保护管理访问

管理网络设备安全

现任明教教主（秦柯）
CCIE Security and Data Center
CCIE 讲师， Yeslab

网络设备安全概述

网络设备容易遭受以下常见威胁：

- 远程访问威胁
  - 未授权的远程访问
- 本地访问和物理威胁
  - 设备损坏
  - 密码恢复
  - 设备失窃
- 环境威胁
  - 极端温度
  - 高湿度
- 电气威胁
  - 电源电压不足
  - 电压峰值
- 维护威胁
  - 操作不当
  - 布线低劣
  - 标记信息不足

保护对特权 EXEC 模式的访问

配置使能密码：

```
Switch(config)#enable password C1sco123
```

配置使能加密密码：

```
Switch(config)#enable secret sanfran
```

验证已配置的密码：

```
Switch#show running-config | include enable
enable secret 5 $1$WPHF$uWo4ucV0/vA1/abu6LlWQ1
enable password C1sco123
```

保护对特权 EXEC 模式的访问（续）

加密明文密码：

```
Switch(config)#service password-encryption
Switch(config)#exit
Switch#show running-config | include enable
enable secret 5 $1$vWZa$2sYQLDv4R4xMtU5NFDrbX.
enable password 7 04785A150C2E1D1C5A
```

保护控制台访问

控制台密码：

```
Switch(config)#line console 0
Switch(config-line)#password C1sco123
Switch(config-line)#login
```

EXEC 超时：

```
Switch(config-line)#exec-timeout 5
```

保护远程访问

虚拟终端密码：

```
Switch(config)#line vty 0 15
Switch(config-line)#login
Switch(config-line)#password cisco
```

EXEC 超时：

```
Switch(config-line)#exec-timeout 5
```

保护远程访问（续）

配置 SSH：

```
Switch(config)#hostname SwitchX
SwitchX(config)#ip domain-name cisco.com
SwitchX(config)#username user1 secret C1sco123
SwitchX(config)#crypto key generate rsa modulus 1024
The name for the keys will be: SwitchX.cisco.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
SwitchX(config)#line vty 0 15
SwitchX(config-line)#login local
SwitchX(config-line)#transport input ssh
SwitchX(config-line)#exit
SwitchX(config)#ip ssh version 2
```

保护远程访问（续）

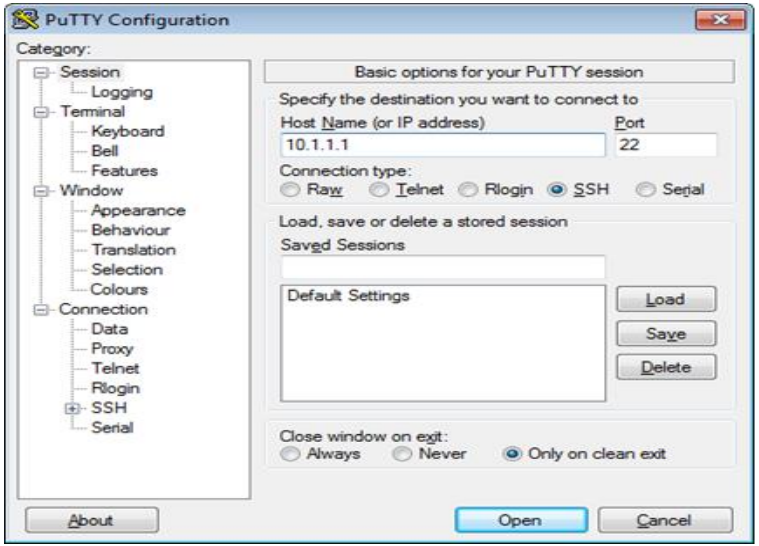
检验是否已启用 SSH：

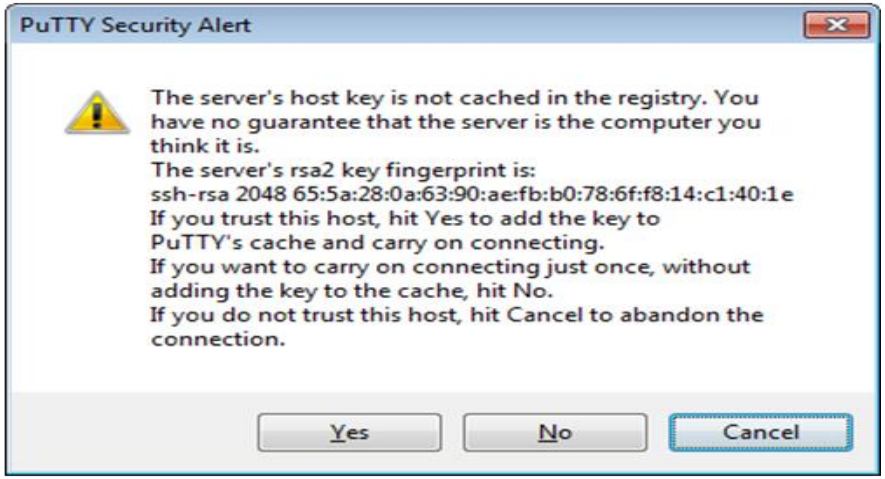
```
Switch#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

检查设备的 SSH 连接：

