JEREMY'S IT LAB

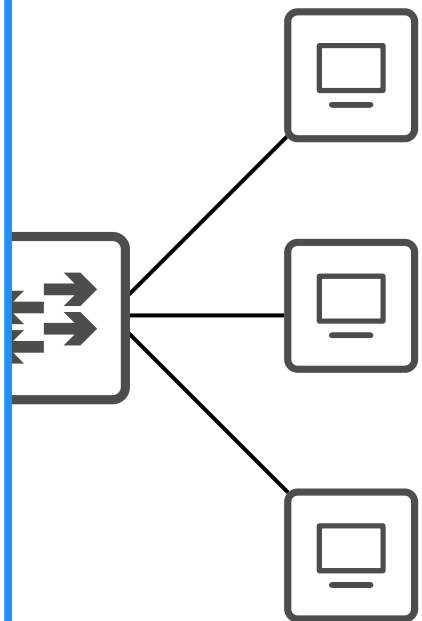
CCNA Day 42

Secure Shell

1.0 Network Fundamentals	20%
2.0 Network Access	20%
3.0 IP Connectivity	25%
4.0 IP Services	10%

4.1 Configure and verify inside source NAT using static and pools
4.2 Configure and verify NTP operating in a client and server mode
4.3 Explain the role of DHCP and DNS within the network
4.4 Explain the function of SNMP in network operations
4.5 Describe the use of syslog features including facilities and levels
4.6 Configure and verify DHCP client and relay
4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
4.8 Configure network devices for remote access using SSH
4.9 Describe the capabilities and function of TFTP/FTP in the network

