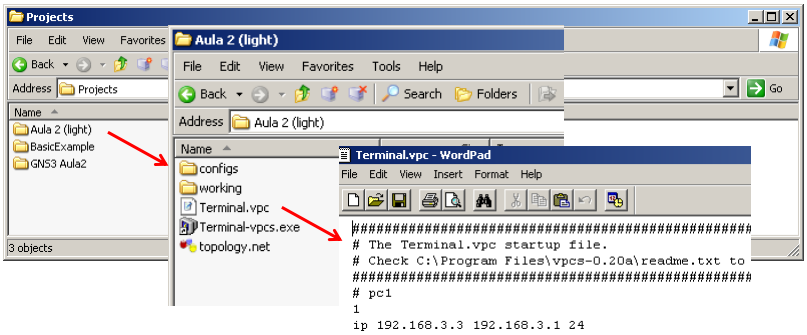
Projeto "SecuringIOS"

Cenário



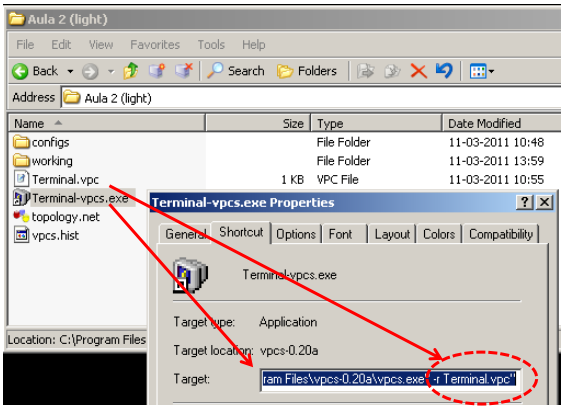
Cenário

1. Iniciar a máquina virtual
2. Localizar projeto:
   - "Desktop\Cisco\GNS3 \Projects\SecuringIOS"



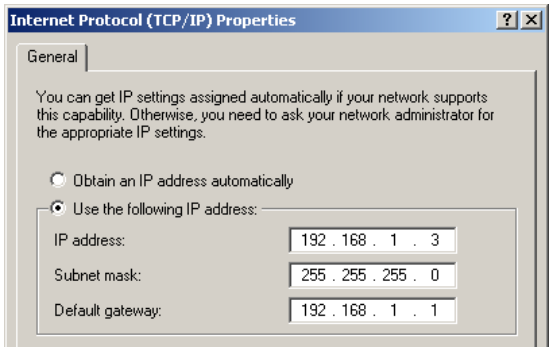
Cenário

3. Iniciar o VPCS (de preferência antes do GNS3)



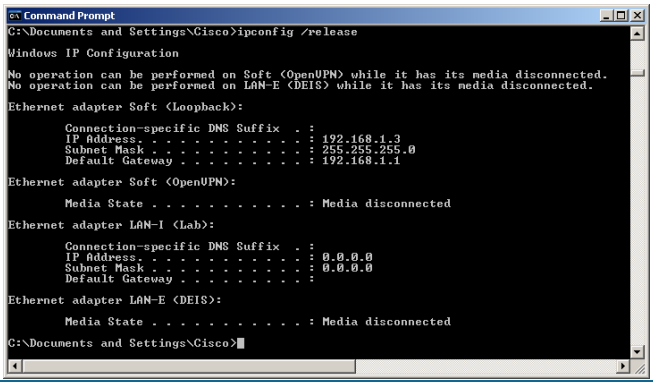
Cenário

4. Configurar convenientemente a interface Soft(loopback) da máquina virtual.



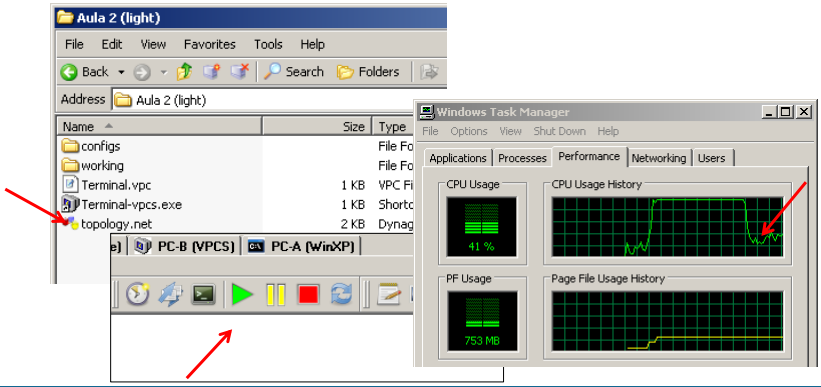
Cenário

5. Desativar ou descartar qualquer configuração que as restantes interfaces locais tenham entretanto obtido



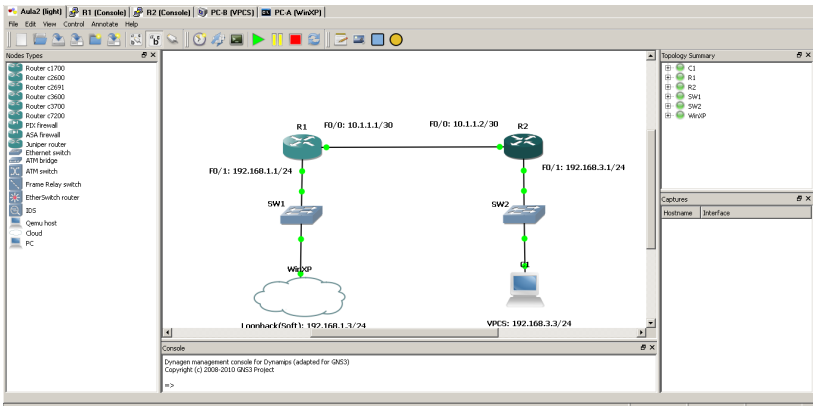
Cenário

6. Lançar o GNS3 + Iniciar os *routers* + consolas + *Command prompt* (WinXP) + [Afinar o Idle PC]



Cenário

7. [Integrar tudo no Wintabber]



Enquadramento Normativo

Enquadramento normativo

ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems - Requirements

Questions	Findings Yes	Findings No	ISO 27001 Control	Standard/Best Practice
Router Policy				
Is a router security policy in place?	☐	☐	A.5.1.1 A.11.4.1	
Disable Unneeded Services				
Are unused interfaces disabled?	☐	☐	A.11.4.4	Unused interfaces on the router should be disabled. Router(config-if)# shutdown
Is DNS lookups for the router turned off?	☐	☐	A.11.5.4 A.12.6.1	This client service is enabled by default and is not required on most routers. The following command is used to turn DNS lookup off. Router(config)#no ip domain-lookup

www.iso27001security.com/ISO27k_Router_security_audit_checklist.rtf

Enquadramento normativo

Questions	Findings Yes	Findings No	ISO 27001 Control	Standard/Best Practice
Is TCP small servers and UDP small servers service disabled on the router? {applicable before Cisco IOS 11.3}	☐	☐	A.12.6.1	These services are rarely used and hence can be disabled. This is disabled by default after Cisco IOS 11.3 Router(config)#no service tcp-small-servers Router(config)#no service udp-small-servers
Is Cisco Discovery Protocol disabled on the router?	☐	☐	A.11.4.4 A.12.6.1.	CDP which is used to obtain information such as the ip address, platform type of the neighboring Cisco devices should be disabled on the router if not used by any application. Router(config)# no cdp run OR Router(config-if)# no cdp enable
Is the finger service disabled on the router? {applicable before Cisco IOS 11.3}	☐	☐	A.11.4.4 A.11.5.4 A.12.6.1	Unauthorized persons can use the information obtained through this command for reconnaissance attacks. This service should be disabled. *Router(config)#no service finger*

Enquadramento normativo

Questions	Findings Yes	Findings No	ISO 27001 Control	Standard/Best Practice
Is Bootp server disabled on the routers?	☐	☐	A.11.4.4 A.11.5.4 A.12.6.1	The Bootp server service which is enabled by default allows other routers to boot from this router. This feature should be disabled on the router as it is rarely used on today's networks. The following command is used to disable the service. Router(config)#no ip bootp server

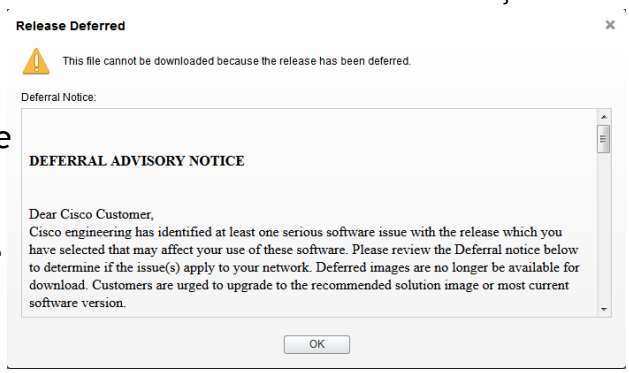
...

- ⇒ Recurso completo disponível no Moodle

Segurança ao nível do IOS

Segurança ao nível do IOS

- O currículo da Cisco infelizmente não alerta para o facto mas … deve haver um cuidado básico de atualização contínua de todo os software, inclusive o que corre nos equipamentos ativos de rede



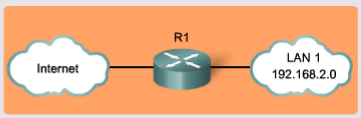
Segurança ao nível dos acessos

Segurança dos *Edge Routers*

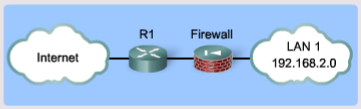
- Os routers periféricos são os alvos mais expostos e também os mais apetecíveis!
- Se forem comprometidos toda a segurança interna pode perder-se.

Routers are used to secure the perimeter of networks.

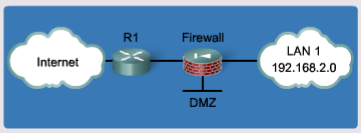
A single router approach:
- One router protecting the LAN.



Defense-in-depth approach:
- A router screening traffic before a dedicated firewall appliance (e.g., ASA).



DMZ approach:
- Variation with a DMZ containing servers that must be accessible from the Internet connected to the firewall appliance.



Segurança dos *Edge Routers*

Segurança Física

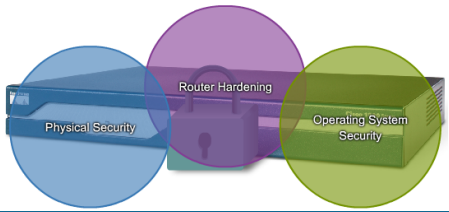
- Espaço (divisão e/ou bastidor) protegido com chave de acesso, climatizado, livre de interferências electroestáticas ou magnéticas, e protegido contra incêndios.
- Alimentação redundante (UPS)

Segurança de Configuração

- Assegurar que apenas os elementos eleitos possuem acesso, com o devido nível, à interface de configuração do *router*.
- Manter desactivados portos, serviços e interfaces não usadas.
- Alguns routers possuem por omissão serviços desnecessários activos!

Segurança do Sistema Operativo

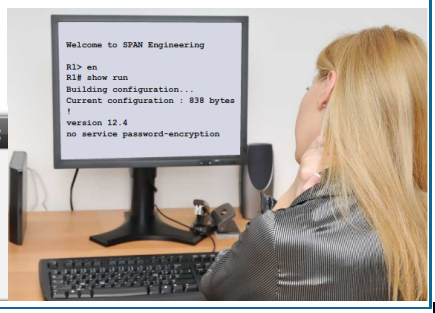
- Equipar o router com o máximo de RAM possível (suporta alguns DoS e permite executar serviços de protecção adicional).
- Escolher a última versão estável do sistema operativo.
- Manter em backup quer a imagem quer a configuração.



Segurança dos *Edge Routers*

- Além dos *routers* periféricos, todos os equipamentos de rede internos devem ser igualmente protegidos.
- A protecção de acesso (físico e remoto) à interface de gestão de todos os dispositivos de rede é indispensável.

Shoulder Surf
Acesso a senhas por simples observação.

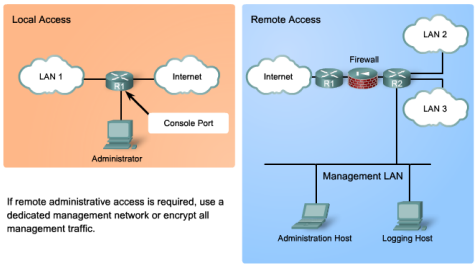


Things to do to secure administrative access to routers:

- Restrict device accessibility
- Log and account for all access
  - Authenticate access
  - Authorize actions
- Present legal notification
- Ensure the confidentiality of data

Segurança dos *Edge Routers*

- Além dos routers periféricos, todos os equipamentos de rede internos devem ser igualmente protegidos.
  - Formas de acesso: *Telnet, Secure Shell (SSH), HTTP, HTTPS, ou Simple Network Management Protocol (SNMP)*
  - Deve preferir-se gestão local (consola) para evitar *eavesdropping*.
  - Quando tal não é praticável preferir SSH a Telnet, HTTPS a HTTP
  - Manter uma rede virtual (VLAN) de gestão independente
  - Especificar nos dispositivos geridos os terminais com previlégios de acesso aos serviços de gestão



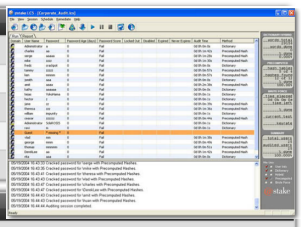
Escolha de *password*

- 10 ou mais caracteres
- Maiúsculas/minúsculas
- Letras, números, espaços
- Evitar "lugares comuns"
- Mudar password com frequência
- Memorizar, não anotar!

