Autenticação, Autorização e Contabilização (AAA)

CCNA Security - Ch. 3 - Authentication, Authorization, and Accounting

Objectivos:

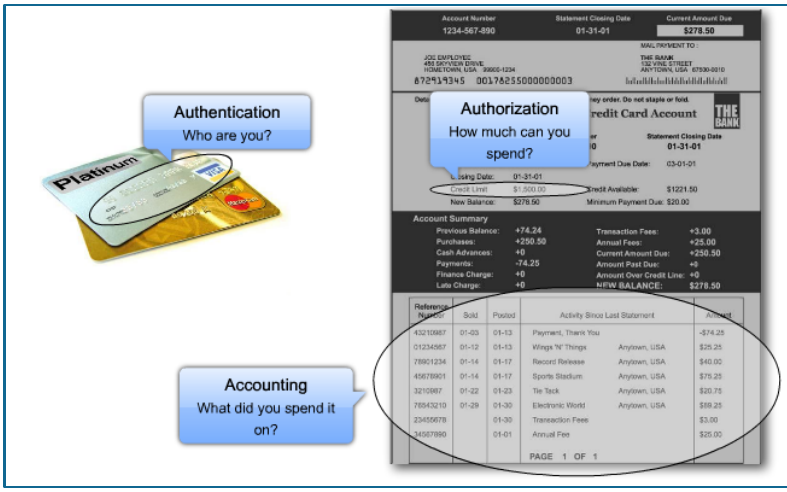
1. Explicar o modo de funcionamento da Autenticação, Autorização e Auditoria (AAA).
2. Configurar um router Cisco com autenticação AAA através da base de dados local.
3. Configurar um router Cisco com autenticação AAA centralizada.

Tópicos

1. Autenticação, Autorização e Auditoria (AAA)
2. AAA Local (ou auto-contida)
3. AAA Centralizado
4. Serviços de Autorização
5. Serviços de Auditoria
6. Cisco Secure ACS (Access Control System)

Autenticação Autorização e Auditoria (AAA)

Autenticação, Autorização e Auditoria (AAA)



Autenticação: baseada em *passwords*

- A autenticação com base apenas em *passwords* para acesso ao *user mode* e ao *privilege mode*:
  - É simples de implementar mas um método inseguro
  - Mais susceptível a ataques de força bruta
  - Impede a auditoria das actividades de gestão realizadas

```
R1(config)# line vty 0 4
R1(config-line)# password cis5cio
R1(config-line)# login
```

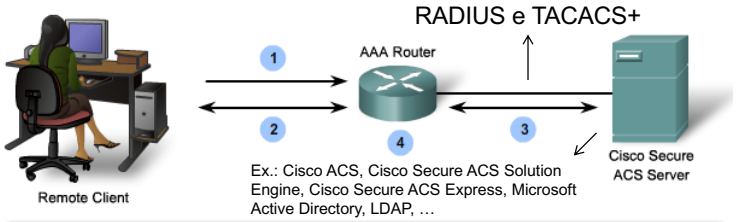
Autenticação: baseada em pares locais *user*/*password*

- Autenticação local
  - Cada equipamento possui uma base de dados dos utilizadores autorizados a efectuar alguma acção de gestão sobre o mesmo
  - Ideal para pequenas redes, impraticável em grandes
  - A gestão de passwords/ permissões tende a ser morosa
  - Em caso de perda da *password* de administrador não havendo backup só é possível recuperar o acesso através de procedimentos específicos de recuperação de *password*

```
R1(config)# username Admin secret Str0ng5rPa55w0rd
R1(config)# line vty 0 4
R1(config-line)# login local
```

Autenticação: baseada em informação centralizada

- Autenticação centralizada
  - Os equipamentos partilham um base de dados central de utilizadores, *passwords* e permissões



1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a remote AAA server.
4. The user is authorized to access the network based on information on the remote AAA Server.

Autenticação: serviços autenticados

- Serviço de acesso remoto para gestão do equipamento
  - Denominado *Character Mode*

Table 4-2 Line Types Generating Character-Mode Traffic Secured by AAA

Line Type	Description
Aux	Auxiliary EIA/TIA-232 DTE port on Cisco routers and Ethernet switches used for modem support and asynchronous access
Console	Console EIA/TIA-232 DCE port on Cisco routers and Ethernet switches used for asynchronous access to device configuration modes
tty	Standard EIA/TIA-232 DTE asynchronous line on a network access server
vty	Virtual terminal line and interface terminating incoming character streams that do not have a physical connection to the access server or router

Access Type	Modes	Router Ports	Common AAA Commands
Remote administrative access	Character Mode provides user and privelege EXEC access	console, vty, aux, and tty	**login**, **exec**, and **enable** commands
Remote network access	Packet Mode provides access to network resources	Dial-up and VPN access	**ppp** and **network** commands

Autenticação: serviços autenticados

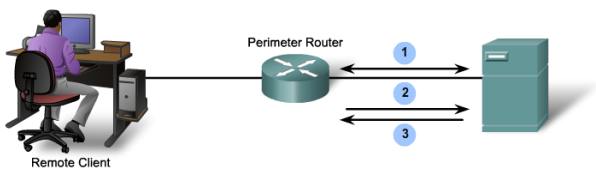
- Serviço de acesso remoto a redes locais
  - Denominado *Packet Mode*

Table 4-3 Protocols Generating Packet-Mode Traffic Secured by AAA

Packet-Mode Type	Description
PPP	PPP on serial or ISDN interfaces
arap	AppleTalk Remote Access Protocol (ARAP) on serial interfaces
NASI	NetWare Access Server Interface (NASI) clients connecting through the access server on serial interfaces

Autorização

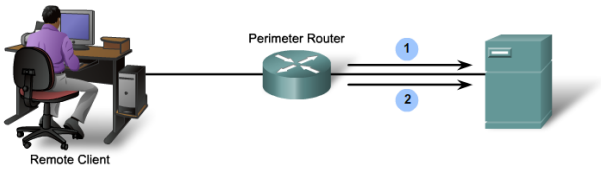
- Decorre imediatamente após a autenticação local/centralizada
- Tipicamente implementado sobre AAA centralizado
- Visa identificar recursos/acções a que o utilizador está restrito
- Conjunto de atributos que descrevem o acesso do utilizador



1. When a user has been authenticated, a session is established with an AAA server.
2. The router requests authorization for the requested service from the AAA server.
3. The AAA server returns a PASS/FAIL for authorization.

Auditoria/Contabilização

- Registo detalhado das actividades efectuados pelos utilizadores autenticados
- Implementado maioritariamente sobre AAA centralizado
- Permite a análise, controlo, análise estatística e afectação de custos (*billing*) na utilização de recursos



1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
2. When the user finishes, a stop message is recorded and the accounting process ends.

Auditoria/Contabilização

Network accounting	Network accounting captures information for all Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or Apple Remote Access Protocol (ARAP) sessions, including packet and byte counts.
Connection accounting	Connection accounting captures information about all outbound connections made from the AAA client, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.
EXEC accounting	EXEC accounting captures information about user EXEC terminal sessions (user shells) on the network access server, including username, date, start and stop times, the access server IP address, and (for dial-in users) the telephone number the call originated from.
System accounting	System accounting captures information about all system-level events (for example, when the system reboots or when accounting is turned on or off).
Command accounting	Command accounting captures information about the EXEC shell commands for a specified privilege level that are being executed on a network access server. Each command accounting record includes a list of the commands executed for that privilege level, as well as the date and time each command was executed, and the user who executed it.
Resource accounting	The Cisco implementation of AAA accounting captures "start" and "stop" record support for calls that have passed user authentication. The additional feature of generating "stop" records for calls that fail to authenticate as part of user authentication is also supported. Such records are necessary for users employing accounting records to manage and monitor their networks.

