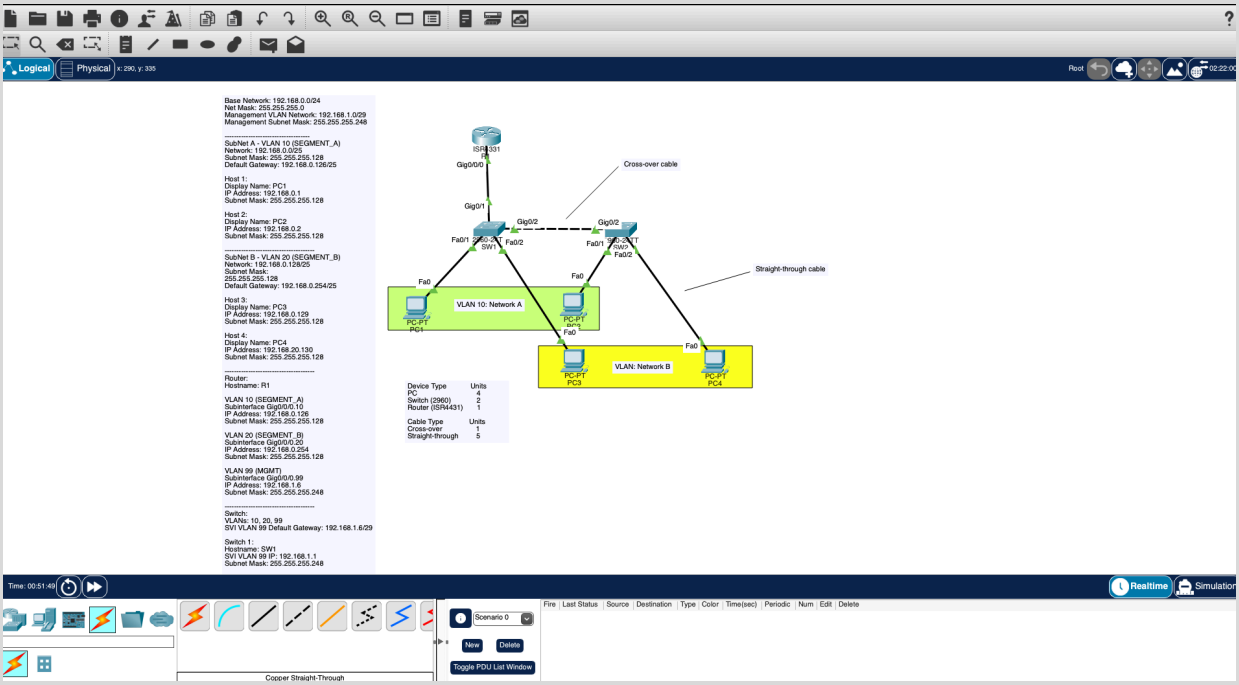
Lab 1: Subnetting, VLAN & Trunk Configuration, Router-on-a-Stick Inter-VLAN Routing, NTP, and Secure Device Access

This lab focuses on implementing foundational Layer 2 and Layer 3 networking concepts by configuring VLANs, trunking, and inter-VLAN routing using Router-on-a-Stick. The lab begins with initial device setup, including hostnames, clock configuration, and NTP synchronization, followed by VLAN creation and access port assignment on switches. Trunk links are configured using 802.1Q with a reassigned native VLAN to enhance security. Inter-VLAN communication is enabled by configuring router subinterfaces, each mapped to a specific VLAN and serving as the default gateway for hosts. Connectivity and functionality are verified through interface, VLAN, trunk, and end-to-end communication testing.

