Minimizing Service Loss and Data Theft with AAA and Dot1x

Section 1:
Purpose of the AAA

Upon completion of this section, you should be able to:

- Explain why AAA is critical to network security.
- Describe the characteristics of AAA.

What Is AAA?

- **Authentication**
- **Authorization**
- **Accounting**

Authentication

For Identifying users including:

- login and password dialog
- challenge and response
- messaging support
- depending on the security protocol you select, encryption

Authorization

For Remote access control including:

- one-time authorization or authorization for each service
- per-user account list and profile
- user group support
- support of IP, IPX, ARA, and Telnet

Accounting

For collecting and sending security server information used for billing, auditing and reporting

- user identities
- start and stop times
- executed commands (such as PPP)
- number of packets
- number of bytes

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.”

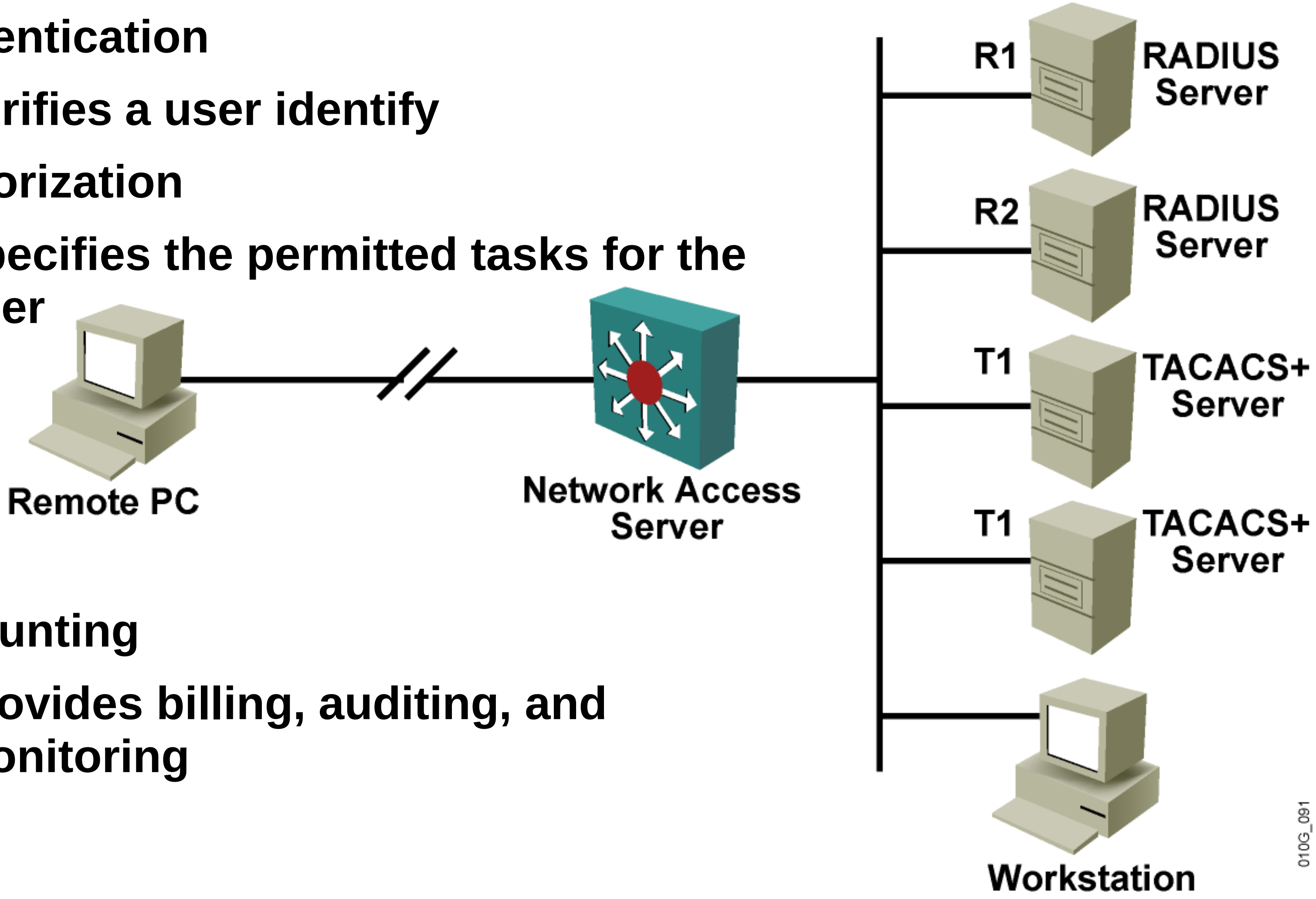
Section 2:
Local AAA and Server-Based AAA Authentication

Upon completion of this section, you should be able to:

- Configure AAA authentication, using the CLI, to validate users against a local database.
- Troubleshoot AAA authentication that validates users against a local database.

