



Securing Device Access

Three Areas of Router Security

Physical Security

Router Operating
System and
Configuration File
Security

Router Hardening



Strong Passwords

Guidelines:

- Use a password length of 10 or more characters.
- Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces.
- Avoid passwords based on easily identifiable pieces of information.
- Deliberately misspell a password (Smith = Smyth = 5mYth).
- Change passwords often.
- Do not write passwords down and leave them in obvious places.

Weak Password	Why it is Weak	Strong Password	Why it is Strong
secret	Simple dictionary password	b67n42d39c	Combines alphanumeric characters
smith	Mother's maiden name	12^h u4@1p7	Combines alphanumeric characters, symbols, and includes a space
toyota	Make of car		
bob1967	Name and birthday of user		
Blueleaf23	Simple words and numbers		

Increasing Access Security

```
R1(config)# security passwords min-length 10
R1(config)# service password-encryption
R1(config)# line vty 0 4
R1(config-line)# exec-timeout 3 30
R1(config-line)# line console 0
R1(config-line)# exec-timeout 3 30
```

```
R1(config)# service password-encryption
R1(config)# exit
R1# show running-config

<output omitted>

line con 0
  exec-timeout 3 30
  password 7 094F471A1A0A
  login
line aux 0
  exec-timeout 3 30
  password 7 094F471A1A0A
  login
line vty 0 4
  password 7 094F471A1A0A
  login
```

Cisco Cracker

094F471A1A0A

Crack it

Password = Cisco

Secret Password Algorithms

Guidelines:

- Configure all secret passwords using type 8 or type 9 passwords
- Use the enable algorithm-type command syntax to enter an unencrypted password

```
Router(config) #
```

```
enable algorithm-type {md5 | scrypt | sha256 } secret unencrypted-password
```

- Use the username name algorithm-type command to specify type 9 encryption

```
Router(config) #
```

```
username name algorithm-type {md5 | scrypt | sha256 } secret unencrypted-password
```

Securing Line Access

```
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# line con 0
R1(config-line)# no password
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line aux 0
R1(config-line)# no password
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
```

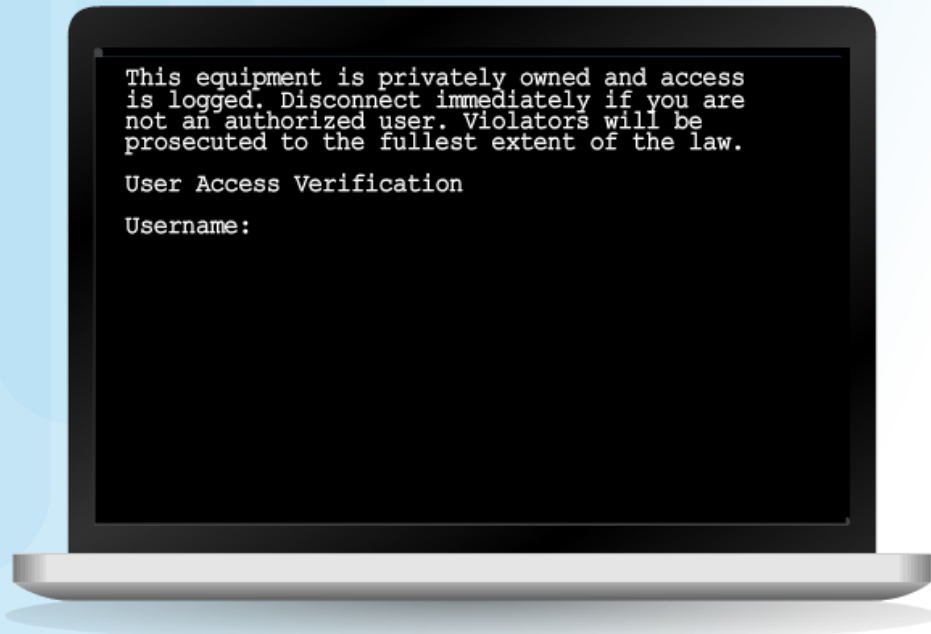
Enhancing the Login Process

Virtual login security enhancements:

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

```
R1(config)#
```

```
banner {motd | exec | login} delimiter message delimiter
```



```
This equipment is privately owned and access  
is logged. Disconnect immediately if you are  
not an authorized user. Violators will be  
prosecuted to the fullest extent of the law.
```

```
User Access Verification
```

```
Username:
```

Configuring Login Enhancement Features

R1(config) #

```
login block-for seconds attempts tries within seconds
```

R1(config) #

```
login quiet-mode access-class {acl-name|acl-number}
```

R1(config) #

```
login delay seconds
```

R1(config) #

```
login on-success log [every login]
```

R1(config) #

```
login on-failure log [every login]
```


Enable Login Enhancements

Command Syntax: login block-for

```
router(config)#
```

```
login block-for seconds attempts tries within seconds
```

```
R1(config)# login block-for 120 attempts 5 within 60
```

Logging Failed Attempts

Generate Login Syslog Messages

```
R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]
R1(config)# security authentication failure rate threshold-rate log
```

Example: show login failures

```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures
```

Username	SourceIPAddr	lPort	Count	TimeStamp
admin	1.1.2.1	23	5	15:38:54 UTC Wed Dec 10 2008
Admin	10.10.10.10	23	13	15:58:43 UTC Wed Dec 10 2008
admin	10.10.10.10	23	3	15:57:14 UTC Wed Dec 10 2008
cisco	10.10.10.10	23	1	15:57:21 UTC Wed Dec 10 2008

```
R1#
```

Configuring SSH

Example SSH Configuration

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

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Feb 16 21:18:41.977: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# ip ssh version 2
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
```

Connecting to an SSH-Enabled Router

Two ways to connect:

- **Enable SSH and use a Cisco router as an SSH server or SSH client.**
- **Use an SSH client running on a host, such as PuTTY, OpenSSH, or TeraTerm.**

Limiting Command Availability

Privilege levels:

- Level 0: Predefined for user-level access privileges.
- Level 1: Default level for login with the router prompt
- Level 2-14: May be customized for user-level privileges.
- Level 15: Reserved for the enable mode privileges.

Levels of access commands:

User EXEC mode (privilege level 1)

- Lowest EXEC mode user privileges
- Only user-level command available at the router> prompt

Privileged EXEC mode (privilege level 15)

- All enable-level commands at the router# prompt

Privilege Level Syntax

```
Router(config) #
```

```
privilege mode {level level | reset} command
```

Command

Description

<i>mode</i>	Specifies the configuration mode. Use the privilege ? command to see a complete list of router configuration modes available on your router.
level	(Optional) Enables setting a privilege level with a specified command.
<i>level</i>	(Optional) The privilege level that is associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15.
reset	(Optional) Resets the privilege level of a command.
<i>command</i>	(Optional) Argument to use when you want to reset the privilege level.

Configuring and Assigning Privilege Levels