```
Switch#show ssh
Connection  Version  Encryption     State              Username
0           1.5      3DES           Session started    cisco
```

保护远程访问（续）



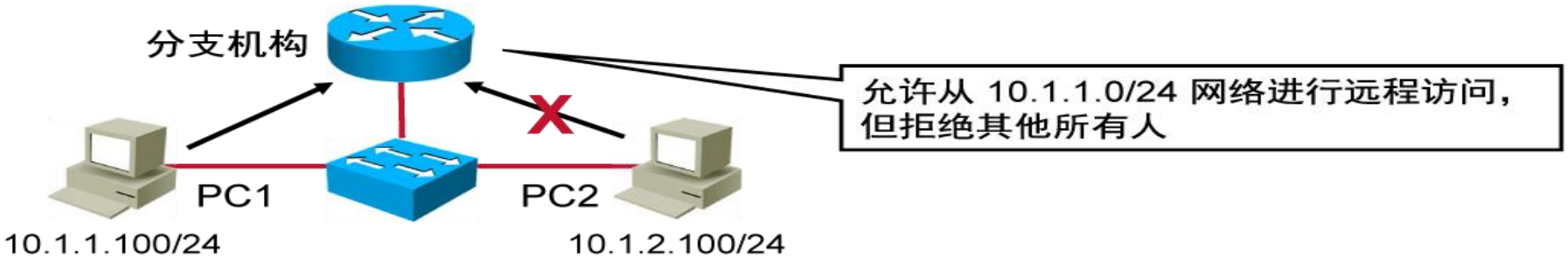


启用远程访问连接

配置交换机上的默认网关 IP 地址

```
SwitchX(config)#ip default-gateway 10.1.1.1
```

使用 ACL 限制远程访问



使用 ACL 允许来自 10.1.1.0 /24 的 Telnet 访问，但拒绝其他所有人：

```
Router(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)#access-list 1 deny any log
```

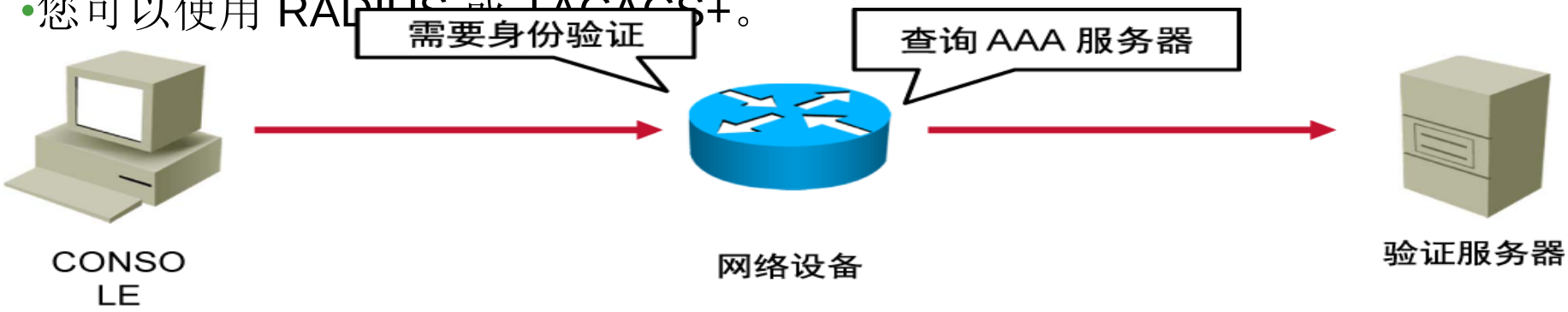
对 vty 线路应用 ACL：

```
Router(config)#line vty 0 15
Router(config-line)#access-class 1 in
```

外部身份验证选项

外部身份验证可能优先于本地身份验证：

- 本地身份验证数据库可能会增加管理负担。
- 外部身份验证具有可扩展性。
- 您可以使用 RADIUS 或 TACACS+。



配置登录提示

配置登录提示：

```
Switch(config)#banner login "Access for authorized users only. Please enter
your username and password."
```

用户连接设备时看到以下消息：

```
Access for authorized users only. Please enter your username and password.
User Access Verification
Username:
```

总结

- 网络设备的安全威胁包括远程访问威胁、物理和本地访问威胁、环境威胁、电气威胁以及维护威胁。
- 您可使用密码来限制访问，从而保护网络设备。
- 您可使用控制台密码，并使用 EXEC 超时设置来防止相连终端访问设备，从而保护对网络设备的控制台访问。
- 您可使用 vty 密码限制访问，并使用 EXEC 超时设置来防止相连终端访问设备，从而保护对网络设备的 Telnet 和 SSH 访问。
- 您可使用 ACL 来限制可以访问设备的用户，从而保护对网络设备的 Telnet 和 SSH 访问。
- 如果您想使用可扩展的选项，而不是本地身份验证数据库，则使用 RADIUS 或 TACACS+ 外部身份验证服务。
- 使用 **banner** 命令可配置登录或 MOTD 提示。

Thank you.