AAA Network Configuration

- Authentication
  - Verifies a user identify
- Authorization
  - Specifies the permitted tasks for the user
- Accounting
  - Provides billing, auditing, and monitoring



Authentication Methods

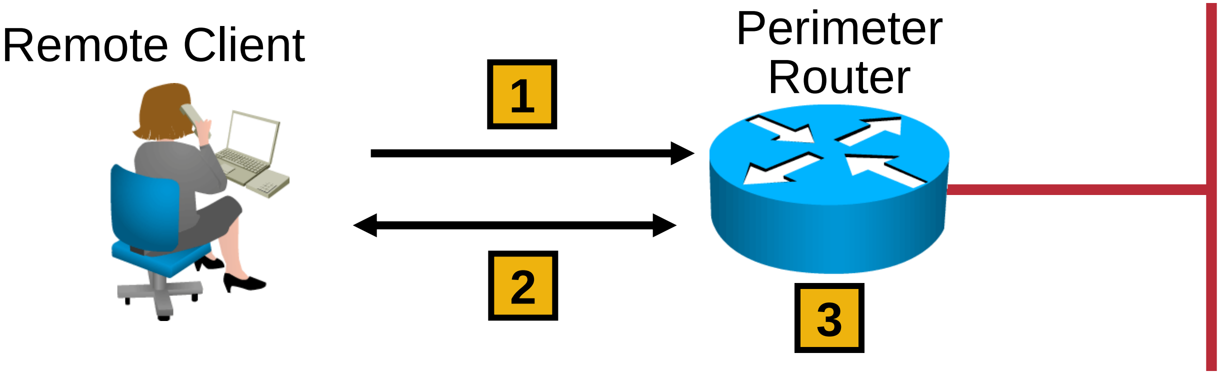
```
Switch(config)#aaa authentication login {default |
list-name} method1 [method2...]
```

- Creates a local authentication list

Cisco IOS AAA supports these authentication methods:

- Enable password
- Kerberos 5
- Kerberos 5-Telnet authentication
- Line password
- Local database
- Local database with case sensitivity
- No authentication
- RADIUS
- TACACS+

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.**

Router Local Authentication Configuration Steps

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

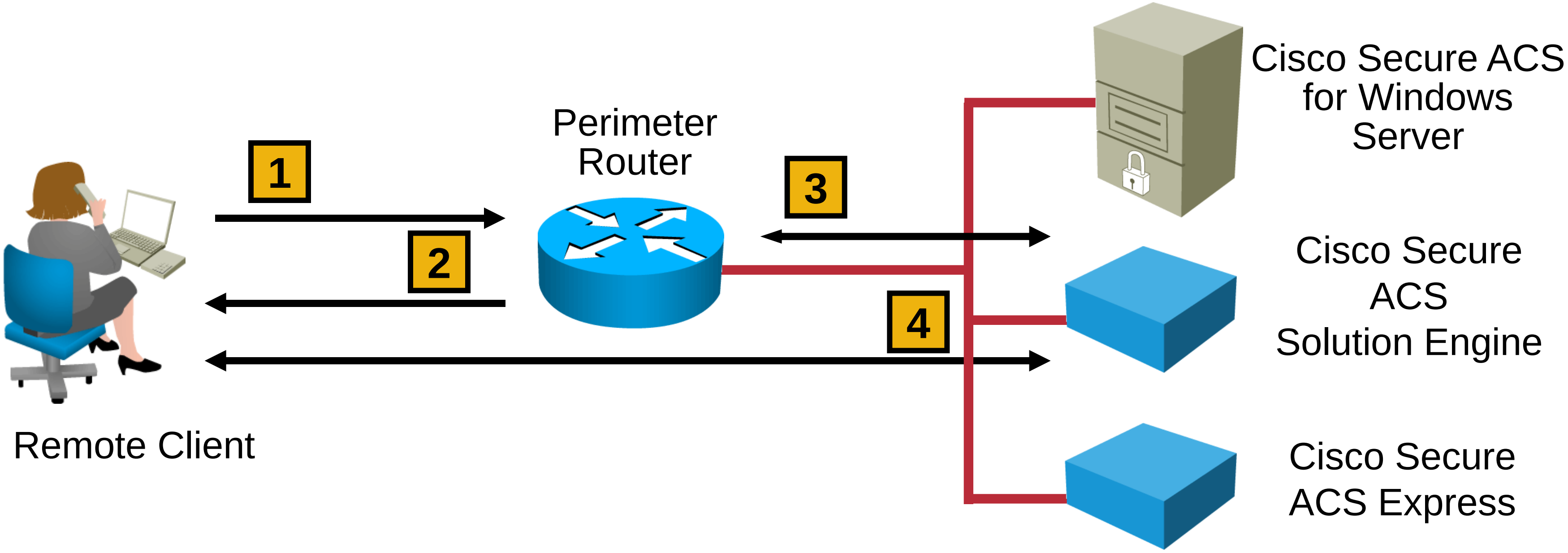
- Add usernames and passwords to the local router database
- Enable AAA globally on the router
- Configure AAA parameters on the router
- Confirm and troubleshoot the AAA configuration

