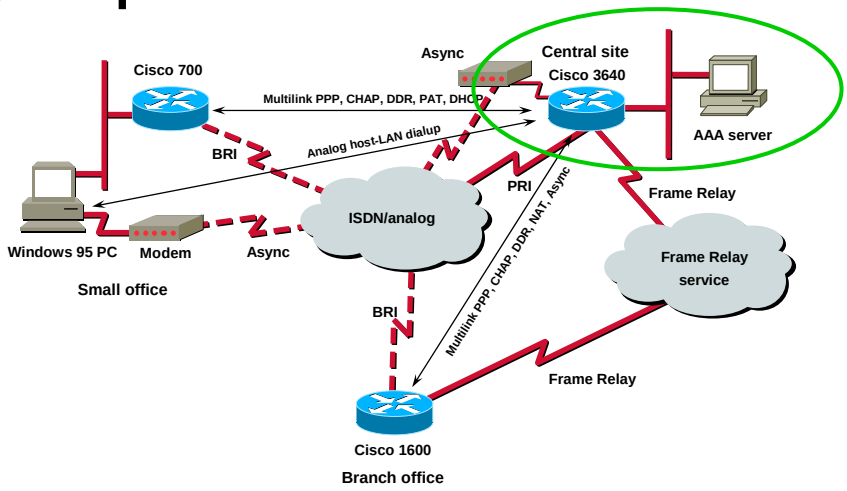
Chapter 12. AAA

Objectives

Upon completion of this chapter, you will be able to perform the following tasks:

- **Describe CiscoSecure features and operations**
- **Configure a router with AAA commands**
- **Use a configured AAA server to control access in a remote access network**

Chapter Activities

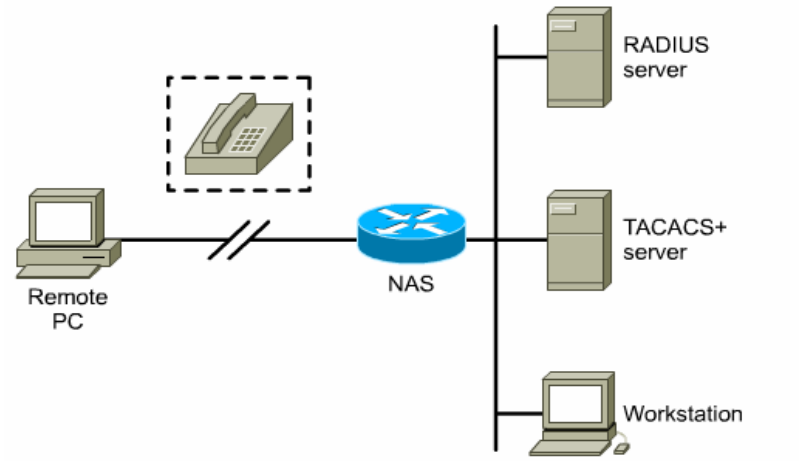


AAA

Advantages of using AAA for Authentication

- AAA provides scalability
- AAA supports standardized security protocols – TACACS+, RADIUS, and Kerberos
  - TACACS+ (Terminal Access Controller Access Control System Plus)
  - RADIUS (Remote Authentication Dial-In User Service)
- AAA allows you to configure multiple backup systems

Security Protocols



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

TACACS+ and RADIUS Compared

TACACS+	RADIUS
Cisco-proprietary enhancement to original TACACS protocol	Open standard developed by Livingston Enterprises
Supports authentication, authorization, and accounting functions	Supports authentication, authorization, and accounting functions
Uses the AAA architecture, which separates authentication, authorization, and accounting	Combines the functions of authentication and authorization
Provides two ways to control the authorization of router commands: on a per-user or per-group basis	Does not allow administrators to control which commands can be executed on a router
Uses TCP	Uses UDP
Normal operation will fully encrypt the body of then packet for more secure communications	Encrypts only the password in the access-request packet. Information such as username, authorization services, and accounting, could be captured by a third party
Offers multiprotocol support	Does not support ARA access, NetBIOS, NASI, or X.25 PAD connections

