CIS 4080
Network Security

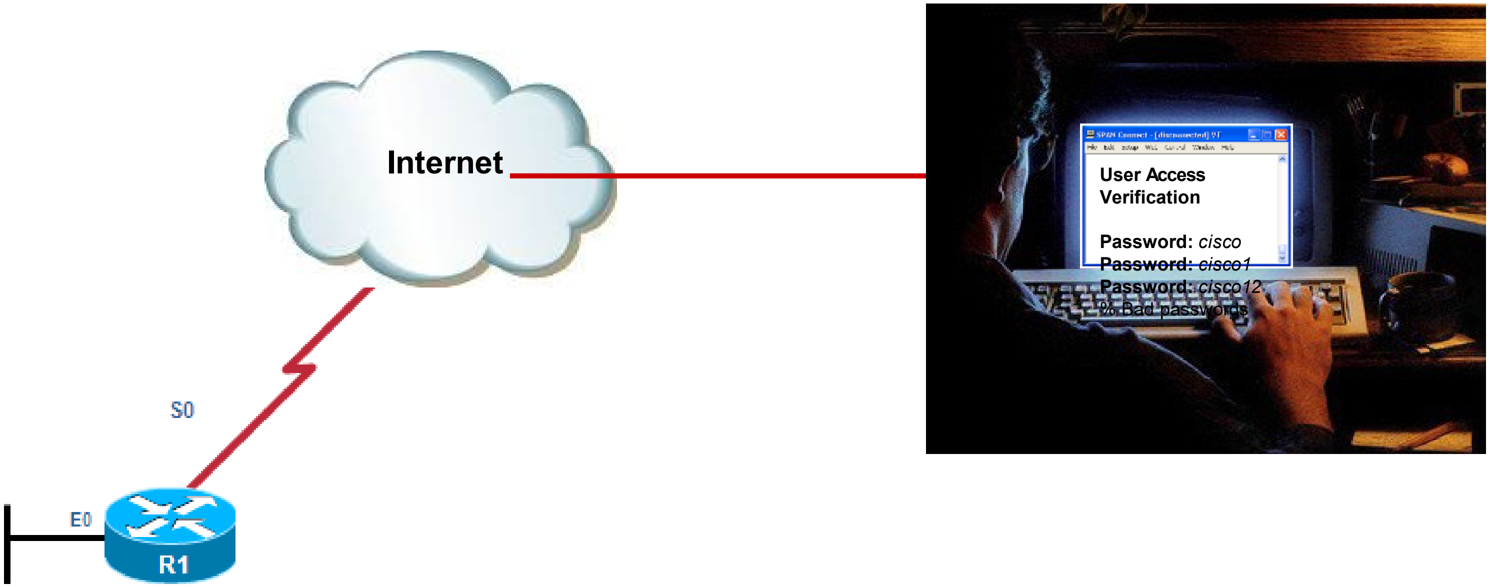
AAA

Managing Administrative Access

- Managing administrative infrastructure access is crucial.
- Methods:
  - Password only
  - Local database
  - AAA Local Authentication (self-contained AAA)

Access Type	Modes	Network Access Server Ports	Common AAA Command Element
Remote administrative access	Character Mode (line or EXEC mode)	tty, vty, auxiliary, and console	**login**, **exec**, and **enable** commands
Remote network access	Packet (interface mode)	Dial-up and VPN access including asynchronous and ISDN (BRI and PRI)	**ppp** and **network** commands

Password Only Method

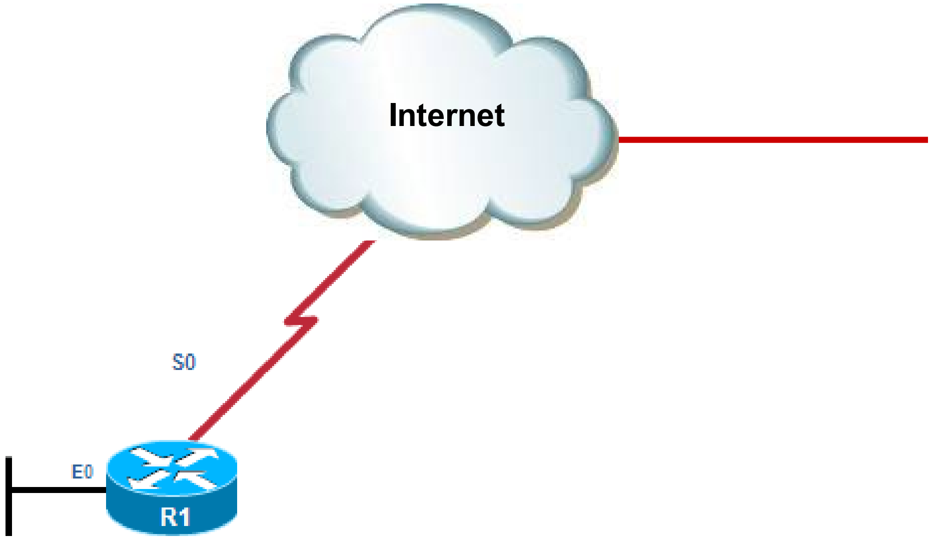


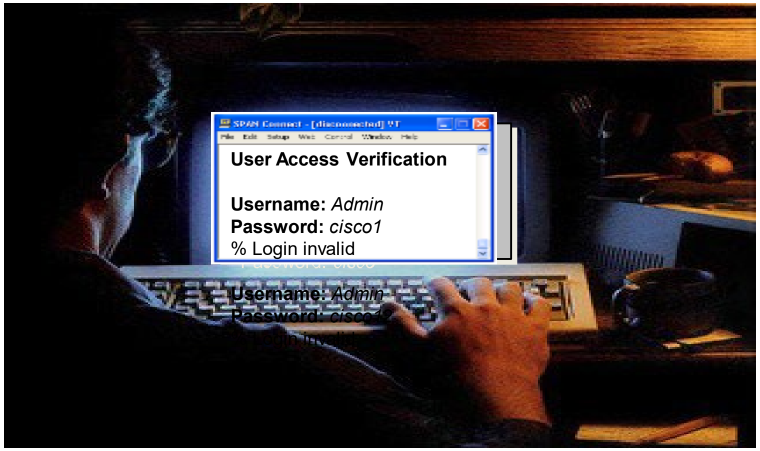
```
User Access
Verification

Password: cisco
Password: cisco1
Password: cisco12
% Bad passwords
```

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

- User EXEC mode or privilege EXEC mode password access is limited and does not scale well.

Local Database Method





User Access Verification

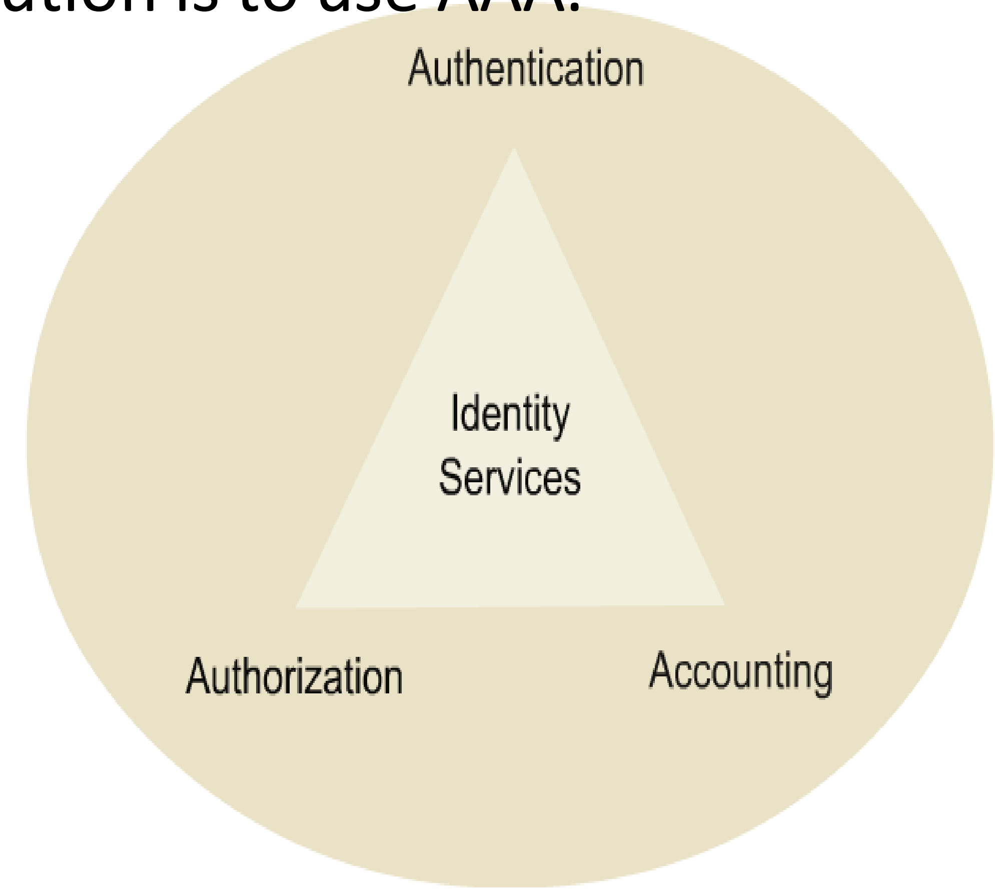
Username: *Admin*
Password: *cisco1*
% Login invalid

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

- It provides greater security than a simple password.
- It’s a cost effective and easily implemented security solution.

Local Database Method

- The problem is this local database has to be replicated on several devices …
  - A better scalable solution is to use AAA.



AAA Security Services

- AAA is an architectural framework for configuring:

Authentication - Who is allowed access?

Authorization - What are they allowed to do?

Accounting - What did they do?

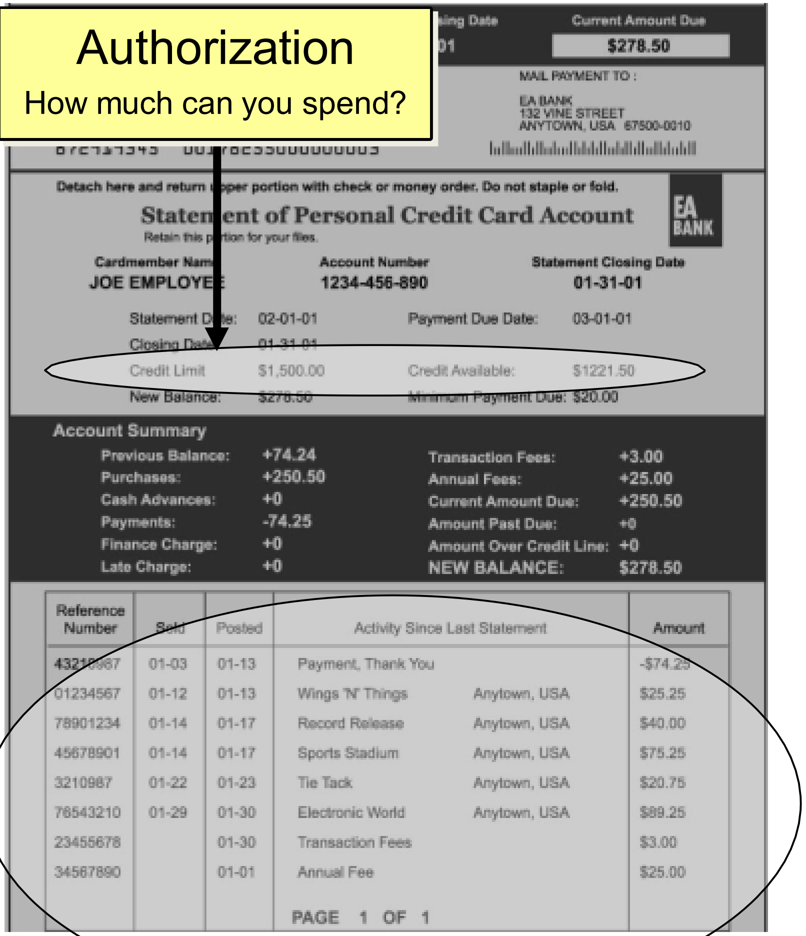
AAA Security Services

Authentication

Who are you?

Authorization

How much can you spend?



sing Date | Current Amount Due
01 | $278.50

MAIL PAYMENT TO :

EA BANK
132 VINE STREET
ANYTOWN, USA 67500-0010

Detach here and return upper portion with check or money order. Do not staple or fold.

Statement of Personal Credit Card Account

Retain this portion for your files.

