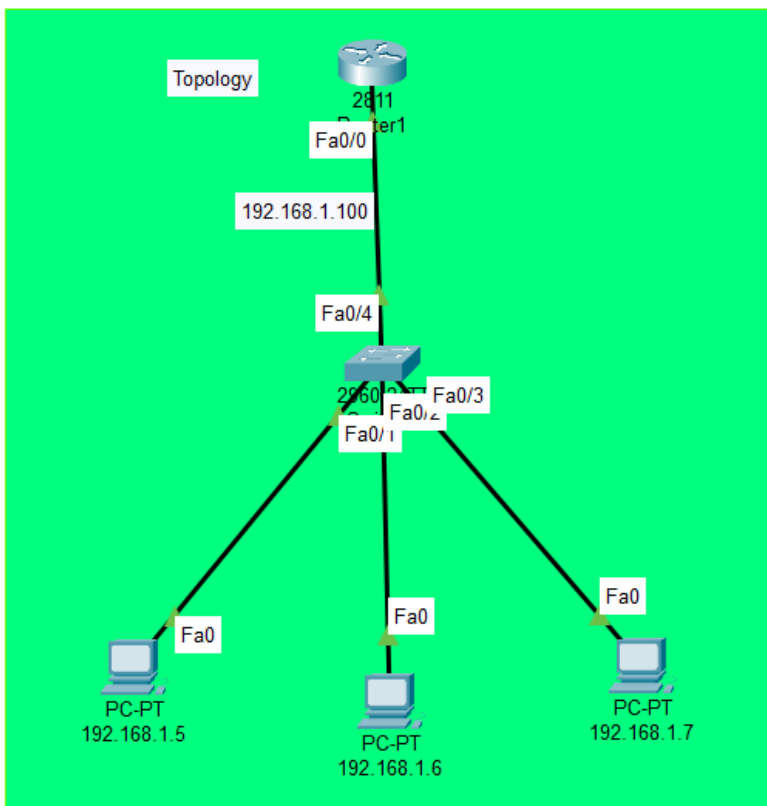


What is SSH?

SSH (Secure Shell) is a **cryptographic network protocol** used to **securely access and manage network devices** over an unsecured network.

Unlike Telnet, **SSH encrypts all data**, including login credentials, making it suitable for **production environments** and **public networks**.

- **Protocol Type:** Application Layer (OSI Layer 7)
- **Transport Protocol:** TCP (Port 22 by default)
- **Security:** Encrypted connection using RSA keys



Importance of SSH

1. **Secure Remote Access:**
Protects against password sniffing and man-in-the-middle attacks.
2. **Widely Used in Enterprises:**
SSH is the **standard** for managing Cisco devices in professional networks.
3. **Encryption & Authentication:**
Supports **public-key authentication** and encrypts the session traffic.

4. Compliance & Auditing:

Required in environments with **security compliance policies** like HIPAA, PCI-DSS, etc.

Uses of SSH

- Remote login to routers, switches, firewalls
- Secure file transfer (with SCP/SFTP)
- Automated configuration and scripting
- Accessing Linux servers and firewalls
- Secure tunneling and port forwarding

How to Configure SSH on a Cisco Router or Switch

Step 1: Set Device Hostname and Domain Name

```
Router> enable
```

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain-name example.com
```

Step 2: Generate RSA Keys

```
R1(config)# crypto key generate rsa
```

- When prompted, enter key size (e.g., 1024 or 2048).
Recommended: 2048 bits

Step 3: Create a Local User

```
R1(config)# username admin secret admin123
```

Step 4: Enable SSH on VTY Lines

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Step 5: Verify SSH Status