AAA
Local
(ou auto-contida)

AAA Local (≡ AAA auto-contida)

- Comportamento idêntico ao comando `login local` no VTY
  - Possibilita porém definir 4 métodos alternativos de autenticação
- Configuração:
  1. Criar utilizadores
  2. Activar AAA
  3. Configurar AAA
  4. Validar configuração

```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case
R1(config)# aaa local authentication attempts max-fail 10
```

1. Criar utilizadores

```
username name secret password
```

2. Activar AAA

```
aaa new-model
```

AAA Local

3. Configurar o AAA
   A. Criar uma lista de métodos de autenticação disponíveis

```
aaa authentication login {default | list-name} method1…[method4]
```

Command	Description
default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method1...[method4]	Identifies the list of methods that the AAA authentication process will query in the given sequence. At least one method must be specified. A maximum of four methods may be specified.

- Podem ser definidas sequências de, no máximo, **quatro** métodos
- Apenas é usado o próximo método da lista quando o actual se encontra indisponível. Quando o método actual nega o acesso ao utilizador o próximo método mesmo que presente não é usado.

AAA Local

Keywords	Descrição
enable	Usa a password de *enable* para autenticação.
krb5	Usa o Kerberos 5 para autenticação.
krb5-telnet	Usa o protocolo de autenticação “Kerberos 5 telnet” quando é feito um acesso telnet ao router.
line	Usa a password da *line* para autenticação.
local	Usa a base de dados local de utilizadores para autenticação.
local-case	Semelhante ao anterior mas sensível a maiúsculas no username.
none	Não usa qualquer autenticação.
cache *group-name*	Uses a cache server group for authentication.
group radius	Usa todos os servidores de RADIUS da lista mencionada.
group tacacs+	Usa todos os servidores de TACACS da lista mencionada.
group *group-name*	Usa um subconjunto de servidores RADIUS ou TACACS+ para autenticação conforme especificado pelos comandos **`aaa group server radius`** ou **`aaa group server tacacs+`**.

AAA Local

3. Configurar o AAA (cont.)
   B. Aplicar a lista às interfaces/linhas de gestão pretendidas

`login authentication` *`list-name`*

- Notas:
  - A lista *default* é usada quando este passo é omitido
  - Se a lista *default* não for explicitamente definida o seu valor por omissão é:

`aaa authentication login default local`

Atenção: Neste caso na consola não é solicitada autenticação

```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case enable
R1(config)# aaa authentication login TELNET-LOGIN local-case
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET-LOGIN
```


AAA Local

3. Configurar o AAA (cont.)
   C. Proteger os modos de autenticação de ataques de força bruta

`aaa local authentication attempts max-fail` *`max`*

- Nota:
  - Ao contrário do comando `login delay`, neste caso a conta fica bloqueada.
- Identificar contas bloqueadas

`show aaa local user lockout`

- Desbloquear contas

`clear aaa local user lockout` {**`username`** *`username`* | ***`all`***}

AAA Local

4. Validar a configuração
   - Acesso aos registos de uma sessão

show aaa user *{all | unique id}*

   - Apenas sessões AAA
   - Sessões AAA:

show aaa sessions

   - Mostra ID das sessões
   - Debug AAA:

debug aaa *option*

```
R1# show aaa sessions
Total sessions since last reload: 4
Session Id: 1
   Unique Id: 175
   User Name: ADMIN
   IP Address: 192.168.1.10
   Idle Time: 0
   CT Call Handle: 0
```

```
R1# debug aaa ?
  accounting
  administrative
  api                  AAA api events
  attr                 AAA Attr Manager
  authentication       Authentication
  authorization        Authorization
  cache                Cache activities
  coa                  AAA CoA processing
  db                   AAA DB Manager
  dead-criteria        AAA Dead-Criteria Info
  id                   AAA Unique Id
  ipc                  AAA IPC
  mlist-ref-count      Method list reference counts
  mlist-state          Information about AAA method list state change and
                       notification
  per-user             Per-user attributes
  pod                  AAA POD processing
  protocol             AAA protocol processing
  server-ref-count     Server handle reference counts
  sg-ref-count         Server group handle reference counts
  sg-server-selection  Server Group Server Selection
  subsys               AAA Subsystem
  testing              Info. about AAA generated test packets
```

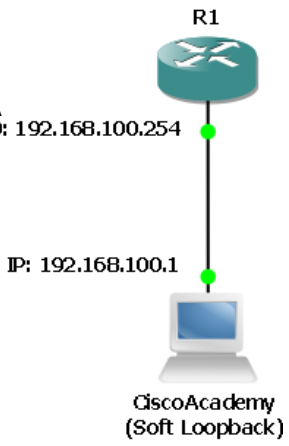

AAA Local

4. Validar a configuração (cont.)

```
R1# debug aaa authentication
113123: Feb 4 10:11:19.305 CST: AAA/MEMORY: create_user (0x619C4940) user=''
ruser='' port='tty1' rem_addr='async/81560' authen_type=ASCII service=LOGIN priv=1
113124: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): port='tty1' list=''
action=LOGIN service=LOGIN
113125: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): using "default" list
113126: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): Method=LOCAL
113127: Feb 4 10:11:19.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113128: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): continue_login
(user='(undef)')
113129: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113130: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113131: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETPASS
113132: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): continue_login
(user='diallocal')
113133: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = GETPASS
113134: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113135: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = PASS
```

AAA Local: Exercício

- Topologia
  1. Localizar o projeto "AAA"
     - Desktop\Cisco\GNS3\Projects\AAA
  2. Abrir o projecto (duplo clique sobre o ficheiro .net)
  3. Configurar os parâmetros IPv4 sobre a interface Soft(Loopback) da VM WinXP
  4. Iniciar R1 e abrir consola
  5. Testar conectividade entre WinXP e R1



AAA Local: Exercício

```
R1#configure terminal
R1(config)#username admin privilege 15 secret adminPass
R1(config)#aaa new-model
R1(config)#aaa authentication login default local none
R1(config)#exit
R1#exit
```

.Criar utilizador local
.Activar serviço AAA
.Configurar método *default* com acesso ao AAA local

.Teste do AAA Local

```
User Access Verification

Username: admin
Password:

R1>
```

Experiência complementar interessante

```
R1(config)#no username admin
```

. Testar agora um acesso por Telnet
⇒ É solicitado apenas o *username* e aceite qualquer valor
Porquê? Porque a base de dados local de *users* deixa de existir.
. Inserir novamente o *user* "admin" na base de dados local de autenticação para prosseguir o exercício

```
R1#configure terminal
R1(config)#aaa authentication login TELNET local
R1(config)#line vty 0 4
R1(config-line)#login authentication TELNET
R1(config-line)#exit
R1(config)#exit
```

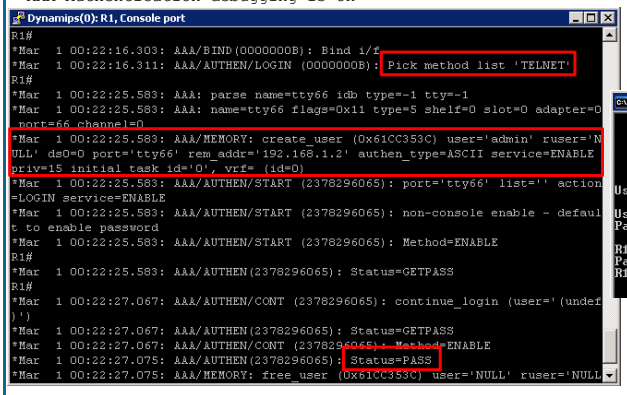
.Configurar autenticação AAA para acesso telnet
.Configurar autenticação AAA no acesso telnet

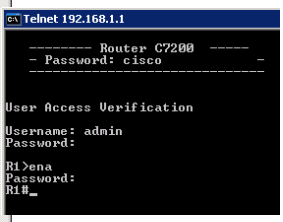
AAA Local: Exercício

```
R1#debug aaa authentication
AAA Authentication debugging is on
```