EA BANK

Cardmember Name	Account Number	Statement Closing Date
JOE EMPLOYEE	1234-456-890	01-31-01

Statement Date:	02-01-01	Payment Due Date:	03-01-01
Closing Date:	01-31-01		
Credit Limit	$1,500.00	Credit Available:	$1221.50
New Balance:	$278.50	Minimum Payment Due:	$20.00

Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	$278.50

Reference Number	Sold	Posted	Activity Since Last Statement		Amount
43210987	01-03	01-13	Payment, Thank You		-$74.25
01234567	01-12	01-13	Wings 'N' Things	Anytown, USA	$25.25
78901234	01-14	01-17	Record Release	Anytown, USA	$40.00
45678901	01-14	01-17	Sports Stadium	Anytown, USA	$75.25
3210987	01-22	01-23	Tie Tack	Anytown, USA	$20.75
76543210	01-29	01-30	Electronic World	Anytown, USA	$89.25
23455678		01-30	Transaction Fees		$3.00
34567890		01-01	Annual Fee		$25.00

PAGE 1 OF 1

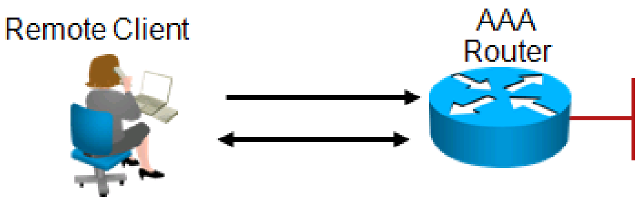
Accounting

What did you spend it on?

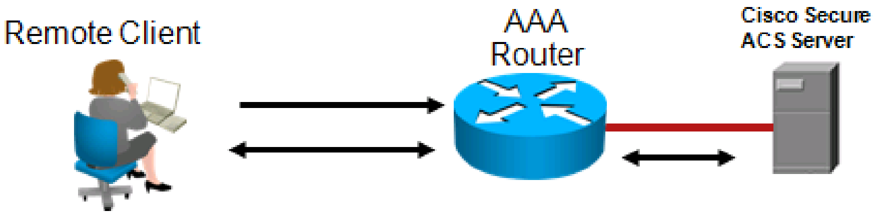
AAA Authentication Methods

- Cisco IOS routers can implement AAA using either:

Local username and password database



Cisco Secure Access Control Server (ACS)



AAA Local Authentication

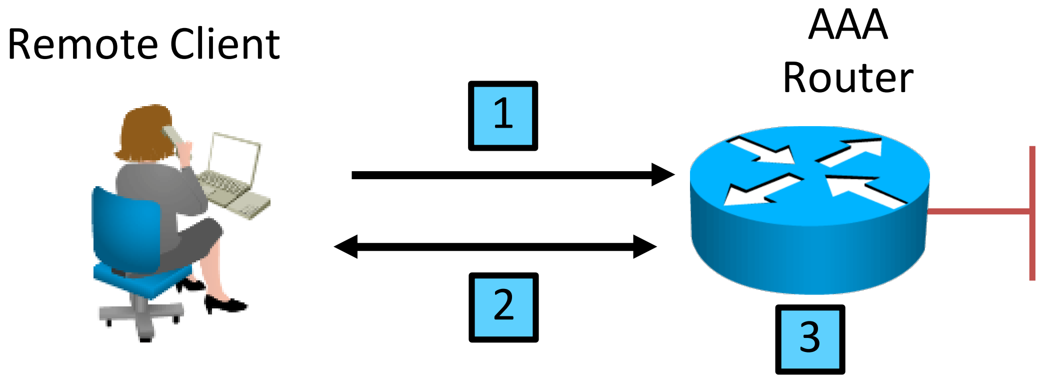
- Also called “Self-contained AAA”, it provides the method of identifying users:
  - Includes login and password dialog, challenge and response, messaging support, …
- It’s configured by:
  - Defining a “named” list of authentication methods.
  - Applying that list to various interfaces (console, aux, vty).
- The only exception is the default method list (“default”) which is automatically applied to all interfaces if no other method list is defined.

AAA Local Authentication

- The named or default authentication method defines:
  - The types of authentication to be performed.
  - The sequence in which they will be performed.
- It *must* be applied to a specific interface before any of the defined authentication methods will be performed.

AAA Local Authentication

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 the local database and the user is authorized to access the network based on information in the local database.

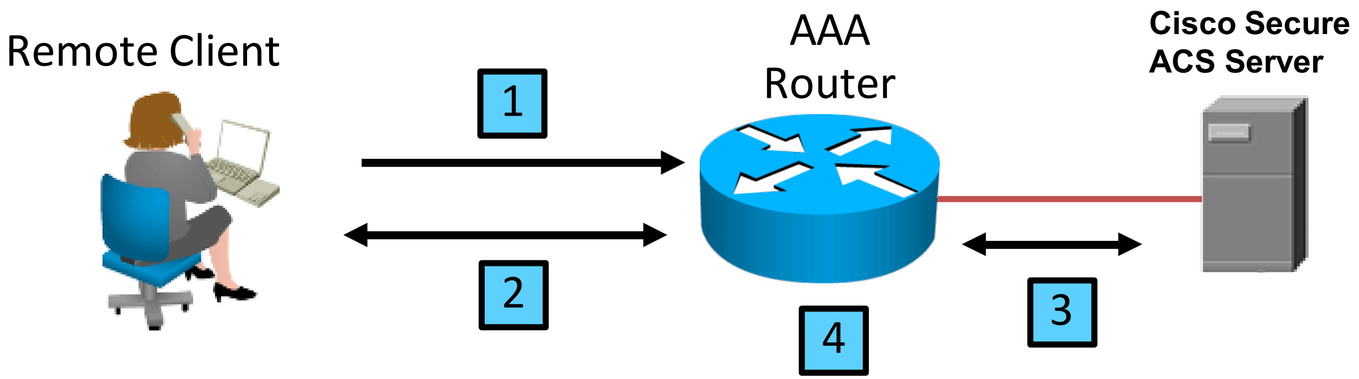


Server-Based AAA Authentication

- Using Cisco Access Control Server (ACS) is the most scalable because all infrastructure devices access a central server.
  - Fault tolerant because multiple ACS can be configured.
  - Enterprise solution.
- The actual server can be:
  - Cisco Secure ACS for Windows Server:
    - AAA services on the router contacts a Cisco Secure Access Control Server (ACS) system for user and administrator authentication.
  - Cisco Secure ACS Solution Engine:
    - AAA services on the router or NAS contact an external Cisco Secure ACS Solution Engine for user and administrator authentication.

Server-Based AAA Authentication

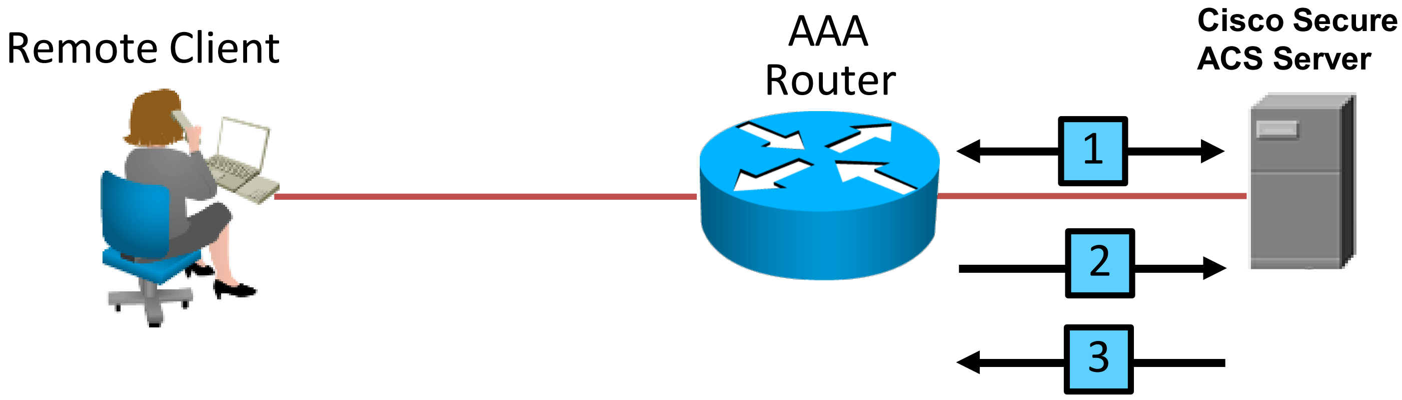
1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a remote AAA server.
4. The user is authorized to access the network based on information on the remote AAA Server.



Authorization

- Provides the method for remote access control.
  - Including one-time authorization or authorization for each service, per-user account list and profile, user group support, etc.
- Once a user has authenticated, authorization services determine which:
  - Resources the user can access.
  - Operations the user is allowed to perform.
    - E.g., "User 'student' can access host serverXYZ using Telnet only."
- As with authentication, AAA authorization is configured by defining a "named" list of authorization methods, and then applying that list to various interfaces.

AAA Authorization

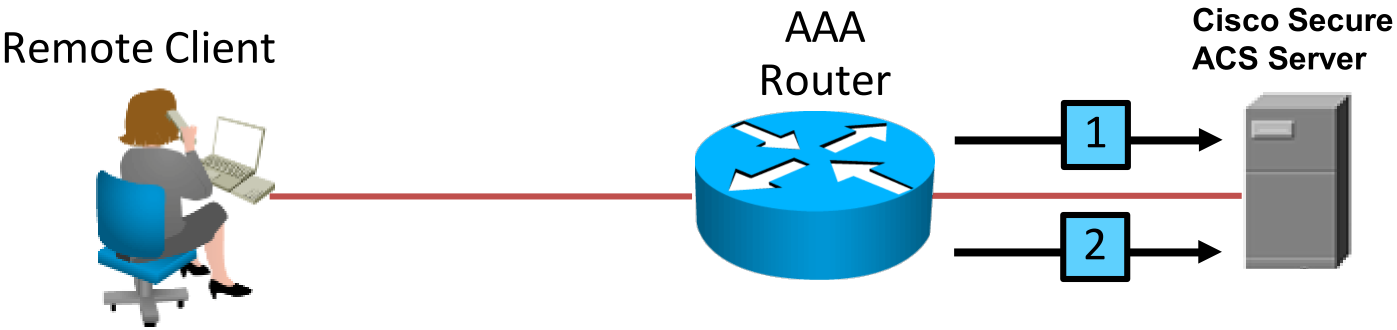


1. User has authenticated and a session has been established to the AAA server.
2. When the user attempts to enter privileged EXEC mode command, the router requests authorization from a AAA server to verify that the user has the right to use it.
3. The AAA server returns a "PASS/FAIL" response.

Accounting

- Provides the method for collecting and sending security server information.
- Used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands, number of packets / bytes, …
- With AAA accounting activated, the router reports user activity to the Terminal Access Controller Access Control System (TACACS+) server in the form of accounting records. See RFC-8907.
- Accounting is configured by defining a “named” list of accounting methods, and then applying that list to various interfaces.

