Cisco Configuration Guide

Basic Configuration

Modes

Cisco IOS has a Command Line Interface (CLI) and it has three command line modes. Each mode has access to a different set of IOS commands.

User Mode

Users can access the User Mode when first logged in to the device. The mode can be identified by the "**>**" symbol after the hostname of the device.
eg:-

- Switch1>

Privileged Mode

Privileged mode allows users to view the system configurations, restart the device, and enter the device configuration mode. The mode can be identified by the "**#**" symbol in the CLI followed by the hostname.

Eg:-

- Switch1#

The user can enter the privileged mode by entering "**enable**" inside the user mode.

Global Configuration Mode

This mode allows the user to modify the running system configuration. From privileged mode, the user can move to Global Configuration Mode by entering "**configure terminal**".

Global Configuration mode can be identified as below

- Switch1(config)#

Global configuration mode has sub configuration modes for devices like switches, routers, and firewalls.

Interface Mode : Switch1(config-if)#
Sub interface Mode : Router1(config-subif)#
Line Mode : Switch1(config-line)#

Accessing the modes in a Switch or Router

Command	Purpose
Switch1> enable	Move to Privileged Mode from User Mode
Switch1# configure terminal	Move to Global Configuration mode
From here you can change the system configurations	
Switch1(config)# hostname LAB_S1	Change the hostname of the switch
LAB_S1(config)#	The hostname get change accordingly

Running configuration

There is a command in cisco devices to see the current running configuration. It will show all the configurations done by the admin to the device. It will be a valuable command to check whether you have configured each device correctly in the lab sessions.

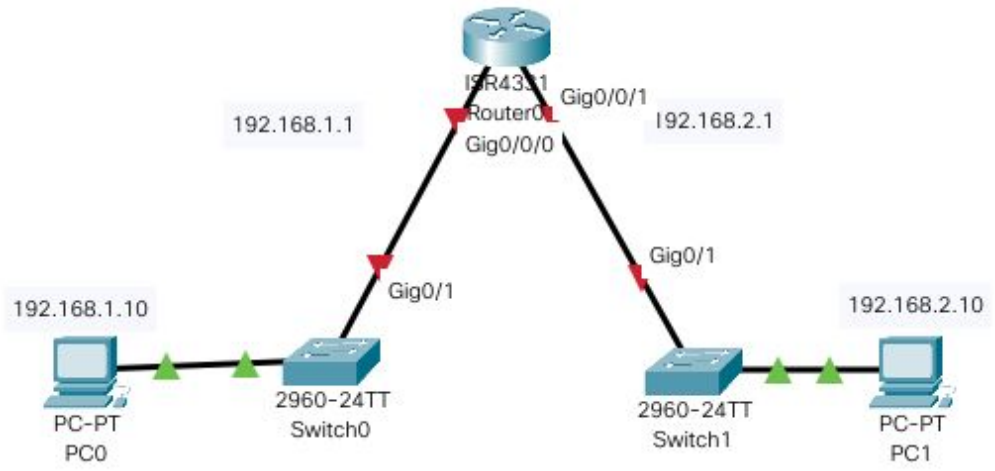
Command	Purpose
Switch1> enable	Move to Privileged Mode from User Mode
Switch1# show running-config	Shows the currently running configuration

In a real hardware device, if some change has done to a running configuration, it has to save to the startup configuration. If not the changes will not affect when the device is restarted. It is also possible to keep a backup of the currently running configuration.

Command	Purpose
Switch1# copy running-config startup-config	Copy currently running configuration to the startup configuration

Router Configuration

Interface Configuration (Gigabit/ Fast Ethernet)

