REVISION SHEET FOR CNW/CPT

Console Password

Nihar@Router> enable

Nihar@Router# configure terminal

Nihar@Router(config)# line console 0

Nihar@Router(config-line)# password your_console_password

Nihar@Router(config-line)# login

Nihar@Router(config-line)# exit

Privileged EXEC Password Protection

switch# config t

switch(config)# enable password nihar123

ALL Security Configuration Commands

2. To configure a console password of *conpass* on VAN-R1, enter the following commands:

```
VAN-R1>enable
VAN-R1#config term
VAN-R1(config)#line con 0
VAN-R1(config-line)#password conpass
VAN-R1(config-line)#login
```

3. To configure an aux password of *auxpass* on VAN-R1, enter the following commands:

```
VAN-R1(config-line)#line aux 0
VAN-R1(config-line)#password auxpass
VAN-R1(config-line)#login
```

4. To configure telnet passwords of *telnetpass* by configuring the VTY ports, enter the following commands:

```
VAN-R1(config-line)#line vty 0 4
VAN-R1(config-line)#password telnetpass
VAN-R1(config-line)#login
```

5. Create an enable password of *enablepass*:

```
VAN-R1(config-line)#exit
VAN-R1(config)#enable password enablepass
```

6. Create an enable secret of *enablesecret*:

```
VAN-R1(config)#enable secret enablesecret
VAN-R1(config)#exit
VAN-R1#
```

Configuring Banners

MOTD banner

The MOTD banner appears before the administrator is asked to log in and is used to display a temporary message that may change from day to day.

Banner motd ‘Keep Out’

Login banner

The login banner displays before the administrator logs in, but after the MOTD banner appears, and is used to display a more permanent message to the administrator.

#Banner login $

#Message

#$

Exec banner

The exec banner is used to display a message after the administrator authenticates to the system and after he enters user EXEC mode.

#Banner exec $

#Message

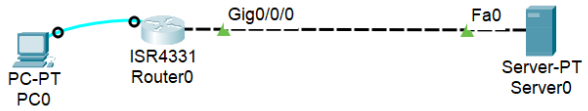
#$

Viewing Configurations

#Show running-config

#show startup-config

Back Up to TFTP Server



STEP1: Set default gateway and IP to server

STEP2: Find the IOS Img name in system **Router# dir flash:** OR **show version | include image**

STEP3: Now copy flash to TFTP -> **Router# copy flash tftp**

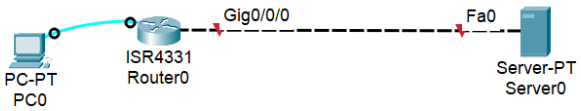
STEP4: Now enter the Details

- 'source': the IOS image file in flash memory to be backed up.
- 'destination': the TFTP server IP address and filename to save the backup file to.
- Example: 'copy flash tftp'
  'Address or name of remote host []? 192.168.1.100'
  'Destination filename [c2600-ios.bin]?'
  '¡
  '26174764 bytes copied in 77.764 secs (337915 bytes/sec)'

Now it is Successfully backup to TFTP server, you can check its file in TFTP server -> Services -> TFTP

Security Bypass

STEP1: Turn off the router and again On it.



STEP2: Go to CLI an press Ctrl+c to interrupt the boot sequence. Now you are Rommon mode (Mini OS).

STEP3: Set the configuration register value to 0x2142. This setting tells the router to ignore the startup configuration during the next boot -> rommon 1 > confreg 0x2142

rommon 2 > reset (It will restart the Router)

STEP4: Now you will find that there is no password needed because it bypass the security.