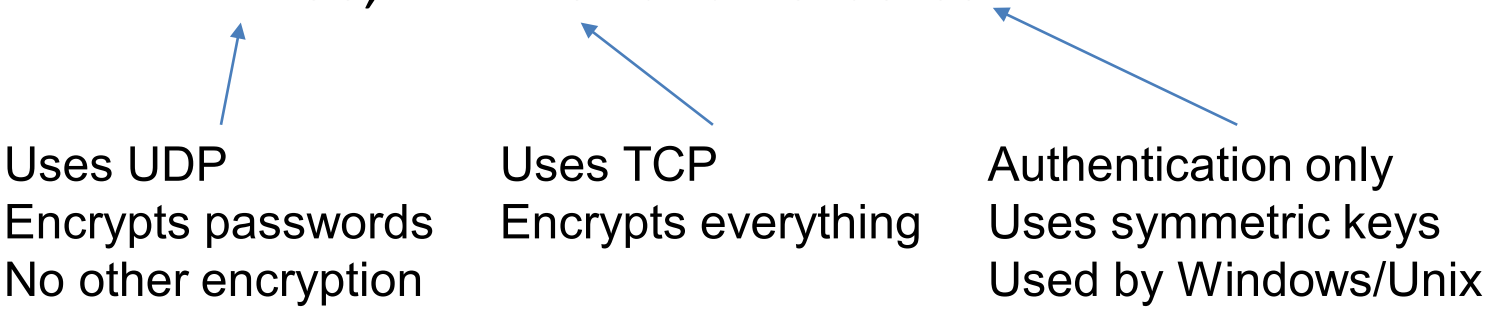
AAA Accounting



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

AAA Benefits

- Increased flexibility and control of access configuration
- Scalability
- Multiple backup systems
- Standardized authentication methods
  - RADIUS, TACACS+ and Kerberos



Uses UDP
Encrypts passwords
No other encryption

Uses TCP
Encrypts everything

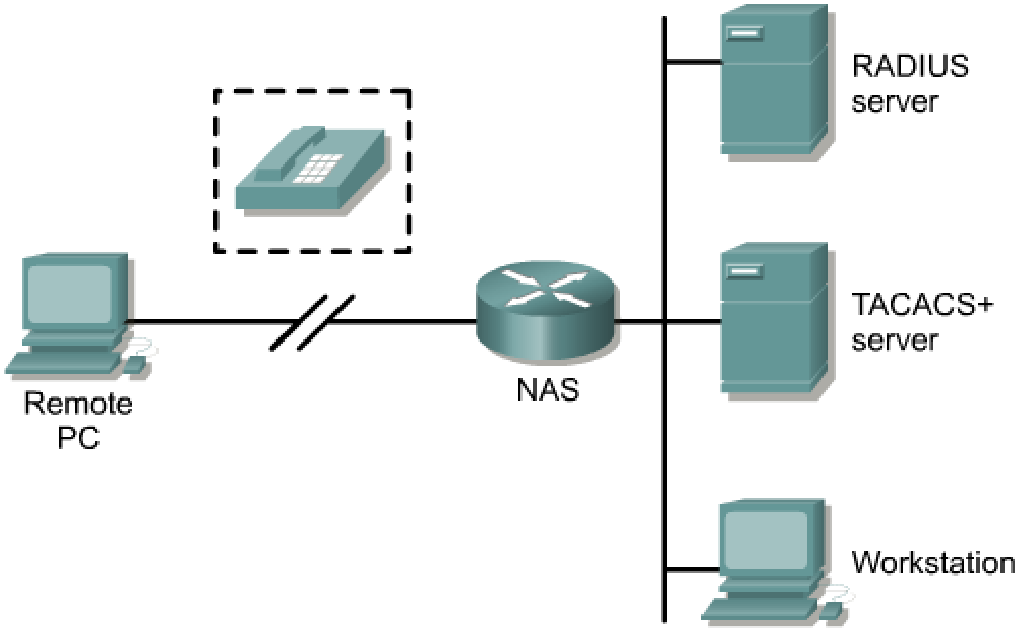
Authentication only
Uses symmetric keys
Used by Windows/Unix

AAA - Scalability

- AAA is typically implemented using a dedicated ACS server to store usernames / passwords in a centralized database.
- Information is centrally entered / updated unlike a local database which must be configured on every router.

AAA – Multiple backup systems

- Fault Tolerance can be configured in a fallback sequence.
  - Consult a security server…
  - If error or none, consult local database, …



A network access server configured for AAA can authenticate and authorize remote users via TACACS+ or RADIUS.

AAA – Standardized Security Protocols

- AAA supports standardized security protocols.
  - TACACS+
    - Terminal Access Controller Access Control System Plus
    - Replaces legacy protocols TACACS and XTACACS
    - At first Cisco proprietary, but now described by RFC-8906.
  - RADIUS
    - Remote Authentication Dial-In User Service

IMPLEMENTING LOCAL AAA AUTHENTICATION

CLI Local Authentication Configuration Steps

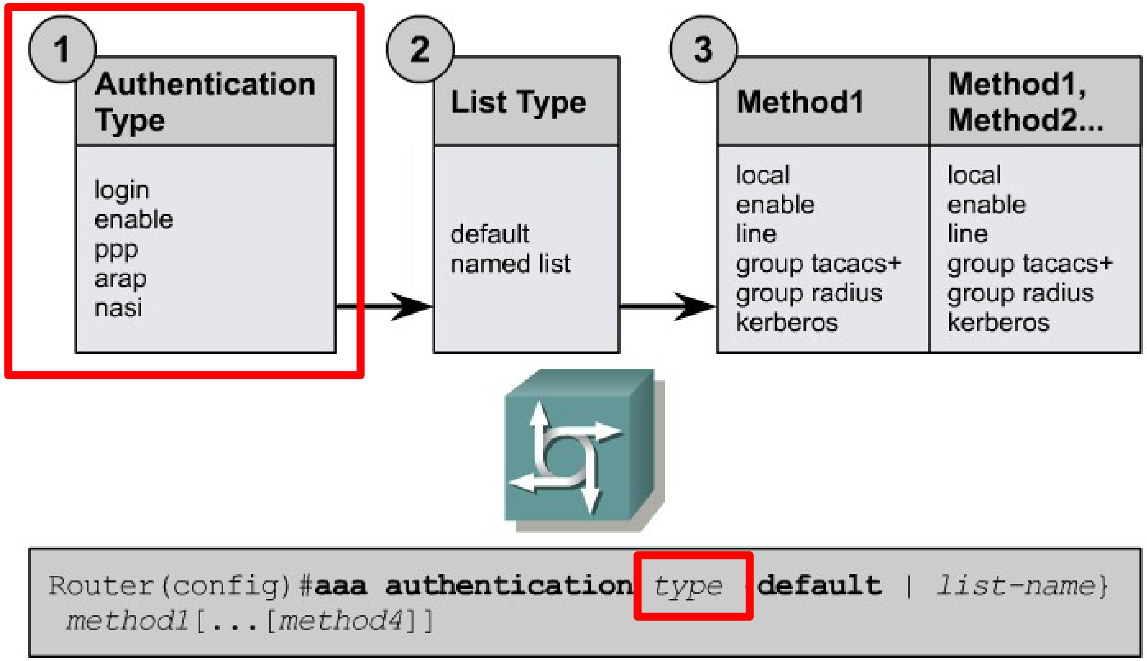
1. Enable AAA by using the global configuration command:
   - **`aaa new-model`**
2. Define the authentication method lists using:
   - **`aaa authentication`**
3. Apply the method lists to a particular interface or line (if required).

Enable AAA

- The **aaa new-model** command enables the AAA feature.
  - AAA commands can now be configured.
  - To disable AAA, use the **no aaa new-model** command.
- CAUTION:
  - Do not issue the command unless you are prepared to configure AAA authentication. Doing so could force Telnet users to authenticate with a username, even if no username database or authentication method is configured.

```
R1(config)#  aaa new-model
```

Configuring Authentication



1 Authentication Type

login
enable
ppp
arap
nasi

2 List Type

default
named list

3 Method1

local
enable
line
group tacacs+
group radius
kerberos

Method1, Method2...

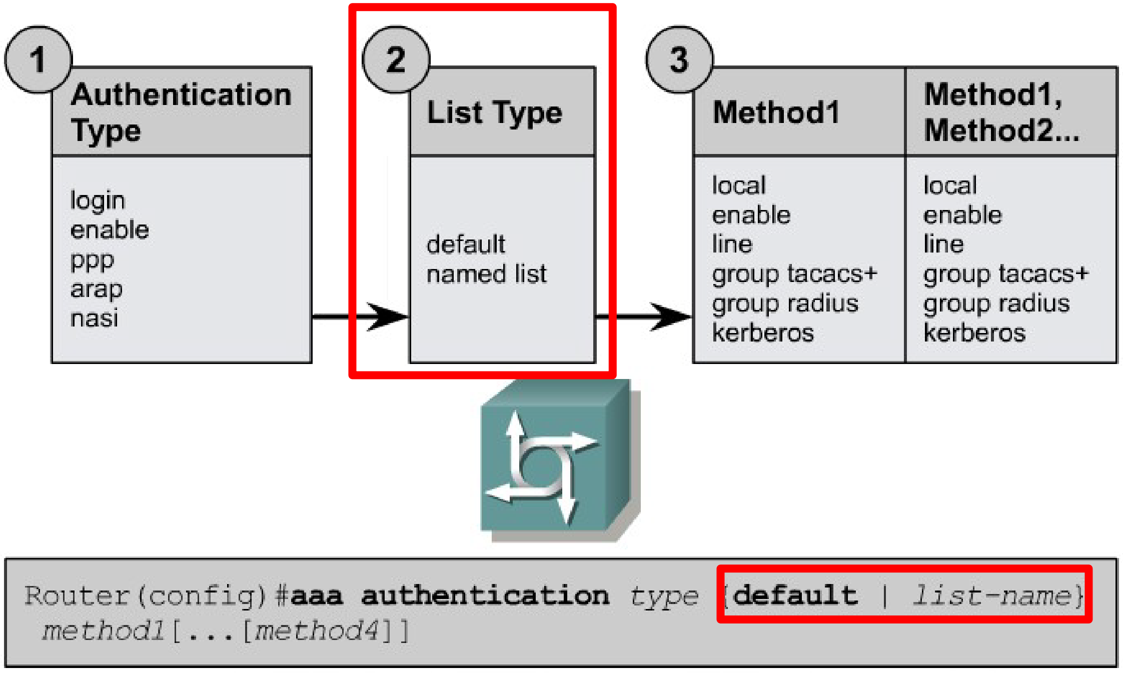
local
enable
line
group tacacs+
group radius
kerberos

```
Router(config)#aaa authentication type default | list-name}
 method1[...[method4]]
```

Use the aaa authentication command to specify the authentication type, method list type, and authentication methods.

- Specify which type of authentication to configure:
  - Login - enables AAA for logins on TTY, VTYs, and con 0.
  - Enable - enables AAA for EXEC mode access.
  - PPP - enables AAA for logins on PPP (packet transfer).

Configuring Authentication



1 Authentication Type

login
enable
ppp
arap
nasi

2 List Type

default
named list

3 Method1

local
enable
line
group tacacs+
group radius
kerberos

Method1, Method2...

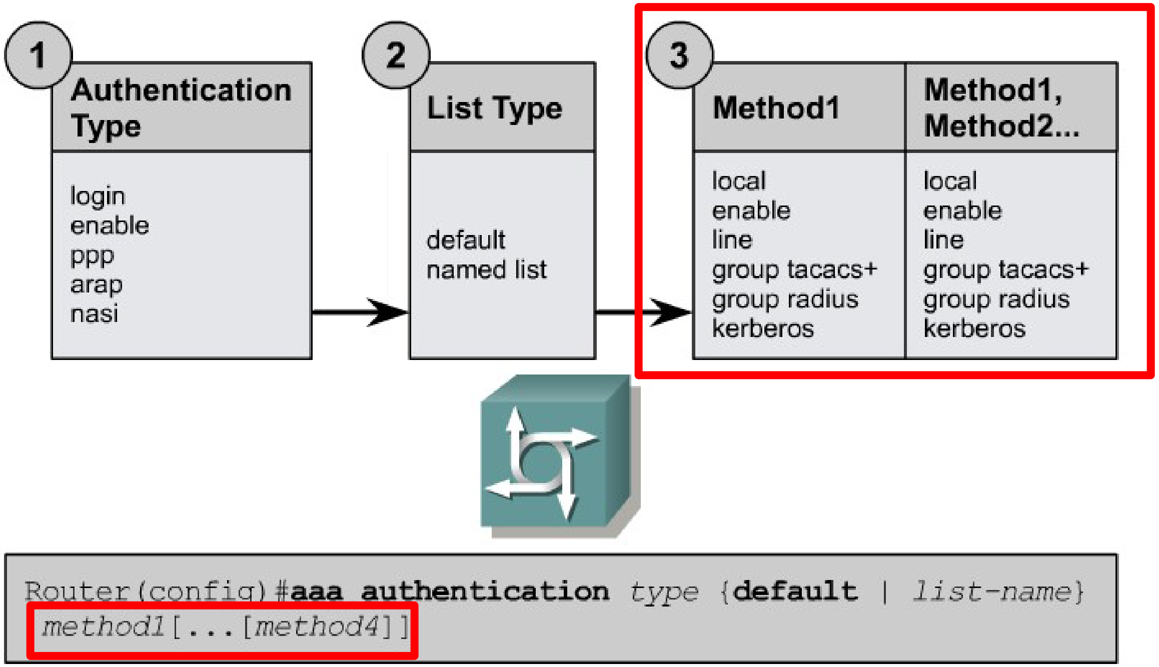
local
enable
line
group tacacs+
group radius
kerberos

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

Use the aaa authentication command to specify the authentication type, method list type, and authentication methods.

- Default method list is automatically applied to all interfaces if no other method list is defined.
- Named lists must be applied to a specific interface before any of the defined authentication methods will be performed.