- Testar a robustez das passwords usadas
- Software: Cain and Abel, John the Ripper, Hydra, ElcomSoft, Lastbit, …

Weak Password	Why it is weak
secret	Simple dictionary password.
smith	Mother's maiden name.
toyota	Make of car.
bob1967	Name and birthday of user.
Blueleaf23	Simple words and numbers.

Strong Password	Why it is strong
b67n42d39c	Combines alphanumeric characters.
12^h u4@1p7	Combines alphanumeric characters, symbols and also includes a space.

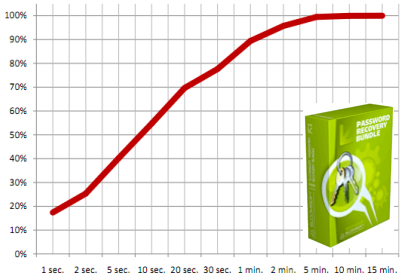


Escolha de *password*

ELCOMSOFT PROACTIVE SOFTWARE

Thunder Tables: Performance

% Keys Recovered	Elapsed Time
50%	8 sec.
90%	1 min.
95%	2 min.
99%	4 min.
100%	13 min.



http://www.elcomsoft.com/presentations/thunder_tables_and_GPUs.pdf

Average attack time is 25 sec.

Escolha de *password*

- 2004: Bill Gates disse que as passwords estavam obsoletas
- Dados de 2012:
  - Uma password de 7 carateres contendo apenas dígitos pode ser quebrada quase instantaneamente
  - Se além de dígitos possuir maiúsculas e minúsculas o tempo cresce para 10 horas
  - Adicionando carateres especiais sobrevive por 8 dias
  - Adicionando um oitavo caracter pode estender a vida por vários séculos mas em média sobreviverá apenas 16 minutos

Protecção do acesso administrativo (IOS)

Restrição de acesso ao modo privilegiado EXEC. Armazenada com o algoritmo de *hashing* MD5 (*Type 5 password*)

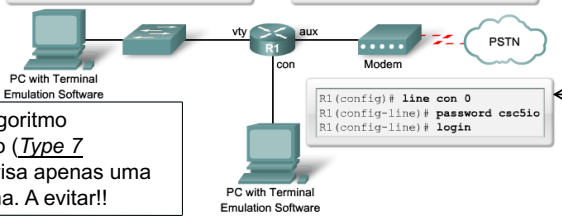
O comando ***no exec*** *veda* o acesso à linha onde é usado.

Com excepção da ***enable secret*** todas as passwords são guardadas em *plain text*. Ao activar o serviço de encriptação, a Cisco usa um algoritmo proprietário fraco (*Type 7 password*) que visa apenas uma protecção mínima. A evitar!!

```
R1(config)# enable secret csc5io
```

```
R1(config)# line vty 0 4
R1(config-line)# password csc5io
R1(config-line)# login
```

```
R1(config)# line aux 0
R1(config-line)# password csc5io
R1(config-line)# login
```




```
R1(config)# line con 0
R1(config-line)# password csc5io
R1(config-line)# login
```

A consola e a porta *aux* por omissão não requerem password (***no login***). No entanto a pass deve ser sempre configurada (**login + password**.

Opções para melhorar a segurança (IOS)

- É possível sobre cada "porta" de acesso
  - Exigir passwords com mais de *n* (0-16) caracteres (IOS 12.3(1))
    `security passwords min-length` *`length`*
  - Encurtar o tempo de inactividade por omissão das sessões (10')
    `exec-timeout` **`<`***`minutes`***`>`** **`[`***`seconds`***`]`**
  - Encriptar todas as passwords
    `service password-encryption`
    - Cifra as passwords existentes e futuras
    - Este comando não protege os ficheiros de configuração pois a função de síntese (*hash function*) aplicada é frágil
    - Depois do desligado (**no**) as passwords existentes continuam cifradas
    - Experimentar *on-line* o Cisco Password Cracker
      http://www.ifm.net.nz/cookbooks/passwordcracker.html

Exercício: Configuração de passwords

`R1(config)#security passwords min-length 8`	Configurar tamanho mínimo de uma password
`R1(config)#enable secret cisco123`	Configurar password de *enable*
`R1(config)#line console 0`	Configurar acesso via consola
`R1(config-line)#password cisco123`	Password
`R1(config-line)#exec-timeout 5 0`	Timeout de inactividade de uma ligação
`R1(config-line)#login`	Activar acesso consola
`R1(config-line)#logging synchronous`	Prevenir logs da consola interromperem um comando
`R1(config-line)#exit`	
`R1(config)#line aux 0`	Configurar acesso via AUX
`R1(config-line)#password cisco123`	
`R1(config-line)#exec-timeout 5 0`	
`R1(config-line)#login`	
`R1(config-line)#exit`	
`R1(config)#line vty 0 4`	Configurar do acesso via TELNET
`R1(config-line)#password cisco123`	
`R1(config-line)#exec-timeout 5 0`	
`R1(config-line)#login`	
`R1(config-line)#exit`	
`R1(config)#service password-encryption`	Activar encriptação das passwords de consola, AUX e TELNET

Autenticação de acesso (IOS)

- Numa grande organização a autenticação pode e deve ser centralizada recorrendo a um servidor TACACS+ ou RADIUS (e.g., *Cisco Secure Access Control Server* (ACS))
- Em redes pequenas, ou como alternativa local quando o acesso ao servidor central não é possível, deve ser criada uma base de dados local de utilizadores.
- Comandos importantes

  `username` *`name`* **`password`** *`password`* (⇒ Fraco: a evitar)

  `username` *`name`* **`secret`** *`password`* (⇒ MD5: preferível)

  `login local`

  ⇒ Comando necessário dentro de cada linha (console, aux, vty, …) para sinalizar ao IOS a possibilidade de usar a base de dados local de utilizadores.

Autenticação de acesso (IOS)

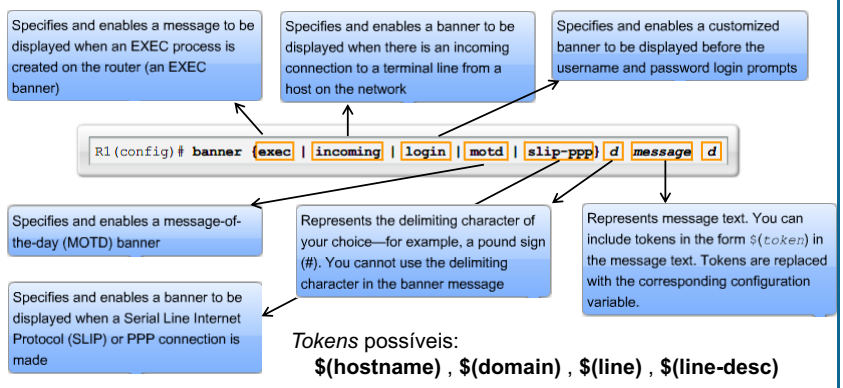
```
R1(config)# service password-encryption
R1(config)# username JR-ADMIN password letmein
% Password too short - must be at least 10 characters. Password
configuration failed
R1(config)# username JR-ADMIN password cisco12345
R1(config)# username ADMIN secret cisco54321
R1(config)# line con 0
R1(config-line)# login local
```

```
R1# show run | include username
username JR-ADMIN password 7 060506324F41584B564347
username ADMIN secret 5 $1$G3oQ$hEvsd5iz76WJuSJvtzs8I0
R1#
```

```
R1 con0 is now available

Press RETURN to get started.

User Access Verification

Username: ADMIN
Password:
R1>
```


Autenticação de acesso (IOS)

- Configuração de mensagens de boas vindas



Tokens possíveis:
$(hostname) , **$(domain)** , **$(line)** , **$(line-desc)**

Autenticação de acesso (IOS)

- Na verdade há mais *tokens* (IOS 12.4)

Token	Description	motd banner	login banner	exec banner	incoming banner	slip-ppp banner
$(hostname)	Router Hostname	Yes	Yes	Yes	Yes	Yes
$(domain)	Router Domain Name	Yes	Yes	Yes	Yes	Yes
$(peer-ip)	IP Address of the Peer Machine	No	No	No	No	Yes
$(gate-ip)	IP Address of the Gateway Machine	No	No	No	No	Yes
$(encap)	Encapsulation Type (SLIP or PPP)	No	No	No	No	Yes
$(encap-alt)	Encapsulation Type Displayed as SL/IP instead of SLIP	No	No	No	No	Yes
$(mtu)	Maximum Transmission Unit Size	No	No	No	No	Yes
$(line)	vty or tty (async) Line Number	Yes	Yes	Yes	Yes	No
$(line-desc)	User-specified description of the Line	Yes	Yes	Yes	Yes	No

Autenticação de acesso (IOS)

- Ordem dos *banners* apresentados
  - Sessão de consola: MOTD > EXEC
  - Sessão VTY: MOTD > LOGIN > EXEC
- Comandos ***no*** com comportamento especial
  - Sessões normais

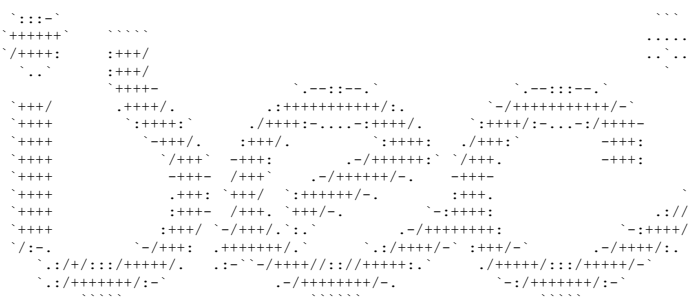
	exec-banner (default)	**no exec-banner**
motd-banner (default)	MOTD banner EXEC banner	None
no motd-banner	EXEC banner	None

  - Sessões Reverse Telnet para linhas assíncronas

	exec-banner (default)	**no exec-banner**
motd-banner (default)	MOTD banner Incoming banner	Incoming banner
no motd-banner	Incoming banner	Incoming banner

Autenticação de acesso (IOS)

- Mensagens de boas vindas às interfaces de gestão devem remeter para a legislação de cibercrime aplicável



http://www.text-image.com/convert/

```
---       UNAUTHORISED ACCESS IS PROHIBITED        ---
---  Entradas nao autorizadas sao punidas por lei  ---
---       (lei 109/2009 de 15 Setembro)            ---
```


Exercício: Acesso através de contas locais

R1(config)#**banner motd $***Unauthorized access strictly prohibited and prosecuted to the full extent of the law***$**	Configurar mensagem do dia
R1(config)#**exit**	
R1(config)#**username** *user01* **password** *0 user01pass*	Criar utilizador com password (encriptação fraca)
R1(config)#**username** *user02* **secret** *user01pass*	Criar utilizador com password MD5
R1(config)#**line console** 0	Configurar acesso consola para utilizar as contas locais
R1(config-line)#**login local**	
R1(config-line)#**exit**	
R1(config)#**line aux 0**	Configurar acesso AUX para utilizar as contas locais
R1(config-line)#**login local**	
R1(config-line)#**exit**	
R1(config)#**line vty 0 4**	Configurar acesso TELENET para utilizar as contas locais
R1(config-line)#**login local**	
R1(config-line)#**exit**	

Segurança de acesso melhorada (IOS)

Virtual Login Security Enhancements

- Implement delays between successive login attempts.
- Enable login shutdown if DoS attacks are suspected.
- Generate system logging messages for login detection.

Protege/detecta ataques DoS e *brute force* (*delay=1s*)

- Como retardar ataques *brute force* ou parar ataques DoS?

```
login block-for seconds attempts tries within seconds
login quiet-mode access-class {acl-name | acl-number}
login delay seconds
show login
show login failures
```

Protege contra ataques *brute force*
O delay é forçado entre tentativas de acesso consecutivas, sejam elas bem ou mal sucedidas.

- Estes comandos apenas reagem em linhas VTY mas **só se tornam efectivos se a autenticação for feita por par *login/password***.
- No *quite-period* apenas são aceites acessos permitidos pelas ACL

Exercício: Segurança de acesso melhorada

Visualizar configuração de ataques via login

```
R1#show login
     No login delay has been applied.
     No Quiet-Mode access list has been configured.

     Router NOT enabled to watch for login Attacks
```

Configurar bloqueio durante 60 segundos após duas tentativas falhadas em menos de 30 segundos

```
R1#configure terminal
R1(config)#login block-for 60 attempts 2 within 30
R1(config)#exit
```

Visualizar configuração de ataques via login após tentativa de ataque

```
R1#show login
     A default login delay of 1 seconds is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 30 seconds or less,
     logins will be disabled for 60 seconds.
```

O router alterna entre modo ***Normal mode*** (*watch mode*) e ***Quiet mode*** (quiet period).

```
     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 47 seconds.
     Denying logins from all sources.
```

Registo de acessos (IOS)

- Como reportar acessos correctos/incorrectos?

```
login on-failure log [every login_attempts]   (default=1)
login on-success log [every login_attempts]
```

- Em alternativa

```
security authentication failure rate threshold-rate log
```

2-1024
Número de autenticações Falhadas no último minuto.