Network Topology:



Network Addressing Plan (Subnetting):

Overall Network:

Parameter	Value
Base Network	192.168.0.0/24
Subnet Mask	255.255.255.0
Management VLAN Network	192.168.1.0/29
Management Subnet Mask	255.255.255.248

Subnet A – VLAN 10 (SEGMENT_A)

Parameter	Host 1 (PC1)	Host 2 (PC2)
IP Address	192.168.0.1	192.168.0.2
Subnet Mask	255.255.255.128	255.255.255.128
Default Gateway	192.168.0.126	192.168.0.126
VLAN	10	10
Network	192.168.0.0/25	

Subnet B – VLAN 20 (SEGMENT_B)

Parameter	Host 3 (PC3)	Host 4 (PC4)
IP Address	192.168.0.129	192.168.0.130
Subnet Mask	255.255.255.128	255.255.255.128
Default Gateway	192.168.0.254	192.168.0.254
VLAN	20	20
Network	192.168.0.128/25	

Router – R1

Interface	Subinterface	IP Address	Subnet Mask	VLAN / Purpose
Gig0/0/0	.10	192.168.0.126	255.255.255.128	VLAN 10 / SEGMENT_A DGW
Gig0/0/0	.20	192.168.0.254	255.255.255.128	VLAN 20 / SEGMENT_B DGW
Gig0/0/0	.99	192.168.1.6	255.255.255.248	VLAN 99 / MGMT DGW

Switch 1 – SW1

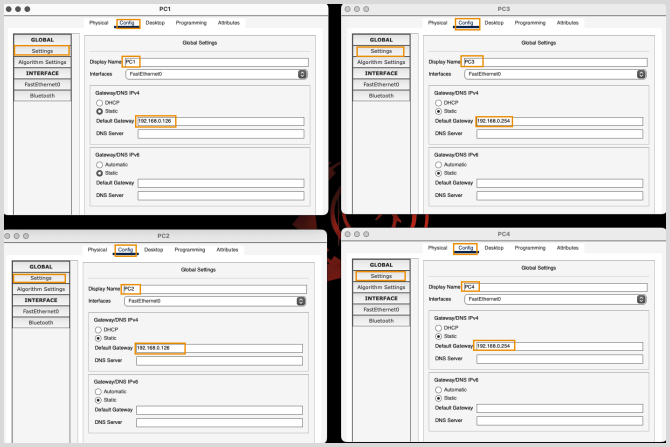
Parameter	Value
Hostname	SW1
VLANs	10, 20, 99
SVI VLAN 99 IP Address	192.168.1.1 /29
Default Gateway	192.168.1.6

Switch 2 – SW2

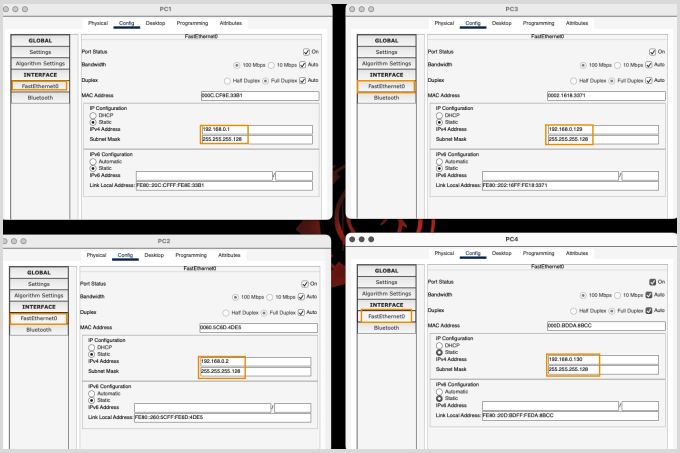
Parameter	Value
Hostname	SW2
VLANs	10, 20, 99
SVI VLAN 99 IP	192.168.1.2 /29
Default Gateway	192.168.1.6

Initial Endpoints (PC1, PC2, PC3, & PC4) Setup:

- Configure Display Name & Default Gateway



• Configure IP Address & Subnet Mask



Initial Router & Switches Setup

- Configure hostnames
- Set system clock
- Configure NTP for time synchronization
- Secure device access (console & VTY)
- Save configurations

Router Configuration:

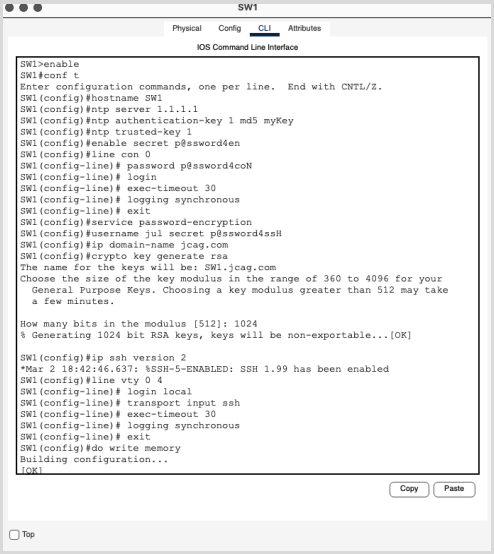
Would you like to enter the initial configuration dialog? [yes/no]: no

! Enter privileged EXEC mode
`enable`
! Enter global configuration mode
`configure terminal`
! Set hostname
`hostname R1`

! Set system clock and timezone

```
exit
clock set 17:22:00 Jan 27 2026          → configure on privilege exec mode
conf t
clock timezone EST -5                   → configure on global config mode
! Configure loopback 0 interface (for NTP source)
interface loopback0
  ip address 1.1.1.1 255.255.255.255
  exit
! Configure NTP master with authentication
ntp master 3                            → optional stratum number
ntp authentication-key 1 md5 myKey
ntp trusted-key 1
! Set enable secret with scrypt (Type 9)          → not an option for ISR4331 Router
enable algorithm-type scrypt secret p@ssword4en
! Set enable secret with MD5 (Type 5)
enable secret p@ssword4en
! Configure console access (set password, standby time, sync with log output)
line con 0
  password p@ssword4coN
  login
  exec-timeout 30
  logging synchronous
  exit
! Encrypt all existing and future plain-text passwords (Type 7)
service password-encryption
! Create local username and secret for login (Type 5)
username jul secret p@ssword
! Configure domain name for crypto keys (needed for SSH)
ip domain-name jcag.com
! Generate RSA keys for SSH
crypto key generate rsa
! When prompted, choose default [512]     → enter 1024 bits (at least 768 bits size for SSH  v2)
! Force SSH version 2
ip ssh version 2
! Configure VTY lines (set VTY line for up to 5 simultaneous users,  login to use local DB for user &
password, transport input SSH only (no Telnet or AUX), standby time, sync to log output)
line vty 0 4
  login local
   transport input ssh
   exec-timeout 30
   logging synchronous
   exit
! Save configuration
do write memory
```

Switch Configuration:



! Enter privileged EXEC mode
`enable`
! Enter global configuration mode
`configure terminal`
! Set hostname
`hostname SW1` → run `hostname SW2` for Switch 2
! Configure NTP server with authentication
```
ntp server 1.1.1.1
ntp authentication-key 1 md5 myKey
ntp trusted-key 1
```
! Set enable secret with scrypt (Type 9 hash) → not an option for Layer 2 Switches
`enable algorithm-type scrypt secret p@ssword4en`
! Set enable secret with MD5 (Type 5)
`enable secret p@ssword4en`
! Configure console access
```
line con 0
  password p@ssword4coN
  login
  exec-timeout 30
  logging synchronous
  exit
```
! Encrypt all plain-text passwords (service password-encryption)
`service password-encryption`
! Create local user for SSH login (Type 5 secret)
`username jul secret p@ssword4ssH`
! Configure domain name for crypto keys (needed for SSH)
`ip domain-name jcag.com`
! Generate RSA keys for SSH
`crypto key generate rsa`
! When prompted, choose default [512] → enter `1024` bits (at least 768 bits size for SSH v2)
! Force SSH version 2
`ip ssh version 2` → failed to enable on L2 Switch (2960), 1.99 enabled

! Configure VTY lines (set VTY line for up to 5 simultaneous users, login to use local DB for user & password, transport input SSH only (no Telnet or AUX), standby time, sync to log output)