Configuring Authentication

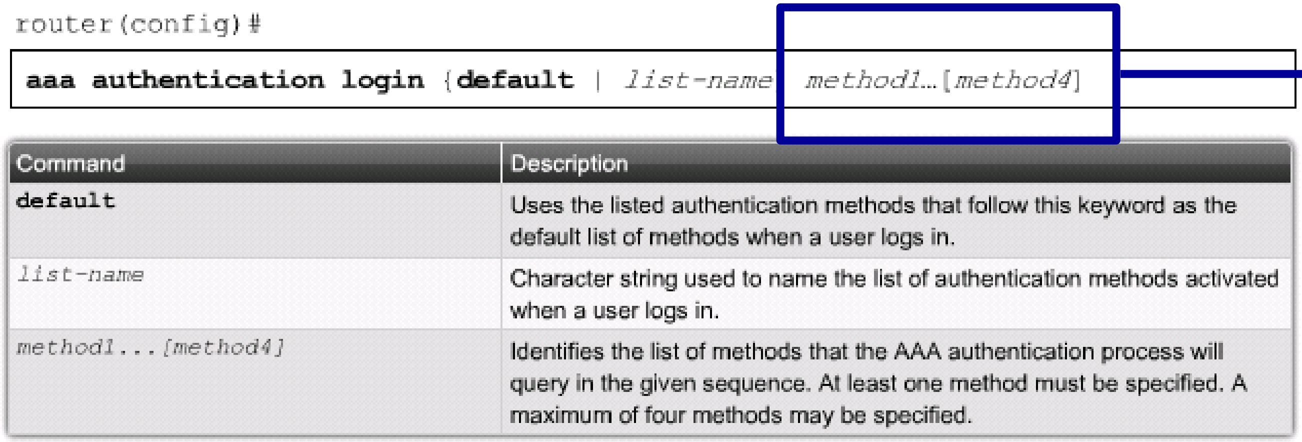


```
Router(config)#aaa authentication type {default | list-name}
 method1[...[method4]]
```

Use the aaa authentication command to specify the authentication type, method list type, and authentication methods.

- Methods list the types of authentication to be performed and the sequence in which they will be performed, such as:
  - Pre-defined passwords (e.g., local, enable, or line)
  - Consulting a TACACS+ / RADIUS / Kerberos server(s)

Configure Authentication



```
router(config)#
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.

Methods	Description
`enable`	Uses the enable password for authentication.
`line`	Uses the line password for authentication.
`local`	Uses the local username database for authentication.
`local-case`	Uses case-sensitive local username authentication.
`none`	Uses no authentication.
`cache` *`group-name`*	Uses a cache server group for authentication.
`group radius`	Uses the list of all RADIUS servers for authentication.
`group tacacs+`	Uses the list of all TACACS+ servers for authentication.
`group` *`group-name`*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **`aaa group server radius`** or **`aaa group server tacacs+`** command.

Lock Accounts with Excessive Failed Attempts

- Optionally, to lock out accounts that have excessive failed attempts, use:
  - **aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts*

```
Router (config)# aaa local authentication attempts max-fail [number-of-unsuccessful-
attempts]
```

  - To remove the number of unsuccessful attempts that was set, use the **no** form of this command.

Keyword	Description
number-of-unsuccessful-attempts	Number of unsuccessful authentication attempts before a connection is dropped.

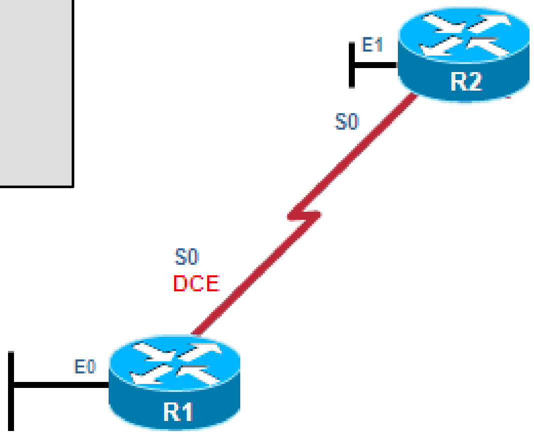
Locking a User Account

- This command locks the user account if the authentication fails and the account stays locked until it is cleared by an administrator using:
  - **`clear aaa local user lockout {username`** *`username`* **`| all}`**
- The command differs from the **`login delay`** command in how it handles failed attempts.
  - The **`login delay`** command introduces a delay between failed login attempts without locking the account.

Configuring Local AAA Authentication

- Add usernames and passwords to the local router database for users that need administrative access to the router.
- Enable AAA globally on the router.
- Configure AAA parameters on the router.
- Confirm and troubleshoot the AAA configuration.

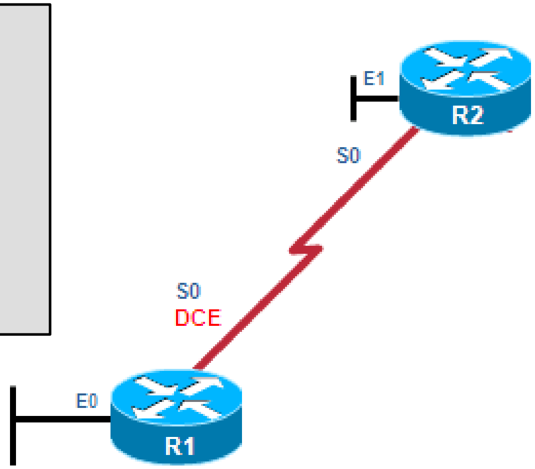
```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case
R1(config)# aaa local authentication attempts max-fail 10
```



Using a Named List

- A default list or a named list can be defined.
  - A default list is automatically applied to all interfaces if no other method list is defined.
  - A named list must be applied to a specific interface before any of the defined authentication methods will be performed.

```
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
```



Display User Information

```
R1# show aaa local user lockout

                Local-user          Lock time
                JR-ADMIN            04:28:49 UTC Sat Dec 27 2008
```

```
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
```

Troubleshooting AAA Authentication

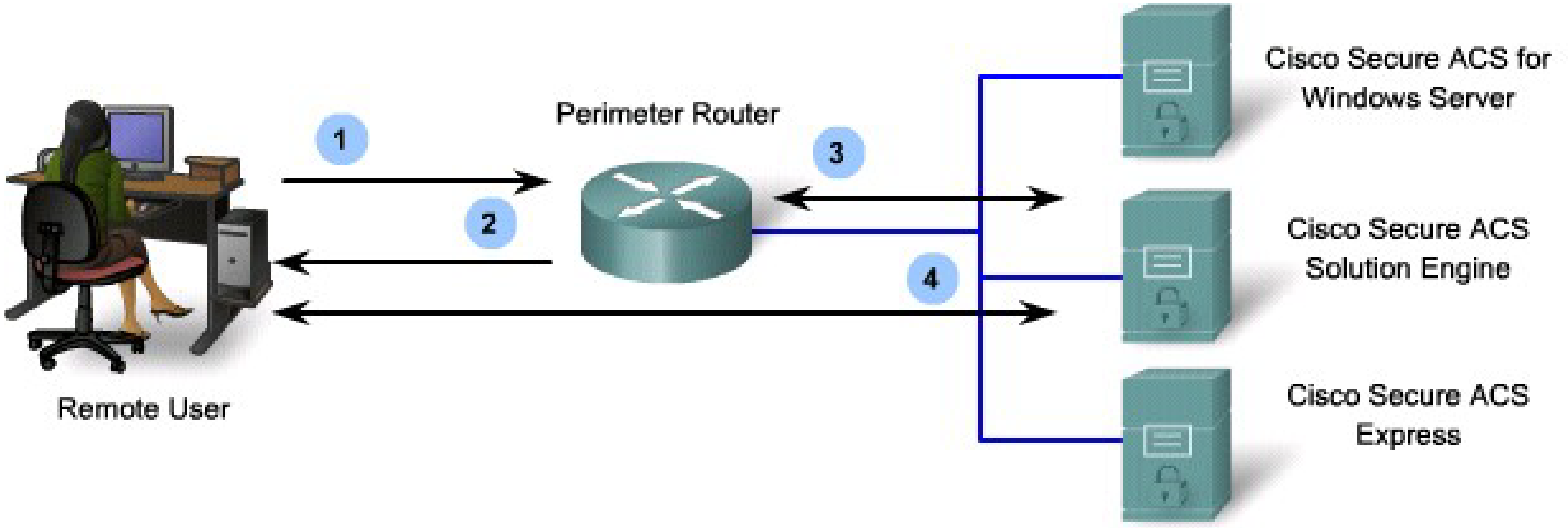
```
R1# debug aaa ?
  accounting             Accounting
  administrative         Administrative
  api                    AAA api events
  attr                   AAA Attr Manager
  authentication         Authentication
  authorization          Authorization
  cache                  Cache activities
  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

R1# debug aaa
```

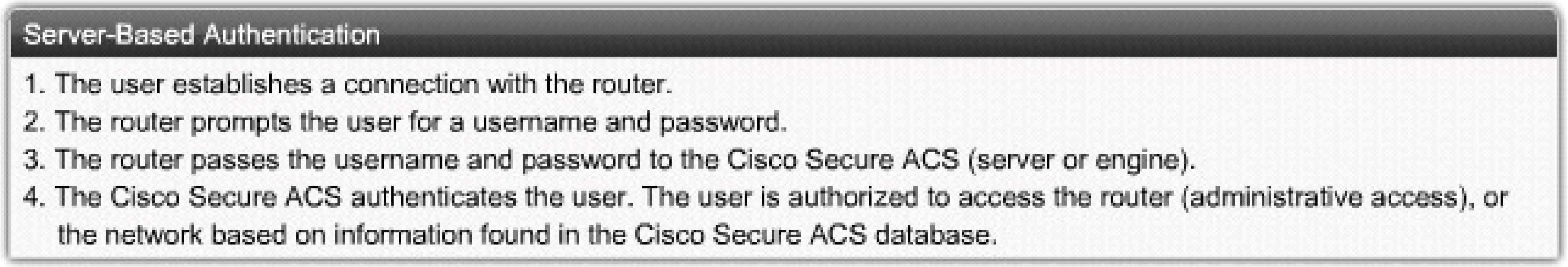
Troubleshooting AAA Authentication