.Activar *debug* da autenticação AAA

.Exemplo de acesso telnet e respectivo *log* de *debug*





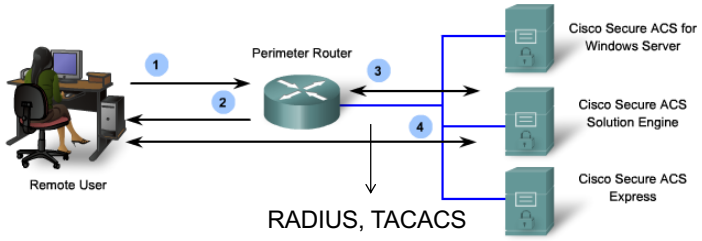
Proposta:
Testar e analisar acesso falhado

```
R1#show aaa user all                R1#show aaa sessions
```


AAA Centralizado (ou *server-based*)

AAA Centralizado

- Podem ser empregues vários servidores (disponibilidade ↑)
- A gestão de utilizadores passa a ser centralizada



Server-Based Authentication

1. The user establishes a connection with the router.
2. The router prompts the user for a username and password.
3. The router passes the username and password to the Cisco Secure ACS (server or engine).
4. The Cisco Secure ACS authenticates the user. The user is authorized to access the router (administrative access), or the network based on information found in the Cisco Secure ACS database.

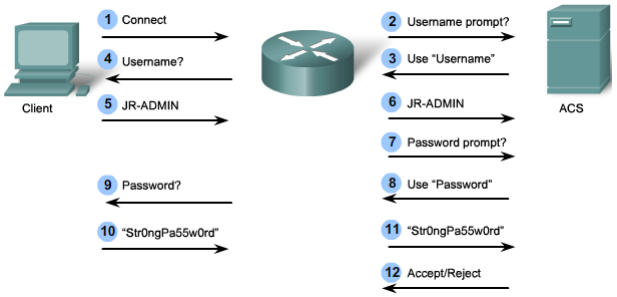
AAA Centralizado: Protocolo RADIUS

- *Remote Dial-in User Services* (RADIUS) IETF RFCs 2865,2866,2867,2868
  - Desenvolvido originalmente pela *Livingston Enterprises*
- Suporta a utilização de *proxies* RADIUS (escalabilidade ↑)
  - Nota: O Eduroam opera numa hierarquia de servidores RADIUS
- Combina autenticação e autorização num só processo
- Suporta tecnologias de acesso remoto como 802.1x e SIP
- Implementa funcionalidades de registo detalhadas
- Opera sobre UDP
- Protege apenas a *password* (MD5)
- A ser substituído pelo DIAMETER (TCP /SCTP)

UDP 1645 ou 1812: autenticação
UDP 1646 ou 1813: auditoria

AAA Centralizado: Protocolo TACACS+

- *Terminal Access Control Access Control Server Plus* (TACACS+)
- Versão melhorada do protocolo TACACS original (incompat.)
- Desenvolvido pela Cisco e actualmente submetido ao IETF
- Os serviços AAA são separados (flexibilidade ↑)



AAA Centralizado: RADIUS vs. TACACS+

- RADIUS
  - Escalável e aberto
  - Encripta apenas password
  - Usa UDP
  - Suporta tecnologias de acesso remoto como IEEE 802.1X e SIP
- TACACS+
  - Incompatível com TACACS
  - Incompatível com XTACACS
  - Separa autenticação/autorização
  - Usa TCP (porto 49)
  - Encripta toda a comunicação

	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation	Combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+
Standard	Mostly Cisco supported	Open/RFC standard
Transport Protocol	TCP	UDP
CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client
Protocol Support	Multiprotocol support	No ARA, no NetBEUI
Confidentiality	Entire packet encrypted	Password encrypted
Customization	Provides authorization of router commands on a per-user or per-group basis	Has no option to authorize router commands on a per-user or per-group basis
Accounting	Limited	Extensive

AAA Centralizado: Configuração

- Passos:
  - Activar o(s) servidor(es) RADIUS/TACACS+
  1. Activar o AAA nos clientes (*routers*, *switches*, …)
  2. Especificar o endereço e chave do servidor RADIUS/TACACS+
  3. Configurar o método AAA de autenticação
  4. Repetir de 2 a 4 para cada servidor secundário

1. Activar o AAA

```
aaa new-model
```


AAA Centralizado: Configuração

2. Especificar o endereço e chave do servidor RADIUS/TACACS+

radius-server host {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**backoff exponential** {**backoff-retry** *number-of-retransmits* | **max-delay** *minutes*}] [**pac** [**key** *encryption-key*] | **key** *encryption-key*]

no radius-server host {*hostname* | *ip-address*}

```
radius-server host {hostname | ip-address}
                  [key string]
```

- Nota: podem ser adicionados vários servidores (disponibilidade↑)

3. Configurar o método AAA de autenticação
   - Exemplo:

```
aaa authentication login default group radius none
```

AAA Centralizado: Configuração

3. Configurar o método AAA de autenticação (cont.)

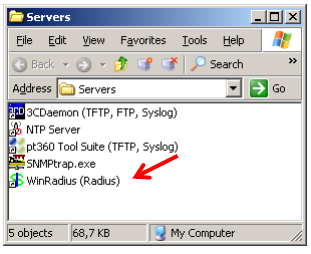
```
R1(config)# aaa authentication type { default | list-name } method1 … [method4]
```

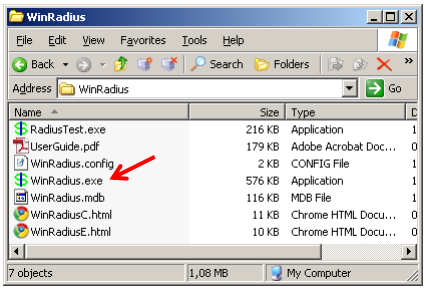
```
R1(config)# aaa authentication login default ?
  enable          Use enable password for authentication.
  group           Use Server-group
  krb5            Use Kerberos 5 authentication.
  krb5-telnet     Allow logins only if already authenticated via Kerberos V
                  Telnet.
  line            Use line password for authentication.
  local           Use local username authentication.
  local-case      Use case-sensitive local username authentication.
  none            NO authentication.
  passwd-expiry   enable the login list to provide password aging support

R1(config)# aaa authentication login default group ?
  WORD      Server-group name
  radius    Use list of all Radius hosts.
  tacacs+   Use list of all Tacacs+ hosts.
```


AAA Centralizado: Exercício

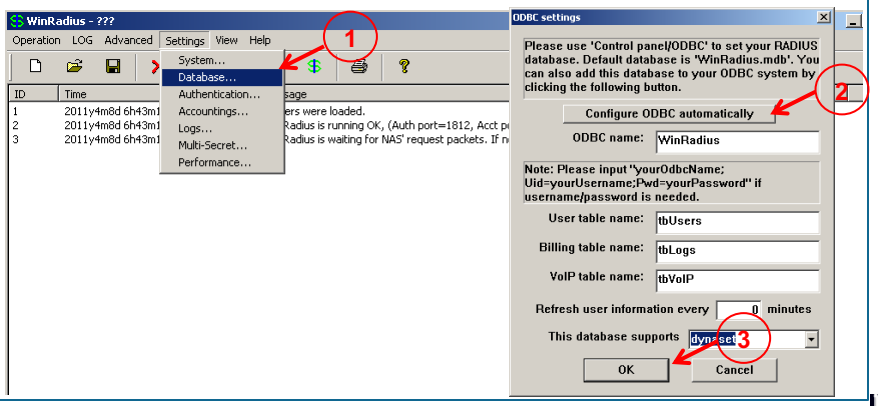
- Activar servidor RADIUS
  - WinXP: Desktop > Servers > WinRadius > WinRadius.exe