Exercício: Registo (*logging*) de acessos

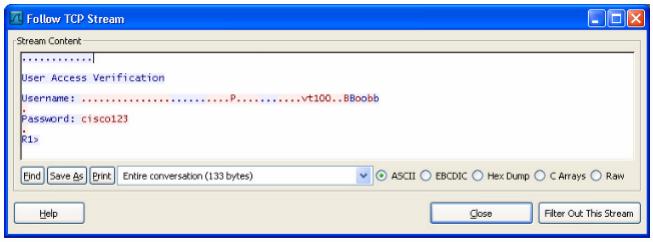
```
R1(config)#login on-success log
R1(config)#login on-failure log every 2
R1(config)#exit
R1#show login
     A default login delay of 1 seconds is applied.
     No Quiet-Mode access list has been configured.
     All successful login is logged.
     Every 2 failed login is logged.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 30 seconds or less,
     logins will be disabled for 60 seconds.

     Router presently in Normal-Mode.
     Current Watch Window
         Time remaining: 17 seconds.
         Login failures for current window: 0.
     Total login failures: 2.
```

Configurar registo de *log* para tentativas de login bem sucedidas e em cada duas tentativas falhadas

Visualizar configuração de ataques via login após configuração

Acesso por *Secure Shell* (SSH) (IOS)

- Deve ser o método preferencial de acesso remoto a dispositivos de rede e servidores substituindo o Telnet
- Oferece confidencialidade e integridade de sessão mesmo em ambientes/redes inseguros/vulneráveis
- Opera no porto TCP 22 (Telnet opera no TCP 23)



By following the Telnet stream, the attacker has captured the administrator's username (Bob) and password (cisco123).

Acesso por *Secure Shell* (SSH) (IOS)

- Requisitos prévios à configuração do acesso SSH
  1. Assegurar que os *routers* suportam SSH
     - Apenas as imagens que suportem a *IPSec feature set* (DES/3DES)
       - No nome destas imagens encontra-se "k8" ou "k9"
       - Ex.: c1841-entservicesk9-mz.124-20.T.bin
     - Versão IOS ≥ 12.1(1)T
  2. Assegurar que cada *router* possui um nome único na rede
  3. Assegurar que cada *router* usa o nome de domínio de rede correcto
  4. Assegurar que cada *router* se encontra configurado para aceitar autenticação por par *username*/*password* (local ou através do serviço AAA)

Acesso por *Secure Shell* (SSH) (IOS)

- Passo 1:
  - Atribuir um nome único ao *router* e o nome do domínio

```
ip domain-name domain-name
```

- Passo 2:
  - Produzir o par de chaves assimétricas (pública/privada)
    - O IOS recorre ao algoritmo RSA (Rivest, Shamir, and Adleman)

```
crypto key generate rsa general-keys modulus
        modulus-size
```

← Aceite: [360, 2048] Recomendado≥1024)

    - Chaves maiores tornam o processamento ligeiramente mais pesado
  - Consultar a chave pública criada

```
show crypto key mypubkey rsa
```

  - Remover um par de chaves gerado previamente

```
crypto key zeroize rsa
```


Acesso por *Secure Shell* (SSH) (IOS)

- Passo 3:
  - Criar ou confirmar que existe uma base de dados local de contas. Atribuir um nome único ao *router* e o nome do domínio

```
username name secret secret
```

- Passo 4:
  - Instruir o *router* para aceitar nos terminais VTY sessões SSH

```
login local
transport input ssh
```

  - O serviço SSH fica activo assim que as chaves são geradas.
  - Podemos permitir diversos métodos de entrada embora isso não seja recomendado

```
transport input telnet ssh
```

Acesso por *Secure Shell* (SSH) (IOS)

Step 1: Configure the IP domain name
Step 2: Generate one-way secret keys
Step 3: Verify or create a local database entry
Step 4: Enable VTY inbound SSH sessions


```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```


Acesso SSH – Comandos opcionais (IOS)

- Versão
  - SSH versão 1 (SSH-1)
    - 1995: Tatu Ylönen (Universidade de Tecnologia de Helsínquia)
    - 1998: Reportada vulnerabilidade de integridade (assegurada por um Código de Redundância Cíclica CRC-32)
    - 2001: Reportadas mais vulnerabilidades:
      - Possibilidade de alterar o último bloco de sessões encriptadas IDEA
      - Possibilidade de um servidor malicioso redireccionar a autenticação do cliente para outro servidor
  - SSH versão 2 (SSH-2)
    - 2006/IETF (tornado *standard*): RFCs 425[0-6],4335,4344/5,4716,4819
    - Troca de chaves Diffie-Hellman + Verificação de Integridade mais robusta: *Message Authentication Code* (MAC)
    - Suporte de múltiplas sessões de *shell* sobre uma única sessão SSH

Mais detalhes na Teórica

Acesso SSH – Comandos opcionais (IOS)

- Versão
  - SSH-1: Cisco IOS ≥ 12.1(1)T
  - SSH-2: Cisco IOS ≥ 12.3(4)T

  `ip ssh version {1 | 2}` ← Por omissão opera em Compability mode. Com este comando forçamos a versão aceite.
- Período de indolência durante a fase de negociação

  `ip ssh time-out seconds` ← Por omissão 120 segundos.
- Número máximo de tentativas de *login*

  `ip ssh authentication-retries integer` ← Por omissão 3.
- Inspecção dos parâmetros presentes

  `show ip ssh`
- Cliente SSH do IOS

  `ssh`

Acesso SSH – Comandos opcionais (IOS)

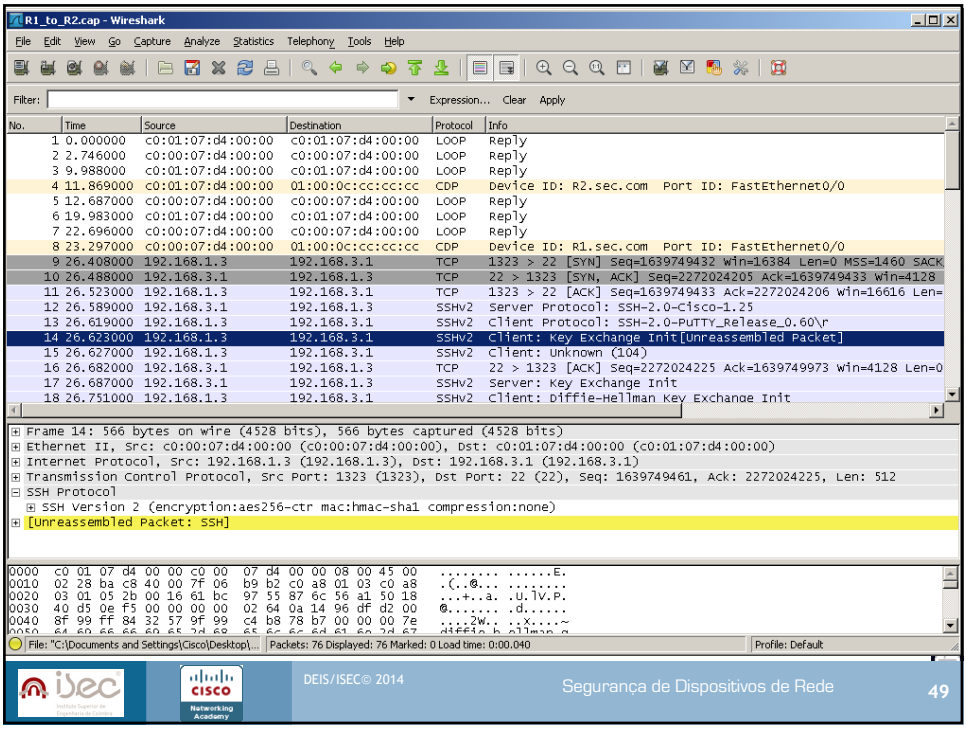

```
R1# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R1#
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ssh version 2
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
R1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 2
R1#
```

Exercício: Acesso via SSH

```
R1(config)#ip domain-name seguranca.dmz                    Configurar do domínio
R1(config)#username admin privilege 15 secret cisco123     Criar utilizador com privilégios (15)
R1(config)#line vty 0 4                                    Configurar acesso remoto
R1(config-line)#privilege level 15                         Definir privilégio de acesso (máximo)
R1(config-line)#login local
R1(config-line)#transport input ssh                        Acesso apenas via SSH
R1(config-line)#exit
R1(config)#crypto key generate rsa general-keys modulus 1024   Gerar par de chaves RSA para
The name for the keys will be: R1.seguranca.dmz                encriptação da comunicação

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]
R1(config)#ip ssh time-out 90                              Configurar timeout do SSH
R1(config)#ip ssh authentication-retries 2                 Configurar número máximo de
R1(config)#exit                                            tentativas de acesso
R1#show ip ssh                                             Visualizar configurações do SSH
SSH Enabled - version 1.99
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
```


Exercício: (Cenário 2)

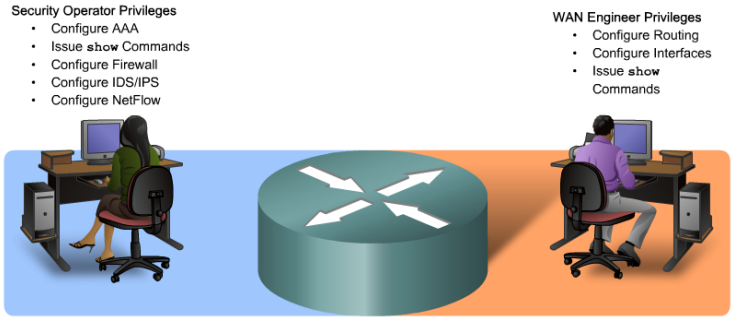
- No WinXP lançar uma sessão Putty (pasta Clients) destinada ao router programado com SSH.



Configuração de perfis administrativos

Perfis administrativos

- Numa organização nem todos os utilizadores devem ter acesso completo aos equipamentos
- Num departamento de IT as competências e responsabilidades estão bem definidas



Perfis administrativos básicos

- Dois modos de acesso administrativo:
  - **User EXEC mode** (nível 1): nível de permissão mínimo que apenas permite acesso a comandos de utilizador

```
Router>
```

É possível, por exemplo, executar o comando: **show ip interface brief**

```
Router> enable
```

Quando não é especificado o nível assume o nível 15.

  - **Privileged EXEC mode** (nível 15): permite acesso a todos os comandos de configuração do equipamento

```
Router#
```

É possível, por exemplo, executar o comando: **show running-config**

Modos de comando

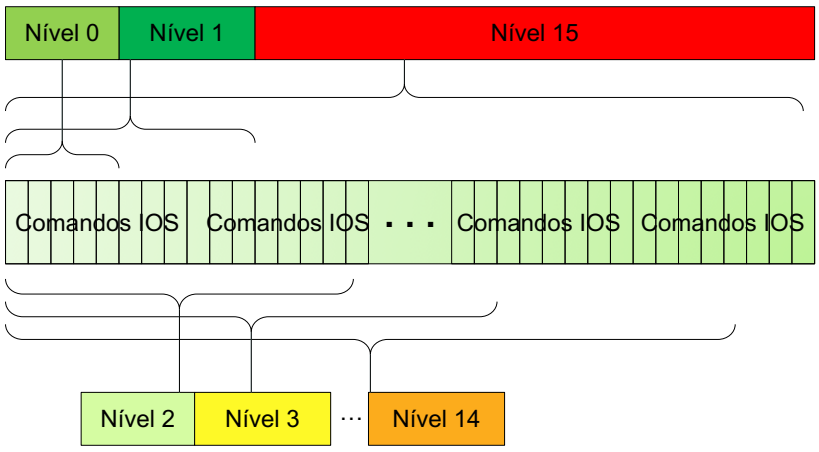
Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the **enable** command.	`Router#`	Issue the **disable** command or the **exit** command to return to user EXEC mode.	• Issue **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the **configure terminal**	`Router(config)#`	Issue the **exit** command or the **end** command to return to privileged	Configure the device.

... Dezenas de *Command Modes*

Criação de perfis administrativos

- Os dois perfis existentes podem não ser suficientes
  - Exemplo: *first-line technical support staff*
- Por vezes é necessário definir perfis de acesso de maior granularidade
- Duas abordagens (i.e. contextos) disponíveis no IOS:
  - *Privilege level*: suficiente quando um gere outros monitorizam
  - *Role-based CLI*: necessário quando se requer controlo + flexível
- Podemos controlar:
  - Quem acede às interfaces de gestão
  - A que subconjunto de operações de gestão pode aceder
  - Que recursos físicos pode gerir

Níveis de privilégio (*Privilege Level*)



Níveis de privilégio (*Privilege Level*)

- Níveis hierárquicos de privilégios
- Nível 0, 1 e 15 estão pré-definidos
- Os níveis 2 a 14 podem ser customizados de acordo com o nível de acesso pretendido
- Comandos permitidos num nível são herdados nos níveis superiores e retirados aos níveis inferiores.

16 Privilege Levels

- Level 0: Predefined for user-level access privileges. Seldom used, but includes five commands: **`disable`**, **`enable`**, **`exit`**, **`help`**, and **`logout`**
- Level 1: The default level for login with the router prompt `router>`. A user cannot make any changes or view the running configuration file.
- Levels 2 –14: May be customized for user-level privileges. Commands from lower levels may be moved up to another higher level, or commands from higher levels may be moved down to a lower level.
- Level 15: Reserved for the enable mode privileges (**`enable`** command). Users can change configurations and view configuration files.

Configuração dos níveis de privilégio

- Alterar o nível de privilégio actual de um comando

```
router(config)#
privilege mode {level level command | reset} command
```

Command	Description
mode	This command argument specifies the configuration mode. Use the **privilege ?** command to see a complete list of router configuration modes available on your router.
level	(Optional) This command enables setting a privilege level with a specified command.
level command	(Optional) This parameter is the privilege level that is associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15.
reset	(Optional) This command resets the privilege level of a command.
command	(Optional) This is the command argument to use when you want to reset the privilege level.

Nota: O acesso aos ficheiros de configuração é inamovível do nível 15, sendo tratado como um caso especial.

- Especificar a *password* de acesso ao nivel definido

```
enable secret level level password
```

Nota: O comando **enable secret level *15 password*** não inutiliza a *password* ***enable secret***, a qual continua a dar acesso ao nível 15.

Configuração dos níveis de privilégio: exemplo

```
R(config)#privilege exec level 2 ping
R(config)#enable secret level 2 cisco2
R(config)#exit
R#disable
R>enable 2
Password:
R#show privilege
Current privilege level is 2
R#show running-config
          ^
% Invalid input detected at '^' marker.