```
R1# show ip ssh
```

```

Router>en
Router#
Router#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#int f0/0
Router(config-if)#ip address 192.168.1.100 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#ex
Router(config)#
Router(config)#hostname R1
R1(config)#ip domain-name aup.com
R1(config)#username rahi secret 8034
R1(config)#crypto key generate rsa
The name for the keys will be: R1.aup.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#line vty 0 4
*Mar 1 0:4:39.166: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:4:39.166: %SSH-5-ENABLED: SSH 1.5 has been enabled
R1(config-line)#
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3

```

Accessing SSH from a Client

From a PC or terminal:

```
ssh admin@192.168.1.1
```

Replace admin with your configured username and 192.168.1.1 with the device IP address.

SSH vs Telnet – Quick Comparison

Feature	SSH	Telnet
Port	22	23
Encryption	Yes (Secure)	No (Plain Text)
Authentication	Local/User + RSA keys	Basic password only
Use Case	Secure production networks	Lab/testing only
Protocol	TCP	TCP

Summary

- SSH is essential for **secure network administration**.
- Always use SSH over Telnet in any **real-world network**.
- Required knowledge for **CCNA, network engineers, and cybersecurity professionals**.

What is the OSI Model?

The **OSI (Open Systems Interconnection)** model is a **conceptual framework** developed by the **International Organization for Standardization (ISO)** that standardizes the functions of a telecommunication or computing system **into seven distinct layers**. It helps in understanding how data moves through a network and how different networking protocols interact.

Application	7
Presentation	6
Session	5
Transport	4
Network	3
Data Link	2
Physical	1

The 7 Layers of the OSI Model

Layer No.	Name	Function	Example Protocols
7	Application	Interface for user and application	HTTP, FTP, DNS, SMTP
6	Presentation	Data translation, encryption, compression	SSL, JPEG, ASCII
5	Session	Manages sessions between systems	NetBIOS, RPC
4	Transport	Reliable delivery, flow control, error check	TCP, UDP
3	Network	Routing, logical addressing (IP)	IP, ICMP, IPSec, RIP
2	Data Link	MAC addressing, error detection	Ethernet, PPP, ARP
1	Physical	Transmission of raw bits over medium	Cables, Hubs, NIC, Fiber

Layer-by-Layer Explanation

1. Physical Layer

- Concerned with **raw data transmission** (bits: 1s and 0s)
- Deals with cables, voltage levels, connectors, physical topology
- Devices: **Hubs, repeaters, cables, NIC (physical)**

2. Data Link Layer

- Handles **node-to-node communication**, error detection, and framing
- Uses **MAC addresses** to identify devices on the same network
- Divided into: **LLC (Logical Link Control)** and **MAC (Media Access Control)**
- Devices: **Switches, NICs**

3. Network Layer

- Responsible for **routing, logical addressing**, and path selection
- Uses **IP addresses**
- Protocols: **IP, ICMP, IGMP, RIP, OSPF**
- Devices: **Routers**

4. Transport Layer

- Ensures **reliable data transfer** between end systems

- Performs **segmentation, flow control, and error recovery**
- Protocols: **TCP (reliable), UDP (unreliable but fast)**

5. Session Layer

- Manages **sessions (dialogues)** between applications
- Handles **connection establishment**, maintenance, and termination
- Example: Keeping multiple browser tabs connected to different websites

6. Presentation Layer

- Translates data between application and network formats
- Handles **encryption, decryption, compression, and encoding**
- Example: SSL/TLS, JPEG, MP3

7. Application Layer

- Closest to the user; provides **network services** directly to applications
 - Protocols: **HTTP, FTP, SMTP, DNS, DHCP**
-

Why is the OSI Model Important?

- Helps standardize **network design and troubleshooting**
 - Encourages **interoperability** between different vendors/devices
 - Assists in **breaking down complex network issues**
 - Forms the foundation for certifications like **CCNA, Network+, CEH**
-

Easy Way to Remember the 7 Layers

From Layer 7 to 1 (Top to Bottom):

All People Seem To Need Data Processing

From Layer 1 to 7 (Bottom to Top):

Please Do Not Throw Sausage Pizza Away