5.0 Security Fundamentals	15%
6.0 Automation and Programmability	10%



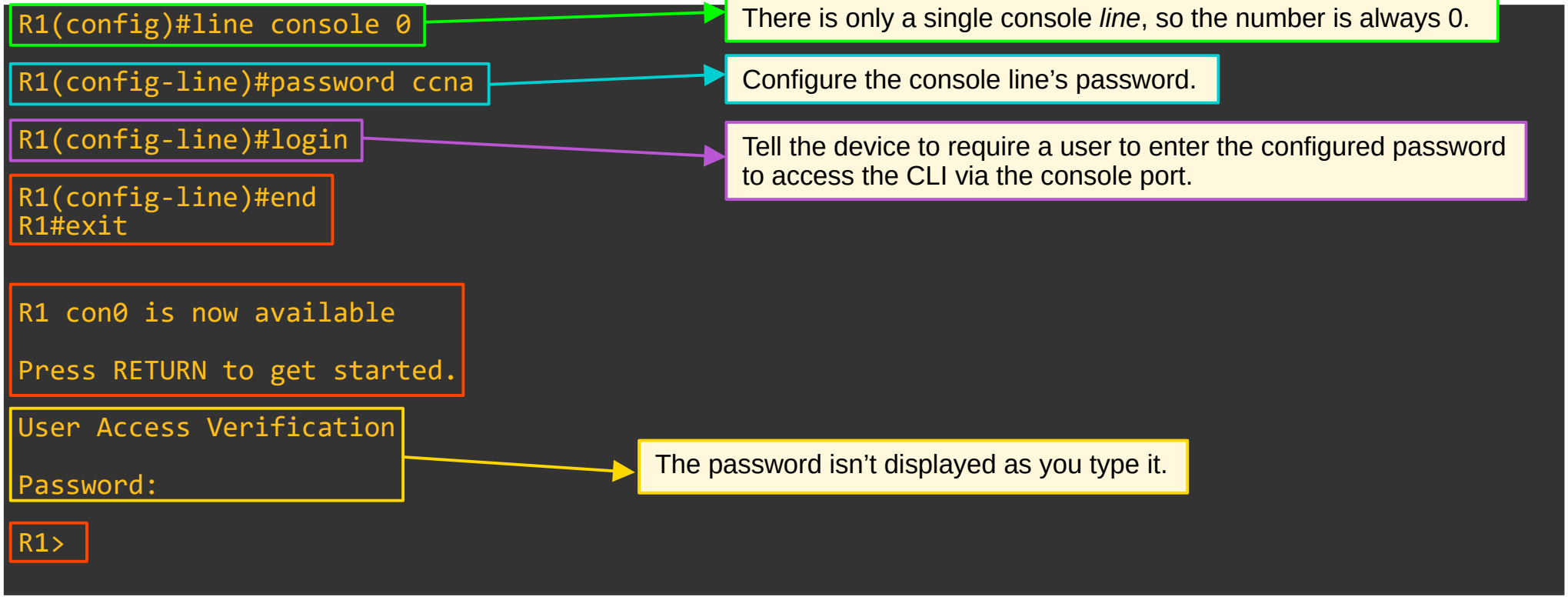
Things we'll cover

- Console port security
- Layer 2 switch management IP
- Telnet
- SSH

Console Port Security – login

- By default, no password is needed to access the CLI of a Cisco IOS device via the console port.

- You can configure a password on the *console line*.
  → A user will have to enter a password to access the CLI via the console port.



Console Port Security – login local

- Alternatively, you can configure the console line to require users to login using one of the configured usernames on the device.

```
R1(config)#username jeremy secret ccnp
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#end
R1#exit
```

Tell the device to require a user to login using one of the configured usernames on the device.

```
R1 con0 is now available


Press RETURN to get started.
```

```
User Access Verification

Username: jeremy
Password:
R1>
```

```
line con 0
 exec-timeout 3 30
 password ccna
 logging synchronous
 login local
```

Log the user out after 3 minutes and 30 seconds of inactivity.

Layer 2 Switch – Management IP

- Layer 2 switches don't perform packet routing and don't build a routing table. They aren't IP routing aware.

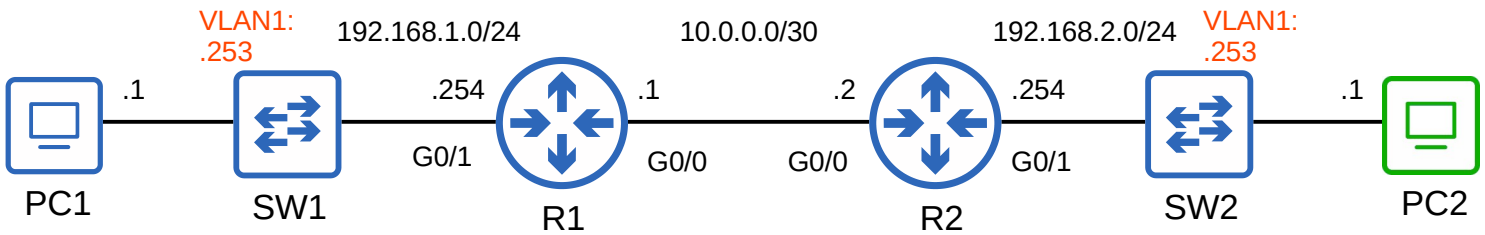
- However, you can assign an IP address to an SVI to allow remote connections to the CLI of the switch (using Telnet or SSH).

```
SW1(config)#interface vlan1
SW1(config-if)#ip address 192.168.1.253 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#exit

SW1(config)#ip default-gateway 192.168.1.254
```