STEP5: Router# copy tftp startup-config

STEP6: Router(config)# config-register 0x2102

STEP7: Now set new Password

STEP8: Router# copy running-config startup-config *OR* write

New password set successfully

Telnet Password

Nihar@Router(config)# line vty 0 4

Nihar@Router(config-line)# password your_vty_password

Nihar@Router(config-line)# login

Nihar@Router(config-line)# exit

SSH Password

Router> enable

Router# configure terminal

Router(config)# hostname Nihar@Router

Router(config)# ip domain-name example.com

Router(config)# crypto key generate rsa

(Choose the key size, e.g., 1024)

Router(config)# line vty 0 15

Router(config-line)# transport input ssh (transport input ssh - Restrict access to SSH only)

Router(config-line)# login local

Router(config-line)# exit

Router(config)# username admin privilege 15 secret your_password

Router(config)# ip ssh version 2

Router(config)# line vty 0 15

Router(config-line)# login local (It means that users must log in with usernames and passwords that have been configured locally on the router)

Router(config-line)# end

CDP (Refer to PPT for Details)

CDP Configuration & Verification

- Both Cisco routers and switches use the same CDP commands.
- CDP is globally enabled by default.
- CDP is also enabled in each interface by default.
- To enable CDP globally:

```
SW-3(config)#cdp run
```

To disable CDP globally:

```
SW-3(config)#no cdp run
```

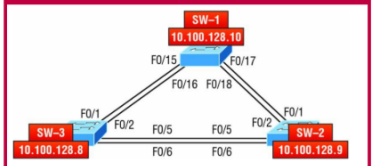
- To enable CDP on specific interface:

```
SW-3(config)#int <name>
SW-3(config-if)#cdp enable
```

To disable CDP on interface:

```
SW-3(config)#int <name>
SW-3(config-if)#no cdp enable
```

Configure the given network



CDP verification

- `show cdp`
- `show cdp neighbors {<cr>|detail}`
- `show cdp interface {<cr>|<name>}`
- `show cdp entry {* | <d name>}`
- `show cdp traffic`

- **Enable CDP:**

```
plaintext
Copy code
Switch(config)# cdp run
```

- **View CDP Neighbors:**

```
plaintext
Copy code
Switch# show cdp neighbors
```

- **View Detailed Information:**

```
plaintext
Copy code
Switch# show cdp neighbors detail
```

- **Disable CDP on a Specific Interface:**

```
plaintext
Copy code
Switch(config-if)# no cdp enable
```

LLDP(Refer to PPT for Details)

- Both Cisco routers and switches use the same LLDP commands.
- **By default**, LLDP is disabled both in globally as well as in each interface.
- To enable LLDP globally:

```
SW-3(config)#lldp run
```

To disable LLDP globally:

```
SW-3(config)# no lldp run
```

- To enable/disable LLDP on a specific interface(tx) for tramsit

```
SW-3(config)# interface <interface name>
SW-3(config-if)# [no] lldp transit
```

- To disable/disable LLDP on a interface(rx) for receive:

```
SW-3(config)# interface <interface name>
SW-3(config-if)# [no] lldp receive
```

- Configure the LLDP timer: `SW-3(config)# LLDP timer seconds`
- Configure the LLDP holdtime: `SW-3(config)# LLDP holdtime seconds`
- Configure the LLDP reinit timer: `SW-3(config)# LLDP reinit seconds`

CDP verification (Check supports for CPT)

- `show lldp ?`
- `show lldp`
- `show lldp neighbors {<cr>|detail}`
- `show lldp entry <device name>`
- `show lldp interface`
- `show lldp traffic`

- **Enable LLDP Globally:**

```
plaintext                                   Copy code
Switch(config)# lldp run
```

- **Enable LLDP on a Specific Interface:**

```
plaintext                                   Copy code
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
```

- **View LLDP Neighbors:**

```
plaintext                                   Copy code
Switch# show lldp neighbors
```

- **View Detailed Information:**

```
plaintext                                   Copy code
Switch# show lldp neighbors detail
```

- **Disable LLDP on a Specific Interface:**

```
plaintext                                   Copy code
Switch(config-if)# no lldp transmit
Switch(config-if)# no lldp receive
```

Comparison of CDP and LLDP

Feature	CDP (Cisco Discovery Protocol)	LLDP (Link Layer Discovery Protocol)
Standard	Cisco proprietary	Open standard (IEEE 802.1AB)
Vendor Support	Cisco devices only	Multi-vendor support
Information Exchanged	Device ID, IP address, port ID, capabilities, platform	Device ID, IP address, port ID, capabilities, platform, TLVs
Default Interval	60 seconds	30 seconds
Default Hold Time	180 seconds	120 seconds
Layer	Data Link (Layer 2)	Data Link (Layer 2)