Local AAA Configuration Example

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

enable secret 5 $1$x1EE$33AXd2VTVvhbWL0A37tQ3.
enable password 7 15141905172924
!
username admin1 password 7 14161606050A7B7974786B
username admin2 secret 5 $1$ErWl$b5rDNK7Y5RHkxX/Ks7Hr00
!
```

Implementing Authentication Using External Servers

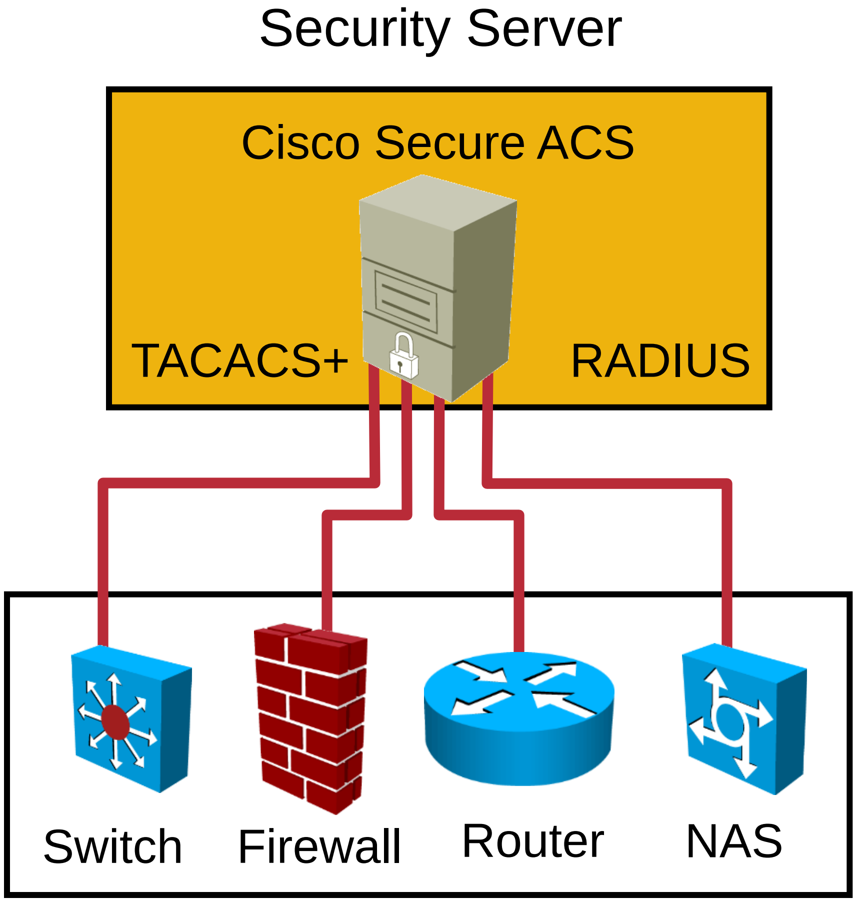


Perimeter Router
1
2
3
4
Cisco Secure ACS for Windows Server
Cisco Secure ACS Solution Engine
Cisco Secure ACS Express
Remote Client

1. The client 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 AAA Protocols

- **TACACS+ and RADIUS are used to communicate between the AAA security servers and authenticating devices.**
- **Cisco Secure ACS supports both TACACS+ and RADIUS:**
  - **TACACS+ remains more secure than RADIUS.**
  - **RADIUS has a robust application programming interface and strong accounting.**



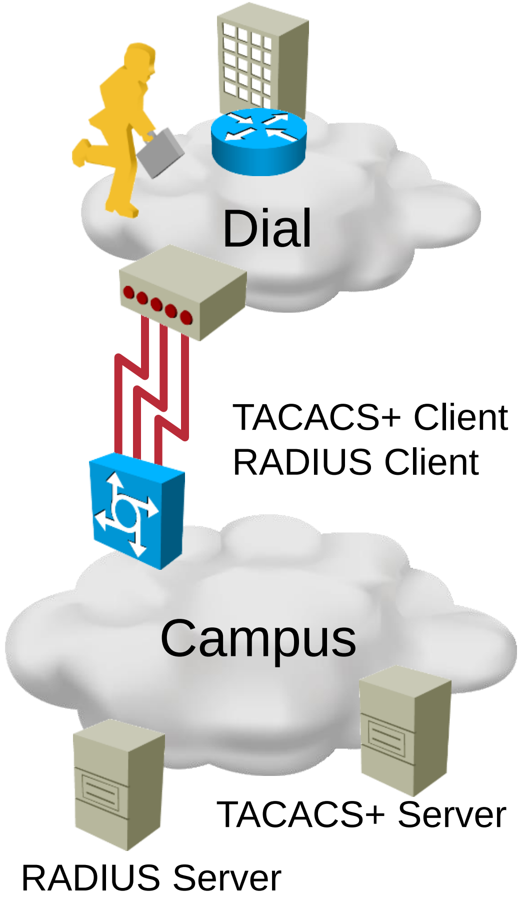
TACACS+ Overview

- Is not compatible with its predecessors TACACS and XTACACS
- Separates authentication and authorization
- Supports a large number of features
- Encrypts all communication
- Utilizes TCP port 49

RADIUS Overview

- RADIUS was developed by Livingston Enterprises.
- RADIUS proxy servers are used for scalability.
- RADIUS combines authentication and authorization as one process.
- DIAMETER is the planned replacement.
- Technologies that use RADIUS include
  - Remote access (i.e., dial-up and DSL)