```
R1# conf t
R1(config)# !Level 5 and SUPPORT user configuration
R1(config)# privilege exec level 5 ping
R1(config)# enable algorithm-type scrypt secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 algorithm-type scrypt
secret cisco5
R1(config)# !Level 10 and JR-ADMIN user configuration
R1(config)# privilege exec level 10 reload
R1(config)# enable algorithm-type scrypt secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 algorithm-type scrypt
secret cisco10
R1(config)# !Level 15 and ADMIN user configuration
R1(config)# enable algorithm-type scrypt secret level 15 cisco123
R1(config)# username ADMIN privilege 15 algorithm-type scrypt secret
cisco123
```

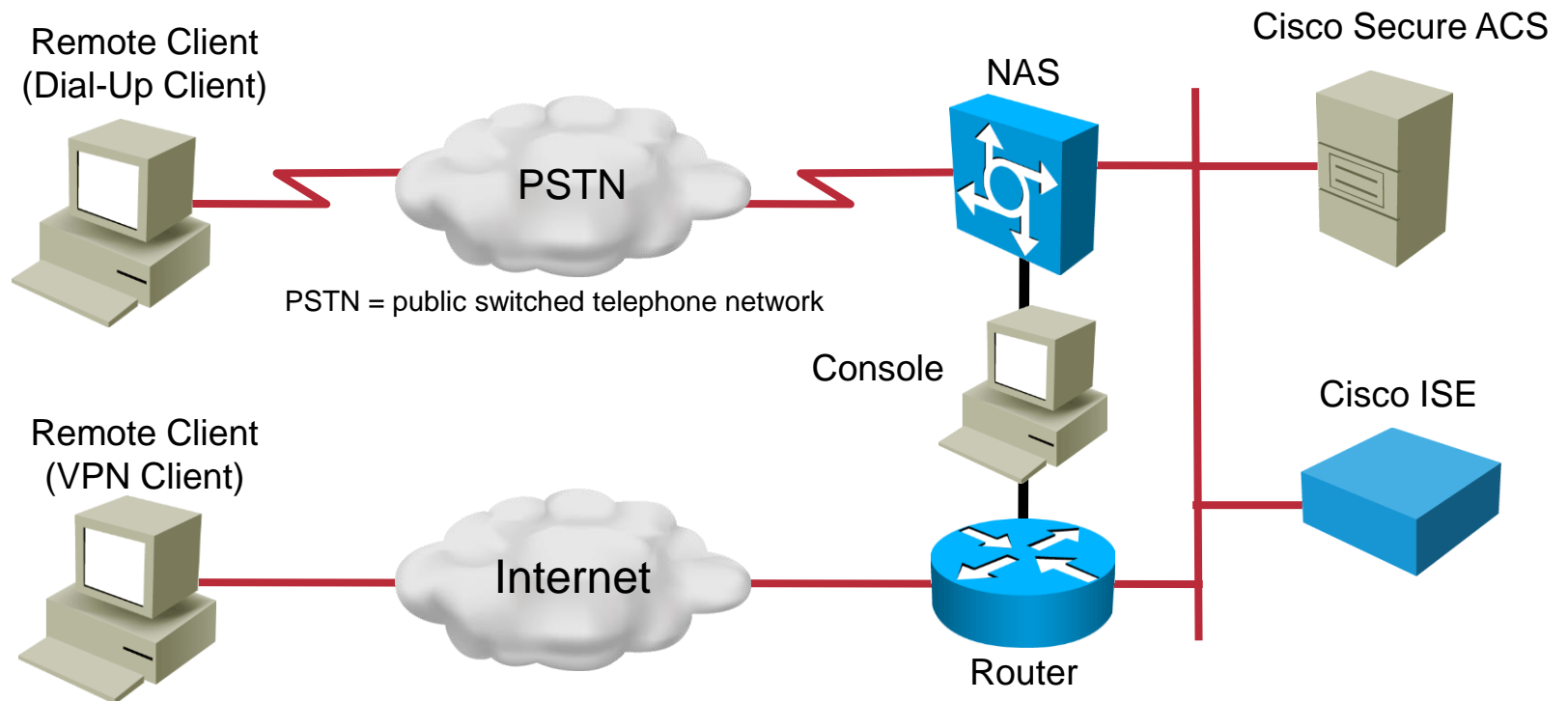


Configuring AAA on a Cisco Router

AAA Model—Network Security Architecture

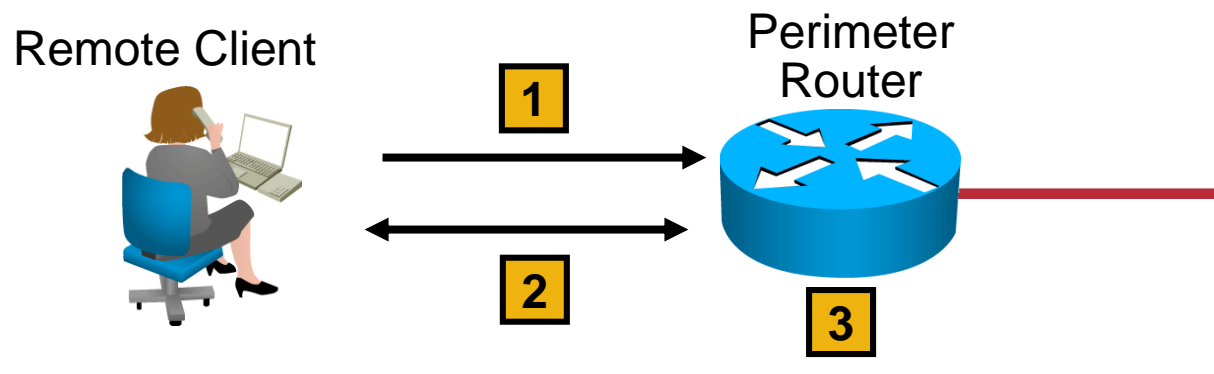
- Authentication
 - Who are you?
 - “I am user **student** and my password **validateme** proves it.”
- Authorization
 - What can you do? What can you access?
 - “User **student** can access host **serverXYZ** using Telnet.”
- Accounting
 - What did you do? How long did you do it?
How often did you do it?