```
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
```

IMPLEMENTING SERVER BASED AAA AUTHENTICATION

Server-Based Solution


Perimeter Router
1
2
3
4
Remote User
Cisco Secure ACS for Windows Server
Cisco Secure ACS Solution Engine
Cisco Secure ACS Express

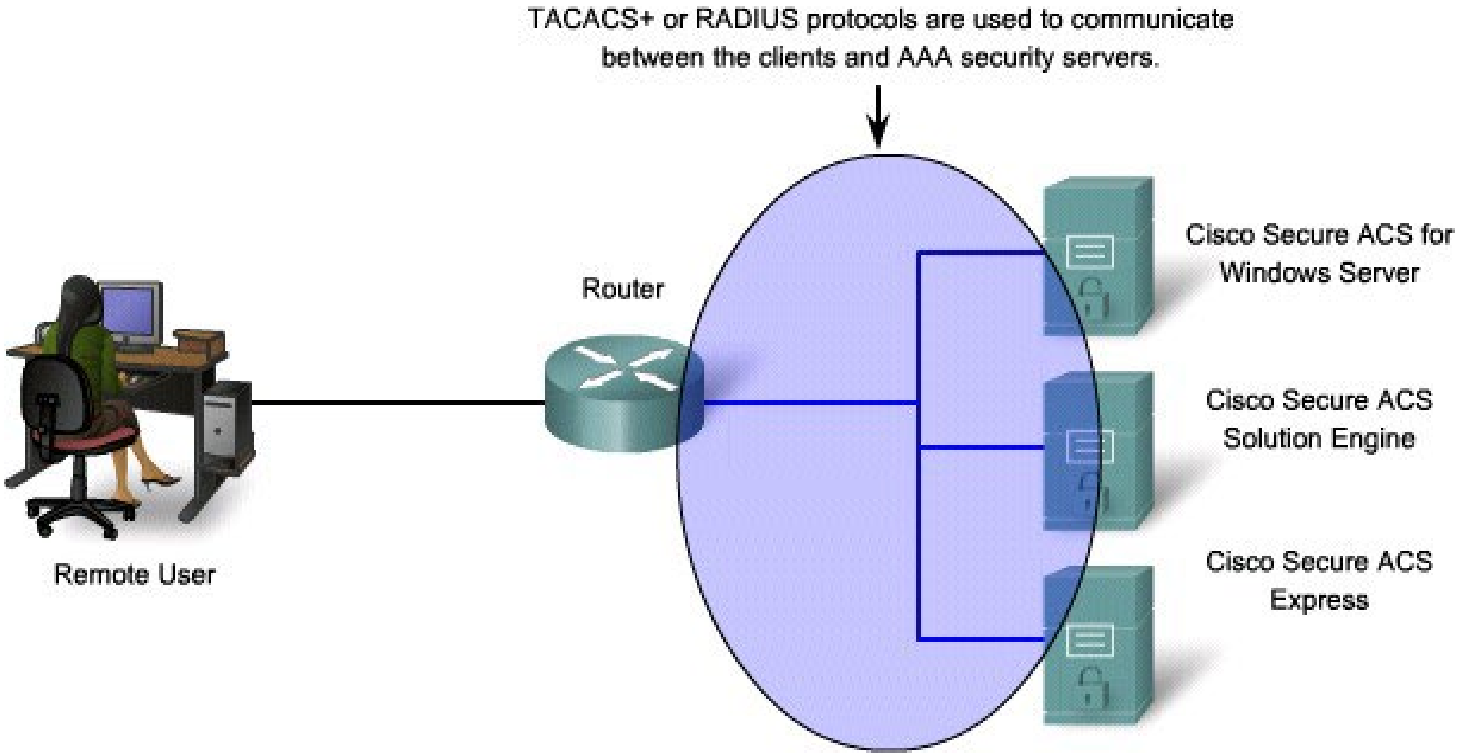


Server-Based Authentication

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.

TACACS+ and RADIUS

- The Cisco ACS family support:
  - Terminal Access Control Access Control Server Plus (TACACS+)
  - Remote Dial-in User Services (RADIUS) protocols

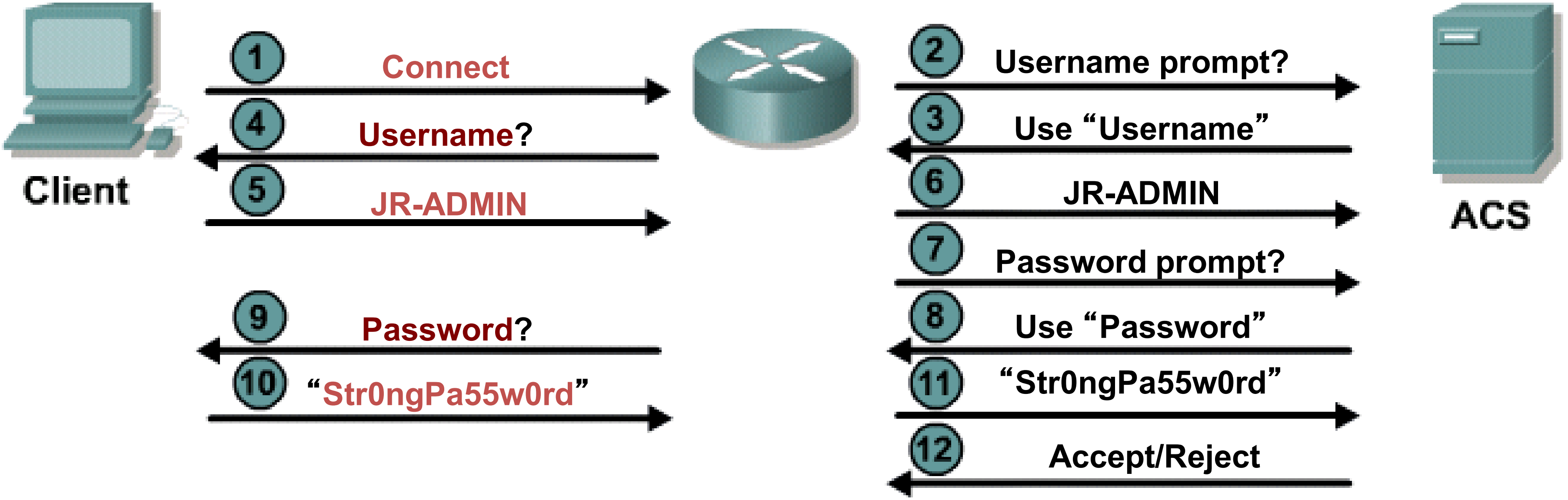

TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.
Router
Remote User
Cisco Secure ACS for Windows Server
Cisco Secure ACS Solution Engine
Cisco Secure ACS Express

TACACS+ and RADIUS

- Both protocols can be used to communicate between client and AAA servers.
- TACACS+ is considered the more secure protocol because all exchanges are encrypted.
- Radius only encrypts the user password.
  - It does not encrypt user names, accounting information, or any other information carried in the radius message.

TACACS+ Authentication

- TACACS+ is a Cisco protocol that provides separate AAA services.
  - Separating the AAA services provides flexibility in implementation, because it is possible to use TACACS+ for authorization and accounting while using another method of authentication.

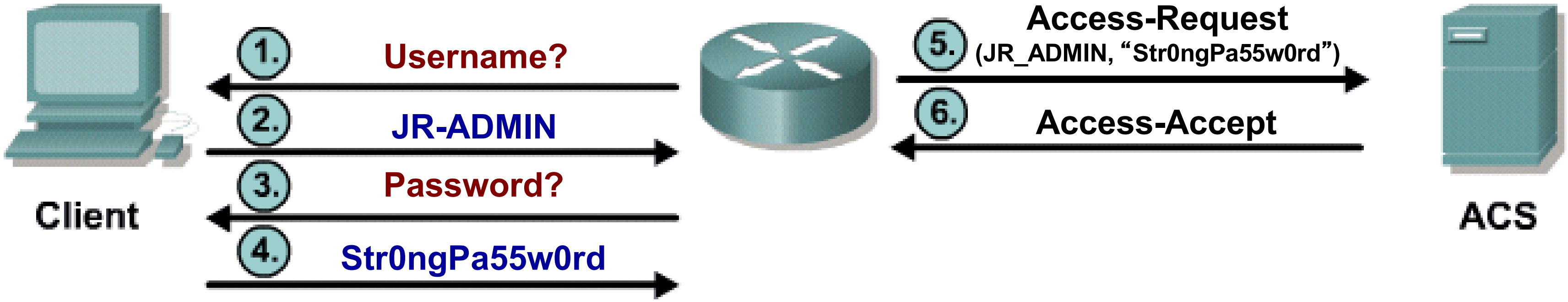


RADIUS Authentication

- RADIUS, developed by Livingston Enterprises, is an open IETF standard AAA protocol for applications such as network access or IP mobility.
  - RADIUS is currently defined by RFCs 2865, 2866, 2867, and 2868.
- The RADIUS protocol hides passwords during transmission but the rest of the packet is sent in plaintext.

RADIUS Authentication

- RADIUS combines authentication and authorization as one process which means that when a user is authenticated, that user is also authorized.
  – RADIUS uses UDP port 1645 or 1812 for authentication and UDP port 1646 or 1813 for accounting.



RADIUS Authentication

- RADIUS is widely used by VoIP service providers because it passes login credentials of a session initiation protocol (SIP) endpoint, such as a broadband phone, to a SIP Registrar using digest authentication, and then to a RADIUS server using RADIUS.
  - RADIUS is also a common authentication protocol that is utilized by the 802.1X security standard.
- The Diameter protocol is the planned replacement for RADIUS.
  - Diameter uses a new transport protocol called Stream Control Transmission Protocol (SCTP) and TCP instead of UDP.

TACACS+ vs. RADIUS

Feature	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 (but now RFC)	Open/RFC standard
Transport Protocol	TCP port 49	UDP port 1645 or 1812 for authentication UDP port 1646 or 1813 for accounting
CHAP	Bidirectional challenge and response as used in 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	Only the password is 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

CISCO SECURE ACS

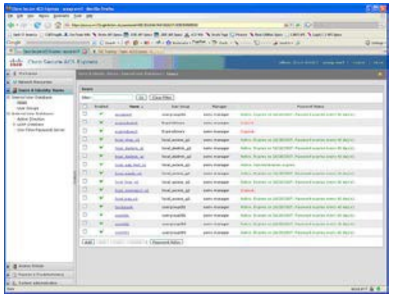
Cisco Secure ACS

- Many enterprise-level authentication servers are on the market today including:
  - Funk's Steel-Belted RADIUS server
  - Livingston Enterprises' RADIUS Authentication Billing Manager
  - Merit Networks' RADIUS
  - Cisco Secure ACS for Windows Server (ACS)
- Cisco ACS is a single solution that offers AAA services using TACACS+ or RADIUS.

Cisco Secure ACS Benefits

Ease of use	• A web-based user interface simplifies the configuration for user profiles, group profiles, and ACS configuration.
Scalability	• ACS is built to provide large networked environments including redundant servers, remote databases, and database replication and backup services.
Extensibility	• Supports the authentication of user profiles that are stored in directories from leading directory vendors, including Sun, Novell, and Microsoft.
Management	• Active Directory support consolidates username and password management.
Administration	• Ability to group network devices together make it easier and more flexible to control the enforcement and changes for all devices in a network.
Product flexibility	• Cisco Secure ACS is available in three options: Cisco Secure ACS Solution Engine, Cisco Secure ACS Express, and Cisco Secure ACS for Windows.
Integration	• Tight coupling with Cisco IOS routers and VPN solutions.
Third-party support	• Cisco Secure ACS offers token server support for any one-time password (OTP) vendor that provides an RFC-compliant RADIUS interface, such as RSA, PassGo, Secure Computing, ActiveCard, Vasco, or CryptoCard.
Control	• Provides dynamic quotas to restrict access based on the time of day, network use, number of logged sessions, and the day of the week.

Cisco Secure ACS Options



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

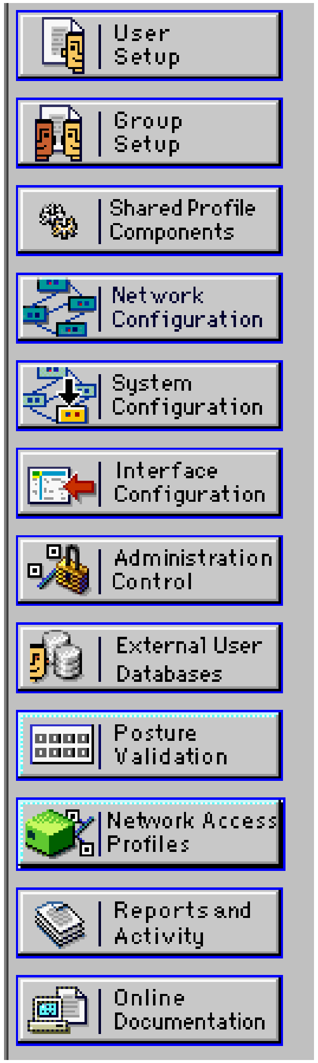
Cisco Secure ACS for Windows can be installed on:

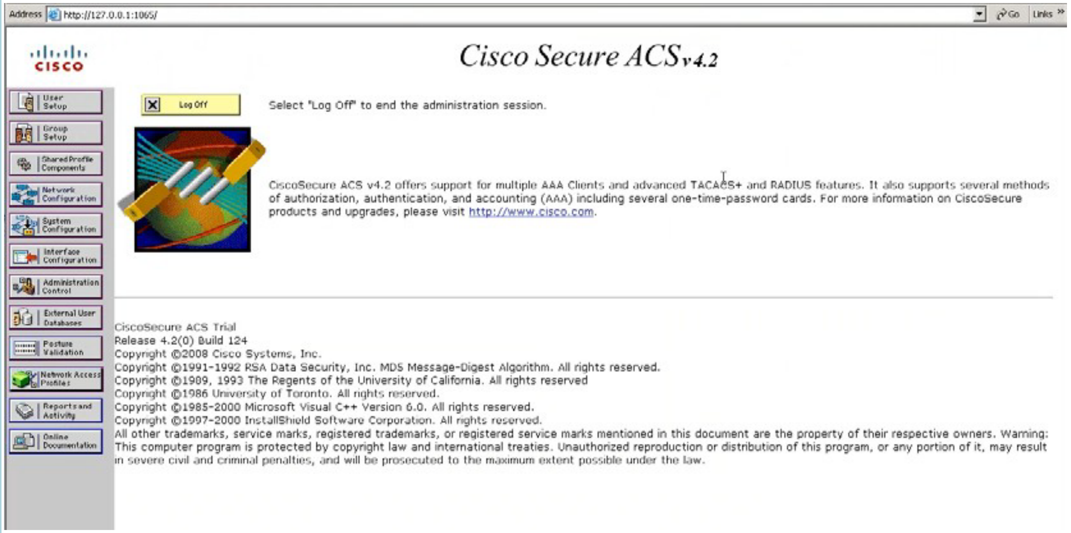
- Windows 2000 Server with Service Pack 4
- Windows 2000 Advanced Server with Service Pack 4
- Windows Server 2003 Standard or Enterprise Edition
- Windows Server 2008 Standard or Enterprise Edition

Cisco Secure ACS Solution Engine

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

Cisco Secure ACS - Home





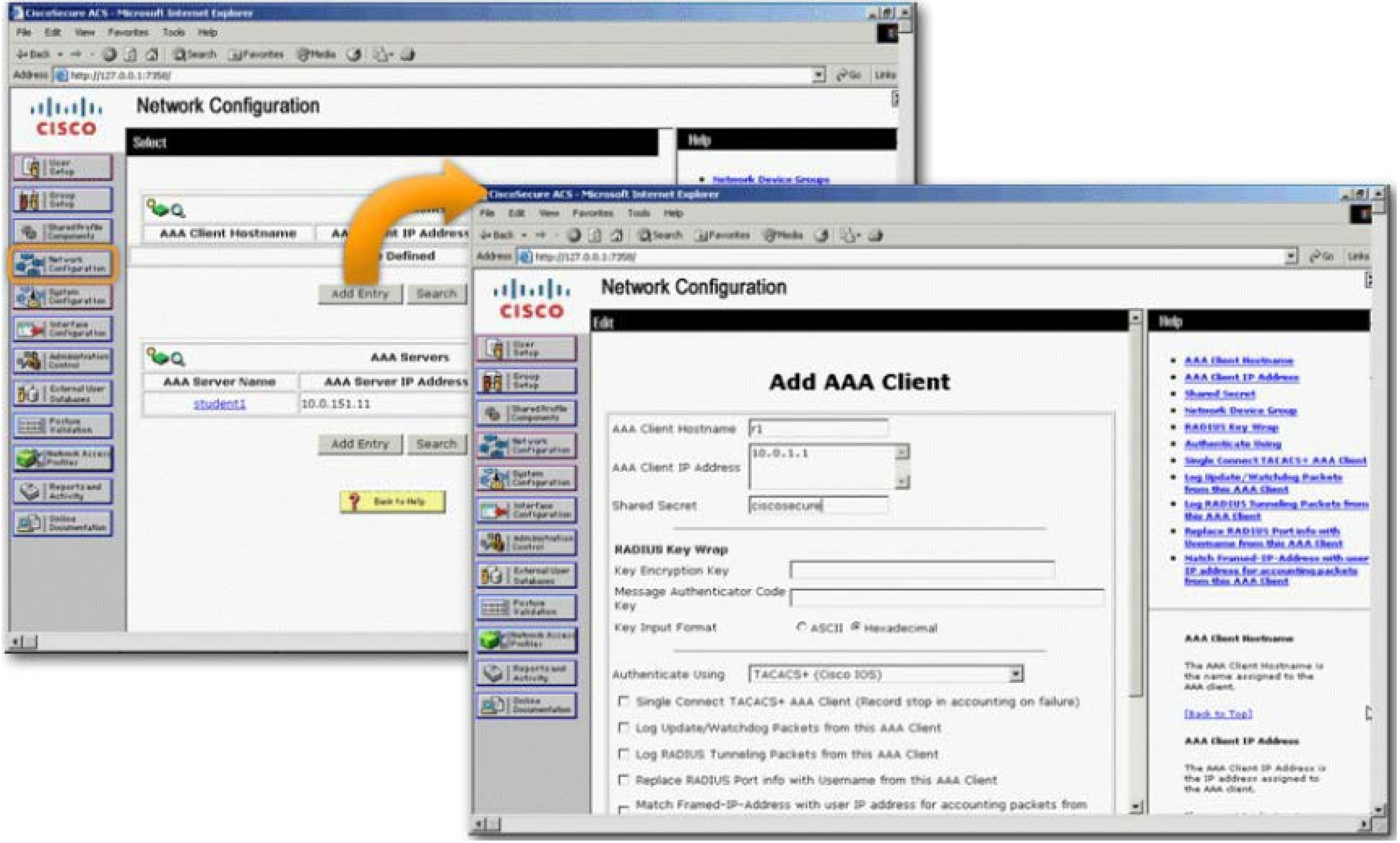
Cisco Secure ACS v4.2

Select "Log Off" to end the administration session.

CiscoSecure ACS v4.2 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit http://www.cisco.com.

CiscoSecure ACS Trial
Release 4.2(0) Build 124
Copyright ©2008 Cisco Systems, Inc.
Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
Copyright ©1909, 1993 The Regents of the University of California. All rights reserved
Copyright ©1986 University of Toronto. All rights reserved.
Copyright ©1985-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.
All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners. Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Cisco Secure ACS - Home



AAA Client Hostname	AAA Client IP Address

AAA Servers

AAA Server Name	AAA Server IP Address
student1	10.0.151.11

Add AAA Client

AAA Client Hostname: r1

AAA Client IP Address: 10.0.1.1

Shared Secret: ciscosecure

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ○ ASCII ● Hexadecimal

Authenticate Using: TACACS+ (Cisco IOS)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

□ Match Framed-IP-Address with user IP address for accounting packets from

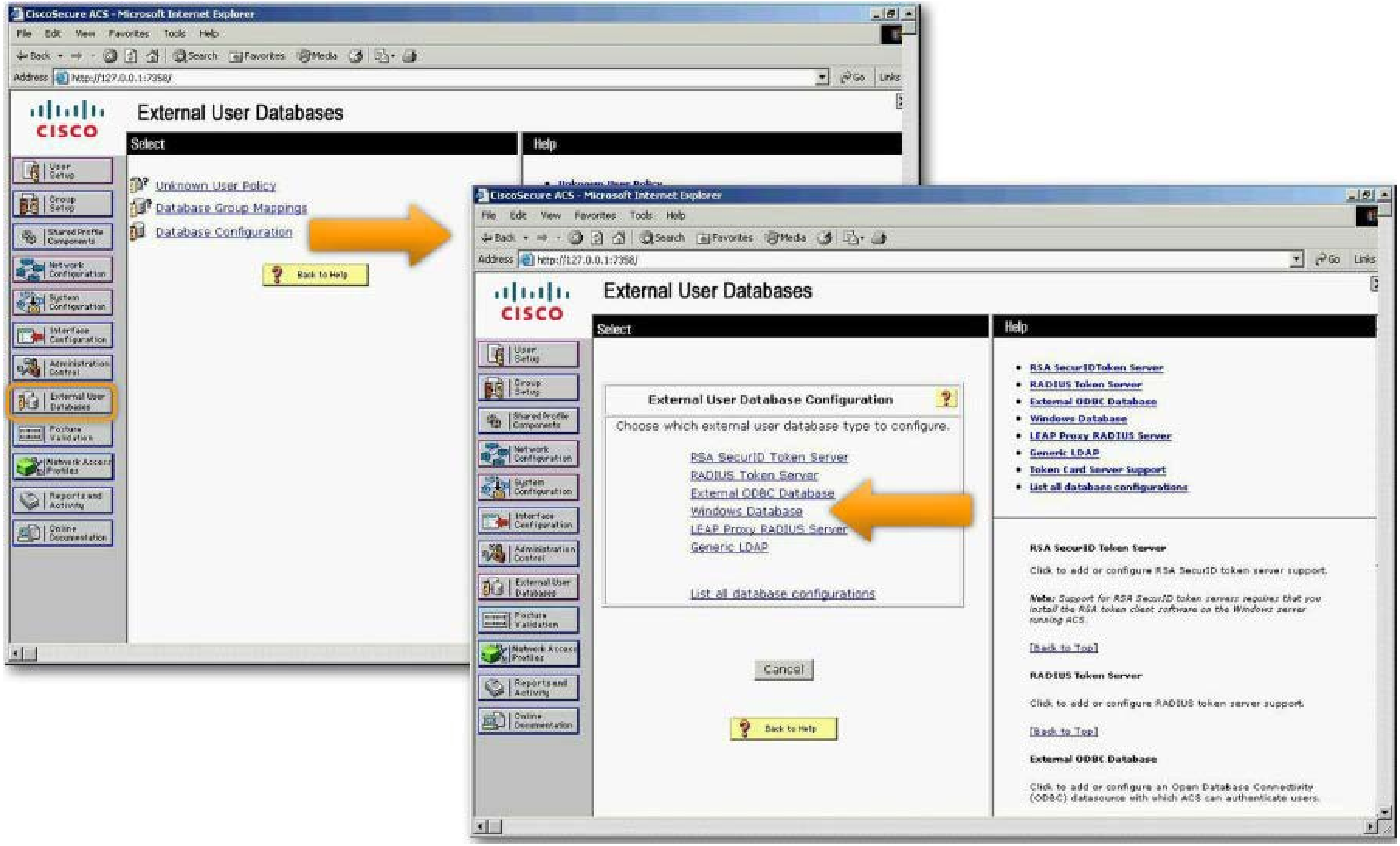
AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

ACS External Databases



External User Databases

Unknown User Policy
Database Group Mappings
Database Configuration

External User Databases

External User Database Configuration

Choose which external user database type to configure.

RSA SecurID Token Server
RADIUS Token Server
External ODBC Database
Windows Database
LEAP Proxy RADIUS Server
Generic LDAP

List all database configurations

- RSA SecurIDToken Server
- RADIUS Token Server
- External ODBC Database
- Windows Database
- LEAP Proxy RADIUS Server
- Generic LDAP
- Token Card Server Support
- List all database configurations

RSA SecurID Token Server

Click to add or configure RSA SecurID token server support.

Note: *Support for RSA SecurID token servers requires that you install the RSA token client software on the Windows server running ACS.*

[Back to Top]

RADIUS Token Server

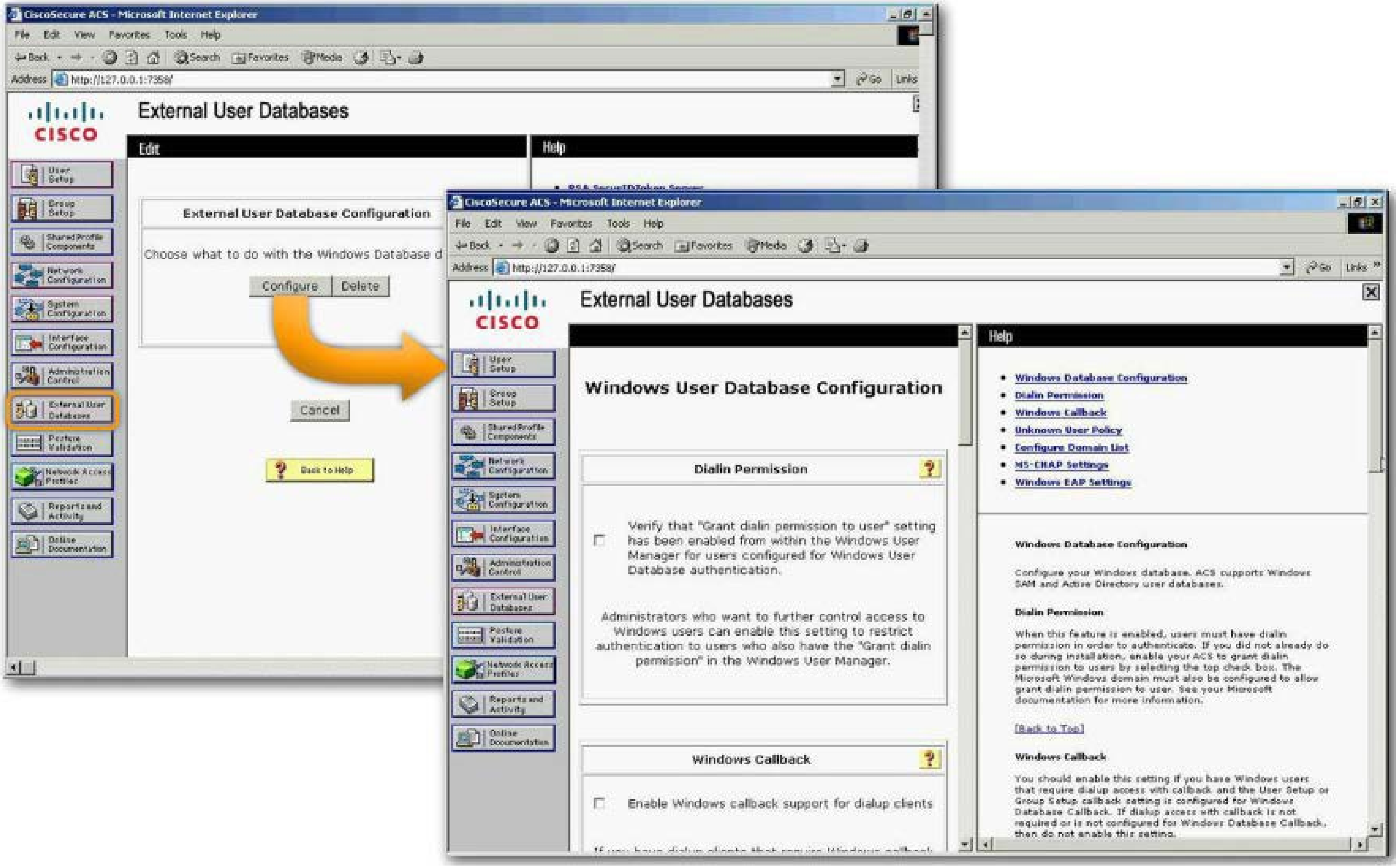
Click to add or configure RADIUS token server support.

[Back to Top]

External ODBC Database

Click to add or configure an Open Database Connectivity (ODBC) datasource with which ACS can authenticate users.

ACS External Databases



External User Databases

External User Database Configuration

Choose what to do with the Windows Database d

External User Databases

Windows User Database Configuration

Dialin Permission

☐ Verify that "Grant dialin permission to user" setting has been enabled from within the Windows User Manager for users configured for Windows User Database authentication.

Administrators who want to further control access to Windows users can enable this setting to restrict authentication to users who also have the "Grant dialin permission" in the Windows User Manager.

Windows Callback

☐ Enable Windows callback support for dialup clients

If you have dialup clients that require Windows callback

- Windows Database Configuration
- Dialin Permission
- Windows Callback
- Unknown User Policy
- Configure Domain List
- MS-CHAP Settings
- Windows EAP Settings

Windows Database Configuration

Configure your Windows database. ACS supports Windows SAM and Active Directory user databases.

Dialin Permission

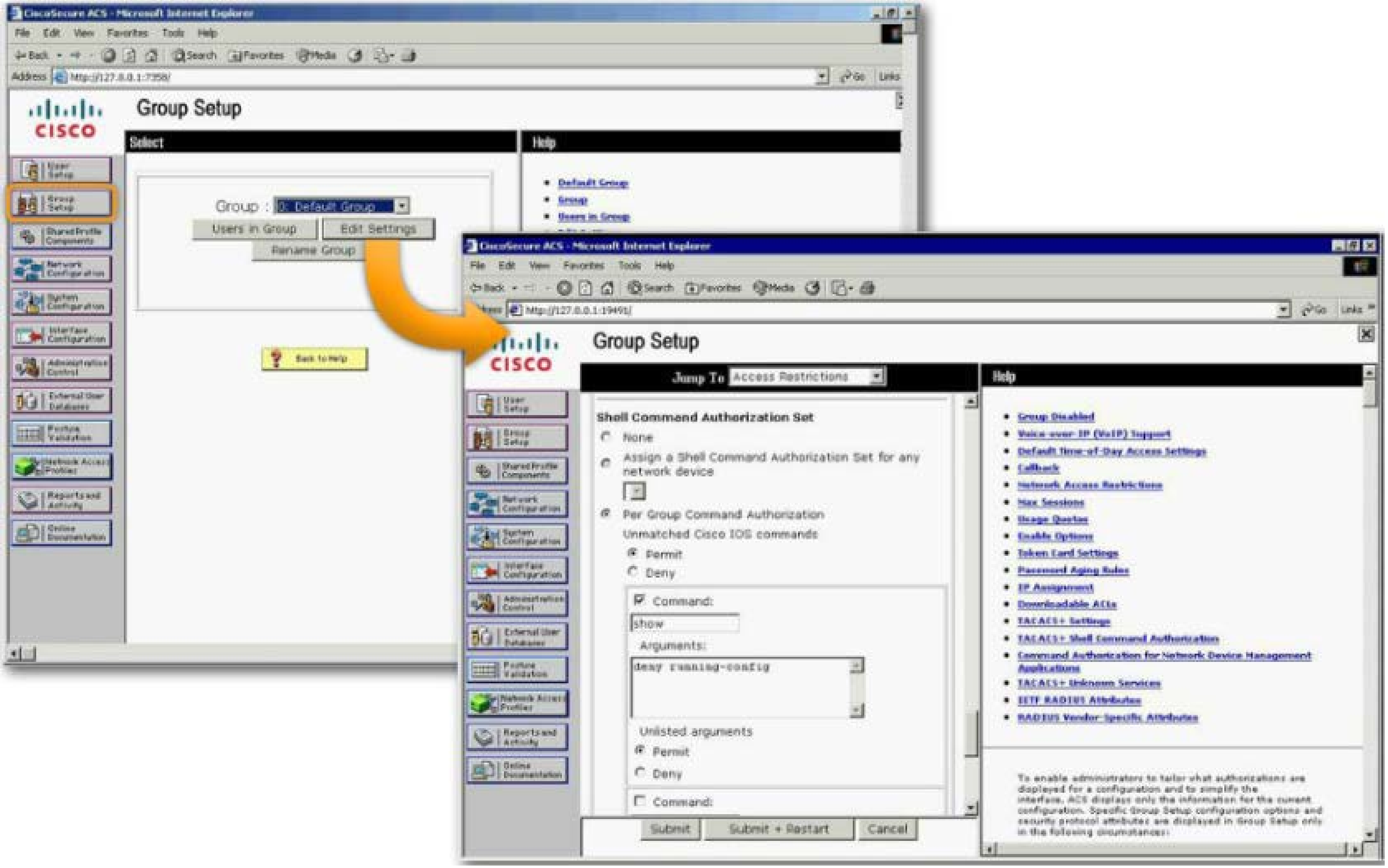
When this feature is enabled, users must have dialin permission in order to authenticate. If you did not already do so during installation, enable your ACS to grant dialin permission to users by selecting the top check box. The Microsoft Windows domain must also be configured to allow grant dialin permission to user. See your Microsoft documentation for more information.

[Back to Top]

Windows Callback

You should enable this setting if you have Windows users that require dialup access with callback and the User Setup or Group Setup callback setting is configured for Windows Database Callback. If dialup access with callback is not required or is not configured for Windows Database Callback, then do not enable this setting.

ACS Group Setup



Group : 0: Default Group

Shell Command Authorization Set

○ None

○ Assign a Shell Command Authorization Set for any network device

● Per Group Command Authorization

Unmatched Cisco IOS commands

● Permit

○ Deny

☑ Command:

show

Arguments:

```
deny running-config
```

Unlisted arguments

● Permit

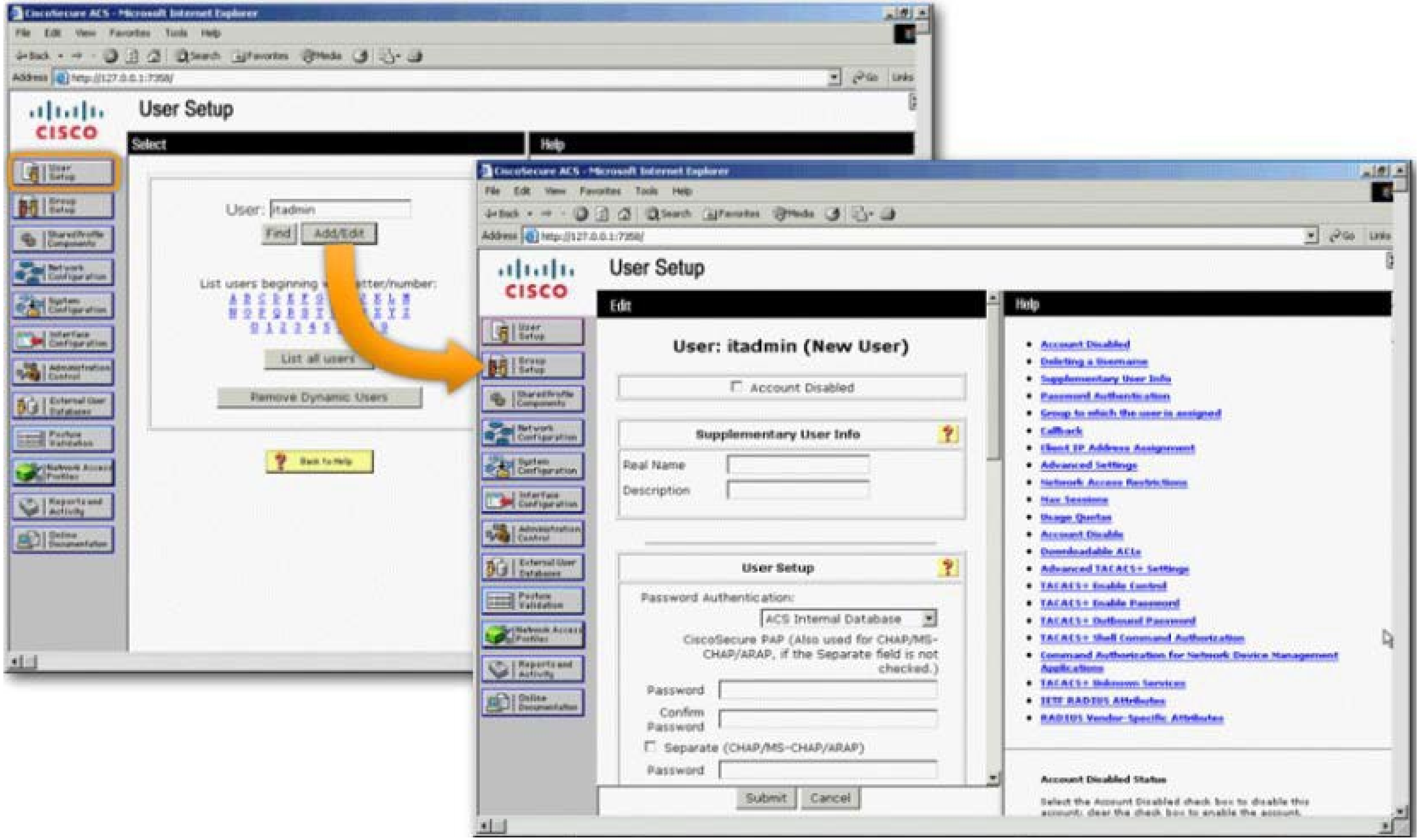
○ Deny

□ Command:

- Group Disabled
- Voice-over-IP (VoIP) Support
- Default Time-of-Day Access Settings
- Callback
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Enable Options
- Token Card Settings
- Password Aging Rules
- IP Assignment
- Downloadable ACLs
- TACACS+ Settings
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, ACS displays only the information for the current configuration. Specific Group Setup configuration options and security protocol attributes are displayed in Group Setup only in the following circumstances:

ACS User Setup



User: itadmin

List users beginning with letter/number:

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

User: itadmin (New User)

□ Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

□ Separate (CHAP/MS-CHAP/ARAP)

Password

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

VoDs

- ACSv5 Demo
  - http://www.cisco.com/assets/cdc_content_elements/flash/netman/acsv5tacacs/player.html

CONFIGURING SERVER BASED AAA AUTHENTICATION

CLI Configuration Steps

1. Enable AAA by using the global configuration command:
   - **`aaa new-model`**
2. Configure security protocol parameters:
   - Server IP address and Key
3. Define the authentication method lists using:
   - **`aaa authentication`**
4. Apply the method lists to a particular interface or line (if required).
5. Optionally configure authorization using the global command:
   - **`aaa authorization`**
6. Optionally configure accounting using the global command:
   - **`aaa accounting`**

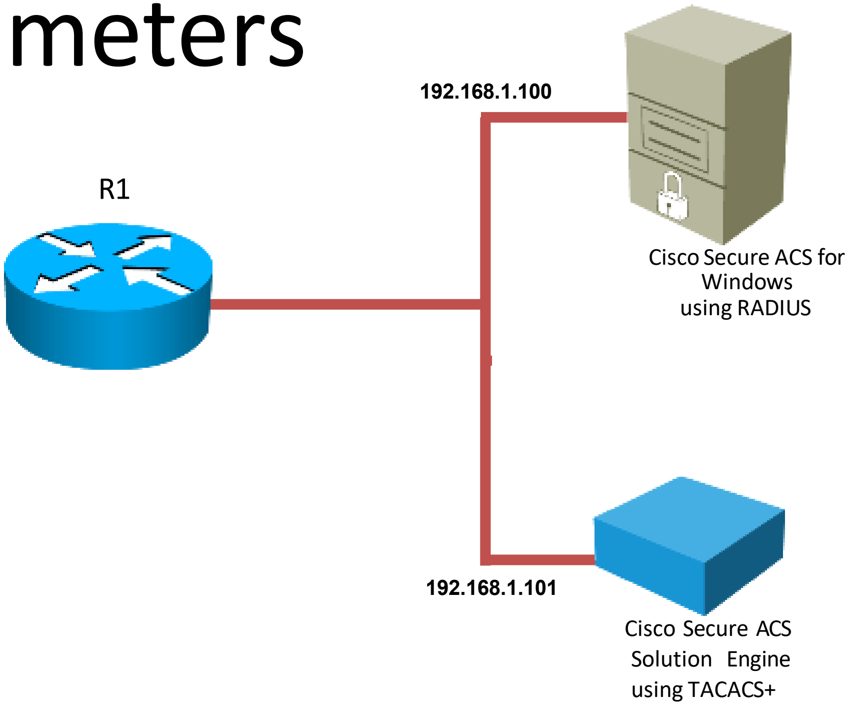
Server-Based AAA Authentication

1. Specify the location of the AAA server that will provide AAA services.
2. Configure the encryption key needed to encrypt the data transfer between the network access server and Cisco Secure ACS.

AAA Configuration Commands

Command	Description
tacacs-server host *ip-address* **single-connection**	• Indicates the address of the Cisco Secure ACS server and specifies use of the TCP single-connection feature of Cisco Secure ACS. • This feature improves performance by maintaining a single TCP connection for the life of the session between the network access server and the Cisco Secure ACS server, rather than opening and closing TCP connections for each session (the default).
tacacs-server key *key*	• Establishes the shared secret encryption key between the network access server and the Cisco Secure ACS server.
radius-server host *ip-address*	• Specifies a RADIUS AAA server.
radius-server key *key*	• Specifies an encryption key to be used with the RADIUS AAA server.

Configuring the AAA Server Parameters


192.168.1.100
R1
Cisco Secure ACS for Windows using RADIUS
192.168.1.101
Cisco Secure ACS Solution Engine using TACACS+

