*privileged EXEC mode*



To return to user EXEC mode from privileged EXEC mode (თითქმის არ გამოიყენება რადგან რასაც privileged ში თითქმის ყველაფრის გამოყენება შეგვიძლია რაც exec -ში.)

**disable**

*global configuration mode*



**conf t**

change the hostname

**hostname R1**

undo a configuration command

**no**

**no hostname R1**

return you to privileged EXEC mode from global configuration mode

**exit**

You can view each configuration file

**show running-config**

**show startup-config**

copy the contents of the running-config file to the startup-config file

**write**

**write memory**

**copy running-config startup-config**

different commands you can use to delete startup-config To return the device to the factory-default configuration

**write erase**

**erase nvram:**

**erase startup-config**

The enable password is a password that you must enter to

access privileged EXEC mode

**enable password**

view the enable password in running-config

R1# **show running-config | include enable**

enable password ccna

After a show command, a pipe ( | ) followed by the

keyword include allows you to filter output to only show

lines including the specified characters ( enable , in this case).

This encrypts all current passwords configured on the device, as well as passwords you configure in the future

R1(config)# **service password-encryption**

R1(config)# **do show running-config | include enab**

enable password 7 0307580507

The service password-encryption command encrypts

passwords using *type 7* encryption. It is a very weak form of

encryption

The *enable secret* is a more secure password that can be

configured to protect access to privileged EXEC mode. It stores

the password as a *hash*, rather than encrypted ciphertext.

*Hashing* can be thought of as one-way encryption; it can’t be

reversed.

R1(config)# **enable secret cisco**

R1(config)# **do show running-config | include enab**

enable secret 9 $9$emuJQV5sVZCY8v$INbrp9XrtfWHieM

enable password 7 0307580507

Use the **disable** command to return to user EXEC mode from privileged EXEC mode.

Use the **reload** command in privileged EXEC mode to restart the device.

The command to view a Cisco switch’s MAC address table

**show mac address-table**

you can manually clear dynamic MAC addresses from a switch’s MAC address table

SW1# **clear mac address-table dynamic**

SW1# **show mac address-table**

Mac Address Table

To clear a specific dynamic MAC

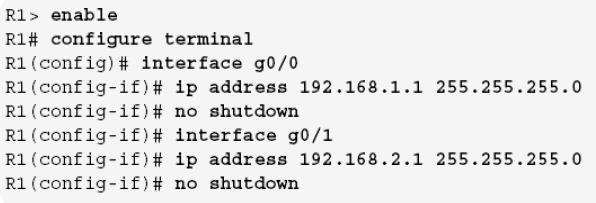
address from the table, you can use the **clear mac addresstable**

**dynamic address** mac-address command. To clear

all dynamic MAC addresses learned on a specific interface, use

the **clear mac address-table dynamic interface**

interface-name command.



convenient command to view a router’s interfaces

**show ip interface brief**

R1# **show ip interface brief**

Interface IP-Address OK? Method Statu

GigabitEthernet0/0 unassigned YES unset admin

GigabitEthernet0/1 unassigned YES unset admin

GigabitEthernet0/2 unassigned YES unset admin

GigabitEthernet0/3 unassigned YES unset admin

command to configure an interface’s IP address

R1(config-if)# **ip address 192.168.1.1 255.255.255**

check that the netmask

R1# **show ip interface**

command to configure SW1’s F0/1 and F0/2 interfaces at the same time

**interface range f0/1-2**

This configures F0/3, F0/4, F0/5, F0/6, F0/7, F0/8,and G0/2.

