

Network Security 1

Module 5 – Cisco Secure Access Control Server



Learning Objectives



Cisco.com

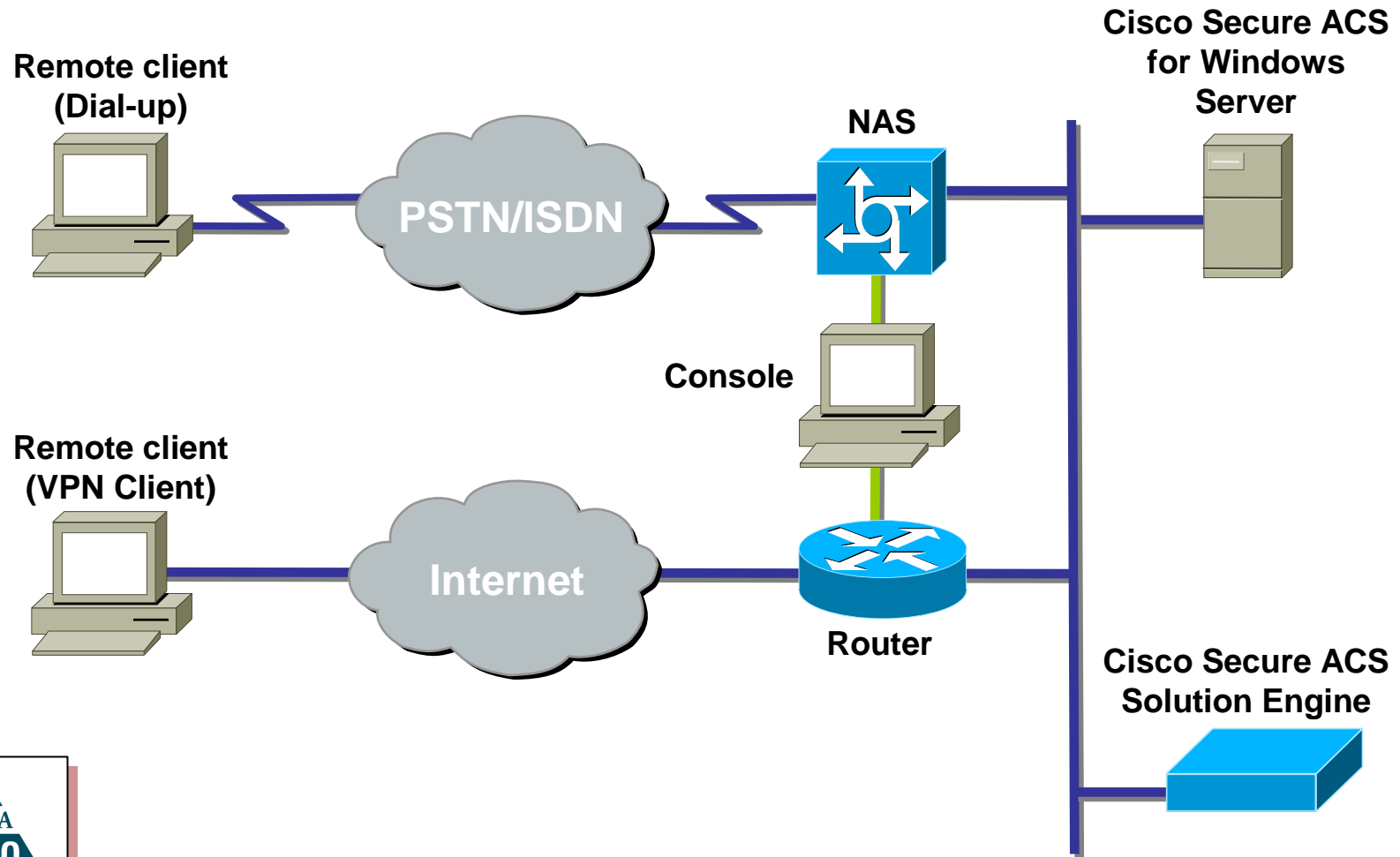
- 5.1 Cisco Secure Access Control Server for Windows
- 5.2 Configuring RADIUS and TACACS+ with CSACS



Cisco Secure ACS Products



Cisco.com



What Is Cisco Secure ACS for Windows Server?