 - “User **student** accessed host **serverXYZ** using Telnet for **15 minutes**.”

Implementing Cisco AAA



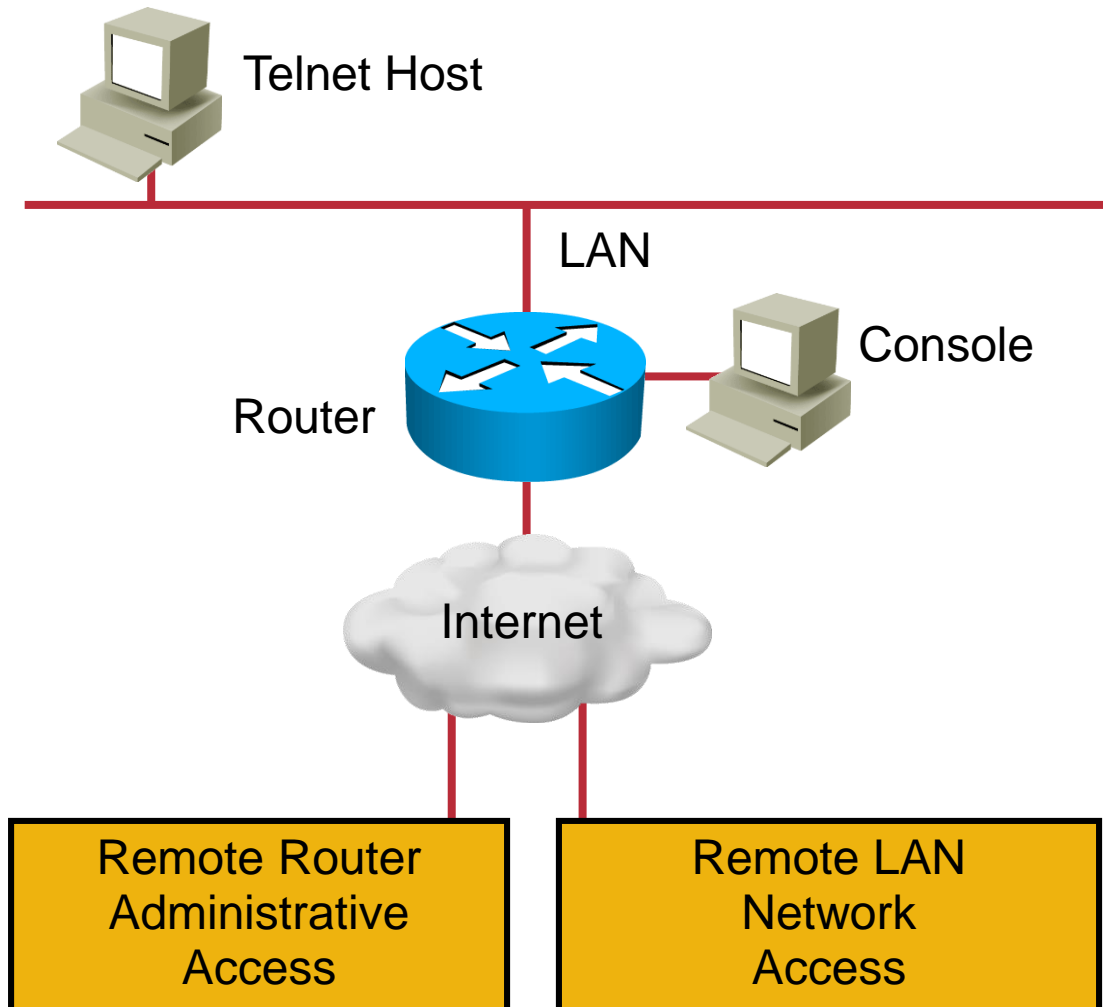
- **Administrative access: console, Telnet, and auxiliary access**
- **Remote user network access: dial-up or VPN access**

Implementing Authentication Using Local Services



1. The client establishes a connection with the router.
2. The router prompts the user for a username and password.
3. The router authenticates the username and password in the local database. The user is authorized to access the network based on information in the local database.

Authenticating Router Access



Router Local Authentication Configuration Steps

The following are the general steps to configure a Cisco router to support local authentication:

- **Add usernames and passwords to the local router database**
- **Enable AAA globally on the router**
- **Configure AAA parameters on the router**
- **Confirm and troubleshoot the AAA configuration**

AAA Configuration Example

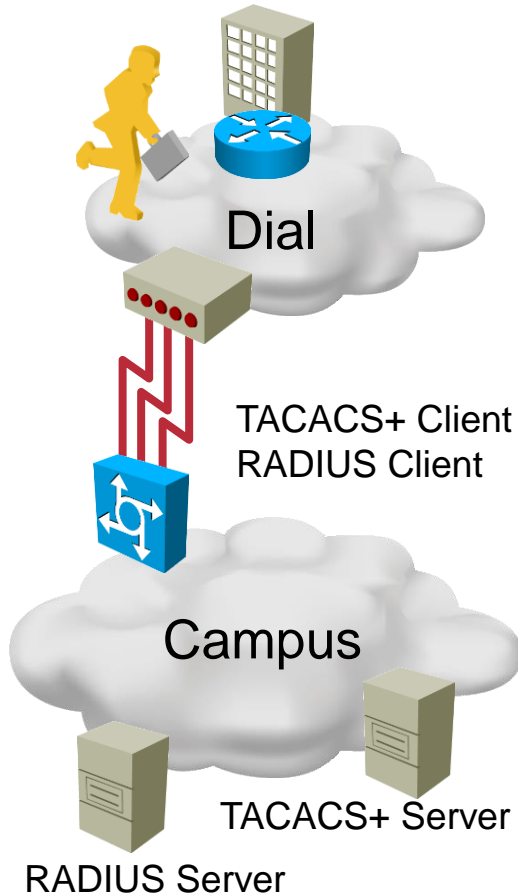
```
aaa new-model
aaa authentication login default local