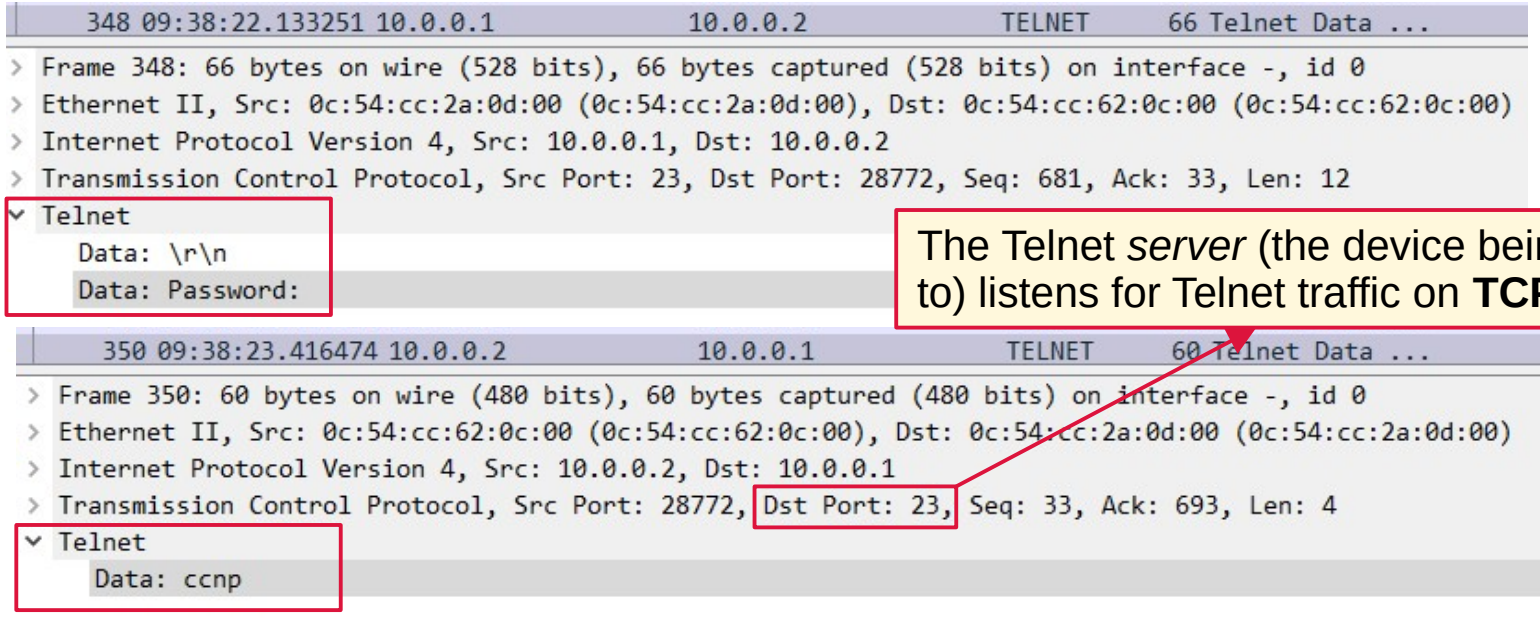
Configure the IP address on the SVI in the same way as on a multilayer switch.
Enable the interface if necessary.

Configure the switch's default gateway.
In this case, PC2 isn't in the same LAN as SW1.
If SW1 doesn't have a default gateway, it can't communicate with PC2.



Telnet

- Telnet (Teletype Network) is a protocol used to remotely access the CLI of a remote host.
- Telnet was developed in 1969.
- Telnet has been largely replaced by SSH, which is more secure.
- Telnet sends data in plain text. No encryption!



The Telnet *server* (the device being connected to) listens for Telnet traffic on **TCP port 23**.

Telnet Configuration

```
SW1(config)#enable secret ccna
SW1(config)#username jeremy secret ccna
SW1(config)#access-list 1 permit host 192.168.2.1

SW1(config)#line vty 0 15

SW1(config-line)#login local

SW1(config-line)#exec-timeout 5 0

SW1(config-line)#transport input telnet

SW1(config-line)#access-class 1 in
```

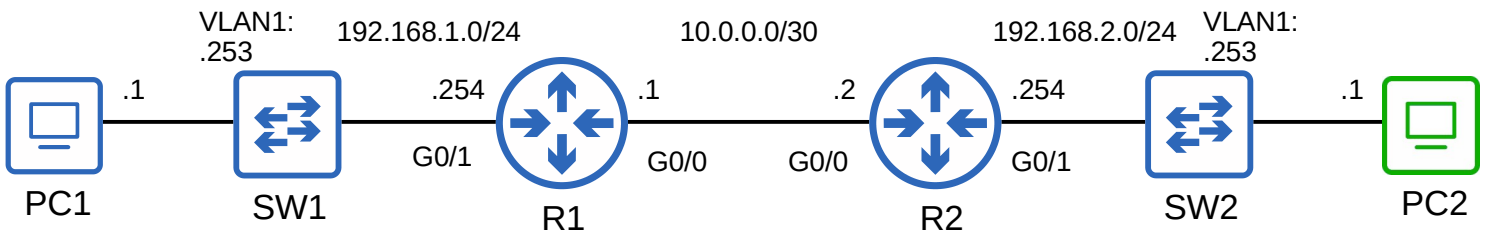
If an enable password/secret isn't configured, you won't be able to access privileged exec mode when connecting via Telnet.