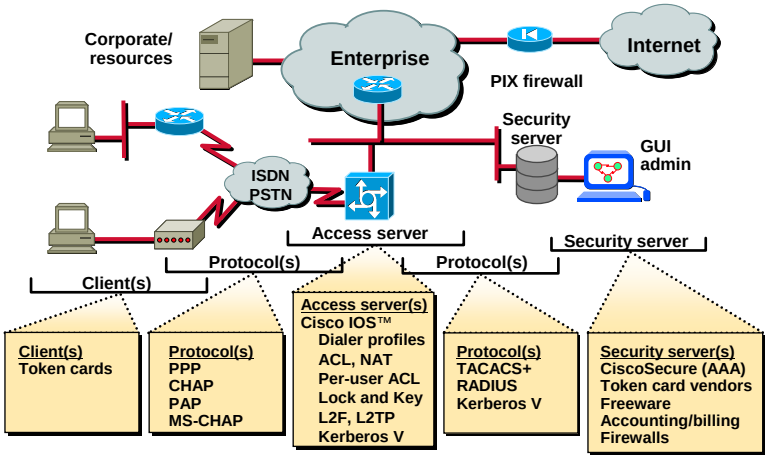
security protocols:

•**TACACS+** - A security application used with AAA that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities.

•**RADIUS** - A distributed client/server system used with AAA that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

•**Kerberos** - A secret-key network authentication protocol used with AAA that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources. Kerberos is based on the concept of a trusted third party that performs secure verification of users and services. The primary use of Kerberos is to verify that users and the network services they use are really who and what they claim to be. To accomplish this, a trusted Kerberos server issues tickets to users. These tickets, which have a limited lifespan, are stored in a user's credential cache and can be used in place of the standard username and password authentication mechanism.

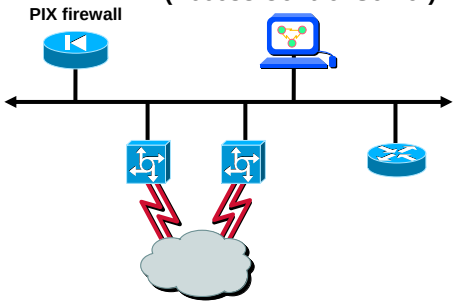
Cisco Security Options Overview



Part of the Solution

CiscoSecure ACS

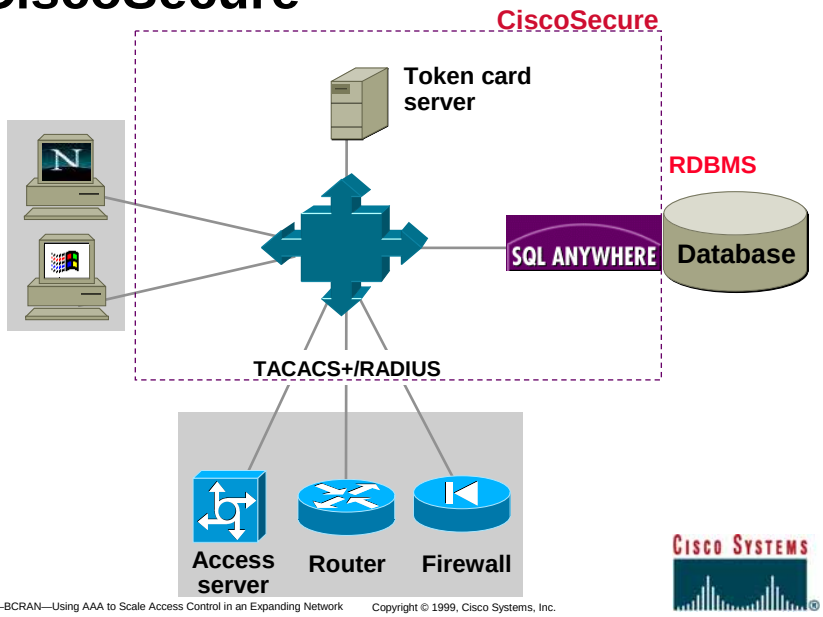
(Access Control Server)