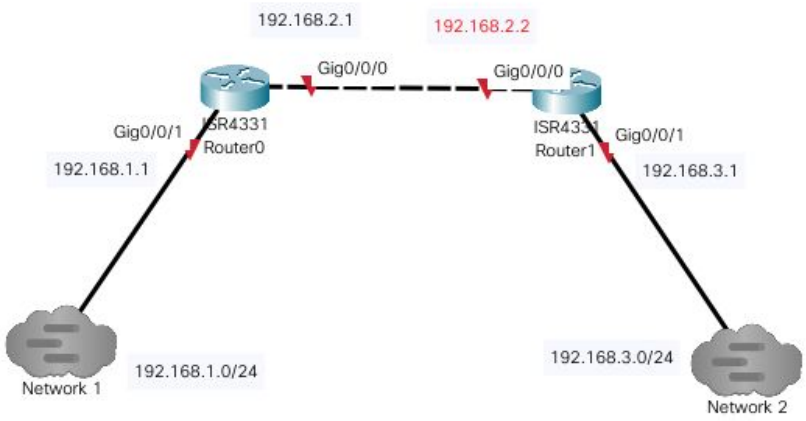


Two networks connected to the router via a router. The following table shows the general steps to configure router ethernet interfaces.

Command	Purpose
configure terminal Eg:- Router0# configure terminal	Enters Global Configuration Mode
Interface *gigabitethernet slot/port* Eg:- Router0(config)# interface gigabitethernet 0/0/0	Enter the configuration mode for Gigabit Ethernet interface
ip address *ip-address mask* Eg:- Router0(config-if)# ip address 192.168.1.1 255.255.255.0	Sets the IP address for selected interface
no shutdown Eg:- Router(config-if)# no shutdown	Enables the Ethernet interface (By default, the interface is in down state)
exit Eg:- Router0(config-if)# exit	Exit from the Interface configuration mode

Similarly, follow the same steps to configure the Gigabit Ethernet 0/0/1 interface.

Routing



Two networks are connected by two routers. Router0 does not have knowledge about the **192.168.3.0/24** network. Similarly, **Router1** does not have knowledge about the **192.168.1.0/24** network. The routers need to configure with static routing or with routing protocols in order to communicate from Network 1 to Network 2.

Static routes

Router0 can gain routes to network 2 (192.168.3.0/24) by the following steps.

Command	Purpose
configure terminal Eg:- Router0# configure terminal	Enters Global Configuration Mode
ip route *ip-address-network mask interface-number[ip-address]* *Eg*:- Router0(config) ip route 192.168.3.0 255.255.255.0 192.168.2.1	Specifies static routes for the IP packets. Here router configure send packets to the 192.168.3.0/24 network via the interface with ip address 192.168.2.1

The same steps should follow to set static routes from **Router1** to **network 1**.

Routing Protocol - RIP basic configuration

RIP allows automatically advertises routing information between the routers via UDP data packets. The following steps show how to configure RIP in **Router0**.

Command	Purpose
configure terminal Eg:- Router0# configure terminal	Enters Global Configuration Mode
router rip Eg:- Router0(config)# router rip	Enables a RIP routing process and enters the router configuration mode.
network *ip-address* Eg:- Router0(config-router)# network 192.168.1.0 Router0(config-router)# network 192.168.2.0	Associate networks connected to the router with the RIP routing process.
exit Eg:- Router0(config-if)# exit	Exit from the Router configuration mode

Routing Protocol - OSPF basic configuration

OSPF needs to be configured similarly in all routers and updates the routing table in each router. The configuration for **Router0** is given below.

Command	Purpose
configure terminal Eg:- Router0# configure terminal	Enters Global Configuration Mode
router ospf *process-id* Eg:- Router0(config)# router ospf 101	Enables OSPF routing and enters router configuration mode.
network *ip-address wildcard-mask* **area** *area-id* Eg:- Router0(config-router)# network 192.168.1.0 0.0.0.255 area 0 Router0(config-router)# network 192.168.2.0 0.0.0.3 area 0	Defines an interface on which OSPF runs and defines the area ID for that interface.
router-id *router-id* Eg:- Router0(config-router)# router-id 1.1.1.1	Assign an identifier for the router
auto-cost reference-bandwidth *bandwidth-mbps* Eg:- Router0(config-router)# auto-cost reference-bandwidth 1000	Set reference bandwidth in Mbps for the automatic cost calculation for each interface.

Similarly, configure all routers to work with OSPF.

Prefer the commands given below to check the ospf status and routing status.

Command	Purpose
show ip route	Display the routing table
show ip protocols	Indicates the parameters the particular protocol is using to send and receive updates, the metrics it is using, and the networks it is advertising.
show ip ospf neighbor	List the neighbor router list.
show ip ospf database	Show OSPF database summary
show ip ospf interface	Show the interface information related to the OSPF.