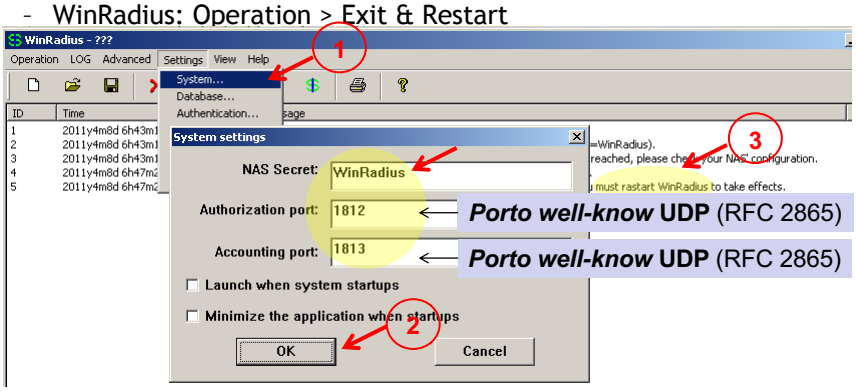
AAA Centralizado: Exercício

- Configurar servidor RADIUS
  - WinRadius: Settings > Database > Configure ODBC Automatically



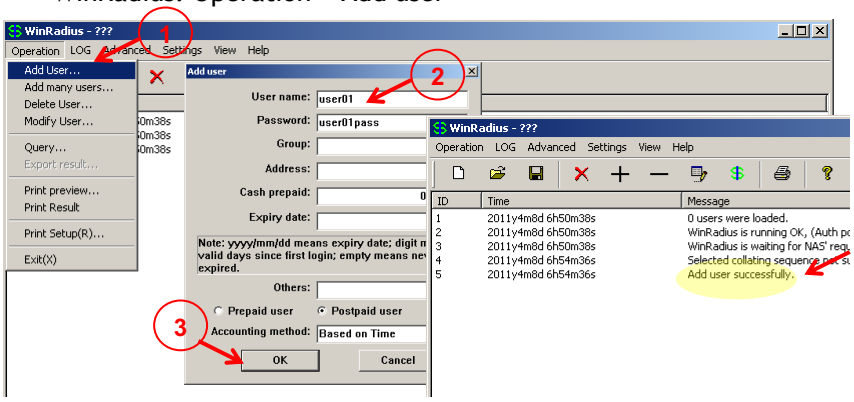
AAA Centralizado: Exercício

- Consultar a configuração por omissão do servidor RADIUS
  - WinRadius: Settings > System
  - WinRadius: Operation > Exit & Restart



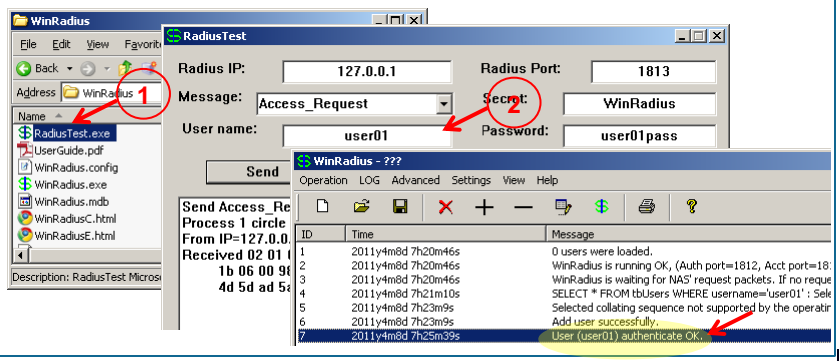
AAA Centralizado: Exercício

- Registar novo utilizador (user01 / user01pass)
  - WinRadius: Operation > Add user

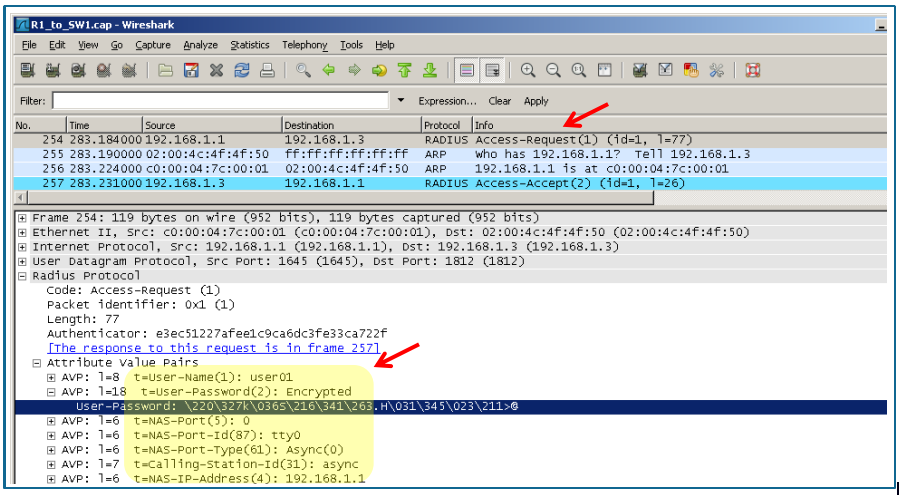


AAA Centralizado: Exercício

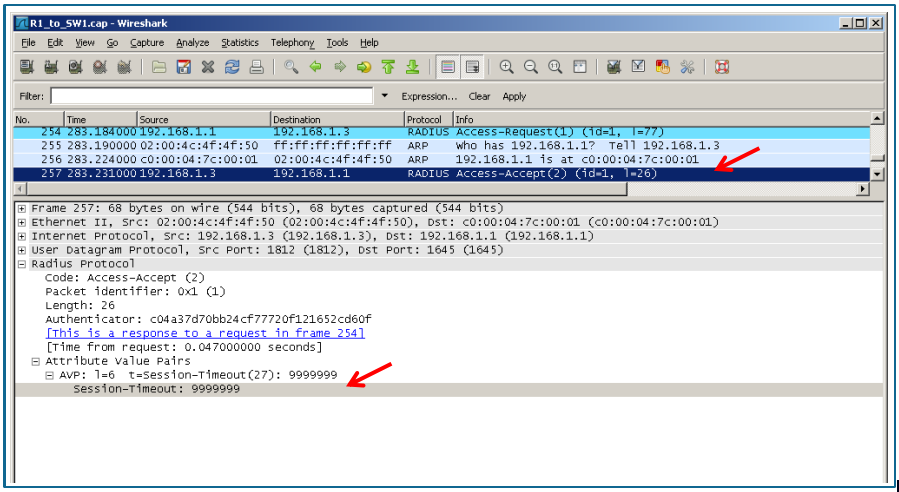
- Verificar o novo registo
  - WinXP: Desktop > Servers > WinRadius > RadiusTest.exe
  - RadiusTest: username/password > Send



AAA Centralizado: Exercício



AAA Centralizado: Exercício



AAA Centralizado: Exercício

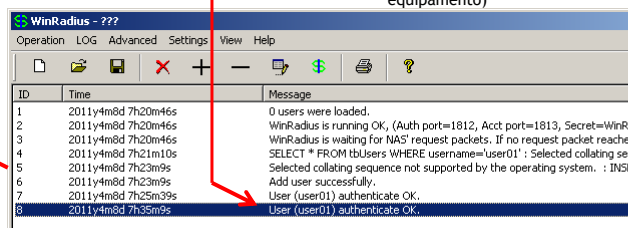
```
R1#configure terminal
R1(config)#aaa new-model
R1(config)#radius-server host 192.168.100.1 auth-port 1812 acct-port 1813 key WinRadius
R1(config)#aaa authentication login default group radius none
R1(config)#aaa authentication login TELNET group radius none
R1(config)#exit
R1#exit
User Access Verification
Username: user01
Password:
R1>enable
Password:
R1#who
    Line       User
Location
*  0 con 0     user01

  Interface    User
Address
```