  - 802.1X
  - SIP

TACACS+/RADIUS Comparison

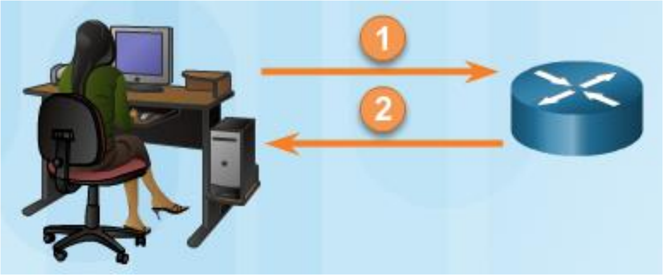


	TACACS+	RADIUS
Functionality	Separates AAA	Combines authentication and authorization
Standard	Mostly Cisco supported	Open/RFC
Transport Protocol	TCP	UDP
CHAP	Bidirectional	Unidirectional
Protocol Support	Multiprotocol support	No ARA, no NetBEUI
Confidentiality	Entire packet encrypted	Password encrypted
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

Comparing Local AAA and Server-Based AAA Implementations

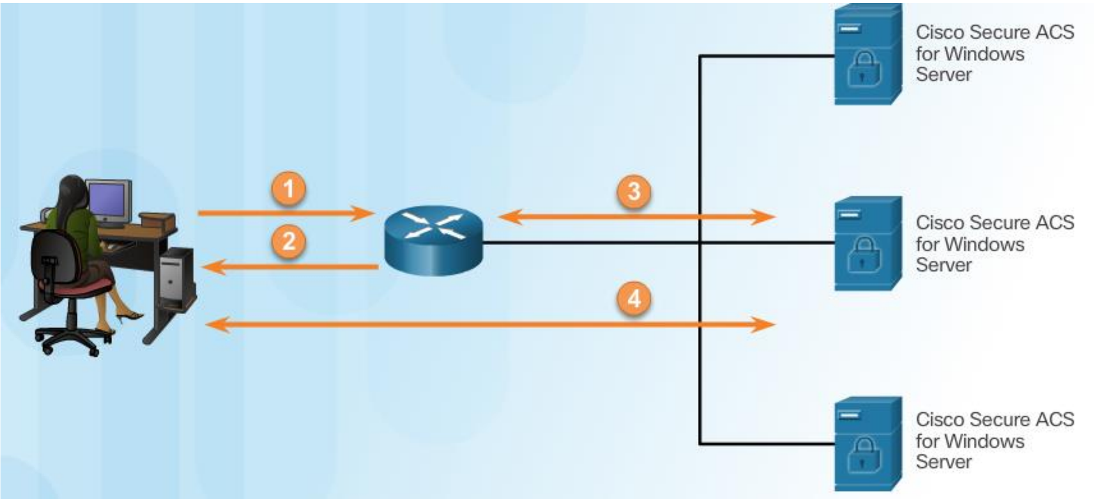
Local authentication:

1. **User establishes a connection with the router.**
2. **Router prompts the user for a username and password, authentication the user using a local database.**



Server-based authentication:

1. **User establishes a connection with the router.**
2. **Router prompts the user for a username and password.**
3. **Router passes the username and password to the Cisco Secure ACS (server or engine)**
4. **The Cisco Secure ACS authenticates the user.**


1
2
3
4
Cisco Secure ACS for Windows Server
Cisco Secure ACS for Windows Server
Cisco Secure ACS for Windows Server

Steps for Configuring Server-Based AAA Authentication with CLI

1. **Enable AAA.**
2. **Specify the IP address of the ACS server.**
3. **Configure the secret key.**
4. **Configure authentication to use either the RADIUS or TACACS+ server.**

AAA Configuration for TACACS+ Example