DHCP configuration

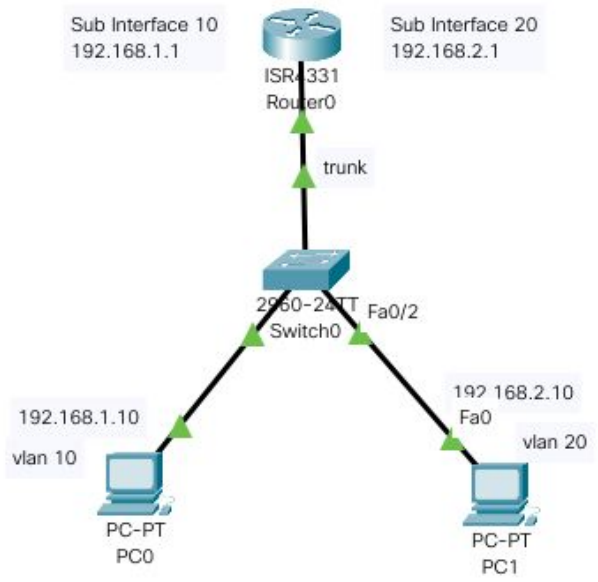
Command	Purpose
configure terminal Eg:- Router0# configure terminal	Enters Global Configuration Mode
ip dhcp pool *name* Eg:- Router0(config)# ip dhcp pool DEPT-POOL	Create DHCP pool name and enter DHCP configuration mode.
network *network-number [mask| prefix length]* Eg:- Router0(dhcp-config)# network 192.168.1.0 255.255.255.0	Specify the subnet network and maks for the DHCP address pool.
default-router *address* Eg:- Router0(dhcp-config)# default-router 192.168.1.1	Set IP address of the default route for a DHCP client.
dns-server *ip-address* Eg:- Router0(dhcp-config)# dns-server 192.168.1.254	Set IP addres of a DNS server that is available to the DHCP client.
domain-name *domain* Eg:- Router0(dhcp-config)# domain-name ce.pdn.ac.lk	Specifies the domain name for the client.
lease *{days [hours [minutes]]}*	Specify the duration of the lease.

Eg:- Router0(dhcp-config)# lease 0 4	This command will not available in Packet Tracer.
exit Eg:- Router0(dhcp-config)# exit	Return to Global configuration mode
ip dhcp excluded-address *ip-address* Eg:- Rotuer0(dhcp-config)# ip dhcp excluded-address 192.168.1.100	Specify IP address that DHCP server should not assign to DHCP clients.

Sub interface configuration

The network is given below consists of two networks in a single switch with VLANs. The intercommunication between VLANs is done by using a router. According to the diagram, the switch is connected to the router via a trunk port (See switch configuration). So traffic from both VLANs transmits via this link. The router interface needs sub interfaces to handle each VLAN.

VLAN	Devices and interfaces
10	PC0 - FastEthernet 0 Switch0 - FastEthernet 0/1 Router 0 - GigabitEthernet 0/0/0.10 (sub interface)
20	PC1 - FastEthernet 0 Switch0 - FastEthernet 0/2 Router 0 - GigabitEthernet 0/0/0.20 (sub interface)

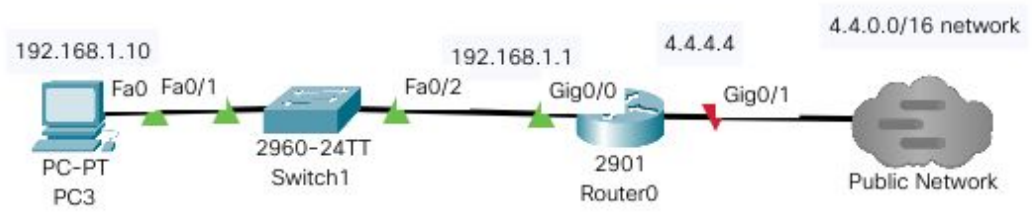


Follow the steps below to configure the subinterface for VLAN 10.