Configure an ACL to limit which devices can connect to the *VTY lines*.

Telnet/SSH access is configured on the VTY lines. There are 16 lines available, so up to 16 users can be connected at once. (VTY stands for Virtual TeleType)

`transport input telnet` allows only Telnet connections.
`transport input ssh` allows only SSH connections.
`transport input telnet ssh` allows both.
`transport input all` allows all connections.
`transport input none` allows no connections.

Apply the ACL to the VTY lines.
***`access-class`** applies an ACL to the VTY lines,
`ip access-group` applies an ACL to an interface.



Telnet Configuration

```
R2#ping 192.168.1.253
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.253, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/11/16 ms
```

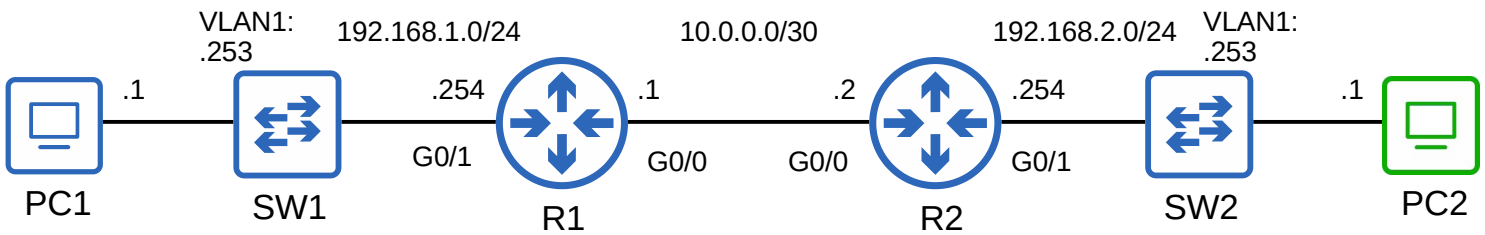
```
R2#telnet 192.168.1.253
Trying 192.168.1.253 ...
% Connection refused by remote host
```

```
line vty 0 4
 access-class 1 in
 exec-timeout 5 0
 login local
 transport input telnet
line vty 5 15
 access-class 1 in
 exec-timeout 5 0
 login local
 transport input telnet
```

```
C:\Users\user>telnet 192.168.1.253
Connecting To 192.168.0.1…

User Access Verification

Username: jeremy
Password:
SW1>
```

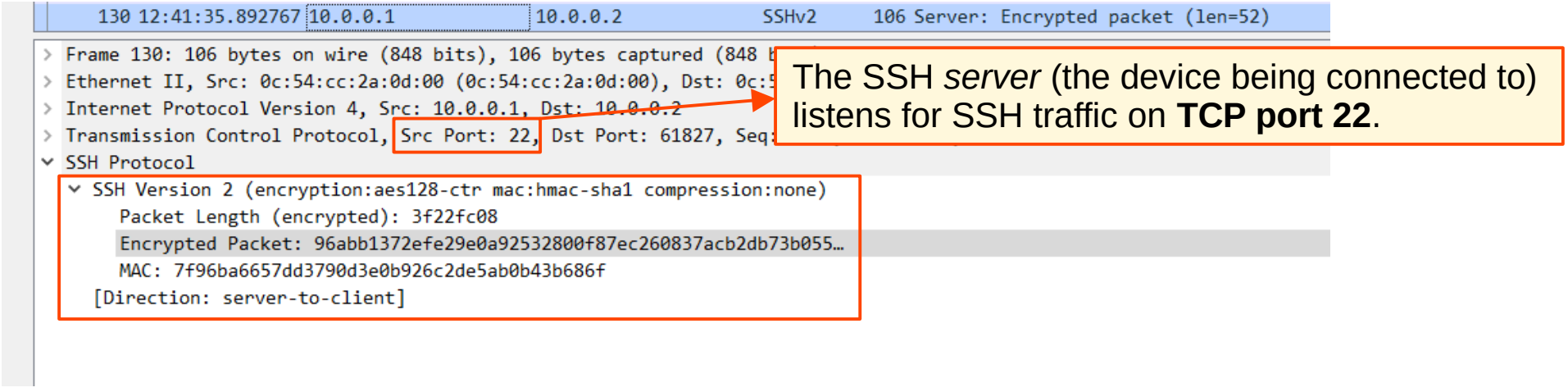


SSH (Secure Shell)

- SSH (Secure Shell) was developed in 1995 to replace less secure protocols like Telnet.