.Activar serviço AAA

.Definir características específicas do servidor RADIUS

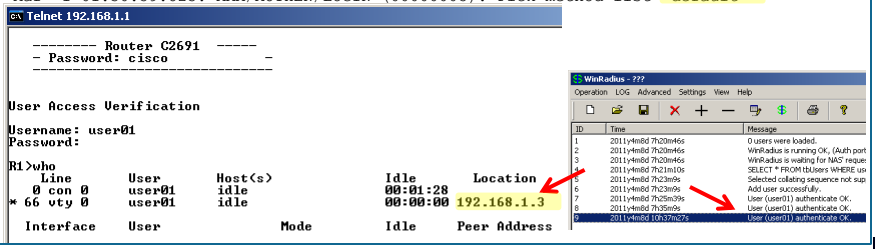
.Configurar método *default* indicando como primeira prioridade acesso ao serviço RADIUS (nota: a opção *none* deverá ser usada exclusivamente durante os ensaios iniciais para evitar perder acesso ao equipamento)



AAA Centralizado: Exercício

- Acesso remoto por *telnet*
  - IOS: Activar `debug` da autenticação AAA
  - WinXp: Cmd > `telnet IP_Router`

```
R1#debug aaa authentication
AAA Authentication debugging is on
R1#
*Mar  1 01:30:59.811: AAA/BIND(00000005): Bind i/f
*Mar  1 01:30:59.823: AAA/AUTHEN/LOGIN (00000005): Pick method list 'default'
```



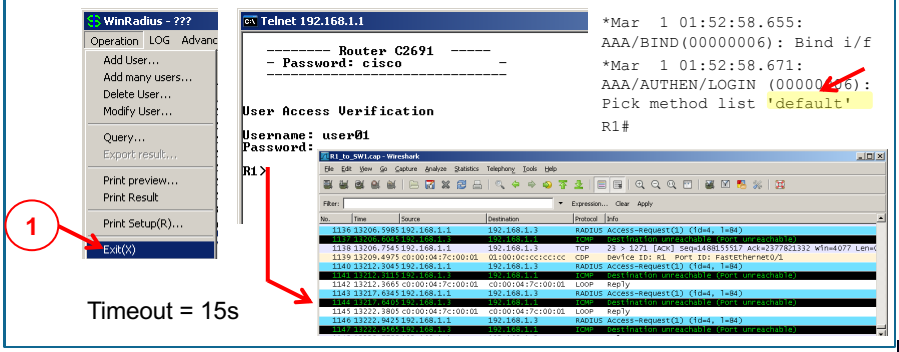
AAA Centralizado: Exercício

- Transição para o nível 15 de privilégios na sessão remota

```
*Mar  1 01:34:56.867: AAA: parse name=tty66 idb type=-1 tty=-1
*Mar  1 01:34:56.871: AAA: name=tty66 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=66
channel=0
*Mar  1 01:34:56.875: AAA/MEMORY: create_user (0x642FE104) user='user01' ruser='NULL'
ds0=0 port='tty66' rem_addr='192.168.100.1' authen_type=ASCII service=ENABLE priv=15
initial_task_id='0', vrf= (id=0)
*Mar  1 01:34:56.879: AAA/AUTHEN/START (3291295330): port='tty66' list='' action=LOGIN
service=ENABLE
*Mar  1 01:34:56.879: AAA/AUTHEN/START (3291295330): non-console enable - default to
enable password
*Mar  1 01:34:56.883: AAA/AUTHEN/START (3291295330): Method=ENABLE
R1#
*Mar  1 01:34:56.883: AAA/AUTHEN(3291295330): Status=GETPASS
R1#
*Mar  1 01:34:58.691: AAA/AUTHEN/CONT (3291295330): continue_login (user='(undef)')
*Mar  1 01:34:58.691: AAA/AUTHEN(3291295330): Status=GETPASS
*Mar  1 01:34:58.695: AAA/AUTHEN/CONT (3291295330): Method=ENABLE
*Mar  1 01:34:58.695: AAA/AUTHEN(3291295330): Status=PASS
*Mar  1 01:34:58.695: AAA/MEMORY: free_user (0x642FE104) user='NULL' ruser='NULL'
port='tty66' rem_addr='192.168.100.1' authen_type=ASCII service=ENABLE priv=15 vrf= (id=0)
```


AAA Centralizado: Exercício

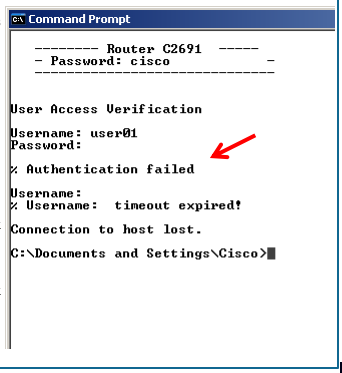
- Cenário: Servidor RADIUS indisponível
  - WinRadius: Operation > Exit
  - WinXp: Cmd > `telnet IP_Router`



AAA Centralizado: Exercício

- Especificar uma lista de serviços de autenticação específica para os acessos por `telnet`
  - Nota: Serviços RADIUS mantêm-se indisponíveis.

```
R1(config)#aaa authentication login TELNET group radius
R1(config)#line vty 0 4
R1(config-line)#login authentication TELNET
R1(config-line)#^Z
R1#
*Mar  1 02:14:28.331: %SYS-5-CONFIG_I: Configured from
console by user01 on console
R1#
*Mar  1 02:15:16.743: AAA/BIND(00000007): Bind i/f
*Mar  1 02:15:16.755: AAA/AUTHEN/LOGIN (00000007): Pick
method list 'TELNET'
R1#
*Mar  1 02:15:48.935: AAA/AUTHEN/LOGIN (00000007): Pick
method list 'TELNET'
R1#
```



AAA Centralizado: Exercício

- Activar serviço RADIUS e testar acesso remoto por `telnet`
  - Adicionar novamente o utilizador *user01/user01pass*
  - Activar o `debug` sobre a comunicação com o serviço RADIUS

```
R1#debug radius
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
Radius elog debugging debugging is off
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging debugging is off

*Mar  1 03:04:26.663: AAA/BIND(00000009): Bind i/f
*Mar  1 03:04:26.663: AAA/AUTHEN/LOGIN (00000009): Pick method list 'TELNET'
*Mar  1 03:04:26.671: RADIUS/ENCODE(00000009): ask "Username: "
*Mar  1 03:04:26.671: RADIUS/ENCODE(00000009): send packet; GET_USER
```

AAA Centralizado: Exercício

```
*Mar  1 03:04:26.663: AAA/BIND(00000009): Bind i/f
*Mar  1 03:04:26.663: AAA/AUTHEN/LOGIN (00000009): Pick method list 'TELNET'
*Mar  1 03:04:26.671: RADIUS/ENCODE(00000009): ask "Username: "
*Mar  1 03:04:26.671: RADIUS/ENCODE(00000009): send packet; GET_USER
R1#
*Mar  1 03:04:28.755: RADIUS/ENCODE(00000009): ask "Password: "
*Mar  1 03:04:28.759: RADIUS/ENCODE(00000009): send packet; GET_PASSWORD
R1#
*Mar  1 03:04:33.119: RADIUS/ENCODE(00000009):Orig. component type = EXEC
*Mar  1 03:04:33.123: RADIUS:  AAA Unsupported Attr: interface         [158] 5
*Mar  1 03:04:33.123: RADIUS:   74 74 79                                    [tty]
*Mar  1 03:04:33.127: RADIUS/ENCODE(00000009): dropping service type, "radius-server
attribute 6 on-for-login-auth" is off
*Mar  1 03:04:33.131: RADIUS(00000009): Config NAS IP: 0.0.0.0
*Mar  1 03:04:33.131: RADIUS/ENCODE(00000009): acct_session_id: 7
*Mar  1 03:04:33.139: RADIUS(00000009): sending
*Mar  1 03:04:33.143: RADIUS/ENCODE: Best Local IP-Address 192.168.100.254 for Radius-
Server 192.168.1.3
*Mar  1 03:04:33.151: RADIUS(00000009): Send Access-Request to 192.168.100.1:1812 id
1645/7, len 84
```