Create VLAN

Switch(config)# vlan 10

Switch(config-vlan)# name HR

Switch#show vlan

Access Port

SW1(config)#int fastEthernet 0/1

SW1(config-if)#switchport mode access

SW1(config-if)#switchport access vlan 10

With multiple interfaces at a time

SW2(config)#int range fastEthernet 0/1-4

SW2(config-if-range)#switchport mode access

SW2(config-if-range)#switchport access vlan 10

SW2(config-if)#exit

In access port we can set one vlan so multiple vlan can't communicate using access port so in order to established multiple valn connection we can either use multiple port to communicate like below or We can use Trunk port which is the next Topic.

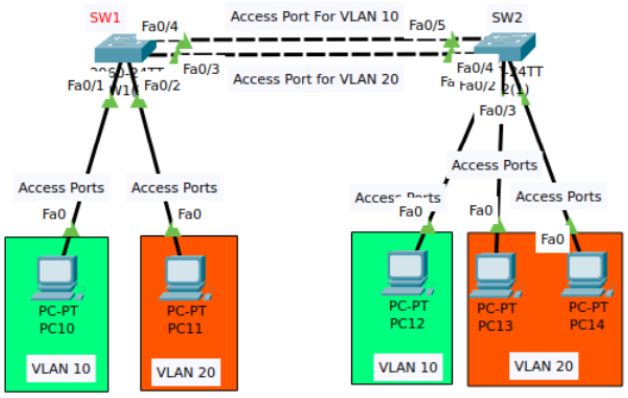
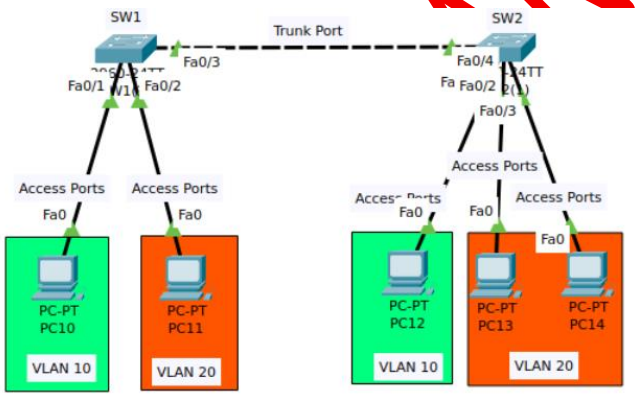


Figure 7: Multiple VLAN with Access Ports

Trunk Port



SW1(config)#vlan 20

SW1(config-vlan)#name Admin

SW1(config-vlan)#ex

SW1(config)#int range fastEthernet 0/2

SW1(config-if)#switchport mode access

SW1(config-if)#switchport access vlan 20

<u>Set Fa0/3 of SW1 as Trunk Port</u>

SW1(config)#int fastEthernet 0/3

SW1(config-if)#switchport mode trunk

Trunking methods create the illusion that instead of a single physical connection between the two trunking devices, a separate logical connection exists for each VLAN between them. When trunking, the switch adds the source port's VLAN identifier to the frame so that the device (typically a switch) at the other end of the trunk understands what VLAN originated this frame and the destination switch can make intelligent forwarding decisions on not just the destination MAC address, but also the source VLAN identifier.

Inter VLAN communication (Using Multiple port)

For each VLAN there will be dedicated access port from layer 3 device (router) to layer 2 device (switch).

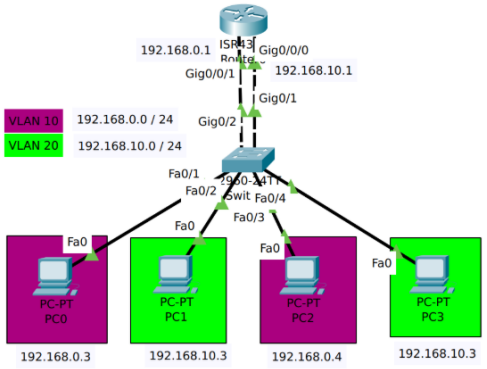


Figure 9: Legacy Inter-VLAN Routing.