```
aaa new-model
!
aaa authentication login TACACS_SERVER tacacs+ local
aaa authorization exec 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
```

Setting Multiple Privilege Levels

```
router(config)#
```

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

- **Level 0 is predefined for user-level access privileges.**
- **Levels 1 to 14 may be customized for user-level privileges.**
- **Level 15 is predefined for enable mode (**enable **command).**

```
Boston(config)#privilege exec level 2 ping
Boston(config)#enable secret level 2 Patriot
```

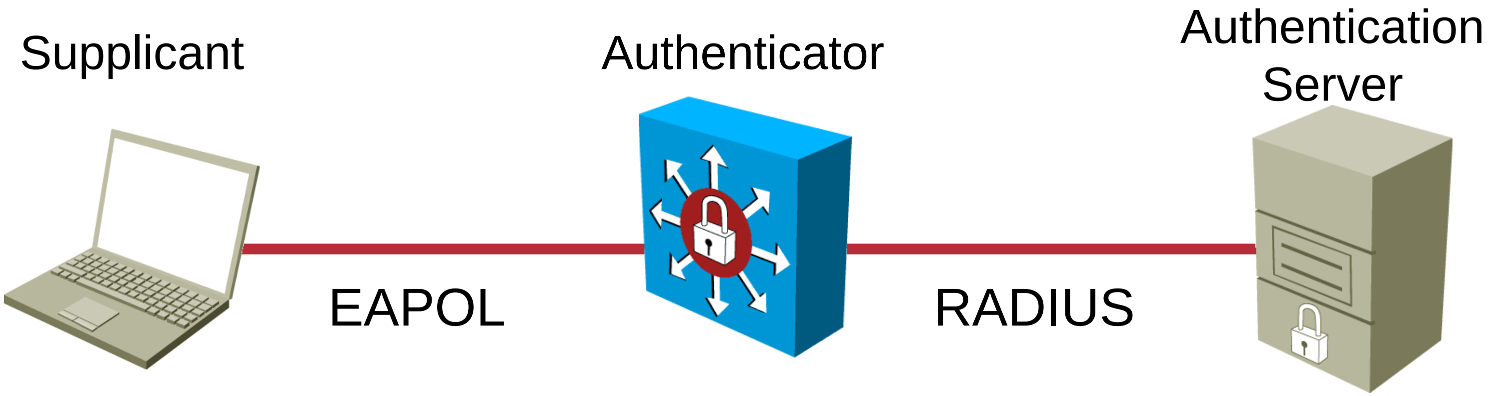
Section 3:

802.1X Authentication

IEEE 802.1x

- Standard set by the IEEE 802.1 working group