```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs-server host 192.168.1.101 single-connection
R1(config)# tacacs-server key TACACS+Pa55w0rd
R1(config)#
R1(config)# radius-server host 192.168.1.100
R1(config)# radius-server key RADIUS-Pa55w0rd
R1(config)#
```

Define Method Lists

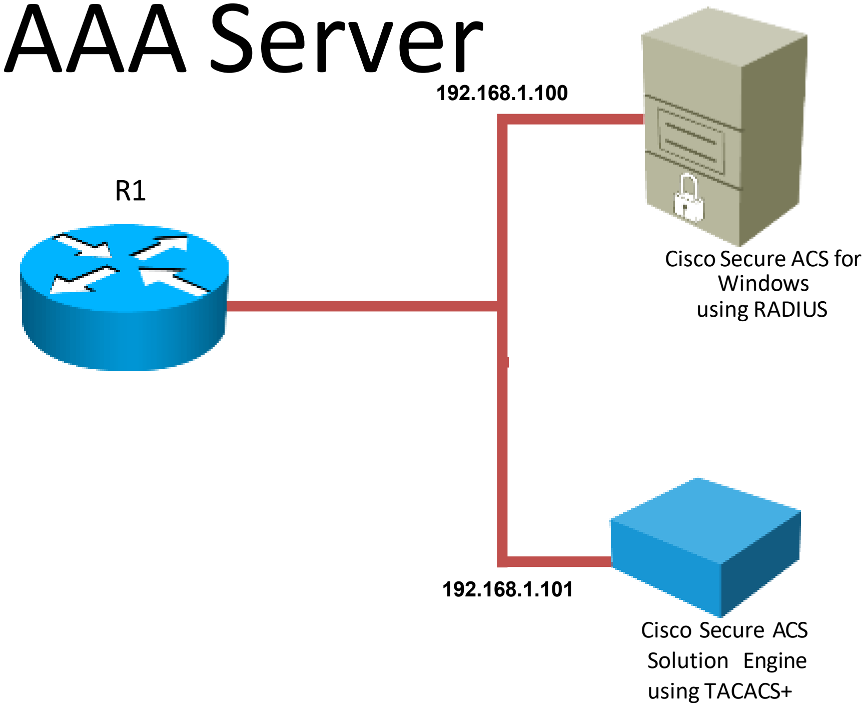
```
R1(config)# aaa authentication login default ?
  enable         Use enable password for authentication.
  group          Use Server-group
  krb5           Use Kerberos 5 authentication.
  krb5-telnet    Allow logins only if already authenticated via Kerberos V
                 Telnet.
  line           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.