- **Provides authentication, authorization, and accounting (AAA) for networks**

Cisco Systems

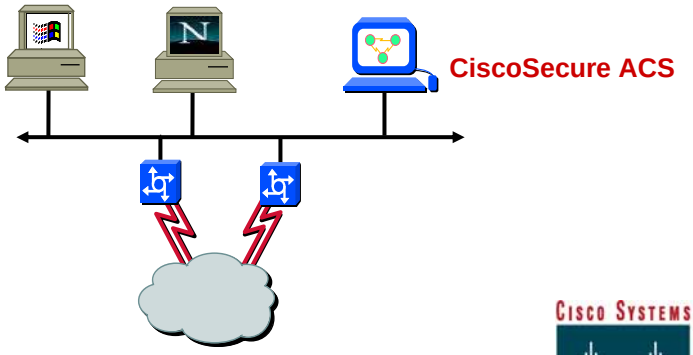
CiscoSecure



Cisco Systems

GUI Client Supported

- CiscoSecure administrator “GUI client”
  - Netscape
  - Internet Explorer



AAA Overview and Configuration

- AAA definition
- AAA operation
- Router access modes

AAA Definition

- Authentication
  - Who are you?
- Authorization
  - What can you do?
- Accounting
  - Who were you?
  - What did you do and how long did you do it?

Router Access Modes

Modes	Router Ports	AAA Command Element
Character mode (line mode or interactive login)	tty, vty, aux, con	*login, exec, nasi connection, arap, enable, command*
Packet mode (interface mode or link protocol session)	async, group-async, BRI, PRI, serial, dialer profiles, dialer rotaries	*ppp, network, arap*

Enabling AAA and Identifying the Server

```
Router(config)#aaa new-model
Router(config)#tacacs-server host 192.168.229.76
                    single-connection
Router(config)#tacacs-server key shared1
```

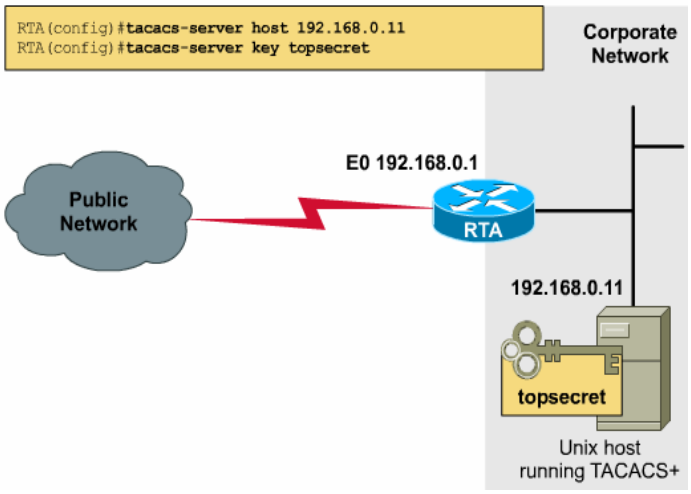
or

```
Router(config)#aaa new-model
Router(config)#radius-server host 192.168.229.76
Router(config)#radius-server key shared1
```

- **TACACS+ or RADIUS**

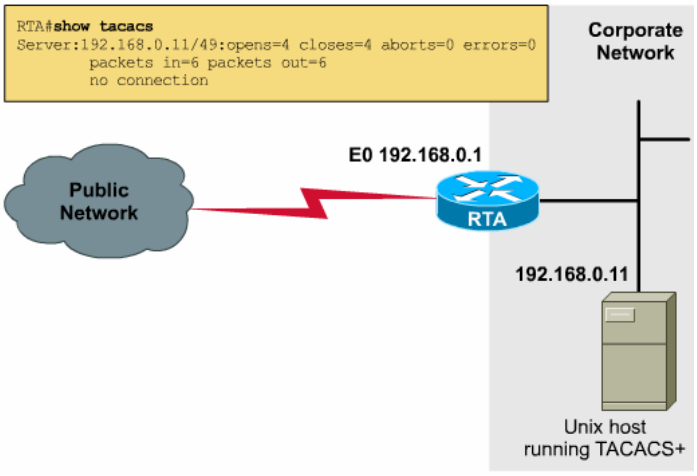
Configuring a TACACS+ Client

```
RTA(config)#tacacs-server host 192.168.0.11
RTA(config)#tacacs-server key topsecret
```