- A framework designed to address and provide port-based access control using authentication
- Primarily an encapsulation definition for EAP over IEEE 802 media (EAPOL is the key protocol.)
- Layer 2 protocol for transporting authentication messages (EAP) between supplicant (user/PC) and authenticator (switch or access point)
- Assumes a secure connection
- Actual enforcement is via MAC-based filtering and port-state monitoring

802.1x Components



Supplicant

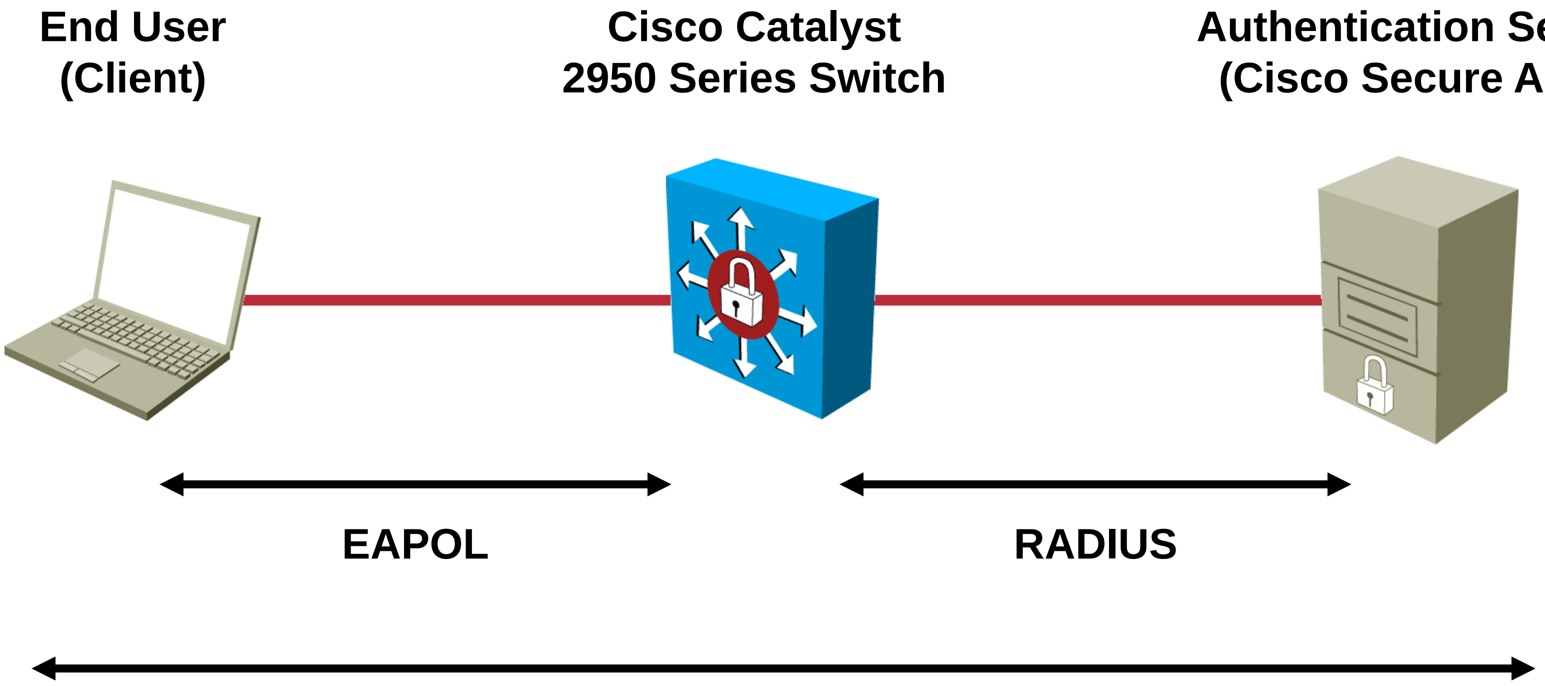
Authenticator

Authentication Server

EAPOL

RADIUS

How 802.1x Works



End User
(Client)

Cisco Catalyst
2950 Series Switch

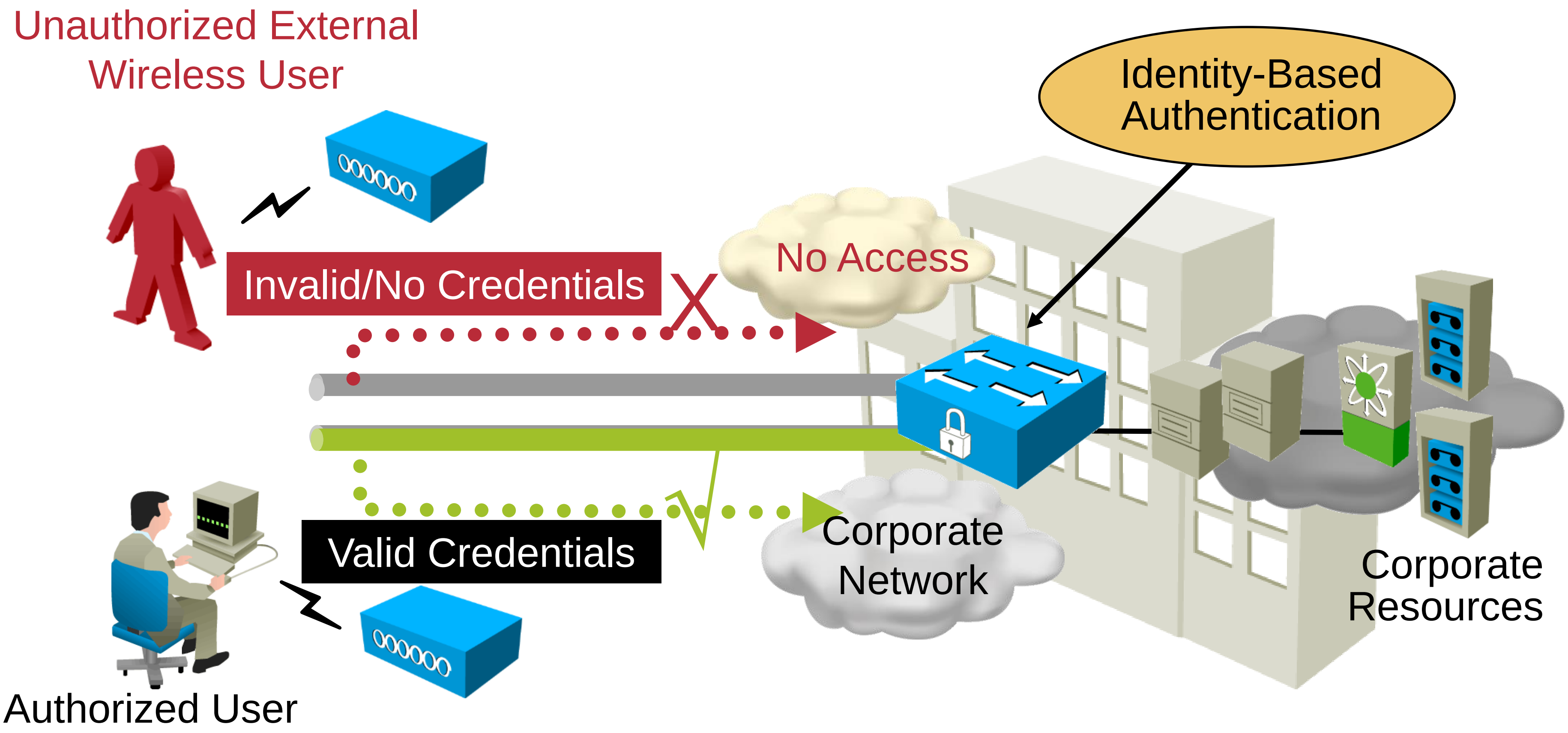
Authentication Server
(Cisco Secure ACS)

EAPOL

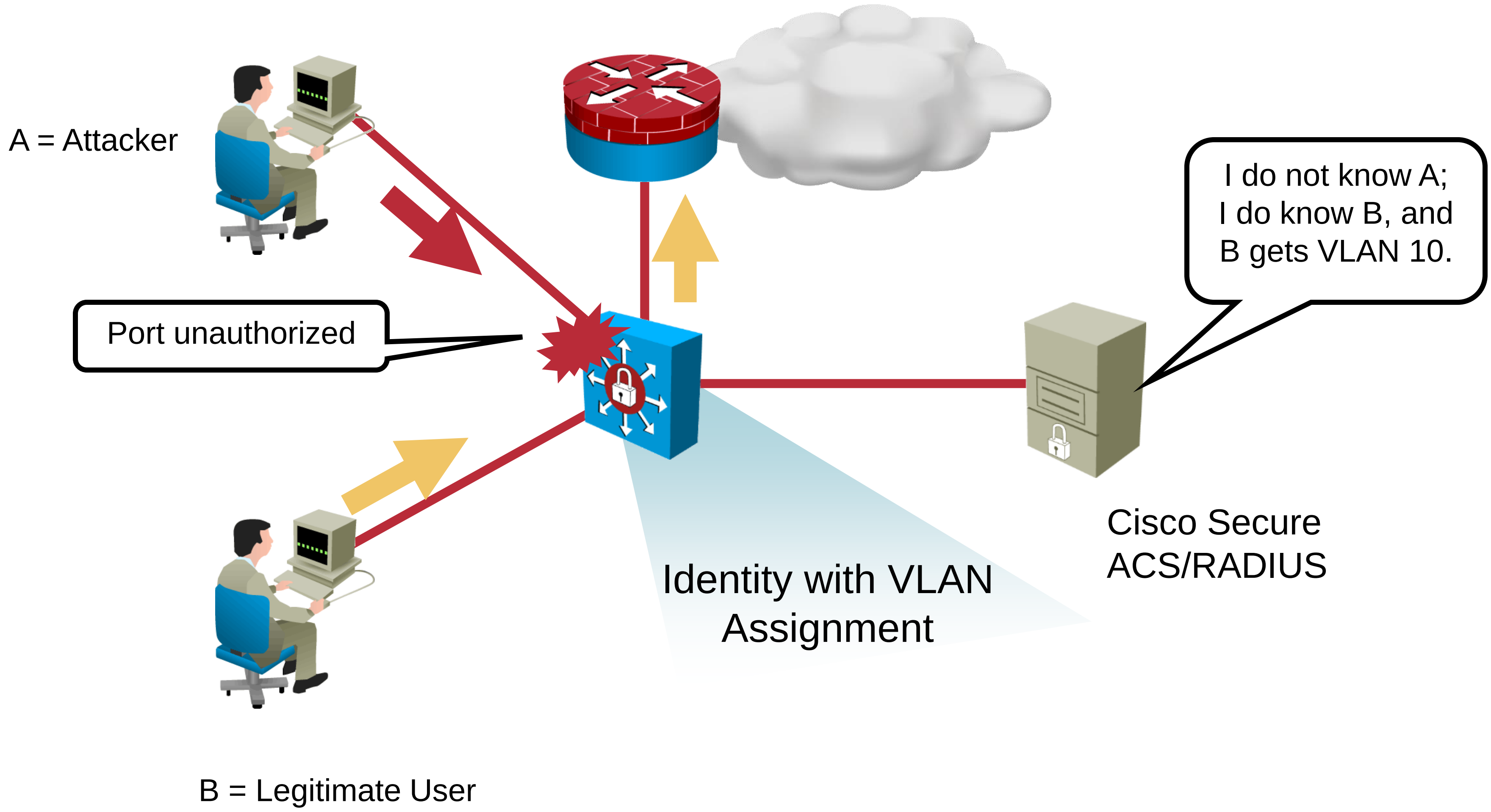