**interface range f0/3-8, g0/2**

view interface descriptions

**show interfaces description**

**show interfaces status (მხოლოდ სვიჩებზე,**the descriptions are displayed in the Name column**)**

The command to manually configure an interface’s speed

**speed** {speed | **auto**} (ან სიჩქარე უნდა ჩაწერო ან autonegotiation ჩართო auto-თი)

view the active configurations for a specific interface

**show running-config interface** *interface-name*

The command to configure an interface’s duplex

**duplex** {**auto** | **full** | **half**}

**show ip route**

To view only the connected routes in R1’s routing table

**show ip route | include C**

configure a static route

**ip route** *destination-network netmask next-hop*

**ip route** *destination-network netmask exitinterface*

**ip route** *destination-network netmask exitinterface next-hop*

default status of VLANs

**show vlan brief**

configuration of vlans

SW1(config)# **vlan 10 (**Creates and names VLAN 10)

SW1(config-vlan)# **name Engineering (** saxelis darqmeva )

SW1(config-vlan)# **vlan 20**

SW1(config-vlan)# **name HR**

In the previous example, the status of each VLAN is active .

However, you can temporarily disable a VLAN by using the

**shutdown** command in VLAN configuration mode

You can manually configure a switch port to operate in access Mode

**switchport mode access**

Then, use

**switchport access vlan** *vlan-id*

SW1(config)# **interface range g0/0-3**

SW1(config-if-range)# **switchport mode access**

SW1(config-if-range)# **switchport access vlan 10**

SW1(config-if-range)# **interface range g1/0-3**

SW1(config-if-range)# **switchport mode access**

SW1(config-if-range)# **switchport access vlan 20**

SW1(config-if-range)# **interface range g2/0-3**

SW1(config-if-range)# **switchport mode access**

SW1(config-if-range)# **switchport access vlan 30**

SW1(config-if)# **switchport trunk encapsulation dot1q**

SW1(config-if)# **switchport mode trunk**

SW1(config-if)#

To verify trunk ports, you can use the command

SW1# **show interfaces trunk**

configure the list of VLANs allowed on the trunk

**SW1(config-if)# switchport trunk allowed vlan**

WORD VLAN IDs of the allowed VLANs when this

➥ in trunking mode

add add VLANs to the current list

all all VLANs

except all VLANs except the following

none no VLANs

remove remove VLANs from the current list

To configure the native VLAN of a trunk port

**switchport trunk native vlan** *vlan-id*

❶ Enables G0/0

❷ Creates the G0/0.10 subinterface

❸ The prompt changes.

R1(config)# **interface g0/0** ❶

R1(config-if)# **no shutdown** ❶

R1(config-if)# **interface g0/0.10** ❷

R1(config-subif)# ❸

command to configure an SVI

**interface vlan** *vlan-id*

command to verify trunkports

**show interfaces trunk**

**switchport mode** command: **switchport mode dynamic auto** and

**switchport mode dynamic desirable**

To view a port’s administrative and operational modes

**show interfaces** interface-name **switchport**

disable DTP

1.Manually configure the port as an access port with **switchport mode access**

2.Explicitly disable DTP with **switchport nonegotiate**

useful command to view the current state of VTP on the switch

SW1# **show vtp status**

VTP Version capable : 1 to 3

VTP version running : 1

VTP Domain Name :

VTP Pruning Mode : Disabled

VTP Traps Generation : Disabled

Device ID : 5254.0008.8000

Configuration last modified by 0.0.0.0 at 4-25-23

Local updater ID is 0.0.0.0 (no valid interface f

Feature VLAN:

--------------

VTP Operating Mode : Server

Maximum VLANs supported locally : 1005

Number of existing VLANs : 5

Configuration Revision : 0

MD5 digest : 0x57 0xCD 0x4

0x56 0x9D 0x4

0 56 0 9 0

❶ SW1 supports VTP version 1 to 3.

❷ SW1 runs VTP version 1 by default.

❸ SW1 is not in a VTP domain.

❹ SW1 is a VTP server by default.

❺ SW1’s VLAN database has five VLANs.

❻ The revision number starts at 0.

Vtp domain name

**vtp domain** domain-name

VTP mode can be configured

**vtp mode** *mode*

configure the VTP version

**vtp version** version