> In computing, a **shell** is a computer program which exposes an operating system's services to a human user or other program. In general, operating system shells use either a command-line interface (CLI) or graphical user interface (GUI), depending on a computer's role and particular operation. It is named a shell because it is the outermost layer around the operating system.[1] [2]

- SSHv2, a major revision of SSHv1, was released in 2006.
- If a device supports both version 1 and version 2, it is said to run 'version 1.99'.
- Provides security features such as data encryption and authentication.



SSH Configuration: Check SSH Support

```
SW1#show version
Cisco IOS Software, vios_l2 Software (vios_l2-ADVENTERPRISEK9-M), Version 15.2(4.0.55)E, TEST
ENGINEERING ESTG_WEEKLY BUILD, synced to  END_OF_FLO_ISP
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Tue 28-Jul-15 18:52 by sasyamal

SW1#show ip ssh
SSH Disabled - version 1.99
%Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): NONE
```

- IOS images that support SSH will have ‘K9’ in their name.
- Cisco exports NPE (No Payload Encryption) IOS images to countries that have restrictions on encryption technologies.
- NPE IOS images do not support cryptographic features such as SSH.

SSH Configuration: RSA Keys

- To enable and use SSH, you must generate an RSA public and private key pair.
- The keys are used for data encryption/decryption, authentication, etc.

```
SW1(config)#ip domain name jeremysitlab.com

SW1(config)#crypto key generate rsa
The name for the keys will be: SW1.jeremysitlab.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

SW1(config)#
*Feb 21 04:22:35.778: %SSH-5-ENABLED: SSH 1.99 has been enabled

SW1(config)#do show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): SW1.jeremysitlab.com
[output omitted]
```

The **FQDN** of the device is used to name the RSA keys.
FQDN = Fully Qualified Domain Name (host name + domain name)

Generate the RSA keys.
`crypto key generate rsa modulus` *`length`*
is an alternate method.
*length must be 768 bits or greater for SSHv2

SSH Configuration: VTY Lines

```
SW1(config)#enable secret ccna
SW1(config)#username jeremy secret ccna
SW1(config)#access-list 1 permit host 192.168.2.1
```

```
SW1(config)#ip ssh version 2
```
(optional, but recommended) Restrict SSH to version 2 only.

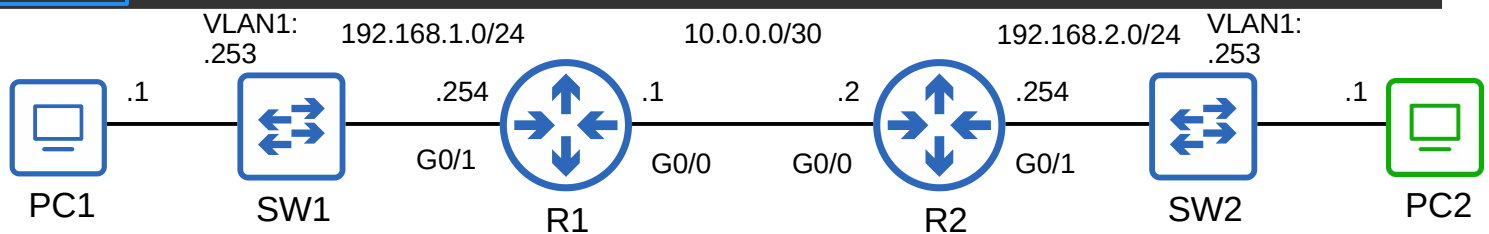
```
SW1(config)#line vty 0 15
```
Configure all VTY lines, just like Telnet.

```
SW1(config-line)#login local
```
Enable local user authentication.
*you cannot use **`login`** for SSH, only **`login local`**.

```
SW1(config-line)#exec-timeout 5 0
```
(optional, but recommended) Configure the exec timeout.

```
SW1(config-line)#transport input ssh
```
Best practice is to limit VTY line connections to SSH only.

```
SW1(config-line)#access-class 1 in
```
(optional, but recommended) Apply the ACL to restrict VTY line connections.