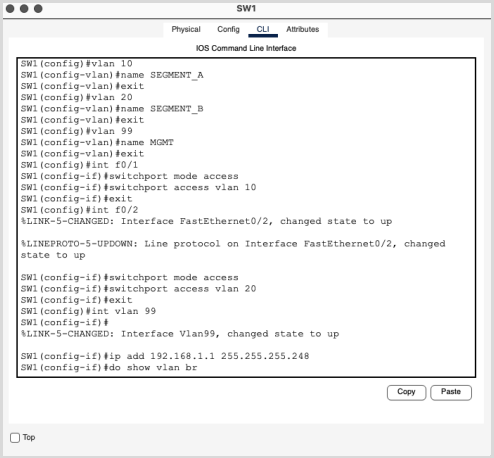
```
line vty 0 4
  login local
  transport input ssh
  exec-timeout 30
  logging synchronous
  exit
```
! Save configuration
```
do write memory
```

! Configure Switch 2 (change input entry accordingly)

Switching (Layer 2)

- Create VLANs
- Assign access ports to VLANs
- Verify VLAN membership
- Configure management VLAN

Switch Configuration:



! VLAN Creation
```
vlan 10
  name SEGMENT_A
  exit
vlan 20
  name SEGMENT_B
  exit
vlan 99
  name MGMT
  exit
```
! Assign VLANs to Access Ports
```
interface fastEthernet 0/1
  switchport mode access
  switchport access vlan 10
  exit
interface fastEthernet 0/2
  switchport mode access
  switchport access vlan 20
  exit
```
! Configure Management VLAN SVI
```
interface vlan 99
```

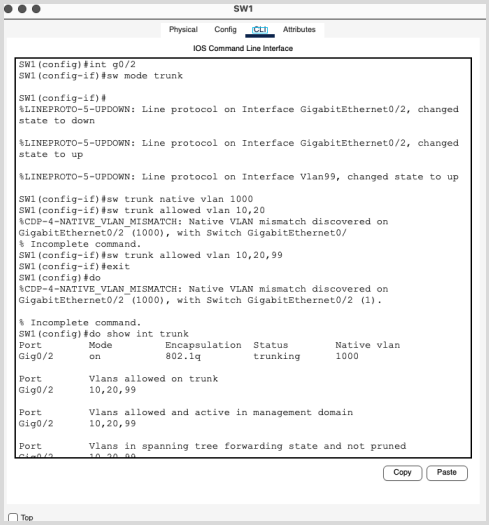
```
  ip address 192.168.1.1 255.255.255.248    → change IP to 192.168.1.2 for SW2
  no shutdown
  exit
```
! Verify VLANs
```
do show vlan brief
```
! Verify Interfaces IP Addressing & Status
```
do show ip interface brief
```

! Configure SW2 (change input entry accordingly)

Trunking

- Configure 802.1Q trunk links
- Reassign native VLAN (non-default VLAN)
- Allow required VLANs on trunks
- Verify trunk status

Switches Configuration:



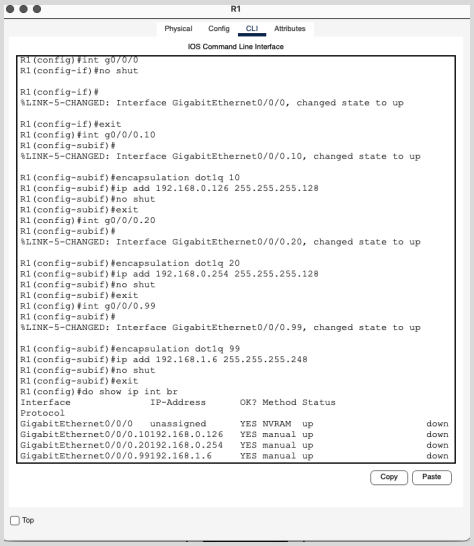
! Configure Trunk on SW1
```
interface gigabitEthernet0/2
 switchport mode trunk
 switchport trunk native vlan 1000
 switchport trunk allowed vlan 10,20,99
 exit
```
! Verification
```
do show interfaces trunk
```

! Configure Switch 2

Inter-VLAN Routing

- Configure Router-on-a-Stick (ROAS)
- Create router subinterfaces
- Assign VLAN tags to subinterfaces
- Configure default gateways for hosts
- Verify inter-VLAN connectivity

