Cisco IOS cheat sheet

Vincevrp

Abstract

Quick reference for commonly used Cisco IOS commands. My goal is to cover most commands used in routing and switching essentials, scaling networks, and connecting networks. This document has not yet been fully translated into English.

Contents

1 Basic configuration

1.1 Modus veranderen

1.1.1 Commando modes

Wanneer je connecteert met een apparaat, kom je in USER EXEC mode:

Voorbeeld prompt:

```
Switch>
```

Schakelen naar de PRIVILEGED EXEC mode met het commando `enable`:

```
Switch> enable
Switch#
```

Terugschakelen naar USER EXEC mode kan met het commando `disable`.

1.1.2 Configuratie modes

We onderscheiden volgende configuratie modes:

Modus	Commando	Prompt
Global configuration mode	configure terminal	Switch(config)#
Line configuration mode	line console 0	Switch(config-line)#
Interface configuration mode	interface vlan 1	Switch(config-if)#

Voor line en interface configuration mode te gebruiken dien je te vertrekken vanuit global configuration mode en de corresponderende line/interface mee te geven met het commando.

Om een bepaalde modus te verlaten gebruiken we het commando `exit`.

1.2 Basisconfiguratie

1.2.1 Naam instellen

Uit te voeren in global configuration mode:

```
hostname naam-van-apparaat
```

1.2.2 Wachtwoorden instellen

1.2.2.1 Privileged exec mode wachtwoord: Uit te voeren in privileged exec mode:

```
enable secret wachtwoord
```

1.2.2.2 Wachtwoord voor bepaalde lijn: Uit te voeren in line configuration mode voor respectievelijke line:

```
password wachtwoord
login
```

Het login commando zorgt ervoor dat het wachtwoord gevraagd wordt bij het verbinden met het apparaat.

1.2.2.3 Alle wachtwoorden encrypteren Uit te voeren in privileged exec mode:

```
service password-encryption
```

1.2.3 Banner instellen

Bij het instellen van een banner moet je steeds een symbool kiezen dat zal dienen als begin- en eindmarkering voor de banner. In onderstaande voorbeelden maken wij gebruik van het dollar-teken ($)

Uit te voeren in global configuration mode:

```
banner motd $ your-text-message $
```

1.2.3.1 Voorbeeld enkele regel:

```
banner motd $ Warning, no unautohrized access allowed! $
```

1.2.3.2 Voorbeeld meerdere regels: Merk op dat de '{ENTER}' duidt op het fysiek indrukken van de enter-toets

```
banner motd ${ENTER}
##############################################{ENTER}
# Warning, no unauthorized access allowed! #{ENTER}
##############################################{ENTER}
${ENTER}
```

1.2.4 IP-adres instellen

Uit te voeren in interface configuration mode voor respectievelijke interface:

```
ip address ip subnetmask
```

Bijvoorbeeld:

```
ip address 0.0.0.0 255.255.255.0
```

1.2.5 Klok en datum instellen

1.2.5.1 Klok tonen Kan worden uitgevoerd vanuit user exec mode:

```
show clock
```

1.2.5.2 Klok instellen Moet worden uitgevoerd vanuit privileged exec mode:

```
clock set tijd maand dag jaar
```

Extra informatie kan worden getoond door het commando `clock set ?`.

1.2.6 Descriptie interface instellen

Uit te voeren in interface configuration mode voor respectievelijke interface:

```
description beschrijving
```

1.2.7 Interface inschakelen

Uit te voeren in interface configuration mode voor respectievelijke interface:

```
no shutdown
```

1.2.8 Configuratie opslaan

Uit te voeren in privileged exec mode:

```
copy running-config startup-config
```

1.3 Hardware en software info tonen

```
show version
```

1.4 IP-lookup uitschakelen

Af en toe komt het voor dat je een commando verkeerd intypt, waardoor de router/switch automatisch een IP-lookup probeert te doen. Dit kan uitgeschakeld worden door:

```
no ip domain-lookup
```

1.5 Factory reset prodecure

1.5.1 Soft reset

Een soft reset schoont de running- en startup-config op. Alle commando's moeten vanuit de privileged exec mode worden uitgevoerd tenzij anders aangegeven.

1. Herlaad de router/switch na de aanpassingen met het commando `reload`.
2. Verwijderen van startup config (dit commando verandert niets aan de boot variabelen, zoals config-register en boot system settings).

   ```
   erase startup-config
   ```

   Of

   ```
   write erase
   ```

1.5.2 Hard reset

Een hard reset is nodig wanneer je het wachtwoord van het apparaat niet meer kent.