Cable Configuration

Interface	VLAN	Port Type
Fa0/1	10	Access
Fa0/2	20	Access
Fa0/3	10	Access
Fa0/4	20	Access
Gig0/1	10	Access
Gig0/2	20	Access
Gig0/0/0	–	No Switchport
Gig0/0/1	–	No Switchport

VLAN database in devices

Device	VLANs
SW	10, 20
R	–

Create VLAN & assign to interfaces

SW(config)#int range f0/1, f0/3, gig0/1

SW(config-if-range)#switchport mode access

SW(config-if-range)#switchport access vlan 10

Assign Default Gateway to router interfaces

R(config)#int gigabitEthernet 0/0/0

R(config-if)#ip address 192.168.0.1 255.255.255.0

R(config-if)#no shutdown

Exit

R(config)#int gigabitEthernet 0/0/1

R(config-if)#ip address 192.168.10.1 255.255.255.0

R(config-if)#no shutdown

Router-on-a-Stick (RoaS)

There will be only one link between switch (layer 2) and router (layer 3) for all VLANs as trunk port.

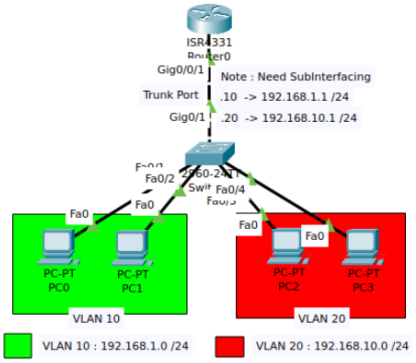


Figure 10: Router-on-a-Stick (RoaS)

Cable Configuration

Interface	VLAN	Port Type
Fa0/1	10	Access
Fa0/2	10	Access
Fa0/3	20	Access
Fa0/4	20	Access
Gig0/1	–	Trunk
Gig0/0/1	–	No Switchport

VLAN database in devices

Device	VLANs
SW	10, 20
R	-

Create VLAN & assign to interfaces

// REFER TO PREVIOUS TOPIC

Set Gig0/1 of SW to trunk port

SW(config)#int range gig 0/1

SW(config-if-range)#switchport mode trunk

Assign Default Gateway to router subinterfaces

R(config)#int gigabitEthernet 0/0/0.10 *Note: 10 indicates VLAN ID 10*

R(config-subif)#encapsulation dot1Q 10 *Note: 10 indicates VLAN ID 10*

R(config-if)#ip address 192.168.1.1 255.255.255.0

R(config-if)#no shutdown

Exit

R(config)#int gigabitEthernet 0/0/0.20 *Note: 10 indicates VLAN ID 10*

R(config-subif)#encapsulation dot1Q 20 *Note: 10 indicates VLAN ID 10*

R(config-if)#ip address 192.168.10.1 255.255.255.0

R(config-if)#no shutdown

RoaS using Multilayer Switch (MLS)

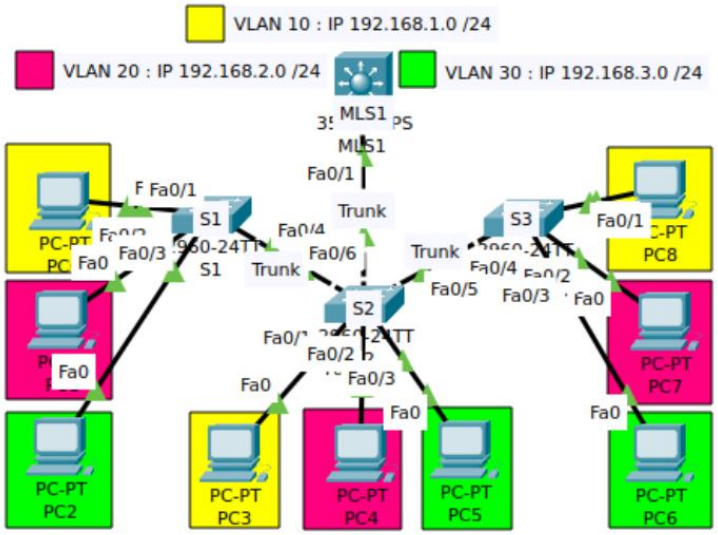


Figure 11: Router-on-a-Stick (RoaS).