R#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/27/52 ms
```

Comando **ping** deslocado do nível 1 para o 2
Password de acesso ao nível 2 programada

Acesso ao *User EXEC mode* em nível 2 solicitado

Acesso a um comando de nível 15 negado

Comando **ping** aceite.

Configuração dos níveis de privilégio: exemplo (cont.)

```
R#disable
R>ping 192.168.1.3                                  .Comando ping indisponível no nível 1
       ^
% Invalid input detected at '^' marker.

R>enable 15                                         .Acesso ao User EXEC mode  em nível 15
Password:
R#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R(config)#privilege exec reset ping                 .A versão no sobre o comando privilege nem
R(config)#exit                                      sempre produz o resultado aparentemente
R#disable                                           espectável. Devemos usar o subcomando reset.
R>ping 192.168.1.1                                  .O comando ping está de novo disponível no nível 1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R>
```


Estabelecer automaticamente o nível de privilégios

- Na definição local de um utilizador é possível especificar o nível de privilégios a que a sessão estará sujeita por omissão.
  username *name* **privilege** *level* **secret** *password*
- Exemplo:

```
R>enable
Password:
R#show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00

  Interface    User               Mode         Idle     Peer Address

R#configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R(config)#username bob privilege 2 secret bobpass
R(config)#exit
R#
```

Estabelecer automaticamente o nível de privilégios

```
*Mar  1 00:03:22.631: %SYS-5-CONFIG_I: Configured from console by console
R#disable
R>show privilege
Current privilege level is 1
R>login
Username: bob
Password:
R#show privilege
Current privilege level is 2
R#show users
    Line       User       Host(s)              Idle       Location
*  0 con 0     bob        idle                 00:00:00

  Interface    User               Mode         Idle     Peer Address

R#enable
Password:
R#show privilege
Current privilege level is 15
R#logout
```


Estabelecer automaticamente o nível de privilégios

- Nas versões atuais o seguinte problema não se verifica!
- Para que um utilizador remoto (VTY), autenticado, fique de imediato com o nível de privilégios que a sua conta permite é necessário "afinar" explicitamente a configuração.

```
aaa authentication login default local
aaa authorization exec default local
```

Ver próximo capítulo!

Configuração dos níveis de privilégio: exemplos

```
R1# conf t
R1(config)# username USER privilege 1 secret cisco
R1(config)#
R1(config)# privilege exec level 5 ping
R1(config)# enable secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 secret cisco5
R1(config)#
R1(config)# privilege exec level 10 reload
R1(config)# enable secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 secret cisco10
R1(config)#
R1(config)# username ADMIN privilege 15 secret cisco123
R1(config)#
```

Se este argumento não for mencionado é criado um *user* que inicia sessões autenticadas com privilégios de nível 15.

In this example, four user accounts were created.
- A USER account with normal, Level 1 access.
- A SUPPORT account with Level 5 and **ping** command access.
- A JR-ADMIN account with the same privileges as the SUPPORT account plus access to the **reload** command.
- An ADMIN account which has all of the regular privileged EXEC commands.

Configuração dos níveis de privilégio: exemplos

```
User Access Verification

Username: user
Password: <cisco>
R1> show privilege
Current privilege level is 1
R1> ping 10.10.10.1
          ^
% Invalid input detected at '^' marker.

R1>
```

```
R1> enable 5
Password:
R1# <cisco5>
R1# show privilege
Current privilege level is 5
R1#
R1# ping 10.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#
R1# reload
Translating "reload"

Translating "reload"

% Unknown command or computer name, or unable to find computer address
R1#
```

```
R1# enable 10
Password:<cisco10>
R1# show privilege
Current privilege level is 10
R1# ping 10.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1# reload

System configuration has been modified. Save? [yes/no]: ^C

R1# show running-config
          ^
% Invalid input detected at '^' marker.
R1#
```

```
R1# enable 15
Password: <cisco123>
R1# show privilege
Current privilege level is 15
R1# show running-config
Building configuration...

Current configuration : 1145 bytes
!
version 12.4

<Output omitted>
```

Configuração dos níveis de privilégio: limitações

- Não permite o controlo do acesso a recursos (interfaces, portas ou *slots*) de um *router*
- Hierarquia rígida de privilégios: um comando autorizado num nível inferior é autorizado em todos os níveis superiores e comandos especificamente definidos em níveis superiores não podem ser autorizados em níveis inferiores
- Autorizar um comando com uma determinada opção implica que todas as sub-opções sejam permitidas também

```
privilege exec level 5 show ip route
```

→ Torna possível no nível 5 executar qualquer comando começado por `show, show ip, show ip route`

- Se quisermos bloquear um conjunto limitado de permissões, é necessário enunciar exaustivamente os restantes comandos autorizados, um em cada comando **privilege** ☹

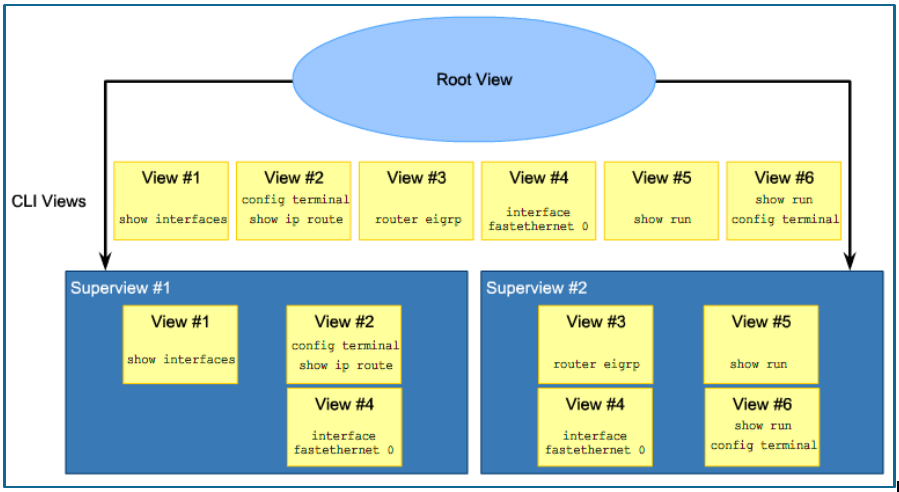
Role-based CLI (IOS ≥ 12.3(11)T)

- Mais flexibilidade que os níveis de permissões
- Baseia-se na criação de vistas (*views*) de configuração para cada perfil de utilizador
- Cada *view* define os comandos CLI que o utilizador tem permissões de executar e os recursos a que tem acesso
- Os utilizadores apenas conseguem visualizar os comandos, interfaces, portas, etc., a que têm acesso

Tipos de Vistas (*Views*)

- *Root View*
  - Possui os mesmos privilégios que um utilizador de nível 15
  - No entanto apenas quando o sistema se encontra na *root view* é que é possível gerir as *views* (criação, alteração e remoção)
- *CLI View*
  - Conjunto de comandos (comandos simples ou com opções específicas)
  - Comandos de uma *CLI View* não dependem das outras vistas
  - O mesmo comando pode existir em várias vistas
- *Superview*
  - União de uma ou mais vistas (i.e., dos respectivos comandos)
  - Não pode receber directamente comandos adicionais
  - Cada *superview* tem a sua *password*
  - Para além da *root view* podem existir 15 *views* (*CLI view* + *superviews*)

Vistas (*Views*)



Criação de vistas

1. Activar AAA (*Authentication, Authorization, and Accounting server*)

```
router(config)# aaa new-model
```

2. Activar *Root View*

```
router# enable view
```

← A *view* assumida por omissão neste comando é "root"

```
enable [view [view-name]]
```

- Command is used to enter the CLI view. Enter the name root or a specific view-name. If no name is specified, root is assumed.
- Remember, the **aaa new-model** command must be configured prior to entering a view.

Parameter	Description
view	Enters root view if no view-name is specified, which enables an adminstrator to configure CLI views. The view keyword is required if you want to configure a CLI view.
view-name	(Optional) Enters or exits a specified CLI view. This keyword can be used to switch from one CLI view to another CLI view.

Criação de vistas

3. Criar uma vista

```
router(config)#
parser view view-name
```

- Creates a view and enters view configuration mode.

4. Proteger a vista com *password*

```
router(config-view)#
secret encrypted-password
```

- Sets a password to protect access to the View.
- Password must be created immediately after creating a view otherwise an error message will appear.

Criação de vistas

5. Associar comandos à vista

```
router(config-view)#
commands parser-mode {include | include-exclusive | exclude} [all]
[interface interface-name | command]
```

- Adds commands or interfaces to a view.

Command	Description
commands	Adds commands or interfaces to a view.
parser-mode	The mode in which the specified command exists, for example EXEC mode.
include	Adds a command or an interface to the view and allows the same command or interface to be added to other views.
include-exclusive	Adds a command or an interface to the view and excludes the same command or interface from being added to all other views.
exclude	Excludes a command or an interface from the view.
all	A "wildcard" that allows every command in a specified configuration mode that begins with the same keyword or every subinterface for a specified interface to be part of the view.
interface *interface-name*	Interface that is added to the view.
command	Command that is added to the view.

Criação de vistas: exercício

```
R1#show parser view                                          .Contexto actual
No view is active ! Currently in Privilege Level Context
R1#configure terminal                                        .Activar AAA
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#aaa new-model                                     .Activar modo VIEW (root)
R1(config)#exit                                               (passaword de enable)
R1#enable view
Password:
*Mar  1 00:31:29.335: %PARSER-6-VIEW_SWITCH: successfully set
to view 'root'.
R1#configure terminal                                        .Criar vista admin1
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#parser view admin1
R1(config)#
*Mar  1 00:34:03.719: %PARSER-6-VIEW_CREATED: view 'admin1'
successfully created.
R1(config-view)#secret admin1pass                            . Proteger a vista (obrigatório)
R1(config-view)#commands exec include show                   .Atribuir permissões para todos os
R1(config-view)#commands exec include configure terminal     comandos começados por show,
R1(config-view)#commands exec include debug                  configure terminal e debug
                                                             . Exercício: do show running
```

Criação de vistas: exercício

```
R1(config-view)#end
*Mar  1 00:44:38.559: %SYS-5-CONFIG_I: Configured from console
by console
R1#enable view admin1                                    .Activar vista admin1
Password:
R1#
*Mar  1 00:45:57.707: %PARSER-6-VIEW_SWITCH: successfully set
to view 'admin1'.
R1#show parser view                                      .Identificar a vista actual
Current view is 'admin1'
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#?                                             .Não é possível configurar nada (os
Configure commands:                                      comandos têm de ser integrados
  do     To run exec commands in config mode             de forma explícita na vista ou a
  exit   Exit from configure mode                        keyword all usada devidamente)
R1(config)#^Z
R1#enable view
R1#disable                                               . Abandono do contexto de vistas
R1>enable                                                . Regresso ao contexto de
Password:                                                privilégios
```


Criação de vistas: exercício

```
R1(config)#parser view admin2                            .Vista admin2:
R1(config-view)#
*Mar  1 13:01:10.040: %PARSER-6-VIEW_CREATED: view
'admin2' successfully created.
R1(config-view)#secret admin2pass
R1(config-view)#commands exec include all show           . Protecção da vista.
R1(config-view)#commands exec include configure terminal . Acesso a todos os comandos show.
R1(config-view)#^Z
*Mar  1 13:02:30.852: %SYS-5-CONFIG_I: Configured from
console by console
R1#enable view admin2
Password:
*Mar  1 13:02:50.452: %PARSER-6-VIEW_SWITCH: successfully
set to view 'admin2'.
R1#show running-config                                   . O acesso à running-config passa a
Building configuration...                                estar disponível (devido à keyword all)
Current configuration : 13 bytes                         mas apenas linhas com os comandos a
!                                                        que temos acesso são mostradas.
!
!
end
```

Criação de vistas: exercício

```
…
R1(config)#parser view admin3
*Mar  1 13:06:27.612: %PARSER-6-VIEW_CREATED: view 'admin3' …
R1(config-view)#secret admin3pass
R1(config-view)#commands exec include all show
R1(config-view)#commands exec include all configure terminal
R1(config-view)#^Z
*Mar  1 13:07:57.636: %SYS-5-CONFIG_I: Configured from …
R1#enable view admin3
Password:
*Mar  1 13:08:14.736: %PARSER-6-VIEW_SWITCH: successfully …
R1#show running-config
Building configuration...