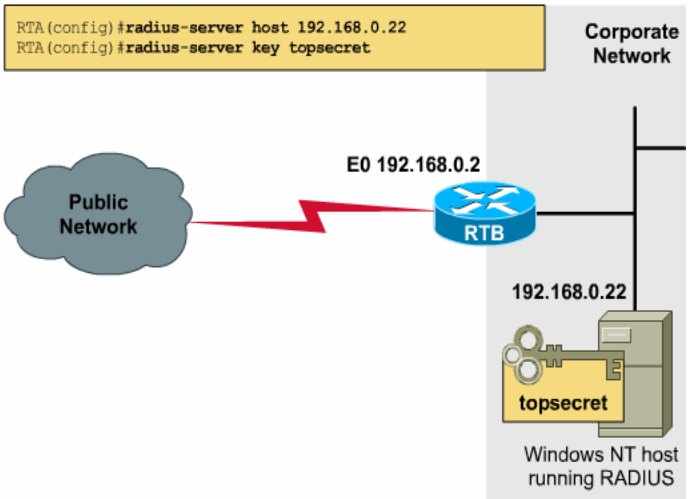
Using the show tacacs Command

```
RTA#show tacacs
Server:192.168.0.11/49:opens=4 closes=4 aborts=0 errors=0
       packets in=6 packets out=6
       no connection
```



Configuring a RADIUS Client

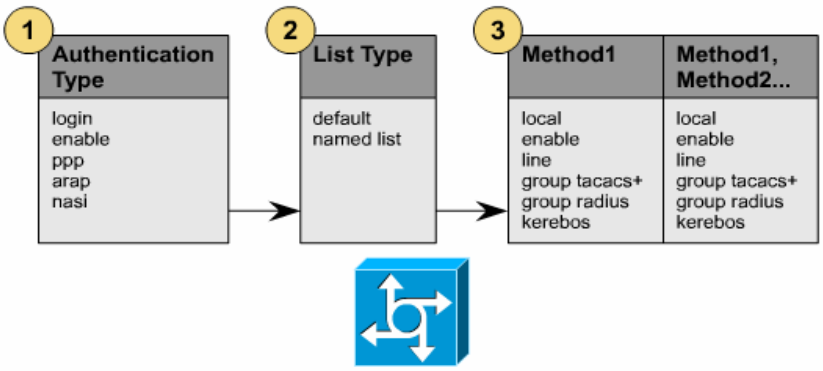
```
RTA(config)#radius-server host 192.168.0.22
RTA(config)#radius-server key topsecret
```



The aaa authentication Command Authentication Types

Keyword	Description
arap	Sets authentication method for ARAP
enable	Sets authentication method for privileged EXEC mode
login	Sets authentication method for logins on terminal lines, virtual terminal lines, and the console
nasi	Sets authentication method for NASI
ppp	Sets authentication method for any authentication protocol supported by PPP (CHAP, PAP, MS-CHAP)

Configuring AAA 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.

AAA Authentication Commands

Router(config)#aaa authentication
{login | enable | arap | ppp | nasi}
default | list-name}
***method1* [*method2* [*method3* [*method4*]]]**

enable line local none tacacs+ radius	enable line none tacacs+ radius	guest auth-guest line local tacacs+	if-needed krb5 local none tacacs+ radius	enable line local none tacacs+

Character Mode Login Example

```
Router(config)#aaa authentication login default tacacs+ local
Router(config)#aaa authentication login user tacacs+ local
Router(config)line con 0
Router(config-line)#login authentication user
Router(config-line)#line 1 48
Router(config-line)#login authentication user
Router(config-line)#line vty 0 4 (this implies “default” list)
```

- **Authentication commands**

AAA Authorization Commands


```
Router(config)#aaa authorization
{network | exec | commands level
                  | config-commands | reverse-access}
{if-authenticated | local | none | radius
                              | tacacs+ | krb5-instance}
```


Character Mode with Authorization Example

```
Router(config)#aaa new-model
Router(config)#aaa authen login default local
Router(config)#aaa authen enable default tacacs+ enable
Router(config)#aaa authorization exec tacacs+ local
Router(config)#aaa authorization command 1 tacacs+ local
Router(config)#aaa authorization command 15 tacacs+ local
```