Cable Configuration

Interface/ Device	VLAN	Port Type
PC 0,3,8	10	Access
PC 1,4,7	20	Access
PC 2,5,6	30	Access
S1 – S2	–	Trunk
S2 – S3	–	Trunk
S2 – MLS1	–	Trunk

VLAN database in devices

Device	VLANs
SW1, SW2, SW3	10, 20, 30
MLS1	10, 20, 30

Create VLANs & assign to interfaces

Set S1-S2 and S2-S3 interface to trunk port

Set Fa0/1 of MLS1 interface to trunk port

MLS(config)#interface FastEthernet0/1

MLS(config-if)#switchport trunk encapsulation dot1q

MLS(config-if)#switchport mode trunk

R1(config-if)#no shutdown

DTP- Dynamic Trunking Protocol

DTP Mode	Generate DTP Messages	Default Frame Tagging
On or trunk	Yes	Yes
Desirable	Yes	No
Auto	No	No
No-negotiate	No	Yes
Off	No	No

Verification command: SW#show int fa0/1 switchport

Dynamic Auto ---------- trunk || dynamic desirable => Trunk mode

Dynamic auto ---------- access || dynamic auto => Access

Administrative Mode	Trunk	Dynamic Desirable	Access	Dynamic Auto
Dynamic Auto	Trunk	Trunk	Access	Access
Dynamic Desirable	Trunk	Trunk	Access	Trunk
Trunk	Trunk	Trunk	✖	Trunk
Access	✖	Access	Access	Access

VTP VLAN Trunking Protocol

- ➔ Three VTP modes: Server, Client and transparent.
- ➔ Cisco switches operate in VTP server mode by default.
- ➔ All servers that need to share VLAN information must use the same domain name and password.
- ➔ A switch can be in only one domain at a time.
- ➔ VTP information is sent between switches only via a trunk port.
- ➔ Switches advertise VTP management domain information as well as a configuration revision number and all known VLANs with any specific parameters.
- ➔ VTP transparent mode: Switches are configured to forward VTP information through trunk ports but not to accept information updates or update their VLAN databases.

1. VTP Server

- It can add/modify/delete VLANs.
- It stores the VLAN database in non-volatile RAM(NVRAM)
- It will increase the **revision number** every time a VLAN is added/modified/deleted.
- It will advertise the latest version of the VLAN databse on trunk interfaces, and the VTP client will synchronize their VLAN database to it.
- VTP server also function as VTP clients. Therefore a VTP server will synchronize to another VTP server with a higher revision number.

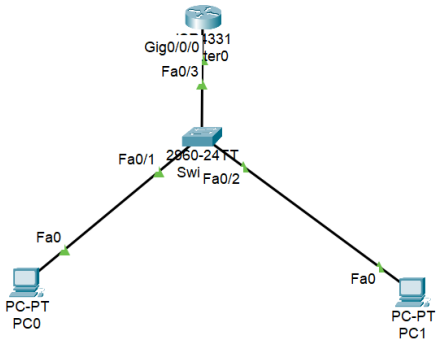
2. VTP Client

- Cannot add/modify/delete VLANs.
- Do not store the VLAN database in non-volatile RAM(NVRAM)
- Will synchronize their VLAN database to the server with the highest revision number in their VTP domain
- Will advertise their VLAN database and forward VTP advertisements to other clients over their trunk ports.

3. VTP Transparent

- Does not participate in the VTP domain or share its VLAN database.
- Maintains its own database in NVRAM. It can add/modify/delete VLANs of own, but they won't be advertised to other switches.
- Will forward VTP advertisements that are in the same domain as it.
- Switches in VTP transparent mode advertise VTP management domain information as well as a configuration revision number and all known VLANs with any specific parameters.
- The whole purpose of transparent mode is to allow remote switches to receive the VLAN database from a VTP Server configured switch through a switch that is not participating in the same VLAN assignments.