Current configuration : 2473 bytes
!
version 12.4
service timestamps debug datetime msec
…
```

.Comutar para a *root view*

. Protecção da vista.

. Acesso a todos os comandos show e todos os comandos de todos os submodos a que dê acesso o comando *configure terminal*.

. O acesso à *running-config* continua disponível (devido à keyword **all** do comando show) mas desta vez o conteúdo do ficheiro é integralmente visível (devido à keywork **all** do comando **configure terminal**).

Criação de vistas: desafio

- Desenvolva uma vista destinada a conferir ao ISP da sua empresa permissões exclusivas de configuração apenas da interface de acesso à Internet (F0/1). O ISP deverá ainda poder consultar a informação necessária para averiguar do seu bom funcionamento.

Criação de vistas: solução

```
R1(config)#parser view admin4
R1(config-view)#secret admin4pass
R1(config-view)#commands exec include all show
R1(config-view)#commands exec include configure terminal
R1(config-view)#commands configure include interface
R1(config-view)# commands configure include-exclusive all interface FastEthernet0/1
R1(config-view)#^Z
R1#enable view admin4
R1#show running-config
Building configuration...
Current configuration : 107 bytes
…
!
interface FastEthernet0/1
 ip address 194.65.52.14 255.255.255.240
 duplex auto
 speed auto
!
!
end
```

. A visão sobre o ficheiro de configuração é limitada a comandos e subcomandos da interface F0/1

Criação de vistas: solução

```
R1-Firewall#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-Firewall(config)#?
Configure commands:
  do          To run exec commands in config mode
  exit        Exit from configure mode
  interface   Select an interface to configure

R1-Firewall(config)#interface ?
  Async              Async interface
  BVI                Bridge-Group Virtual Interface
  CDMA-Ix            CDMA Ix interface
  ...

R1-Firewall(config)#interface null ?
  <0-0>  Null interface number

R1-Firewall(config)#interface null 0
                                   ^
% Invalid input detected at '^' marker.
```

. De forma ilusória o IOS sugere argumentos a que a presente vista não possui acesso (bug?)

Criação de vistas: solução

```
R1-Firewall(config)#interface f0/0
                    ^
% Invalid input detected at '^' marker.

R1-Firewall(config)#interface f0/1
R1-Firewall(config-if)#?
Interface configuration commands:
  access-expression       Build a bridge boolean access expression
  ...

R1-Firewall(config-if)#ip address 194.65.52.14 255.255.255.240
R1-Firewall(config-if)#no shut
```

. Não é conferido acesso à F0/0

. É conferido acesso à F0/1

. É conferida possibilidade de efectuar a sua configuração

Criação de super-vistas (*superviews*)

- Semelhante à criação de vistas
- Em vez de associar comandos são associadas vistas
- É necessário estar na *root view* para configurar super-vistas

Criação de super-vistas (*superviews*)

1. Criar uma super-vista

```
router(config)#
parser view view-name superview
```

- Appending the keyword **superview** to the **parser view** command creates a superview and enters view configuration mode.

2. Atribuir *password*

```
router(config-view)#
secret encrypted-password
```

- Sets a password to protect access to the Superview.
- Password must be created immediately after creating a view otherwise an error message will appear.

3. Integrar vistas na super-vista

```
router(config-view)#
view view-name
```

- Adds a CLI view to a superview.
- Multiple views may be added.
- Views may be shared between Superviews.

Criação de super-vistas: exemplo

- Criação de uma super-vista

```
R1(config)# parser view USER superviewv
* Mar  1 09:56:26.465 : %PARSER-6-SUPER_VIEW_CREATED: super view 'USER' successfully
created.
R1(config-view)# secret cisco
R1(config-view)# view SHOWVIEW
*Mar  1 09:56:33.469: %PARSER-6-SUPER_VIEW_EDIT_ADD: view SHOWVIEW added to superview
USER.
R1(config-view)# exit
R1(config)#
R1(config)# parser view SUPPORT superview
*Mar  1 09:57:33.825 : %PARSER-6-SUPER_VIEW_CREATED: super view 'SUPPORT'
successfully created.
R1(config-view)# secret cisco1
R1(config-view)# view SHOWVIEW
*Mar  1 09:57:45.469: %PARSER-6-SUPER_VIEW_EDIT_ADD: view SHOWVIEW added to superview
SUPPORT.
R1(config-view)# view VERIFYVIEW
*Mar  1 09:57:57.077: %PARSER-6-SUPER_VIEW_EDIT_ADD: view VERIFYVIEW added to
superview SUPPORT.
R1(config-view)#exit
R1(config)#
```

```
R1# show running-config

<output omitted>

!
parser view SUPPORT superview
 secret 5 $1$VplOSBBB1N68Z2ekr/aLH1edts.
 view SHOWVIEW
 view VERIFYVIEW
!
parser view USER superview
 secret 5 $1$E4k5$ukHyfYP7dHOC48N8pxm4s/
 view SHOWVIEW
!
parser view JR-ADMIN superview
 secret 5 $1$8kx2$rbAe/ji2200mQ1yw.568g0
 view SHOWVIEW
 view VERIFYVIEW
 view REBOOTVIEW
!
```

- Configuração de uma super-vista

Criação de super-vistas: exemplo

```
R1# enable view USER
Password:
*Mar  1 09:59:46.197: %PARSER-6-VIEW_SWITCH: successfully set to view 'USER'.

R1# ?
Exec commands:
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  show    Show running system information

R1#
R1# show ?
  flash:   display information about flash: file system
  version  System hardware and software status

R1#
```

```
R1# enable view SUPPORT
Password:
*Mar  1 10:00:11.353: %PARSER-6-VIEW_SWITCH: successfully

R1# ?
Exec commands:
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  ping    Send echo messages
  show    Show running system information

R1#
```

```
R1# enable view JR-ADMIN
Password:
*Mar  1 10:00:28.365: %PARSER-6-VIEW_SWITCH: successfully set to view 'JR-ADMIN'.

R1# ?
Exec commands:
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  ping    Send echo messages
  reload  Halt and perform a cold restart
  show    Show running system information

R1#
```


Criação de super-vistas: exemplo

```
R1# show parser view
No view is active ! Currently in Privilege Level Context
R1#
R1# enable view
Password:
*Mar  1 10:38:56.233: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
R1#
R1# show parser view
Current view is 'root'
R1#
R1# show parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
 SUPPORT *
 USER *
 JR-ADMIN *
 ADMIN *
-------(*) represent superview-------
R1#
```

Associação de vistas a utilizadores

- Na definição local de um utilizador é possível especificar a *view* por omissão que lhe é atribuída após autenticação

```
username name view view-name secret password
```

- O IOS tem de ser instruído para usar a base de dados local

```
aaa authentication login default local
aaa authorization exec default local
```

- Ainda assim os acessos por consola fogem por omissão à aplicação da view. Para evitar isso:

```
aaa authorization console
```

- Exercício: Crie um utilizador "gestor" e associe-lhe a *view* "admin4" de modo que assim que inicie uma sessão fique sob o efeito da mesma.

Ver próximo capítulo!

Segurança e monitorização

Resiliência do IOS e da configuração

- Se um atacante ganhar acesso a um router, para além de poder alterar configurações do equipamento, pode remover os ficheiros de configuração e a imagem do IOS
- A recuperação da configuração ou da imagem do IOS irá aumentar a indisponibilidade da rede

A compromised router can be erased by an attacker.

Resiliência do IOS e da configuração

- Permite recuperação rápida do *router*.
- Mantém cópia segura da configuração.
- O IOS do *router* é protegido contra acções destrutivas.
- O par de protecções é denominado *bootset*.

Cisco IOS Resilient Configuration facts

- The configuration file in the primary bootset is a copy of the running configuration that was in the router when the feature was first enabled.
- The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image file.
- The feature automatically detects image or configuration version mismatch.
- Only local storage is used for securing files, eliminating scalability maintenance challenges from storing multiple images and configurations on TFTP servers.
- The feature can be disabled only through a console session.

O *router* deve estar equipado com um disco PCMCI A ATA (Personal Computer Memory Card International Association / Advanced Technology Attachment.

Resiliência do IOS e da configuração: exercício

```
R1(config)#secure boot-image
R1(config)#secure boot-config
R1(config)#exit
R1#show secure bootset
R1#
IOS resilience router id 4294967295
```

.Tornar a imagem do IOS e a *running-config* apenas visíveis e acessíveis em modo ROMMON

.Visualizar ficheiros arquivados em modo seguro

Nota: esta capacidade apenas pode ser desactivada por consola.

```
IOS image resilience version 12.4 activated at 19:47:43 UTC Sun Feb 27 2011
Secure archive flash:c1841-advipservicesk9-mz.124-20.T1.bin type is image (elf)
[]
  file size is 37081324 bytes, run size is 37247008 bytes
  Runnable image, entry point 0x8000F000, run from ram

IOS configuration resilience version 12.4 activated at 19:48:23 UTC Sun Feb 27 2011
Secure archive disk0:.runcfg-20110227-194823.ar type is config configuration archive
size 2812 bytes

R1#sh flash:
```

Visualizar o conteúdo da *flash*

Resiliência do IOS e da configuração: recuperação

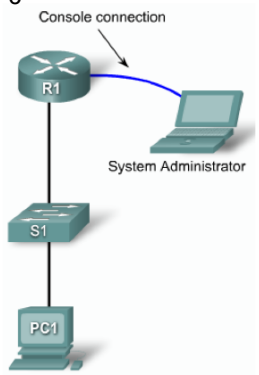
1. Reiniciar o *router* (comando **`reload`**)
2. Enviar a sequência de *break* ("Ctrl + break") repetidamente durante o arranque para levar o *router* ao modo ROMMON
3. Com o comando **`dir`** inspeccionar o conteúdo da *flash*.
   - Com **`show secure bootset`** é possível identificar o *router*
4. Com o comando **`boot`** seguido do nome do ficheiro do sistema operativo descoberto no passo anterior reiniciar o *router*.
5. No modo de configuração global: **`configure terminal`**
6. Com o comando **`secure boot-config restore`** *`filename`* restaurar a configuração original do equipamento

- Nota: Em 5) pode ser necessário o *bypass* da password.

Recuperação do controlo do *router* desconhecendo as passwords configuradas

Abordado no CCNA1

1. Aceder ao *router* por consola
2. Repetir sequência de *break* ("**`Ctrl + Break`**") até o *router* entrar em ROMMON
3. Alterar registo de configuração de modo a ignorar configuração (**`confreg 0x2142`**)
4. Reiniciar o router: **`reset`**
5. Entrar no modo privilegiado: **`enable`**
6. Repor a configuração existente:
   - **`copy startup-config running-config`**
   - **`configure terminal`** + Alterar passwords
7. Restaurar a configuração resiliente
   - **`secure boot-config restore`** *`filename`*
8. Repor a configuração de arranque
   - **`copy running-config startup-config`**



Desactivar o sistema de recuperação de controlo

- Importante quando a segurança física é fraca

```
R1(config)# no service password-recovery
WARNING:
Executing this command will disable password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes/no]: yes
R1(config)
```

```
R1# show running-config
Building configuration...