Router Configuration:



! Enable physical interface

```
interface GigabitEthernet0/0/0
  no shutdown
  exit
```

! Configure subinterface for VLAN 10

```
interface GigabitEthernet0/0/0.10
  encapsulation dot1q 10
  ip address 192.168.0.126 255.255.255.128
  no shutdown
  exit
```

! Configure subinterface for VLAN 20

```
interface GigabitEthernet0/0/0.20
  encapsulation dot1q 20
  ip address 192.168.0.254 255.255.255.128
  no shutdown
  exit
```

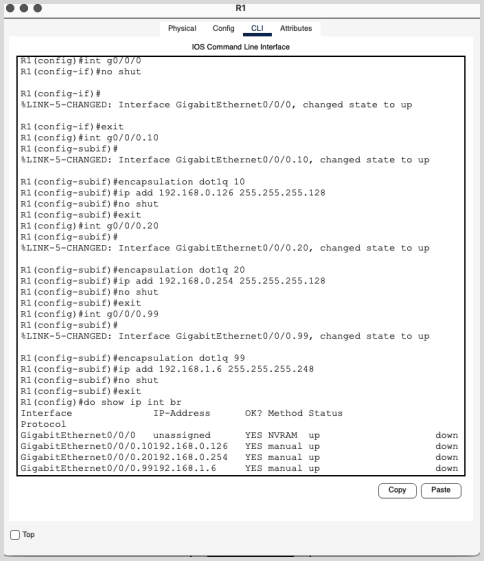
! Configure subinterface for VLAN 99 (Management)

```
interface GigabitEthernet0/0/0.99
  encapsulation dot1q 99
  ip address 192.168.1.6 255.255.255.248
  no shutdown
  exit
```

! Verify interfaces

```
do show ip interface brief
```

SW1 Configuration:



! Configure Trunk on SW1

```
interface gigabitEthernet0/2
 switchport mode trunk
 switchport trunk native vlan 1000
 switchport trunk allowed vlan 10,20,99
 exit
```

! Verification

```
do show interfaces trunk
```

Verification & Testing

- Verify configurations (VLANs, trunking, and interfaces)
- Test end-to-end connectivity using ping
- Validate routing between VLANs

Category	**Command**	**Notes / What It Shows**
Interface & IP	show ip interface brief	Displays IP addresses, interface status (up/down), and protocol status.
Routing/Inter-VLAN	show running-config	Confirm subinterfaces, VLAN encapsulation, and IP assignments.
	ping <destination_IP>	Verify inter-VLAN routing is working.
VLANs	show vlan brief	Displays VLAN IDs, names, status, and assigned ports.
SVI/Mgmt VLAN	show ip interface brief	Shows SVI IP address, status, and protocol.
	ping <SVI_IP>	Confirms switch management connectivity to router.
Trunking	show interfaces trunk	Displays trunk status, encapsulation, native VLAN, and allowed VLANs.
	show interfaces <int> sw	Shows mode (access/trunk), native VLAN, and operational details.
CDP/Neigh Discovery	show cdp neighbors	Displays connected Cisco devices, local interface, remote device, and capabilities.
	show cdp neighbors detail	Displays IP addresses of neighbors and more detailed info.
NTP	show ntp associations	Displays NTP associations and stratum info.
	`show running-config	include ntp`	

Device Security	`show running-config	include username`	
	`show running-config	include enable`	
	`show running-config	section line vty`	
General Verification	show startup-config	Confirms configuration was written to NVRAM.
	ping <neighbor_IP>	Confirms connectivity to switches, PCs, or other routers.
	ping <PC_in_other_VLAN>	Verifies that Router-on-a-Stick routing is working.

Successful Pings from PC1 (VLAN 10):

192.168.0.2 (PC2: VLAN 10)

192.168.0.129 (PC3: VLAN 20)

192.168.0.130 (PC$: VLAN 20)

Successful SSH from PC1 to R1:

ssh -l jul 192.168.1.6

password: p@ssword