DHCP



Router> enable

Router# configure terminal

Router(config)# ip dhcp excluded-address 192.168.1.1 (If you want to exclude certain IP addresses from the range)

Router(config)# ip dhcp pool LAN_POOL

Router(dhcp-config)# network 192.168.1.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.1.1

Router(dhcp-config)# domain-name cnw.edu

Router(dhcp-config)# exit

Router(config)# end

Router# show running-config | include dhcp

DHCP server

DNS

Lookup :- In the context of networking and DNS (Domain Name System), a "lookup" refers to the process of resolving a domain name (like www.example.com) into an IP address (like 192.168.1.1) or vice versa. This process is essential for devices to communicate over a network, as IP addresses are

used to route data between devices, while domain names are more user-friendly for humans to remember and use.

ROUTER As DNS

Router> enable

Router# configure terminal

Router(config)# ip dns server

Router(config)# ip host server1 192.168.1.10

Router(config)# ip host server2 192.168.1.11

Router(config)# ip domain-name example.com

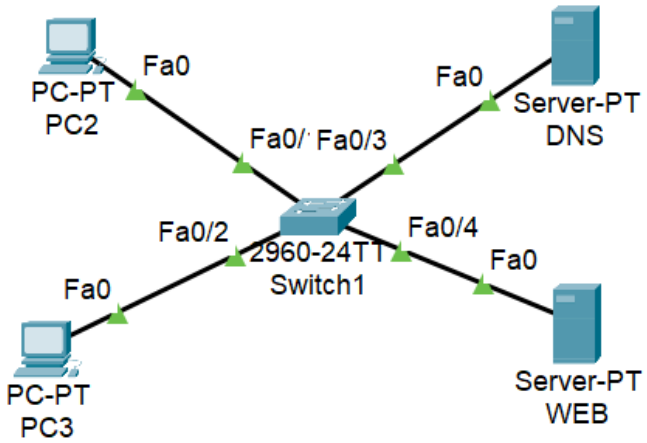
Router(config)# exit

Router# show running-config | include dns

Router# show running-config | include host

Router# show hosts

Using Server



STEP1-> Set the IP in every system. In dns set dns ip address.

STEP2-> Turn on DNS in DNS server & add web address to it.

STEP3-> Turn on DNS in web server.

NAT

Network Address Translation (NAT) is a method used in networking to modify network address information in IP packet headers while they are in transit across a traffic routing device. Its main purpose is to improve security and decrease the number of IP addresses an organization needs.

Static NAT

Basic Configuration

Router> enable

Router# configure terminal

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0 (Private)

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface GigabitEthernet0/1

Router(config-if)# ip address 200.1.1.1 255.255.255.0 (Public)

Router(config-if)# no shutdown

Router(config-if)# exit

Map the internal IP to the external IP

Router(config)# ip nat inside source static 192.168.1.2 200.1.1.2

Configure the interfaces to specify which is inside and which is outside

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ip nat inside

Router(config-if)# exit

Router(config)# interface GigabitEthernet0/1

Router(config-if)# ip nat outside

Router(config-if)# exit

Verify the Configuration:-

Router# show ip nat translations

Dynamic NAT

Setup a Network Topology

Config Router

Router> enable

Router# configure terminal

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface GigabitEthernet0/1

Router(config-if)# ip address 200.1.1.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

Configure NAT Pool:

Router(config)# ip nat pool MY_POOL 200.1.1.10 200.1.1.20 netmask 255.255.255.0

Configure Access List:

Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

Configure Dynamic NAT (Mapping):

Router(config)# ip nat inside source list 1 pool MY_POOL

Configure the interfaces

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ip nat inside

Router(config-if)# exit

Router(config)# interface GigabitEthernet0/1

Router(config-if)# ip nat outside

Router(config-if)# exit

Verify the Configuration:

Router# show ip nat translations