Current configuration : 836 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service password-recovery
```

```
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 platform with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x8000f000, size: 0xcb80
```

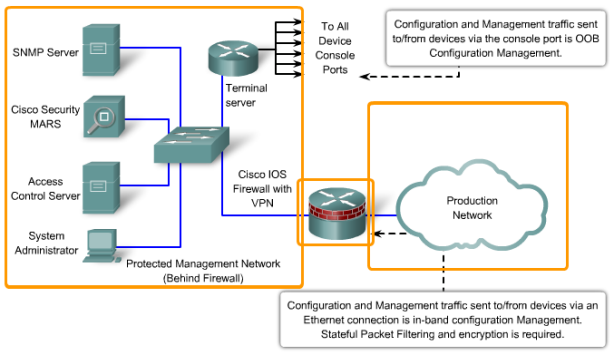
Desactivar o sistema de recuperação de controlo

- Nalguns equipamentos não é suportado:

```
R1(config)#no service password-recovery
Password recovery disable mode is not supported by the
 current ROMMON.
Please upgrade the ROMMON if you want to use this feature.
```

- Notas adicionais:
  - Trata-se de um comando escondido do IOS
  - Previne acesso ao modo ROMMON
  - É gerada no arranque a seguinte mensagem:
    - "PASSWORD RECOVERY FUNCTIONALITY IS DISABLED."
  - Como recuperar um *router* nesta condição?
    - Ctrl + Break 5 segundos após o IOS ser descomprimido
    - Neste caso a configuração é apagada automaticamente e o processo de recuperação de controlo automaticamente habilitado
    - Se o IOS local não existir é necessário trocar a *flash* do router

In-band management vs. Out-of-band management



Gestão OOB

- Fornece os níveis mais elevados de segurança e mitiga o risco de transferir informação confidencial sobre protocolos de gestão inseguros.

Gestão In-band

- Limitada aos dispositivos que necessitam de ser geridos ou monitorizados de forma remota.
- Usar IPsec, SSH, ou SSL quando possível.
- Limitar a abertura do canal de gestão ao tempo estritamente necessário

Registo de eventos (*logs*)

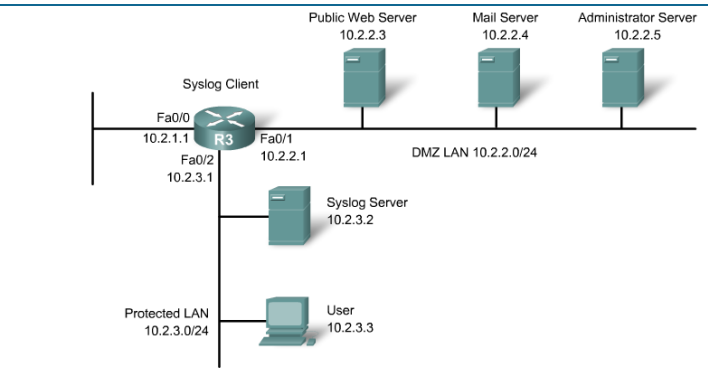
- O registo de eventos de um *router* é uma peça importante na análise e monitorização de uma rede
- Informação indispensável na análise de problemas
- É necessário identificar os eventos importantes e prioritários a registar
  - Exemplo: Sistemas de detecção de intrusões podem monitorizar estes registos e detectar/reportar possíveis intrusões
- Activar o registo de eventos:

```
R1(conf)#logging on
```


Registo de eventos (*logs*)

- Pode ser feito de diversas formas:
  - Consola: é um modo operacional enquanto o acesso é feito localmente. As mensagens no entanto não são guardadas pelo *router* para análise posterior.
  - Linhas de terminal: Trata-se de um modo possível que sofre das mesmas desvantagens que o modo consola.
    - `R1(conf)#logging monitor level`
  - *Buffered logging*: O registo de eventos neste caso é guardado na memória volátil do *router*, não sobrevivendo a *reboots*
    - `R1(conf)#logging buffered level`
  - Syslog: O router envia mensagens a um serviço externo.
  - SNMP *traps*: O registo de eventos é mapeado numa *trap* SNMP entregue a um gestor SNMP externo.

Registo de eventos (*logs*) por Syslog



- A syslog server is a device that accepts and processes log messages from one or more syslog clients.
- A syslog client is a router or other type of equipment that generates log messages and forwards them to a syslog server.

Registo de eventos (*logs*) por Syslog: exercício

- Activar no terminal um servidor Syslog
- No *router*:

```
R1(config)#logging on                                  .Activar registo de eventos (logging)
R1(config)#service timestamps log datetime msec        .Activar registo de tempo dos eventos
R1(config)#[logging source-interface loopback 0]       .Endereço de origem das notificações.
R1(config)#logging host 192.168.1.3                    .Servidor(es) Syslog destinatário(s)
R1(config)#logging trap ?                              .Configurar nível de detalhe dos logs
<0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
```

High level

Low level

Level	Keyword	Description	Definition
0	emergencies	System is unusable.	LOG_EMERG
1	alerts	Immediate action is needed.	LOG_ALERT
2	critical	Critical conditions exist.	LOG_CRIT
3	errors	Error conditions exist.	LOG_ERR
4	warnings	Warning conditions exist.	LOG_WARNING
5	notification	Normal but significant condition.	LOG_NOTICE
6	informational	Informational messages only.	LOG_INFO
7	debugging	Debugging messages.	LOG_DEBUG

Registo de eventos (*logs*) por Syslog: exercício

. Configuração de *logging* activa

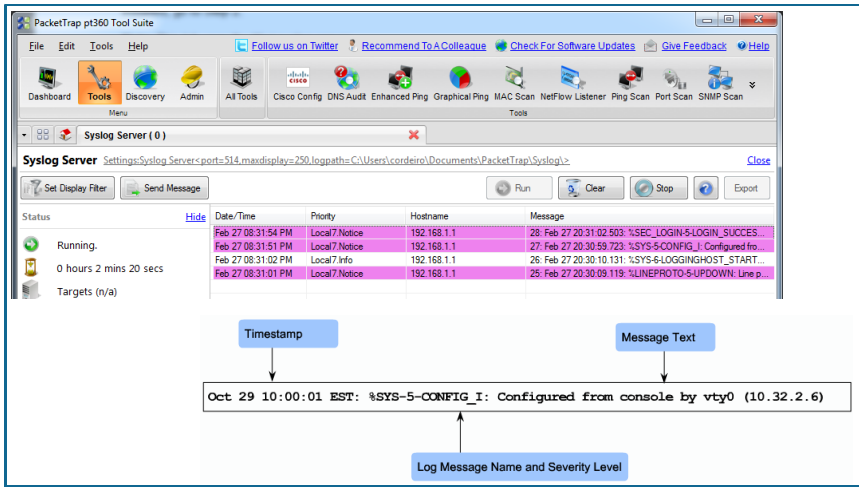
```
R1#show logging
Syslog logging: enabled (1 messages dropped, 1 messages rate-limited,
            0 flushes, 0 overruns, xml disabled, filtering disabled)
Console logging: level debugging, 22 messages logged, xml disabled,
                 filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
                 filtering disabled
Buffer logging: disabled, xml disabled,
                filtering disabled
Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Trap logging: level informational, 25 message lines logged
```


Registo de eventos (*logs*) por Syslog: exercício

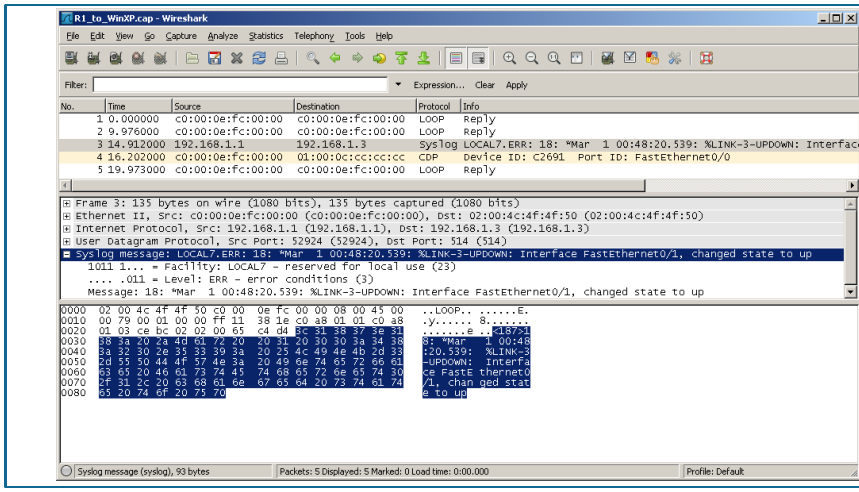
- Nível de severidade dos eventos: exemplo

Syslog Level and Name	Definition	Example
0 LOG_EMERG	A panic condition normally broadcast to all users	Cisco IOS software could not load
1 LOG_ALERT	A condition that should be corrected immediately, such as a corrupted system database	Temperature too high
2 LOG_CRIT	Critical conditions; for example, hard device errors	Unable to allocate memory
3 LOG_ERR	Errors	Invalid memory size
4 LOG_WARNING	Warning messages	Crypto operation failed
5 LOG_NOTICE	Non-error conditions that may require special handling	Interface changed state, up or down
6 LOG_INFO	Informational messages	Packet denied by ACL
7 LOG_DEBUG	Messages that contain information that is normally used only when debugging a program	Packet type invalid

Registo de eventos (*logs*) por Syslog: exercício



Registo de eventos (*logs*) por Syslog: exercício



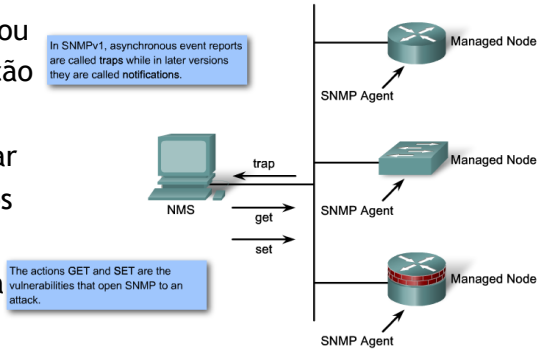
Registo de eventos (*logs*) por SNMP

- *Simple Network Management Protocol* (SNMP)
  - Protocolo de monitorização e configuração de equipamentos de redes TCP/IP
  - Três versões:
    - SNMP v1
    - SNMP v2
    - SNMP v3
  - Componentes:
    - Gestores - Network Management Systems (NMS)
    - Agentes – Managed Nodes (MN)
    - Bases de dados – Management Information Bases (MIB)

Abordado no CCNA4

SNMP

- As MIBs contêm a informação sobre as configurações e funcionamento dos equipamentos
- Os MN disponibilizam o acesso às MIBs aos NMS
- Os NMS lêem (*get*) e/ou alteram (*set*) a informação das MIBs dos MN
- Os *set* podem provocar acções nos equipamentos
- Os MN podem enviar notificações (*traps*) para os NMS



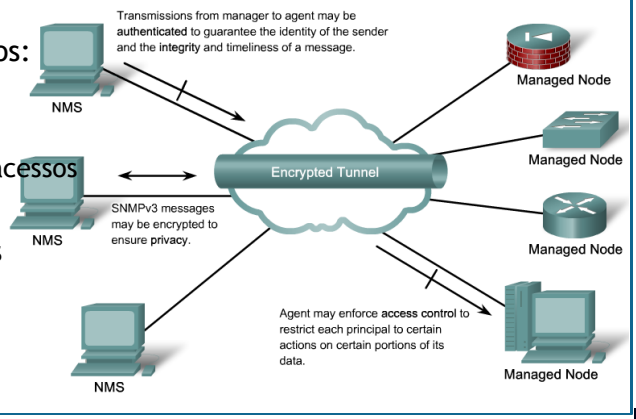
SNMP v1 e v2

- *Comunity String*
  - *Password* que permite autenticar os NMS nos MN
  - Valor típico: "public"
- Tipos de *Comunity String*:
  - *Read-only*: permite acesso de leitura a todas as MIBs
  - *Read-write*: permite acesso de leitura e escrita a todas as MIBs
- Nível de segurança baixo. Recomendado utilizar VLANs privadas especificamente votadas à gestão da rede.

Community Strings Facts:
- Used to authenticate messages between a management station and an SNMPv1 or SNMPv2 engine
- Read-write community strings can get and set information in an agent.
- Set access is equivalent to having the enable password for a device.

SNMP v3

- Resolve as questões de segurança das versões anteriores
- Inclui os serviços:
  - Autenticação
  - Privacidade
  - Controlo de acessos
- Integridade das mensagens
- Autenticação
- Encriptação



SNMP v3

- Três níveis de acesso
  - **noAuth:** Autenticação da mensagem através de correspondência de *username* ou *community*
  - **auth:** Autenticação da mensagem através do método *Hashed Message Authentication Code* (HMAC), o método *Message Digest 5* (MD5) ou o método *Secure Hash Algorithms* (SHA).
  - **Priv:** Autenticação da mensagem através do método HMAC MD5 ou HMAC SHA e cifra usando o algoritmo *Data Encryption Standard* (DES), *Triple DES* (3DES), ou *Advanced Encryption Standard* (AES).

Network Time Protocol (NTP)

RFC 1305

- Uma análise correcta e consistente do registo de eventos pressupõe uma correlação temporal dos mesmos.
- É importante manter a data e a hora dos equipamentos de rede consistente (i.e. sincronizada).
- Formas de ajuste da data e hora no IOS:
  - Manual
  - *Network Time Protocol* (NTP)

```
R1# clock set 10:28:00 DEC 16 2008
R1#
*Dec 16 10:28:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated
from 16:07:17 UTC Tue Dec 16 2008 to 10:28:00 UTC Tue Dec 16 2008,
configured from console by console.
R1#
```

Network Time Protocol (NTP)

RFC 1305

```
Router(config)#
ntp master [stratum]
```

- Makes the system an authoritative NTP server.
- The stratum number is the number of hops away from an authoritative source such as an atomic clock.

```
Router(config)#
ntp server {ip-address | hostname} [version number] [key keyid]
[source interface] [prefer]
```

- Allows the software clock to be synchronized by an NTP time server.