AAA Centralizado: Exercício

```
*Mar  1 03:04:33.155: RADIUS:  authenticator D2 F0 AB 12 26 D6 4E FD - F9 D9 F9 F4 8A 1C
C6 26
*Mar  1 03:04:33.155: RADIUS:  User-Name           [1]   8   "user01"
*Mar  1 03:04:33.159: RADIUS:  User-Password       [2]   18  *
*Mar  1 03:04:3
R1#3.159: RADIUS:  NAS-Port            [5]   6   66
*Mar  1 03:04:33.159: RADIUS:  NAS-Port-Id         [87]  7   "tty66"
*Mar  1 03:04:33.159: RADIUS:  NAS-Port-Type       [61]  6   Virtual
[5]
*Mar  1 03:04:33.159: RADIUS:  Calling-Station-Id  [31]  13  "192.168.100.1"
*Mar  1 03:04:33.159: RADIUS:  NAS-IP-Address      [4]   6   192.168.100.254
*Mar  1 03:04:33.215: RADIUS: Received from id 1645/7 192.168.100.1:1812, Access-Accept,
len 26
*Mar  1 03:04:33.215: RADIUS:  authenticator 7F 41 7A CE 98 8C 2F 26 - 58 D7 46 BA 64 02
C9 60
*Mar  1 03:04:33.219: RADIUS:  Session-Timeout     [27]  6   9999999
*Mar  1 03:04:33.227: RADIUS(00000009): Received from id 1645/7
```

AAA Centralizado: Exercício

- Com um servidor RADIUS que suporte o par AV-Pair é possível estabelecer um nível de privilégio *default* para os utilizadores durante a autenticação

Note: The server must support Cisco av-pairs.

- seven Password = **passwdxyz**
- Service-Type = **Shell-User**
- cisco-avpair =**shell:priv-lvl=7**

FreeRADIUS
The world's most popular RADIUS Server

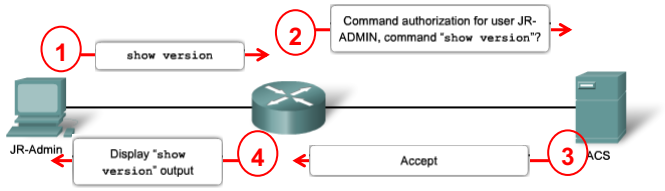
http://freeradius.org/

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008009465c.shtml

Serviço de Autorização

AAA Centralizado: Serviço de Autorização

- O RADIUS não separa os processos de autenticação de autorização e por conseguinte não permite a granularidade que o TACACS+ oferece
  - Por omissão no TACACS+ o IOS estabelece uma sessão TCP com o ACS por cada comando executado o que pode tornar as sessões lentas.



AAA Centralizado: Serviço de Autorização

- Configuração

Serviços de rede: (PPP, SLIP, ARAP

Iniciar uma *shell* em *EXEC mode*

Comandos do modo EXEC (só TACACS+)

```
aaa authorization {network | exec | commands level}
{default | list-name} method1...[method4]
```

```
R1(config)# aaa authorization exec default ?
  group              Use server-group.
  if-authenticated   Succeed if user has authenticated.
  krb5-instance      Use Kerberos instance privilege maps.
  local              Use local database.
  none               No authorization (always succeeds).

R1(config)# aaa authorization exec default group ?
  WORD     Server-group name
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.
```

AAA Centralizado: Serviço de Autorização

- Configuração: tipos de autorização disponíveis

```
R1(config)#aaa authorization ?
  auth-proxy       For Authentication Proxy Services
  cache            For AAA cache configuration
  commands         For exec (shell) commands.
  config-commands  For configuration mode commands.
  configuration    For downloading configurations from AAA server
  console          For enabling console authorization
  exec             For starting an exec (shell).
  multicast        For downloading Multicast configurations from an AAA server
  network          For network services. (PPP, SLIP, ARAP)
  reverse-access   For reverse access connections
  template         Enable template authorization

R1(config)#aaa authorization commands ?
  <0-15>  Enable level

R1(config)#aaa authorization commands 15 default group ?
  WORD     Server-group name
  tacacs+  Use list of all Tacacs+ hosts.
```

Para uma granularidade ao nível do comando a única opção é o TACACS+

AAA Centralizado: Serviço de Autorização

- ATENÇÃO
  - Por omissão o IOS permite que todos os utilizadores possuam acesso completo ao sistema … no entanto, quando o serviço de autorização AAA se torna activo, por omissão os utilizadores passam a não possuir qualquer acesso!
  - Antes de activar a autorização AAA é boa prática criar um utilizador com poderes totais

```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default group tacacs+
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
```

AAA Centralizado: Serviço de Autorização

- Como permitir que um utilizador registado localmente fique de imediato no seu nível de privilégios após aceder pelo VTY?
  1. Criar o utilizador
     ```
     username admin privilege 15 secret adminpass
     ```
  2. Activar o AAA
     ```
     aaa new-model
     ```
  3. Activar a autenticação com base local
     ```
     aaa authentication login default local
     ```
  4. Autorizar a criação de um processo EXEC
     ```
     aaa authorization exec default local
     ```
  - Nota: experimentar depois de entrar por Telnet o resultado do comando: `show privilege`

AAA Centralizado: Serviço de Autorização

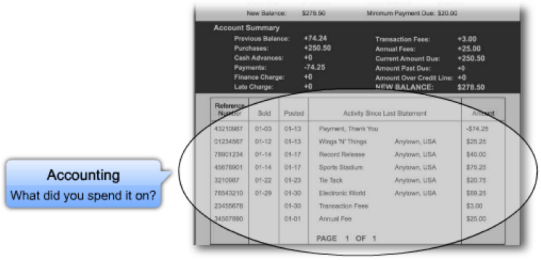
- Para entrar noutros serviços com autenticação AAA é preciso indicá-lo especificamente. Por exemplo para o acesso por SDM ser possível, é necessário:

```
1. username admin privilege 15 secret adminpass
2. aaa new-model
3. aaa authentication login default local
4. aaa authorization exec default local
5. ip http secure-server
6. ip http authentication aaa
```

Serviço de Auditoria (*Accounting*)

AAA Centralizado: Serviço de Auditoria

- Registo de actividades para controlo, cobrança (*billing*) ou auditoria
  - Permite produzir relatórios detalhados dos dados obtidos
  - Permite monitorizar os acessos e acções (ao nível da segurança)
  - Manter um histórico de alterações da rede/equipamentos



AAA Centralizado: Serviço de Auditoria

aaa accounting {auth-proxy | system | network | exec | connection | commands *level* | dot1x}
{default | *list-name* | guarantee-first} [vrf *vrf-name*] {start-stop | stop-only | none}
[broadcast] {radius | group *group-name*}

```
R1(config)# aaa accounting {network | exec | connection} { default |
list-name } {start-stop | stop-only | none} [broacast] method1…[method4]
```

```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default group tacacs+
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
R1(config)# aaa accounting exec default start-stop group tacacs+
R1(config)# aaa accounting network default start-stop group tacacs+
```


AAA Centralizado: Serviço de Auditoria

auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
network	Runs accounting for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Protocols (NCPs), and AppleTalk Remote Access Protocol (ARAP).
exec	Runs accounting for the EXEC shell session.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler and disassembler (PAD), and rlogin.
commands *level*	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15. Só TACACS+
dot1x	Provides information about all IEEE 802.1x-related user events.
default	Uses the listed accounting methods that follow this keyword as the default list of methods for accounting services.