1. Schakel de router/switch uit door deze uit het stopcontact te halen.
2. Sluit de console kabel aan en stel een console verbinding op.
3. Hou de `mode` knop ingedrukt en steek de stekker opnieuw in het stopcontact. Laat de `mode` knop pas los eens er karakters worden weergegeven op het scherm.
4. Terwijl het bootproces bezig is, voer je de toetsencombinatie `Ctrl+Pausebreak` in.
5. Voer volgende commando's in:

   ```
   Switch: flash_init
   Switch: dir flash:
   Switch: flash:config.text flash:config.backup
   Switch: boot
   ```

6. Hernoem de configuratie files en verwijder de wachtwoorden

   ```
   Would you like to enter the inital configuration dialog? no
   Switch> enable
   SW1# renameflash:config.backup config.text
   SW1# copy flash:config.text system:running-config
   SW1# config terminal
   SW1(config)# no enable secret.
   SW1(config)# exit
   SW1(config)# wr
   ```

1.5.3 Reset VLAN information

1. Controleer de vlan informatie met het commando `show vlan`.
2. Controleer de vlan.dat file met het commando `dir`.
3. Delete de VLAN.dat file met het commando `delete flash:vlan.dat`.

2 Routing and Switching Essentials

2.1 IP configuration

2.1.1 IPv4 instellen

Interface configuration mode:

ip address *ip-address subnetmask*

no shutdown

Verificatie:

show ip interface brief

2.1.2 IPv6 instellen

Interface configuration mode:

ipv6 address *ip-address* / *prefix-length* [link-local | eul-64]

no shutdown

Genereer link-local adres:

ipv6 enable

Stel eigen static link-local adres in:

Dit wordt gebruikt i.p.v. gegenereerd link-local adres.

ipv6 address *ip-address* / *prefix-length* link-local

Verificatie:

show ipv6 interface brief

2.2 Static routing

2.2.1 IPv4 static routes

Global configuration mode:

ip route *network-address subnet-mask* [*ip-address* | *exit-int*]

Static route

ip route *network-address subnet-mask* [*next-hop-ip* | *exit-intf*]

Fully specified static route

ip route *network-address subnet-mask exit-intf next-hop-ip*

Directly connected static route

ip route *network-address subnet-mask exit-intf*

Default route

ip route 0.0.0.0 0.0.0.0 [*exit-intf* | *next-hop-ip*]

Verificatie:

show ip route *static*

2.2.2 IPv6 static routes

The ipv6 unicast-routing global configuration command must be configured to enable the router to forward IPv6 packets

ipv6 route *ipv6-prefix/prefix-length [ipv6 address | exit-int]*

Default static route

ipv6 route ::/0 [ipv6-address | exit-intf]

Enable IPv6 unicast-routing

ipv6 unicast-routing

Verificatie:

show ipv6 route *static*

2.2.3 Floating static routes

Aanschouw volgende administrative distance waarden:

- EIGRP = 90
- IGRP = 100
- OSPF = 110
- IS-IS = 115
- RIP = 120

IPv4:

ip route 0.0.0.0 0.0.0.0 value

IPv6:

ipv6 route 0.0.0.0 0.0.0.0 value

2.3 RIP

Enable RIP (v1)

router rip

Switch to RIPv2

version 2

Enable RIP routing for network:

network *network-address*

Disable auto-summary

no auto-summary

Passive interface

passive-interface *int-name*

Propagate default route

default-information originate

Verificatie:

show ip protocols

2.4 Remote access & security

2.4.1 SSH

Global configuration mode:

> ip domain-name cisco crypto key generate rsa username admin secret ccna line vty 0 15 transport input ssh login local exit ip ssh version 2 exit

2.4.2 Port security

Disable unused ports

> interface range fa0/1-9 shutdown

Configure port security

> switchport port-security mac-address *mac-addr*

Sticky

> switchport port-security mac-address sticky *mac-addr*

Violation modes

- **Protect**: When limit of secure MAC is reached, drop packets with unknown source address.
- **Restrict**: Same as protect but with notification
- **Shutdown** (default): Violation causes interface to shutdown

> switchport port-security violation [protect | restrict | shutdown]

Verificatie:

> show port-security interface *[interface-id]* show port-security address

2.5 VLANs

VLAN types:

- **Default**: All switch ports become part of default VLAN to allow any device to connect with other devices.
- **Native**: Is assigned to a trunk port. It supports traffic coming from many VLANs.
- . . .