```
Router(config-if)#
ntp broadcast client
```

- Configures device to receive NTP broadcast messages on the interface.

Network Time Protocol (NTP): exercício

- Ajuste manual do tempo

R1

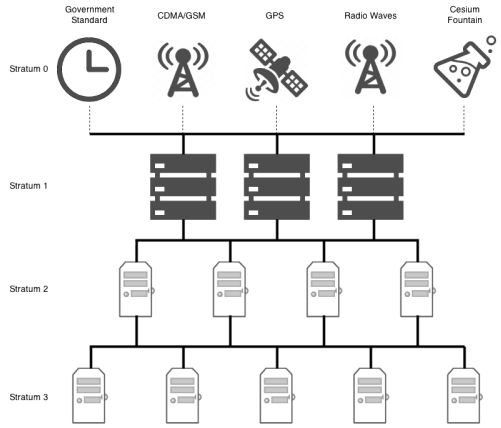
```
R1#show clock
*00:15:40.031 UTC Fri Mar 1 2002
R1#
R1#clock set 11:26:20 13 Apr 2011
R1#s
*Apr 13 11:26:20.000: %SYS-6-CLOCKUPDATE: System clock has been updated from
00:17:06 UTC Fri Mar 1 2002 to 11:26:20 UTC Wed Apr 13 2011, configured from console
by console.
R1#show clock detail
11:27:20.563 UTC Wed Apr 13 2011
Time source is user configuration
```

R2

```
R2#show clock detail
*00:18:18.875 UTC Fri Mar 1 2002
No time source
```

Network Time Protocol (NTP): exercício

- Propagação hierárquica



Public NTP Primary (stratum 1) Time Servers
http://wpollock.com/AUnix2/NTPstratum1PublicServers.htm

Stratum 1 NTP Network Time Servers Available In The UK, Europe
http://www.timetools.co.uk/2013/07/25/ntp-server-uk/

Network Time Protocol (NTP): exercício

- Ajuste do tempo com base no NTP

R1

```
R1(config)#ntp master 3 ← Stratum
R1(config)#do show clock detail
11:30:07.295 UTC Wed Apr 13 2011
Time source is NTP
R1(config)#end
R1#debug ntp ?
  adjust          NTP clock adjustments
  authentication  NTP authentication
  events          NTP events
  loopfilter      NTP loop filter
  packets         NTP packets
  params          NTP clock parameters
  refclock        NTP reference clocks
  select          NTP clock selection
  sync            NTP clock synchronization
  validity        NTP peer clock validity
R1#debug ntp packets
NTP packets debugging is on
```

R2

```
R2(config)#ntp server 10.1.1.1
R2(config)#^Z
Apr 13 11:40:47.797: %SYS-5-CONFIG_I:
Configured from console by console
R2#show clock detail
11:30:52.113 UTC Wed Apr 13 2011
Time source is NTP
```

Network Time Protocol (NTP): exercício

- Ajuste do tempo com base no NTP (cont.)

R1

```
Apr 13 11:48:44.835: NTP: stateless xmit packet to 10.1.1.2:
Apr 13 11:48:44.835:  leap 0, mode 4, version 3, stratum 3, ppoll 128
Apr 13 11:48:44.839:  rtdel 0000 (0.000), rtdsp 0002 (0.031), refid 7F7F0701 (127.127.7.1)
Apr 13 11:48:44.839:  ref D1500C0A.F9D8F9D4 (11:48:26.975 UTC Wed Apr 13 2011)
Apr 13 11:48:44.843:  org D1500C1C.C80B3EAA (11:48:44.781 UTC Wed Apr 13 2011)
Apr 13 11:48:44.843:  rec D1500C1C.D0DF4D50 (11:48:44.815 UTC Wed Apr 13 2011)
Apr 13 11:48:44.847:  xmt D1500C1C.D51B7585 (11:48:44.832 UTC Wed Apr 13 2011)
R1#
Apr 13 11:49:48.787: NTP: rcv packet from 10.1.1.2 to 10.1.1.1 on FastEthernet0/0:
Apr 13 11:49:48.787:  leap 0, mode 3, version 3, stratum 4, ppoll 128
Apr 13 11:49:48.791:  rtdel 00DD (3.372), rtdsp 05E6 (23.041), refid 0A010101 (10.1.1.1)
Apr 13 11:49:48.791:  ref D1500C1C.E5B9B469 (11:48:44.897 UTC Wed Apr 13 2011)
Apr 13 11:49:48.795:  org D1500C1C.D51B7585 (11:48:44.832 UTC Wed Apr 13 2011)
Apr 13 11:49:48.795:  rec D1500C1C.E5B9B469 (11:48:44.897 UTC Wed Apr 13 2011)
Apr 13 11:49:48.795:  xmt D1500C5C.C811906A (11:49:48.781 UTC Wed Apr 13 2011)
Apr 13 11:49:48.799:  inp D1500C5C.C8ADDC70 (11:49:48.783 UTC Wed Apr 13 2011)
R1#
```

Periodicidade ≅ 1 minuto

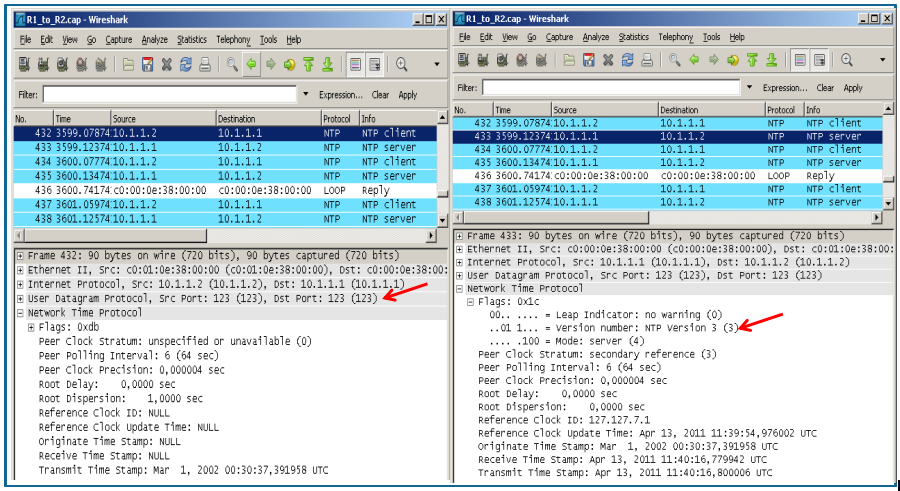
Network Time Protocol (NTP): exercício

- Ajuste do tempo com base no NTP (cont.)

R2

```
R2#show ntp status
Clock is synchronized, stratum 4, reference is 10.1.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is D1500AAF.DEDCB356 (11:42:39.870 UTC Wed Apr 13 2011)
clock offset is 2.2110 msec, root delay is 0.29 msec
root dispersion is 18.80 msec, peer dispersion is 16.57 msec
R2#show ntp associations
      address         ref clock     st  when  poll reach  delay  offset    disp
*~10.1.1.1         127.127.7.1       3    10    64  377    -0.3    2.21    17.5
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
R2#sh ntp associations detail
10.1.1.1 configured, our_master, sane, valid, stratum 3
ref ID 127.127.7.1, time D1500E0A.F9D8B6E2 (11:56:58.975 UTC Wed Apr 13 2011)
our mode client, peer mode server, our poll intvl 256, peer poll intvl 256
root delay 0.00 msec, root disp 0.03, reach 377, sync dist 23.697
delay 15.93 msec, offset -25.7252 msec, dispersion 15.70
precision 2**18, version 3
…
```

Network Time Protocol (NTP): exercício



Network Time Protocol (NTP): Autenticação

Router(config)#

```
ntp authenticate
```

- Enables the authentication feature

Router(config)#

```
ntp authentication-key key-number md5 key-value
```

- Defines the authentication keys

Router(config)#

```
ntp trusted-key key-number
```

- Authenticates the identity of a system to which NTP will synchronize
- Key number corresponds to key number in the **ntp authentication-key** command

Network Time Protocol (NTP): Autenticação

```
R2# show ntp associations detail
10.10.10.1 configured, our_master, sane, valid, stratum 2
ref ID 127.127.7.1, time CCF29760.A8F4DB7D (21:08:48.659 UTC Tue Dec 16 2008)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.03, reach 17, sync dist 1886.810
delay 23.41 msec, offset 0.9618 msec, dispersion 1875.08
precision 2**18, version 3
org time CCF2979B.8E2195E9 (21:09:47.555 UTC Tue Dec 16 2008)
rcv time CCF2979B.90E1A99D (21:09:47.565 UTC Tue Dec 16 2008)
xmt time CCF2979B.8AE1EA33 (21:09:47.542 UTC Tue Dec 16 2008)
filtdelay =    23.41   23.47   23.61   23.41    0.00    0.00    0.00    0.00
filtoffset =    0.96    0.94    0.94    0.66    0.00    0.00    0.00    0.00
filterror =     0.02    0.99    1.97    2.94 16000.0 16000.0 16000.0 16000.0

R2# conf t
R2(config)# ntp authenticate
R2(config)# ntp authentication-key 1 md5 cisco123
R2(config)# ntp trusted-key 1
R2(config)# ^Z
R2# show ntp associations detail | include 10.10.10.1
10.10.10.1 configured, our_master, sane, valid, stratum 16
R2#
<a few minutes later>
R2# show ntp associations detail | include 10.10.10.1
10.10.10.1 configured, authenticated, our_master, sane, valid, stratum 2
R2#
```


Network Time Protocol (NTP): exercício

- Ajuste do tempo com base no NTP (cont.)

1 R1

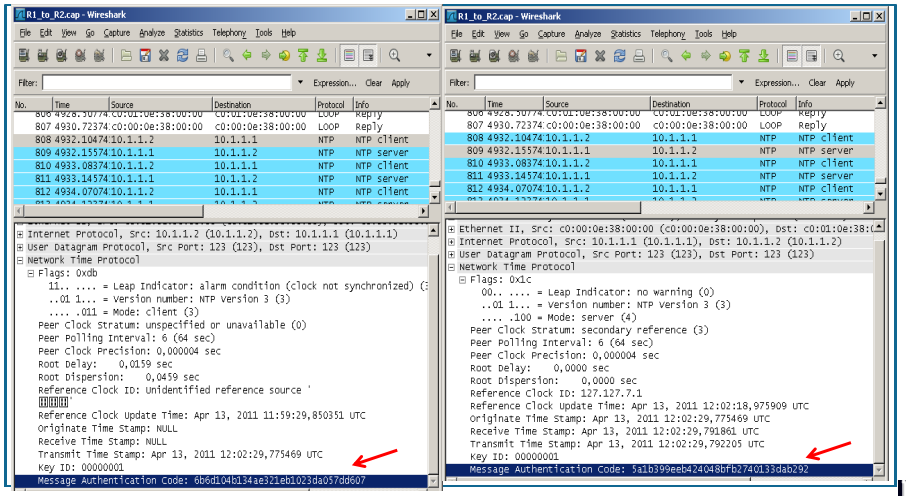
```
R1#undebug all
All possible debugging has been turned off
R1#debug ntp authentication
NTP authentication debugging is on

R1#configuration terminal
Enter configuration commands, one per line.
End with CNTL/Z.
R1(config)#ntp authenticate
R1(config)#ntp authentication-key 1 md5 cisco
R1(config)#
Apr 13 12:02:29.791:  Authentication key 1
Apr 13 12:02:29.791:  Authentication key 1
Apr 13 12:02:30.795:  Authentication key 1
Apr 13 12:02:30.795:  Authentication key 1
…
R1#show clock
12:08:16.683 UTC Wed Apr 13 2011
```

2 R2

```
R2#configuration terminal
Enter configuration commands, one per line.
End with CNTL/Z.
R2(config)#ntp authentication-key 1 md5 cisco
R2(config)#ntp authenticate
R2(config)#ntp trusted-key 1
R2(config)#ntp server 10.1.1.1 key 1

R2(config)#end
R2#show ntp associations detail | include
10.1.1.1
10.1.1.1 configured, authenticated, our_master,
sane, valid, stratum 3