Command	Purpose
configure terminal Eg:- Router0# configure terminal	Enters Global Configuration Mode
interface *{port.subinterface}* Eg:- Router0(config)# interface gigabitethernet 0/0/0.10	Selects the interface and enters the subinterface configuration mode. The sub interface name can be any name. It does not want to be the same as VLAN id.
Encapsulation dot1q *vlan-id* Eg:- Router0(config-subif)# encapsulation dot1q 10	Configure 802.1Q encapsulation for the sub interface.
ip address ip-address mask Eg:- Router0(config-subif)# ip address 192.168.1.1 255.255.255.0	Set IP address for the subinterface in the same network associated to VLAN.

Dynamic NAT Configuration

Dynamic address mapping between public and private networks performs by dynamic NAT in a router.



The source IP address of all packets transmitted from inside network (192.168.1.0/24) needs to be converted to a public IP address in the outside network. According to the diagram Gig0/0 is the interface holding the **inside** network and Gig0/1 is the interface holding the **outside** network.

Note - The basic interface configuration needed to be done before preceding for NAT configuration.

- IP for Gig0/0 needs to assigned
- IP for Gig0/1 needs to assigned

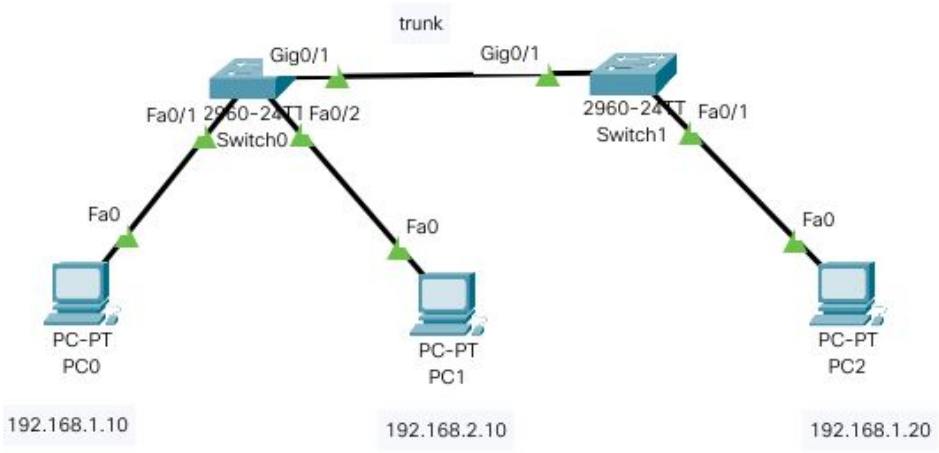
Follow the below steps for the configuration.

Command	Purpose
Define Inside and Outside Interfaces	
configure terminal Eg:- Router0# configure terminal	Enters Global Configuration Mode
interface *interface-type port* Eg:- Router0(config)# interface GigabitEthernet 0/0	Enter interface configuration mode.
ip nat *{inside | outside}* Eg:- Router0(config-if)# ip nat inside	Define inside and outside interfaces according to the network setup.
exit Eg:- Router0(config-if)# exit	Return to Global configuration mode
Define ACLs	
access-list *access-list-id* **permit** *network wildcard* Eg:- Router0(config)# access-list 1 permit 192.168.1.0	Create an access-list permitting traffic from inside network

0.0.0.255	
Nat configuration	
ip nat pool *pool-name lower-ip higher-ip* **netmask** *network-mask* Eg:- Router0(config)# ip nat pool MY_POOL 4.4.4.10 4.4.4.20 netmask 255.255.255.0	Create public IP address pool to use by the router for translating.
ip nat inside source list *access-list-id* **pool** *pool-name* Eg:- Router0(config)# ip nat inside source list 100 pool MY_POOL	Translate all addresses specified in the access list to the pool of public addresses.

Switch Configuration

VLAN



The network setup illustrated consists of 3 PCs connected to 2 VLANs via 2 Switches. Two switches connected via trunk ports.

VLAN	Devices and interfaces
10	PC0 - FastEthernet 0 Switch0 - FastEthernet 0/1

	PC2 - FastEthernet 0 Swicth1 - FastEthernet 0/1
20	PC1 - FastEthernet 0 Switch0 - FastEthernet 0/2

The steps are given below to configure the VLANs in Swicth0.