AAA Centralizado: Serviço de Auditoria

list-name	Character string used to name the list of at least one of the following accounting methods: • **group radius**—Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command. • **group tacacs+**—Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command. • **group** *group-name*—Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name* argument.
guarantee-first	Guarantees system accounting as the first record.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration. • VRF is used *only* with system accounting.
start-stop	Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.
stop-only	Sends a "stop" accounting record for all cases including authentication failures regardless of whether the **aaa accounting send stop-record authentication failure** command is configured.
none	Disables accounting services on this line or interface.

AAA Centralizado: Serviço de Auditoria

broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
radius	Runs the accounting service for RADIUS.

AAA Centralizado: Serviço de Auditoria

group *group-name*	Specifies the accounting method list. Enter at least one of the following keywords: • **auth-proxy**—Creates a method list to provide accounting information about all authenticated hosts that use the authentication proxy service. • **commands**—Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level. • **connection**—Creates a method list to provide accounting information about all outbound connections made from the network access server. • **exec**—Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times. • **network**—Creates a method list to provide accounting information for SLIP, PPP, NCPs, and ARAP sessions. • **resource**—Creates a method list to provide accounting records for calls that have passed user authentication or calls that failed to be authenticated. • **tunnel**—Creates a method list to provide accounting records (Tunnel-Start, Tunnel-Stop, and Tunnel-Reject) for virtual private dialup network (VPDN) tunnel status changes. • **tunnel-link**—Creates a method list to provide accounting records (Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject) for VPDN tunnel-link status changes.

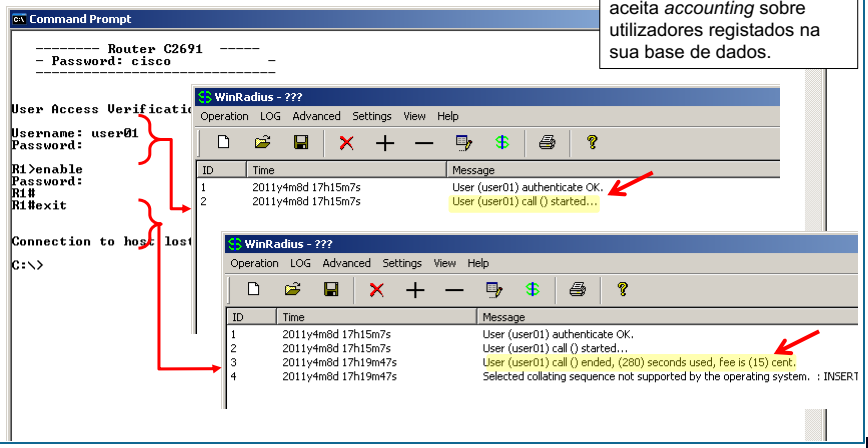
AAA Centralizado: Serviço de Auditoria

delay-start	Delays PPP network start records until peer IP address is known.
send	Sends records to the accounting server.
stop-record	Generates stop records for a specified event.
authentication	Generates stop records for authentication.
failure	Generates stop records for authentication failures.
success	Generates stop records for authenticated users.
remote-server	Specifies that the users are successfully authenticated through access-accept, by a remote AAA server.

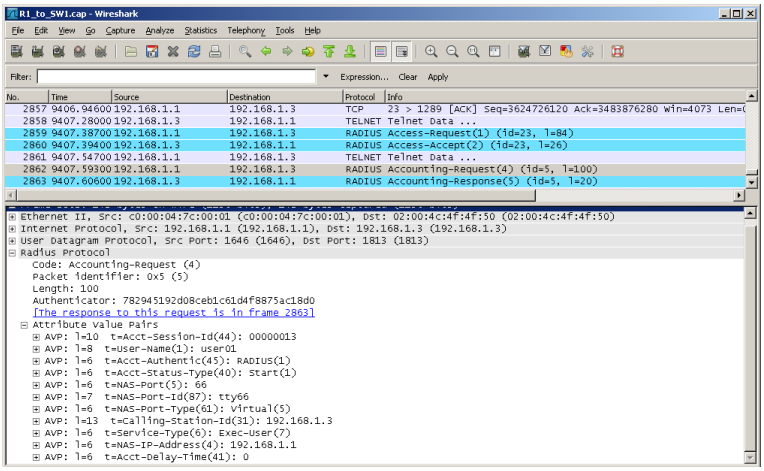
AAA Centralizado: Exercício

```
R1(config)#aaa accounting exec default start-stop group radius
```

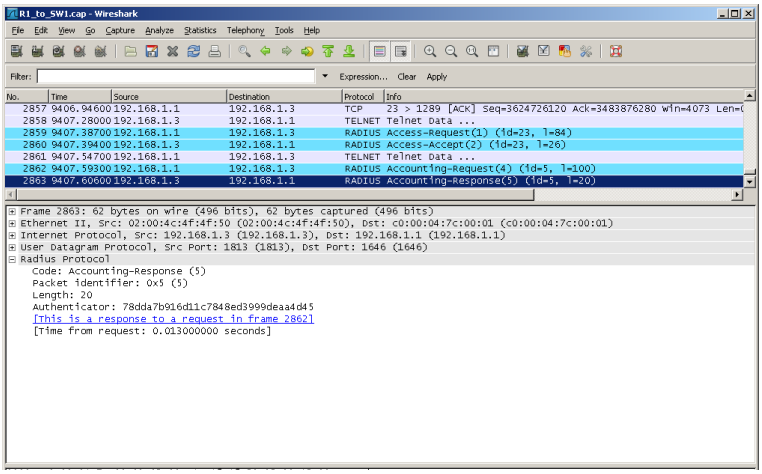
Nota: O WinRadius apenas aceita *accounting* sobre utilizadores registados na sua base de dados.



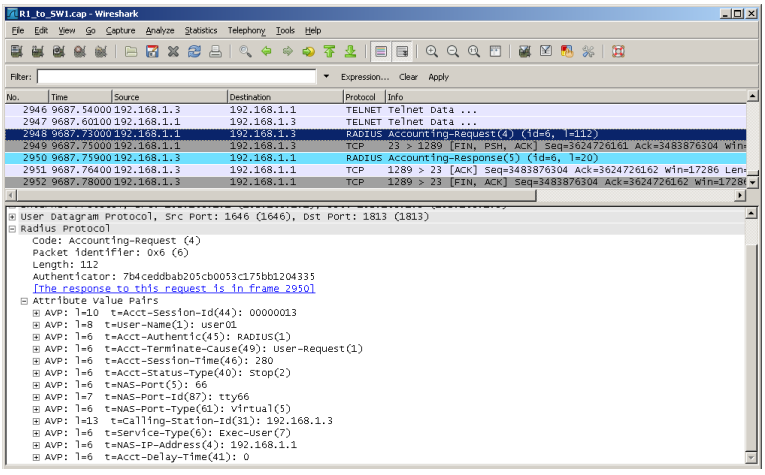
AAA Centralizado: Exercício



AAA Centralizado: Exercício



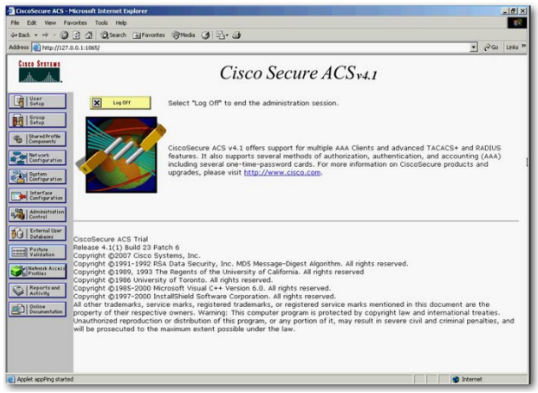
AAA Centralizado: Exercício



Cisco Secure Access Control Server (ACS)