R2#show clock
12:08:16.683 UTC Wed Apr 13 2011
```

3

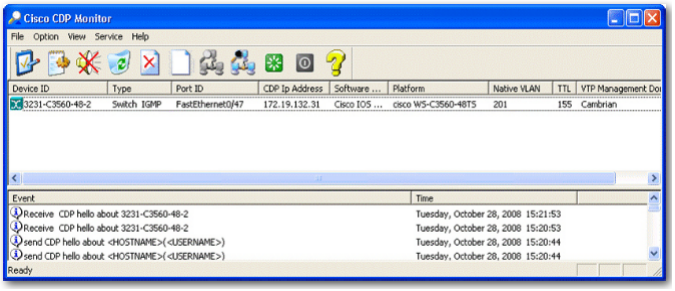
Network Time Protocol (NTP): exercício



Auditoria de Segurança

Auditoria de segurança

- Os *routers* Cisco por comodidade e compatibilidade possuem por omissão um conjunto de serviços activos que podem constituir vulnerabilidades.
  - E.g.: Cisco Discovery Protocol (CDP)



Auditoria de segurança

- Existe um conjunto de procedimentos sistemáticos que devem ser tidos em conta na colocação de um equipamento de rede em produção
  - Desactivar serviços e interfaces desnecessários
  - Torná-los transparentes a sondas e *scans* (ex: ICMP)
  - Desactivar serviços e proxy de *Address Resolution Protocol* (ARP)
  - Desactivar e restringir serviços de administração (e.g.,: SNMP)
  - Obrigar a adoptar protocolos seguros de acesso (SSH,HTTPS, …)
  - Desactivar o processamento de *broadcasts* IP dirigidos
  - …

Auditoria de segurança

- Estado dos serviços e intervenção recomendada

Feature	Default	Recommendation
Cisco Discovery Protocol (CDP)	Enabled	Should be disabled globally or on a per-interface basis if it is not required.
Configuration autoloading	Disabled	Should remain disabled when not in use by the router.
FTP server	Disabled	Should be disabled when it is not required.
TFTP server	Disabled	It should be disabled when it is not required.
Network Time Protocol (NTP) service	Disabled	It should remain disabled when it is not required.
Packet assembler/disassembler (PAD) service	Enabled	It should be explicitly disabled when not in use.
TCP and User Datagram Protocol (UDP) minor services	Enabled in versions 11.3 and later	Disable this service explicitly.
Maintenance Operation Protocol (MOP) service	Enabled on most Ethernet interfaces	It should be explicitly disabled when it is not in use.
Simple Network Management Protocol (SNMP)	Enabled	Disable this service when it is not required.
HTTP or HTTPS configuration and monitoring	Setting is Cisco device dependent.	Disable service if it is not required. If this service is required, restrict access to the router HTTP or HTTPS service using access control lists (ACLs).
Domain Name System (DNS)	Enabled	Disable when it is not required. If the DNS lookup service is

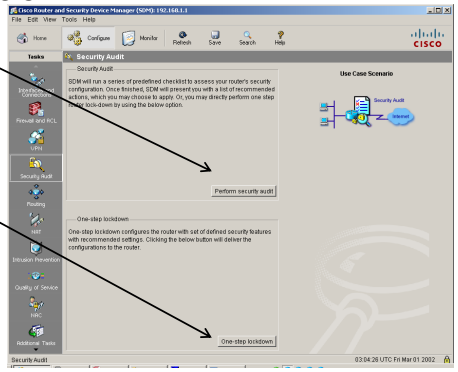
Auditoria de segurança

- Estado dos serviços e intervenção recomendada

Feature	Default	Recommendation
monitoring	device dependent.	restrict access to the router HTTP or HTTPS service using access control lists (ACLs).
Domain Name System (DNS)	Enabled	Disable when it is not required. If the DNS lookup service is required, ensure that you set the DNS server address explicitly.
Internet Control Message Protocol (ICMP) redirects	Enabled	Disable when it is not required.
IP source routing	Enabled	Disable this service when it is not required.
Finger service	Enabled	Disable this service when it is not required.
ICMP unreachable notifications	Enabled	Disable on interfaces to untrusted networks.
ICMP mask reply	Disabled	Disable on interfaces to untrusted networks.
IP identification service	Enabled	Service should be explicitly disabled.
TCP keepalives	Disabled	Should be enabled globally to manage TCP connections and prevent certain denial of service (DoS) attacks. Service is enabled in Cisco IOS Software releases before Cisco IOS Release 12.0 and is disabled in Cisco IOS Release 12.0 and later. Disable this service when it is not required.
Gratuitous ARP (GARP)	Enabled	Disable gratuitous ARPs on each router interface unless this service is needed.
Proxy ARP	Enabled	Disable this service on each interface unless the router is being used as a LAN bridge.

Auditoria de segurança

- Três ferramentas disponíveis
  - **Security Audit Wizard**
    - SDM
    - Interactivo
  - **One-Step Lockdown**
    - SDM
    - Não interactivo
  - **Cisco AutoSecure**
    - CLI
    - Configurável



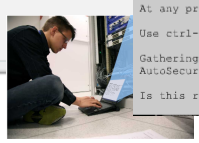
AutoSecure (IOS ≥ 12.3)

- Modo interactivo (por omissão)/não interactivo

```
router#
auto secure [no-interact | full] [forwarding | management]
[ntp | login | ssh | firewall | tcp-intercept]
```

```
R1# auto secure ?
  firewall        AutoSecure Firewall
  forwarding      Secure Forwarding Plane
  full            Interactive full session of AutoSecure
  login           AutoSecure Login
  management      Secure Management Plane
  no-interact     Non-interactive session of AutoSecure
  ntp             AutoSecure NTP
  ssh             AutoSecure SSH
  tcp-intercept   AutoSecure TCP Intercept
  <cr>

R1#
```

```
R1# auto secure
        --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security
of the router but it will not make router
absolutely secure from all security attacks ***

All the configuration done as part of AutoSecure
will be shown here. For more details of why and
how this configuration is useful, and any possible
side effects, please refer to Cisco documentation
of AutoSecure.

At any prompt you may enter '?' for help.

Use ctrl-c to abort this session at any prompt.

Gathering information about the router for
AutoSecure

Is this router connected to internet? [ no] :yes
```



AutoSecure (IOS ≥ 12.3)

- Serviços do plano de gestão (*Management plane*)
  - Desativa BOOTP, CDP, FTP, TFTP, PAD, UDP, e TCP *small servers*, MOP, ICMP (*redirects*, *mask-replies*), IP *source routing*, Finger, *password encryption*, TCP keepalives, gratuitous ARP, proxy ARP, e directed broadcast
  - Notificação com *banners*
  - Funções de segurança de *login* e *password*
  - NTP Seguro
  - Acesso seguro SSH
  - Ativa serviço de TCP *intercept* (proteção contra *TCP SYN-flooding*)
- Serviços do plano operacional (*Forwarding plane*)
  - Enables Cisco Express Forwarding (CEF)
  - Enables traffic filtering with ACLs
  - Implements Cisco IOS firewall inspection for common protocols

AutoSecure

```
router#
auto secure [no-interact | full] [forwarding | management]
[ntp | login | ssh | firewall | tcp-intercept]
```

Parameter	Description
no-interact	(Optional) The user will not be prompted for any interactive configurations. No interactive dialogue parameters will be configured, including usernames or passwords.
full	(Optional) The user will be prompted for all interactive questions. This is the default setting.
forwarding	(Optional) Only the forwarding plane will be secured.
management	(Optional) Only the management plane will be secured.
ntp	(Optional) Specifies the configuration of the Network Time Protocol (NTP) feature in the AutoSecure command-line interface (CLI).
login	(Optional) Specifies the configuration of the Login feature in the AutoSecure CLI.
ssh	(Optional) Specifies the configuration of the SSH feature in the AutoSecure CLI.
firewall	(Optional) Specifies the configuration of the Firewall feature in the AutoSecure CLI.
tcp-intercept	(Optional) Specifies the configuration of the TCP-Intercept feature in the AutoSecure CLI.

Exercício: AutoSecure

```
R3#auto secure
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]:
```

.Início da configuração do router através do *auto secure*

Exercício: AutoSecure

```
R1# auto secure
--- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of the router, but it will
not make it absolutely resistant to all security attacks ***

AutoSecure will modify the configuration of your device. All configuration
changes will be shown. For a detailed explanation of how the configuration
changes enhance security and any possible side effects, please refer to
Cisco.com for Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

<continued>
```

- **auto secure** with no keyword defaults to interactive mode.

Welcome | Identify Edge | Management Plane | Banner | Password | Secure Interfaces | Forwarding Plane

Exercício: AutoSecure

```
Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]:

Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES manual up                    up
FastEthernet0/1        192.168.11.1    YES manual up                    up
FastEthernet0/1/0      unassigned      YES unset  up                    down
FastEthernet0/1/1      unassigned      YES unset  up                    down
FastEthernet0/1/2      unassigned      YES unset  up                    down
FastEthernet0/1/3      nassigned       YES unset  up                    down
Serial0/0/0            192.168.2.101   YES manual up                    up
Serial0/0/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual up                    down
Enter the interface name that is facing the internet: Serial 0/0/0
Invalid interface name
```

- The outside interface is identified to establish the edge of the network.
- Interface names must be entered exactly as displayed in the prompting output.

Welcome | Identify Edge | Management Plane | Banner
Password | Secure Interfaces | Forwarding Plane

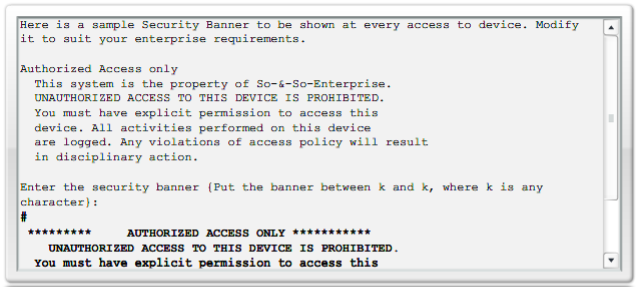
Exercício: AutoSecure

```
Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

<continued>
```

- AutoSecure automatically disables unnecessary services.

Welcome | Identify Edge | Management Plane | Banner
Password | Secure Interfaces | Forwarding Plane

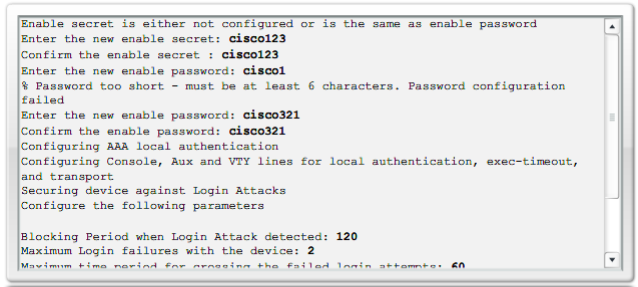
Exercício: AutoSecure



- AutoSecure prompts for a banner and provides a sample.

Welcome | Identify Edge | Management Plane | **Banner**
Password | Secure Interfaces | Forwarding Plane

Exercício: AutoSecure



- Password security and **login block-for** command parameters are gathered.
- SSH is configured.

Welcome | Identify Edge | Management Plane | Banner
Password | Secure Interfaces | Forwarding Plane

Exercício: AutoSecure

```
Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

<continued>
```

- Common security commands are applied to all interfaces.
- Some features are interface specific (e.g. FastEthernet versus Serial).

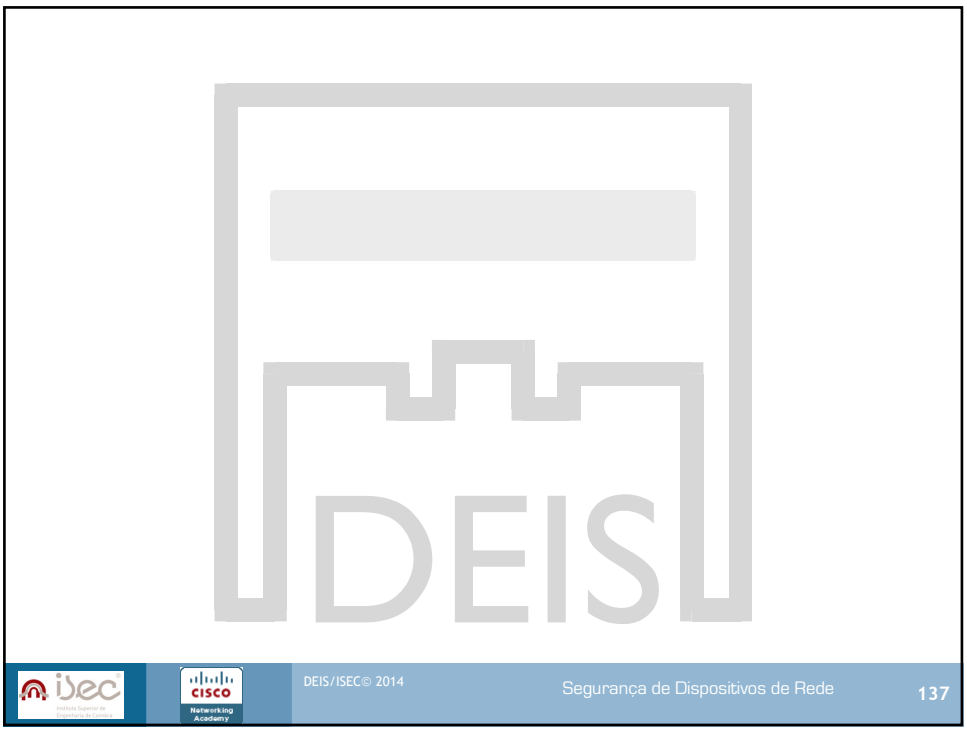
Welcome | Identify Edge | Management Plane | Banner
Password | Secure Interfaces | Forwarding Plane

Exercício: AutoSecure

```
Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected to internet

Configure CBAC Firewall feature? [yes/no]: yes
```

- Forwarding plane is secured.
- Includes enabling CEF, enabling unicast reverse path forwarding and configuring extensive firewall features for common protocols.

Welcome | Identify Edge | Management Plane | Banner
Password | Secure Interfaces | Forwarding Plane



Referências

- CCNA Security Ch. 2 – Securing Network Devices
- Cisco Guide to Harden Cisco IOS Devices, ID 13608, Cisco Systems
- Cisco IOS Password Encryption Facts, ID 107614, Cisco Systems
- Configuring Secure Shell on Routers and Switches Running Cisco IOS, ID 4145, 2009, Cisco Systems
- Cisco IOS Security Command Reference – Release 12.4, 2008, Cisco Systems
- Cisco IOS Security Configuration Guide – Release 12.4, 2008, Cisco Systems


Obrigado pela atenção. Alguma dúvida?
DEIS/ISEC© 2014
Segurança de Dispositivos de Rede
139