Cisco.com

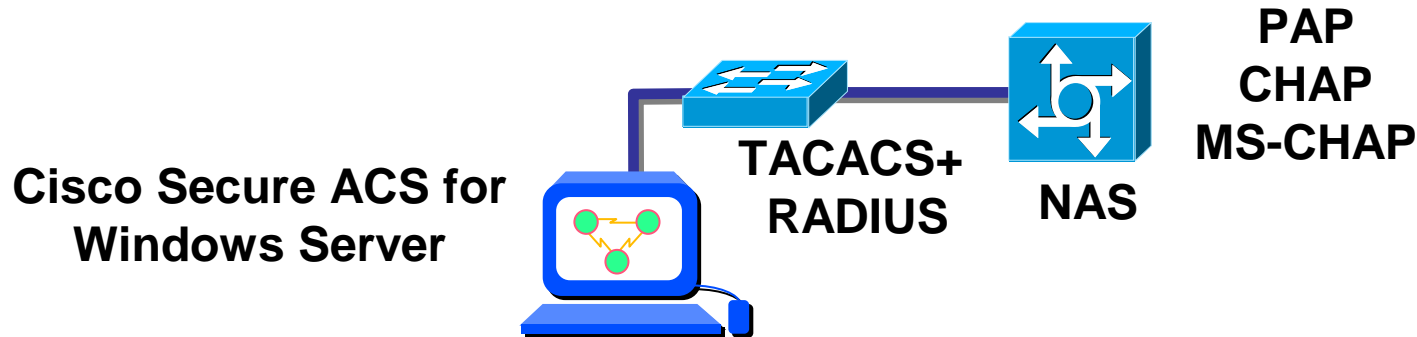
- Provides AAA services to network devices that function as AAA clients, such as routers, NASs, PIX Security Appliances, or VPN Concentrators
- Helps centralize access control and accounting, in addition to router and switch access management
- Allows network administrators to quickly administer accounts and globally change levels of service offerings for entire groups of users
- Uses the TACACS+ and RADIUS protocols to provide AAA services that ensure a secure environment
- Can authenticate against many popular token servers