R1(config)# aaa authentication login default group
```

AAA Authentication Commands

```
R1(config)# aaa authentication login default group tacacs+ group radius local-case
```

Parameter	Description
default	• This command creates a default that is automatically applied to all lines and interfaces, specifying the method or sequence of methods for authentication.
group *group-name* **group radius** **group tacacs+**	• These methods specify the use of an AAA server. • The group radius and group tacacs+ methods refer to previously defined RADIUS or TACACS+ servers. • The group-name string allows the use of a predefined group of RADIUS or TACACS+ servers for authentication (created with the aaa group server radius or aaa group server tacacs+ command).

Configuring the AAA Server


192.168.1.100
R1
Cisco Secure ACS for Windows using RADIUS
192.168.1.101
Cisco Secure ACS Solution Engine using TACACS+

```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs-server host 192.168.1.101 single-connection
R1(config)# tacacs-server key TACACS+Pa55w0rd
R1(config)#
R1(config)# radius-server host 192.168.1.100
R1(config)# radius-server key RADIUS-Pa55w0rd
R1(config)#
R1(config)# aaa authentication login default group tacacs+ group radius local-case
R1(config)#
```

Troubleshooting Server-Based Authentication

```
R1# debug aaa authentication
AAA Authentication debugging is on
R1#
14:01:17: AAA/AUTHEN (567936829): Method=TACACS+
14:01:17: TAC+: send AUTHEN/CONT packet
14:01:17: TAC+ (567936829): received authen response status = PASS
14:01:17: AAA/AUTHEN (567936829): status = PASS
```

Troubleshooting Server-Based Authentication

```
R1# debug tacacs ?
  accounting      TACACS+ protocol accounting
  authentication  TACACS+ protocol authentication
  authorization   TACACS+ protocol authorization
  events          TACACS+ protocol events
  packet          TACACS+ packets
  <cr>
```

```
R1# debug radius ?
  accounting      RADIUS accounting packets only
  authentication  RADIUS authentication packets only
  brief           Only I/O transactions are recorded
  elog            RADIUS event logging
  failover        Packets sent upon fail-over
  local-server    Local RADIUS server
  retransmit      Retransmission of packets
  verbose         Include non essential RADIUS debugs
  <cr>

R1# debug radius
```

Troubleshooting Server-Based Authentication

```
R1# debug tacacs
TACACS access control debugging is on
R1#

13:53:35: TAC+: Opening TCP/IP connection to 192.168.1.101 using source 192.48.0.79
13:53:35: TAC+: Sending TCP/IP packet number 416942312-1 to 192.168.1.101
(AUTHEN/START)
13:53:35: TAC+: Receiving TCP/IP packet number 416942312-2 from 192.168.60.15
13:53:35: TAC+ (416942312): received authen response status = GETUSER
13:53:37: TAC+: send AUTHEN/CONT packet
13:53:37: TAC+: Sending TCP/IP packet number 416942312-3 to 192.168.1.101
(AUTHEN/CONT)
13:53:37: TAC+: Receiving TCP/IP packet number 416942312-4 from 192.168.60.15
13:53:37: TAC+ (416942312): received authen response status = GETPASS
13:53:38: TAC+: send AUTHEN/CONT packet
13:53:38: TAC+: Sending TCP/IP packet number 416942312-5 to 192.168.1.101
(AUTHEN/CONT)
13:53:38: TAC+: Receiving TCP/IP packet number 416942312-6 from 192.168.60.15
13:53:38: TAC+ (416942312): received authen response status = FAIL
13:53:40: TAC+: Closing TCP/IP connection to 192.168.60.15
```

SERVER BASED AUTHORIZATION

Authorization

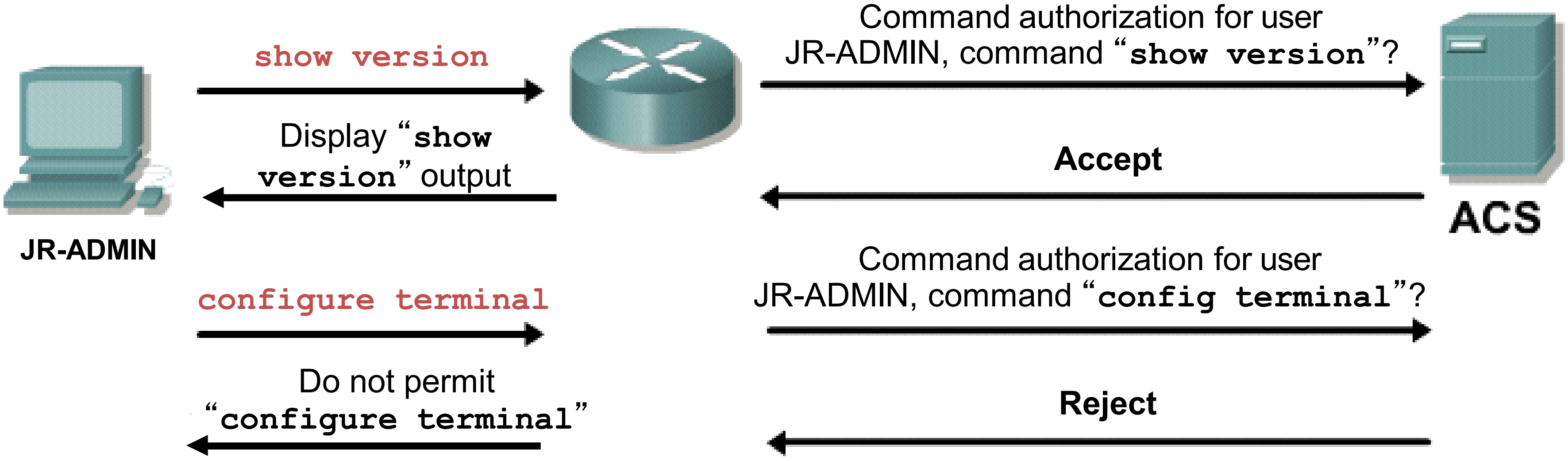
- Use to limit the services available to a user.

- Router uses the user's profile information, located either in the local user database or on the security server, to configure the user's session.
  - User is then granted access to a requested service only if the information in the user profile allows it.

```
Router(config)#
```

```
aaa authorization type { default | list-name } method1 … [method4]
```

Command Authorization



show version

Display "**show version**" output

Command authorization for user JR-ADMIN, command "**show version**"?

Accept

configure terminal

Do not permit "**configure terminal**"

Command authorization for user JR-ADMIN, command "**config terminal**"?

Reject

Configuring Authorization Type

```
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).
  ipmobile         For Mobile IP services.
  multicast        For downloading Multicast configurations from an AAA server
  network          For network services. (PPP, SLIP, ARAP)
  prepaid          For diameter prepaid services.
  reverse-access   For reverse access connections
  template         Enable template authorization
R1(config)# aaa authorization exec ?
  WORD     Named authorization list.
  default  The default authorization list.
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.
```

Configuring Authorization

```
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 authentication login TELNET-LOGIN local-case


R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET-LOGIN
R1(config-line)# ^Z
```

SERVER BASED ACCOUNTING

Accounting

- Defines the way accounting will be performed and the sequence in which they are performed.
- Named lists enable you to designate a particular security protocol to be used on specific lines or interfaces for accounting services.

```
Router(config)#
```

```
aaa accounting type { default | list-name } record-type method1 … [method2]
```

Configuring Accounting

```
R1(config)# aaa accounting ?
  auth-proxy         For authentication proxy events.
  commands           For exec (shell) commands.
  connection         For outbound connections. (telnet, rlogin)
  delay-start        Delay PPP Network start record until peer IP address is known.
  exec               For starting an exec (shell).
  gigawords          64 bit interface counters to support Radius attributes 52 & 53.
  multicast          For multicast accounting.
  nested             When starting PPP from EXEC, generate NETWORK records before EXEC-STOP
record.
  network            For network services. (PPP, SLIP, ARAP)
  resource           For resource events.
  send               Send records to accounting server.
  session-duration   Set the preference for calculating session durations
  suppress           Do not generate accounting records for a specific type of user.
  system             For system events.
  update             Enable accounting update records.
R1(config)# aaa accounting exec ?
  WORD     Named Accounting list.
  default  The default accounting list.
R1(config)# aaa accounting exec default ?
  none        No accounting.
  start-stop  Record start and stop without waiting
  stop-only   Record stop when service terminates.
R1(config)# aaa accounting exec default start-stop?
  broadcast  Use Broadcast for Accounting
  group      Use Server-group
R1(config)# aaa accounting exec default start-stop group ?
  WORD     Server-group name
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.
```

Configuring Accounting Sample Config

```
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 authentication login TELNET-LOGIN local-case
R1(config)# aaa authorization exec group tacacs+
R1(config)# aaa authorization network group tacacs+
R1(config)# aaa accounting exec start-stop group tacacs+
R1(config)# aaa accounting network start-stop group tacacs+
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET-LOGIN
R1(config-line)# ^Z
```