enable secret 5 $1$x1EE$33AXd2VTVvhhbWL0A37tQ3.
enable password 7 15141905172924
!
username admin1 password 7 14161606050A7B7974786B
username admin2 secret 5 $1$ErWl$b5rDNK7Y5RHkxX/Ks7Hr00
!
```



Configuring AAA on a Cisco Router Using an External Database

TACACS+/RADIUS Comparison



	TACACS+	RADIUS
Functionality	Separates AAA	Combines authentication and authorization
Standard	Mostly Cisco supported	Open/RFC
Transport Protocol	TCP	UDP
CHAP	Bidirectional	Unidirectional
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

Applying an Authentication Policy

```
Router(config)#line vty 0 4  
Router(config-line)#login authentication TACACS_SERVER
```


AAA Configuration for TACACS+ Example

```
aaa new-model
!
aaa authentication login TACACS_SERVER tacacs+ local
aaa authorization exec tacacs+
aaa accounting exec start-stop tacacs+
!
!
tacacs-server host 10.0.1.11
tacacs-server key ciscosecure
!
line vty 0 4
  login authentication TACACS_SERVER
```

debug tacacs

```
router#debug tacacs
14:00:09: TAC+: Opening TCP/IP connection to 10.1.1.4/49
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 10.1.1.4/49
(AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 10.1.1.4/49
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 10.1.1.4/49
(AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 10.1.1.4/49
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 10.1.1.4/49
(AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 10.1.1.4/49
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 10.1.1.4/49
```