SSH Configuration

1) Configure host name
2) Configure DNS domain name
3) Generate RSA key pair
4) Configure enable PW, username/PW
5) Enable SSHv2 (only)
6) Configure VTY lines

```
Router(config)#crypto key generate rsa
% Please define a hostname other than Router.
Router(config)#hostname R2
R2(config)#crypto key generate rsa
% Please define a domain-name first.
R2(config)#ip domain name jeremysitlab.com
R2(config)#crypto key generate rsa
The name for the keys will be: R2.jeremysitlab.com
[output omitted]
```

Connect: **`ssh -l`** *`username ip-address`* OR **`ssh`** *`username@ip-address`*

You have to know how to configure SSH for the CCNA exam, so make sure to do the practice lab!

Command Summary

```
SW1# show version
SW1# show ip ssh
SW1(config)# ip default-gateway ip-address
SW1(config)# line con 0
SW1(config)# line vty 0 15
SW1(config)# crypto key generate rsa
SW1(config)# ip ssh version 2
SW1(config-line)# login [local]
SW1(config-line)# transport input [protocols | all | none]
SW1(config-line)# exec-timeout minutes seconds
SW1(config-line)# access-class acl in
```

```
> telnet ip-address
> ssh -l username ip-address
> ssh username@ip-address
```

Things we covered

- Console port security
- Layer 2 switch management IP
- Telnet
- SSH

Quiz 1

You issue the **`crypto key generate rsa`** command on a Cisco router, but the command is rejected. Which of the following might be the cause? (select two)

a) A host name hasn't been configured.

b) The **`ip ssh version 2`** command hasn't been configured.

c) The **transport input ssh** command hasn't been configured.

d) Only switches can generate RSA keys.

e) A DNS domain name hasn't been configured.

f) SSH version 1.99 is enabled.

Quiz 2

Which of the following commands would allow both Telnet and SSH to be used to connect to the VTY lines of a device? (select two, each answer is a complete solution)

a) transport input default

b) transport input none

c) transport input telnet ssh

d) transport input all

```
R1(config-line)#transport input ?
  all       All protocols
  lapb-ta   LAPB Terminal Adapter
  lat       DEC LAT protocol
  mop       DEC MOP Remote Console Protocol
  none      No protocols
  pad       X.3 PAD
  rlogin    Unix rlogin protocol
  ssh       TCP/IP SSH protocol
  telnet    TCP/IP Telnet protocol
  udptn     UDPTN async via UDP protocol
  v120      Async over ISDN
```

Quiz 3

You want to allow only 192.168.1.1 to connect to R1 via SSH. Which of the following configurations fulfills that requirement?

a)
```
R1(config)#access-list 199 permit tcp host 192.168.1.1 any eq 23
R1(config)#line vty 0 15
R1(config-line)#access-class 199 in
```

b)
```
R1(config)#access-list 199 permit tcp host 192.168.1.1 any eq 22
R1(config)#line vty 0 15
R1(config-line)#access-class 199 in
```

c)
```
R1(config)#access-list 199 permit tcp host 192.168.1.1 any eq 22
R1(config)#line con 0
R1(config-line)#access-group 199 in
```

d)
```
R1(config)#access-list 199 permit tcp host 192.168.1.1 any eq 22
R1(config)#line vty 0 15
R1(config-line)#access-group 199 in
```

e)
```
R1(config)#access-list 199 permit udp host 192.168.1.1 any eq 22
R1(config)#line vty 0 15
R1(config-line)#access-class 199 in
```

Quiz 4

Which of the following statements about SSH are true? (select two)

a) RSA keys are optional but recommended.

b) K9 IOS images support SSH.

c) SSH version 1.99 was released between version 1 and version 2.

d) SSH sends data in plain text.

e) NPE IOS images support SSH.

f) A key length of at least 768 bits is required for SSHv2.

Quiz 5

A network admin using PC1 is remotely configuring SW1 by connecting to the CLI of SW1 via SSH. What is the role of SW1 in this situation?

a) SSH peer

b) SSH server

c) SSH client

d) None of the above