Creating VLAN

Command	Purpose
configure terminal Eg:- Swicth0# configure terminal	Enters Global Configuration Mode
vlan *vlan-id* Eg:- Swicth0(config)# vlan 10	Create a VLAN
name *vlan-name* Eg:- Switch0(config-vlan)# name DEPT_1	Names the VLAN
ip address ip-address mask Eg:- Switch0(config-subif)# ip address 192.168.1.1 255.255.255.0	Set IP address for the VLAN interface.
exit Eg:- Switch0(config-vlan)# exit	Return to Global configuration mode

Adding ports to VLAN

Command	Purpose
interface *fastethernet slot/port* Eg:- Switch0(config)# interface fastethernet 0/0	Enter the configuration mode for the Fast Ethernet interface
switchport mode access Eg:- Switch0(config-if)# switchport mode access	Change interface mode to access. The default mode is access.
switchport access vlan *vlan-id* Eg:- Switch0(config-if)# switchport access vlan 10	Sets the access mode of the interface to the specified VLAN.

Set access mode to trunk of an interface

Command	Purpose
interface *interface-type slot/port* Eg:- Switch0(config)# interface gigabitethernet 0/0	Enter the configuration mode for the interface
switchport mode trunk Eg:- Switch0(config-if)# switchport mode trunk	Change interface mode to trunk.
Only for L3 Switches **switchport trunk encapsulation dot1q** Eg:- Switch0(config-if)# switchport trunk encapsulation dot1q	Set 802.1q encapsulation for the port that is configured as trunk.

Access Control Lists (ACLs) configuration (Router and L3 Switch)

Access-list (ACL) is a set of rules defined for controlling the network traffic through a network. Once an ACL is created, it can be applied for the inbound or outbound interface of a device.

There are two types of ACLs that can be created in a cisco device as **standard** and **extended**. Standard ACLs are made using the source IP address only. ACL ids from 1-99 and 1300-1999 are assign for standard ACLs. ACL ids from 100-199 and 2000-2699 uses for extended ACLs.

Every ACL is followed by **denying all** rules at the end of the list. So that needs to be taken care of when creating ACLs.

There is a vast range of configurations to set up ACLs. Some basic configurations needed for lab sessions provided below.

Note- Try online references and help from Cisco IOS to find out more options on creating ACLs.

Standard ACL

Command	Purpose
Deny or allow single ip address	
access-list *access-list-id<1-99>* **{permit | deny } host** *ip-address* Eg:- Router0(config)# access-list 1 deny host 192.168.1.10	Block packets from the host with IP 192.168.1.10 through the applied interface.
Deny or allow packets from a selected network	
access-list *access-list-id<1-99>* **{permit | deny}** *network wildcard-address* Eg:- Router0(config)# access-list 1 deny 192.168.1.0 0.0.0.255	Block packets from all source IPs from hosts defined by wildcard address 0.0.0.255 in network 192.168.1.0.
Deny or allow packets from any source IP	
access-list *access-list-id<1-99>* **{permit | deny} any** Eg:- Router0(config)# access-list 1 deny any	Block packets from all source IPs.
access-list *access-list-id<1-99>* **permit any** Eg:- Router0(config)# access-list 1 permit any	This needs to be added end of each ACL to allow other traffic that is not denied through the network.

Extended ACL

Command	Purpose
Deny or allow from source ip range to destination ip range	
access-list *access-list-id<100-199>* **{permit | deny } ip** *source-ip wildcard-bits destination-ip wildcard-bits* Eg:- Router0(config)# access-list 100 deny host 192.168.1.0 0.0.0.255 4.4.4.0 0.0.0.255	Deny traffic from 192.168.1.0/24 network to 4.4.4.0/24 network.
Extended ACLs have many options to select the source and destination IPs and ports. Use help "?" in CLI to search for needed arguments for your specific need.	

Applying ACL to an interface

The ACL can be applied to the inbound traffic or outbound traffic of an interface.

Command	Purpose
configure terminal Eg:- Router0# configure terminal	Enters Global Configuration Mode
interface *interface-type {port | id}* Eg:- Router0(config)# interface FastEthernet 0/0	Select the interface to apply the ACL. It can be a physical interface or VLAN interface
ip access-group *{access-list-id | name}* **{in | out}** Eg:- Router0(config-if)# ip access-group 1 out	Apply ACL with id 1 to the selected interface's outbound traffic.