RADIUS

The actual authentication conversation occurs between the client and the authentication server using EAP. The authenticator is aware of this activity, but it is just an intermediary.

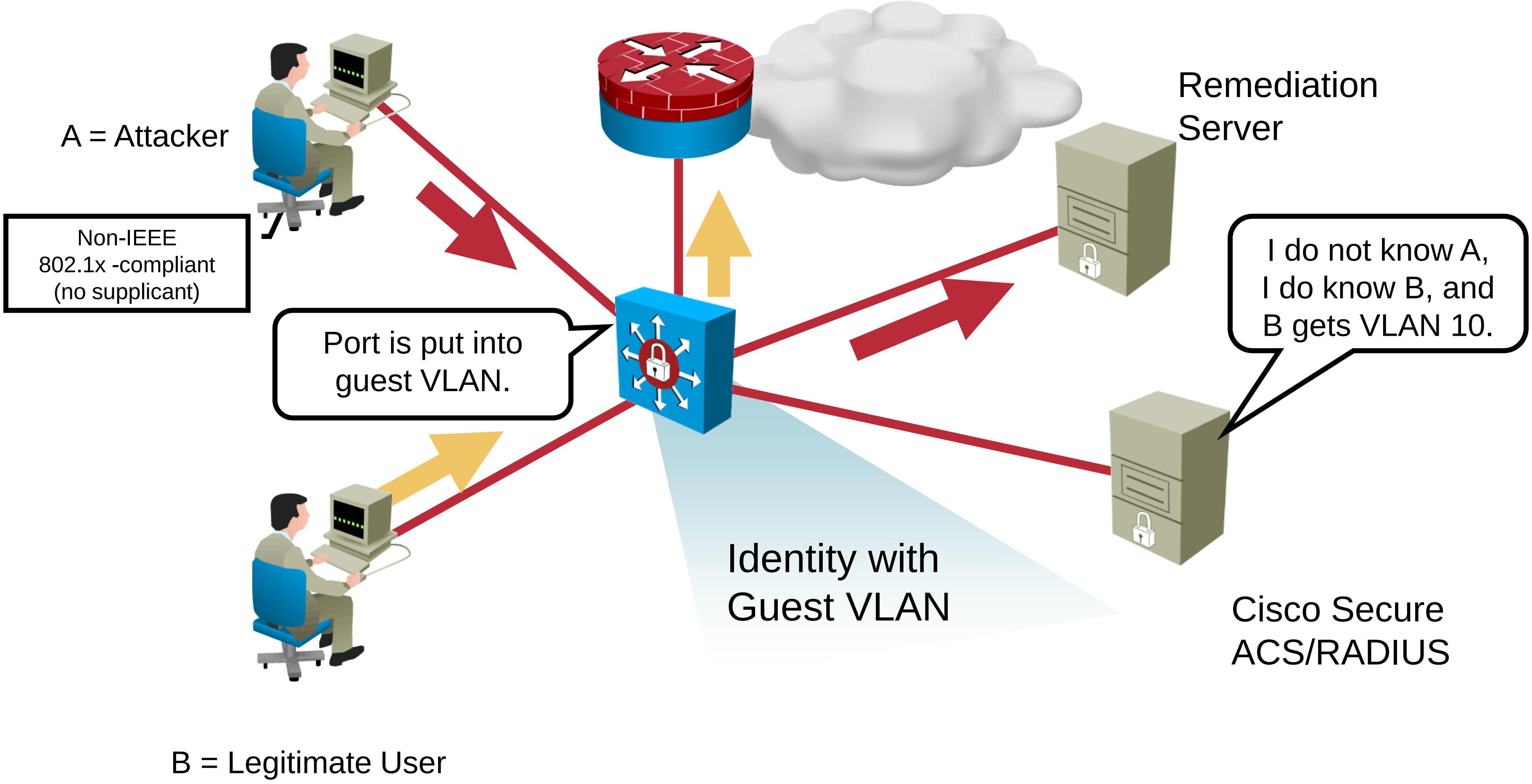
Concepts of 802.1x in Action



802.1x and VLAN Assignment



802.1x and the Guest VLAN



A = Attacker

Non-IEEE
802.1x -compliant
(no supplicant)

Port is put into
guest VLAN.

Remediation
Server

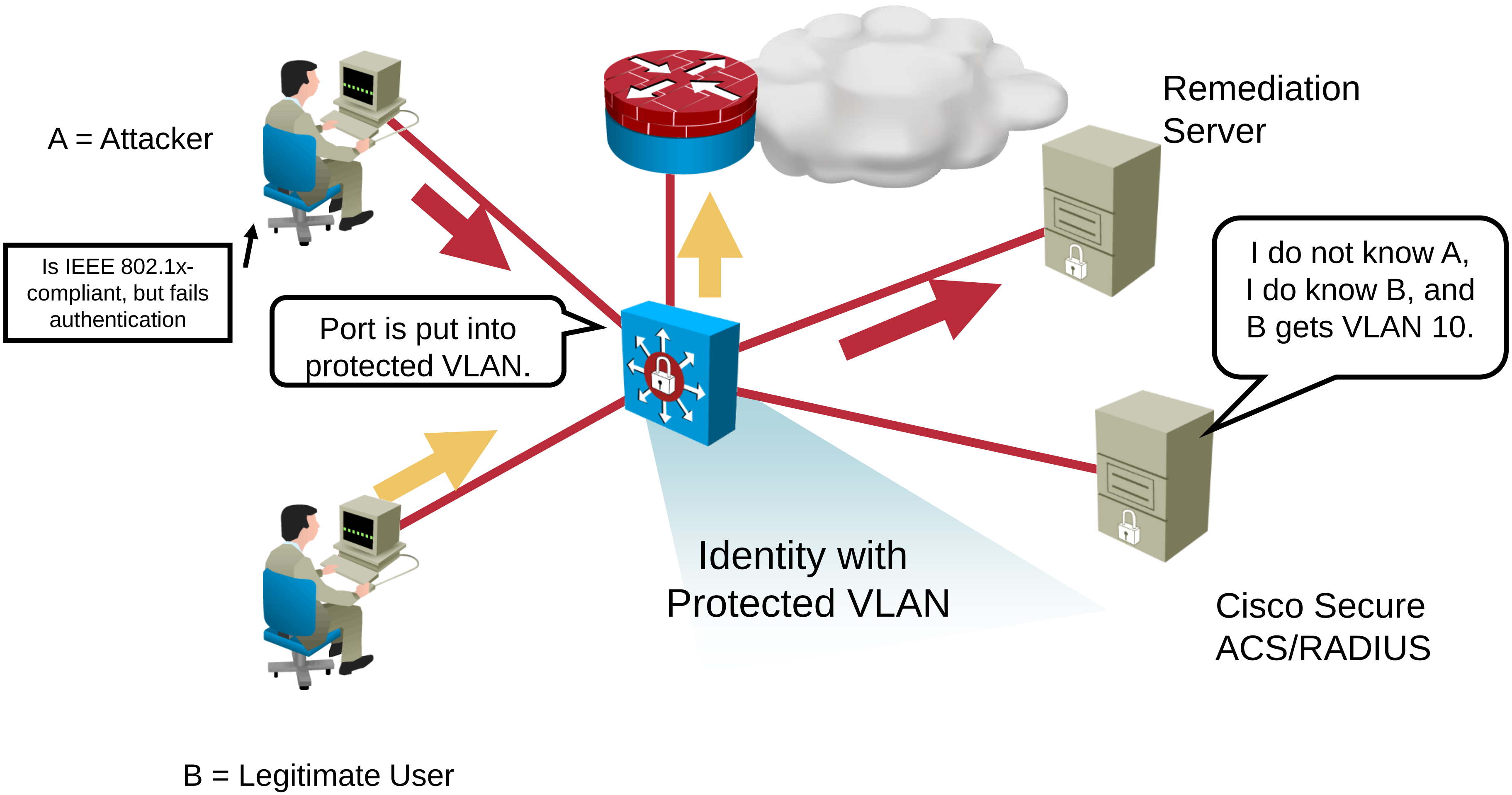
I do not know A,
I do know B, and
B gets VLAN 10.

Identity with
Guest VLAN

Cisco Secure
ACS/RADIUS

B = Legitimate User

802.1x and the Restricted VLAN


A = Attacker
Is IEEE 802.1x-compliant, but fails authentication
Port is put into protected VLAN.
Remediation Server
I do not know A, I do know B, and B gets VLAN 10.
Identity with Protected VLAN
Cisco Secure ACS/RADIUS
B = Legitimate User

Configuring 802.1x

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

- Enables AAA

```
Switch(config)#aaa authentication dot1x {default} method1
[method2…]
```

- Creates an 802.1x port-based authentication method list

```
Switch(config)#dot1x system-auth-control
```

- Globally enables 802.1x port-based authentication

```
Switch(config)#interface type slot/port
```

- Enters interface configuration mode:

```
Switch(config-if)#switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
```

- Enables 802.1x port-based authentication on theinterface

CISCO