Cisco Secure ACS: Funcionalidades

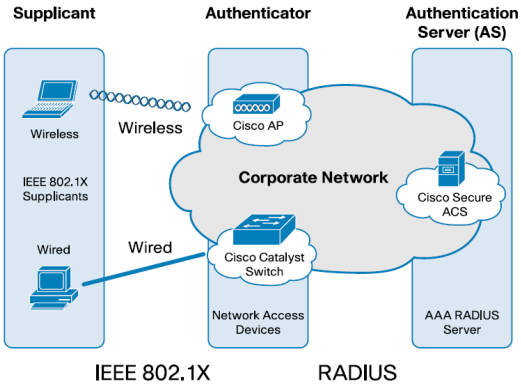
- Cisco Secure ACS
  - Centraliza a gestão de autenticação e privilégios
  - RADIUS/TACACS+
  - LDAP: integração c/ Microsoft AD, Sun, …
  - Perfis de grupos de utilizadores e de grupos de dispositivos
  - Controlos de acesso temporalmente variáveis



Cisco Secure ACS: Integração

- Cisco Secure ACS
  - Integração com a arquitectura *Identity-Based Networking Services* (IBNS)
  - Integração com o *Network Access Control* – iniciativa da indústria, lide-rada pela Cisco, que usa a infra-es-trutura de rede

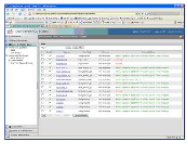
para forçar a aplicação de políticas de segurança da instituição.



Cisco Secure ACS: Modalidades

Cisco Secure ACS Operating Systems
- Windows 2000 Server with Service Pack 4
- Windows 2000 Advanced Server with Service Pack 4
- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition

Cisco Secure ACS Solution Engine
- A highly scalable dedicated platform that serves as a high-performance ACS
- 1U, rack-mountable
- Preinstalled with a security-hardened Windows software, Cisco Secure ACS software
- Support for more than 350 users



Cisco Secure ACS Express 5.0
- Entry-level ACS with simplified feature set
- Support for up to 50 AAA device and up to 350 unique user ID logins in a 24-hour period

Cisco Secure ACS: Pré-requisitos

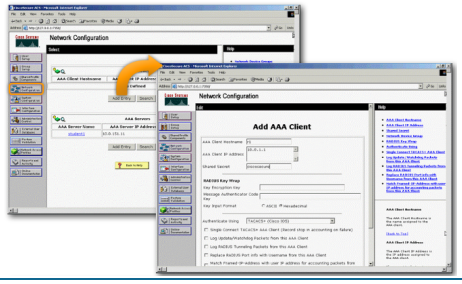
- Para usar o Cisco ACS:
  - Clientes AAA (*routers*, *switches*, …): IOS ≥ 11.2
  - Clientes Cisco não AAA: configurados com TACACS+/RADIUS
  - Utilizadores WiFi, *dial-in*,… têm de poder contactar clientes AAA
  - Os clientes AAA devem poder contactar o servidor ACS
  - Os portos devem necessários devem estar abertos
  - Um dos browsers suportados deve estar presente no servidor ACS
  - Todas as interfaces de rede no servidor ACS devem estar activas
    - De outro modo a Microsoft CryptoAPI torna o processo de instalação do ACS muito elnto
  - Configuração inicial `http://127.0.0.1:2002.`
  - Configuração remota (quando existir pelo menos um utilizador) `http://hostname:2002`

Cisco Secure ACS: Configuração

Cisco Secure ACS: Configuração

A. Criação de um cliente AAA

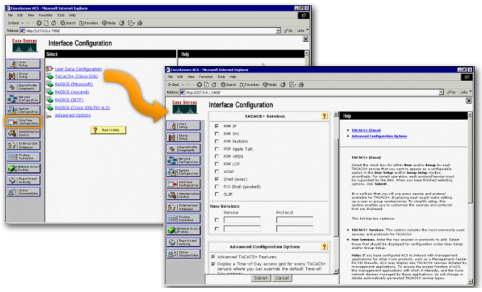
1. Clicar em **Network Configuration**
2. Na secção de clientes AAA clicar em **Add Entry**
3. Preencher o formulário do cliente (i.e., do router, switch, etc.)
4. Clicar **Submit and Apply**.



Cisco Secure ACS: Configuração

B. Configuração da interface com o utilizador

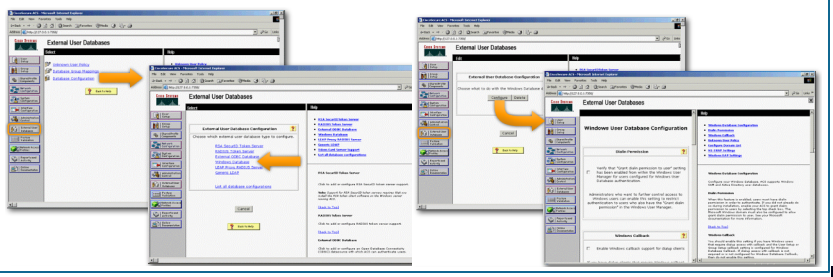
1. Configuração disponível para clientes tipo:
   - User Data Configuration
   - TACACS+ (Cisco IOS)
   - RADIUS (Microsoft)
   - Advanced Options
   - RADIUS (Ascend)
   - RADIUS (IETF)
   - RADIUS (IOS/PIX)



Cisco Secure ACS: Configuração

C. Utilização de bases de dados externas (ex. *Active Directory*)

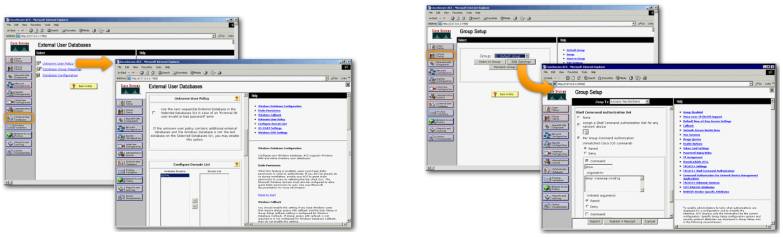
1. Clicar em **External User Databases**
2. Clicar em **Database Configuration**
3. Clicar em Windows Database
4. Clicar em **Configure**



Cisco Secure ACS: Configuração

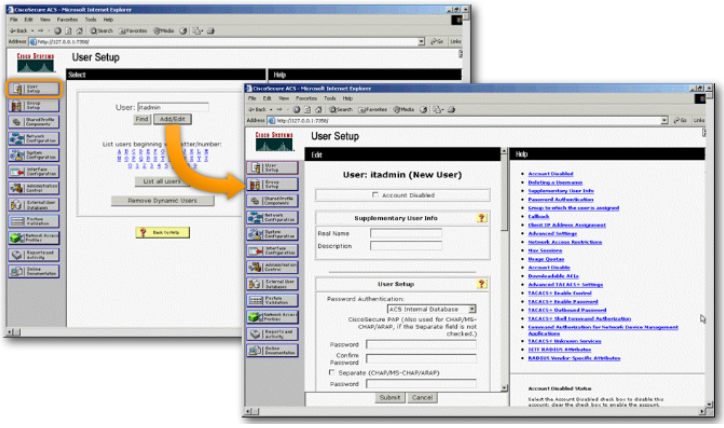
D. Configuração de utilizadores e grupos

- Se o ACS usa DB externa a autenticação pode ser:
  - Exclusiva: apenas usa a base de dados externa - *specific user assignment*
  - Alternativa apenas recorre à base de dados externa se o utilizador não se encontrar registado na base de dados do próprio ACS
- As políticas de autorização são definidas por grupo no ACS
  - Exemplo: que comandos do IOS estão disponíveis



Cisco Secure ACS: Configuração

E. Criação de utilizadores na base de dados local do ACS



Referências

- CCNA Security Ch. 3 – Authentication, Authorization, and Accounting
- User Guide for the Cisco Secure Access Control System 5.0, Cisco Systems

Obrigado pela atenção. Alguma dúvida?