Cisco Secure ACS General Features



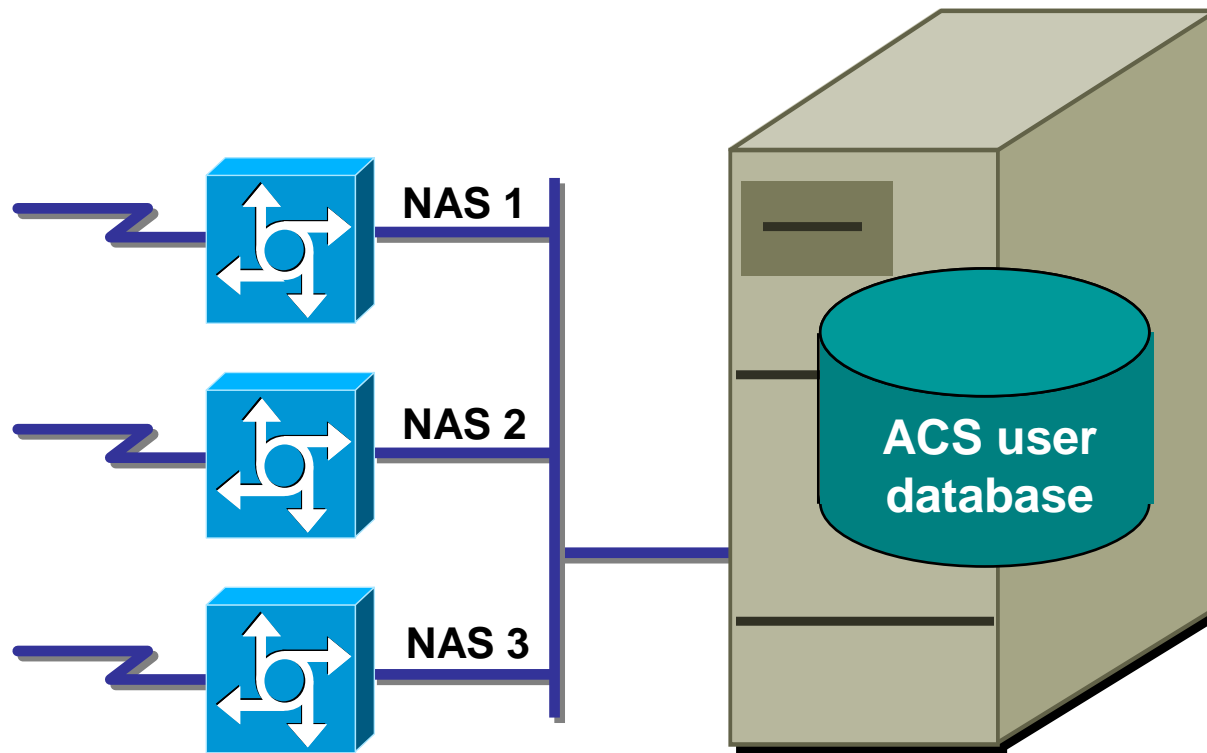
Cisco.com



- Uses TACACS+ or RADIUS between Cisco Secure ACS and NAS
- Allows authentication against Windows 2000 user database, ACS user database, token server, or other external databases
- Supports PAP, CHAP, and MS-CHAP authentication on the NAS



Cisco Secure ACS User Database



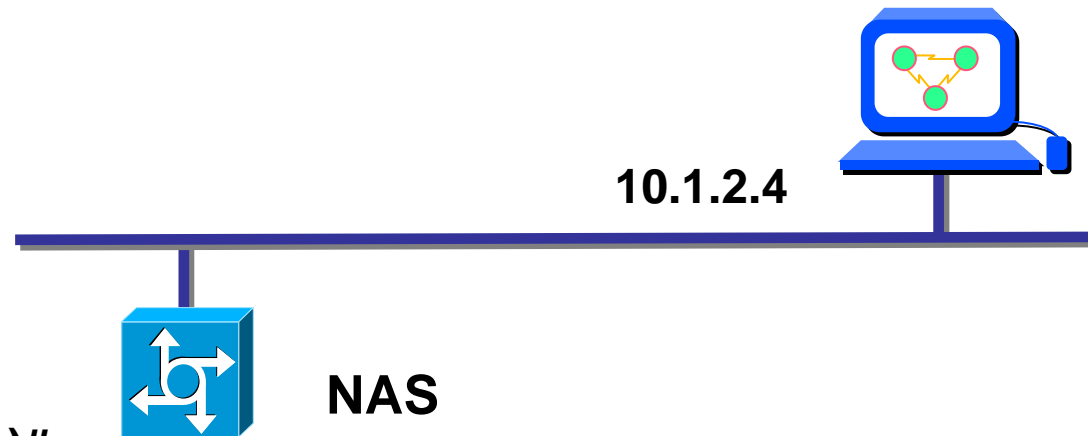
Module 5 – Cisco Secure Access Control Server

5.2 Configuring RADIUS and TACACS+ with CSACS



Globally Enable AAA

Cisco Secure ACS for Windows Server



```
router(config)#
```

```
aaa new-model
```

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



tacacs-server Commands

The two commands shown here can be used to share the key with all servers

or

This command can be used for a single server



```
router(config)#
```

```
tacacs-server key keystring
```

```
router(config)# tacacs-server key 2bor!2b@?
```

```
router(config)#
```

```
tacacs-server host ipaddress
```

```
router(config)# tacacs-server host 10.1.2.4
```

```
router(config)#
```

```
tacacs-server host ipaddress key keystring
```

```
router(config)# tacacs-server host 10.1.2.4 key  
2bor!2b@?
```

AAA Configuration Commands

router(config)#

```
aaa authentication {login | enable default | arap | ppp |  
  nasi} {default | list-name} method1 [method2 [method3  
  [method4]]]
```

router(config)#

```
aaa authorization {network | exec | commands level | reverse-  
  access} {default | list-name}  
  {if-authenticated | local | none | radius | tacacs+ | krb5-  
  instance}
```

router(config)#

```
aaa accounting {system | network | exec | connection |  
  commands level}{default | list-name} {start-stop | wait-  
  start | stop-only | none} [method1 [method2]]
```



aaa authentication login syntax

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in.
method	Specifies at least one of the following keywords.
enable	Uses the enable password for authentication.
krb5	Uses Kerberos 5 for authentication.
krb5-telnet	Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router.
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.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ commands.



RADIUS Server Command

The two commands shown here can be used to share the key with all servers

```
router(config)#
```

```
radius-server key keystring
```

```
router(config)# radius-server key 2bor!2b@?
```

```
router(config)#
```

```
radius-server host {host-name | ipaddress}
```

```
router(config)# radius-server host 10.1.2.4
```

This command can be used for a single server

```
router(config)#
```

```
radius-server host ipaddress key keystring
```

```
router(config)# radius-server host 10.1.2.4 key  
2bor!2b@?
```