Packet Mode Example

```
Router(config)#username admin password xxxxx
Router(config)#aaa authentication ppp default if-needed tacacs+
Router(config)#aaa authentication ppp user if-needed tacacs+
Router(config)#aaa authorization network tacacs+ if-authenticated
Router(config)#interface groupasync1
Router(config-if)#ppp authentication chap        (default list implied)
Router(config-if)#interface async16
Router(config-if)#ppp authentication chap user
Router(config-if)#line 1 16
```

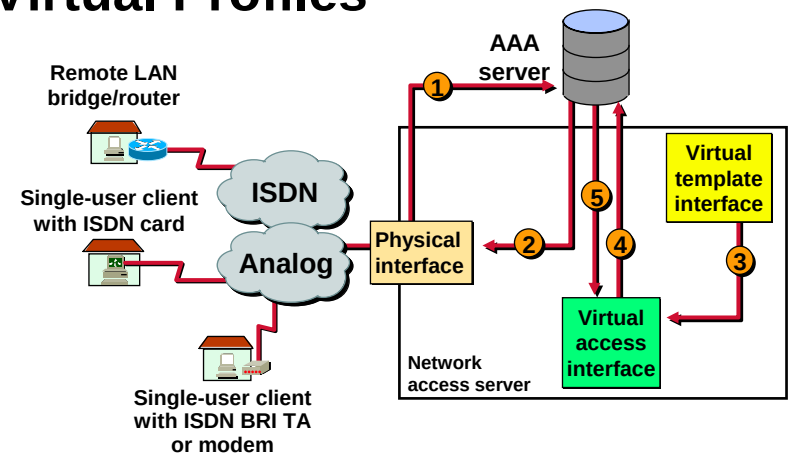

AAA Accounting Commands


```
Router(config)#aaa accounting
{command level | connection | exec | network | system}
{start-stop | stop-only | wait-start}
{tacacs+ | radius}
```

Accounting Example

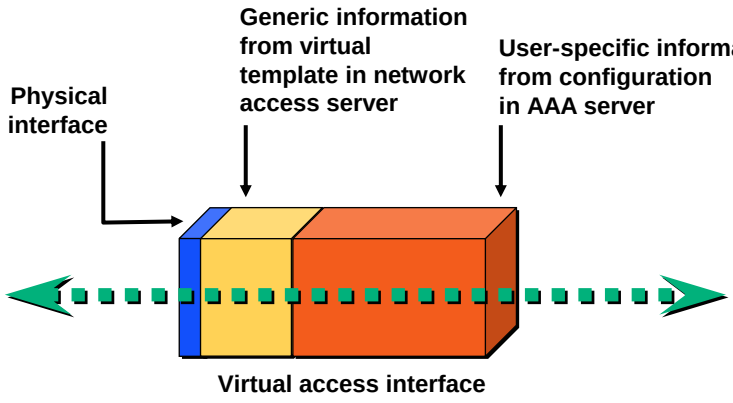
```
Router(config)#aaa accounting network start-stop tacacs+
Router(config)#aaa accounting exec start-stop tacacs+
Router(config)#aaa accounting command 15 start-stop tacacs+
Router(config)#aaa accounting connection start-stop tacacs+
Router(config)#aaa accounting system wait-start tacacs+
```


Virtual Profiles



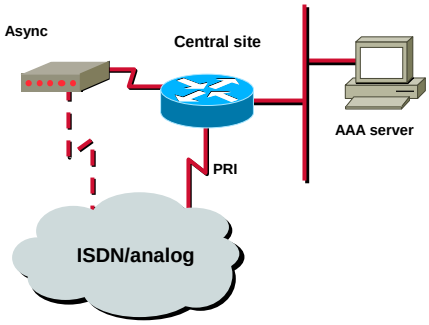
- **Profiles stored in centralized server**

Building a Virtual Profile



- Components of a virtual access interface

Laboratory Exercise: Visual Objective



Summary

After completing this chapter, you should be able to perform the following tasks:

- **Describe CiscoSecure features and operations**
- **Configure a router with AAA commands**
- **Use a configured AAA server to control access in a remote access network**

Review Questions

- **What is authentication?**
- **What is authorization?**
- **What is accounting in regard to a dialup networking environment?**

Blank Page For IG Pagination