VLAN maken

```
configure terminal
vlan 20
name student
end
```

Assign ports to VLAN

```
configure terminal
interface *interface_id*
switchport mode access
switchport access vlan *vlan_id*
end
```

Assign ip to VLAN

```
int vlan *nummer*
ip add *ip* *sub*
no shutdown
exit
ip default-gateway *ip*
```

Set VTP

```
vtp domain *naam*
```

Voice VLAN

```
switchport voice vlan *vlan_id*
```

Configure Trunk Links

```
configure terminal
interface *interface_id*
switchport mode trunk
switchport trunk native vlan *vlan_id*      #Specify a native VLAN for untagged
    frames
switchport trunk allowed vlan *vlan-list*   #Specify list of VLANs to be allowed on
    trunk link
end
```

Configure router-on-a-Stick subinterface configuration

```
interface g0/0.10
encapsulation dot1q 10
ip address 172.17.10.1 255.255.255.0

interface g0/0
no shutdown

vlan 10
interface f0/5
switchport mode trunk
end
```

Verificatie

show vlan brief show interfaces f0/18 switchport

2.6 ACL

Types:

- **Inboud ACL**: Incoming packets are processed before they are routed to the outbound interface
- **Outbound ACL**: Incoming packets are routed to the outbound interface, and then they are processed through the outbound ACL.

2.6.0.1 Wildcard masking

Neem 255.255.255.255 en trek er de subnetmask van af

Binary:

```
0 = match the value
1 = ignore the value
```

Voorbeelden:

```
IP-Address  192.168.1.1

IP must match exactly:

    Wildcard mask 0.0.0.0

Anything will match:

    Wildcard mask 255.255.255.255
```

ACL instellen

access-list access-list-number { deny | permit | remark } source [source-wildcard] [log]

ACL toevoegen aan interface

ip access-group { access-list-number | access-list-name } { in | out }

ACL voor SSH

```
line vty 0 15
login local
transport input ssh
access-class 21 in
exit
```

Verificatie:

show access-lists

3 Scaling Networks

3.1 Scaling VLANs

3.1.1 VTP

VTP Server

```
vtp mode server
vtm domain ?
```

VTP Client

```
vtp mode client
vtp domain ?
```

Verificatie

```
show vtp status
```

```
show vlan brief
```

3.1.2 DTP

Verificatie

```
show dtp interface f0/1
```

3.2 STP

```
config-if
spanning-tree mode ?
spanning-tree vlan 1,10,20 root primary
spanning-tree portfast
spanning-tree bpduguard enable
```

Verificatie

```
show cdp neighbors
show spanning-tree vlan
```

3.3 L3 Inter VLAN routing

```
int g0/2
no switchport
ip addr ip sub
```

Enable routing:

```
ip routing
```

3.4 NTP

```
clock set
ntp server in
```

3.5 CDP

```
show cdp (interface/neighbours)
cdp enable
```

3.6 Etherchannel

```
interface range Fa0/1-2
channel-group 1 mode active/desirable
interface port-channel 1
switchport mode trunk
switchport trunk allowed vlan 1,2,20

show interfaces port-channel 1
show etherchannel summary
show etherchannel port-channel
```

LACP: active/passive PagP: desirable/auto

3.7 HSRP

```
interface
standy version 2
standby 1 ip
standby 1 priority 100
standby 1 preempt
no shut
```

Verificatie

```
show standby brief
```

3.8 OSPF

```
router ospf 10
router-id
network x.x.x.x wildcardmask area area-id
passive-interface gigabitethernet 0/0

interface
bandwidth X



clear ip ospf process
show ip protocols
show ospf interface serial 0/0/0
show ip ospf
show ip ospf neighbor
show ip ospf interface brief
show ip ospf database
```

3.8.1 Propagete default static route in OSPF updates

```
default-information originate
```

3.8.2 OSPFv3

```
ipv6 unicast routing
ipv6 router ospf 10
router-id 1.1.1.1
ipv6 ospf area



clear ipv6 ospf process
```

3.9 EIGRP

```
router eigrp 1
eigrp router-id
network network-addr wildcardmask
```

3.9.1 Configure passive interfaces

```
router eigrp 1
passive-interface gigabitethernet 0/0
```

3.9.2 Propagating a default static route within the EIGRP routing domain

```
redistribute static
```

3.9.3 Bandwidth utilization

```
interface
ip bandwidth-percent eigrp as-number percent
```

3.9.4 Hello and Hold timers

```
interface
ip hello-interval eigrp 1 50
ip hold-time eigrp 1 150
```

Verificatie

```
show ip protocols
show ip eigrp neighbors
show ip eigrp topology
show ip eigrp topology all-links
show running-config | section eigrp 1
```

3.9.5 EIGRPv6

```
ipv6 unicast-routing
ipv6 router eigrp 2
eigrp router-id 2.0.0.0
no shutdown
```

3.9.6 Bandwidth utilization

```
interface
ipv6 bandwidth-percent eigrp as-number percent
```

3.9.6.1 Configure passive interfaces

```
ipv6 router eigrp 2
passive-interface gigabitethernet 0/0
```

3.9.7 Hello and Hold timers

```
interface
ipv6 hello-interval eigrp 1 50
ipv6 hold-time eigrp 1 150
```

Verificatie

```
show ipv6 protocols
show ipv6 eigrp neighbors
show ipv6 route
```

4 Connecting Networks

4.1 HDLC Encapsulation

```
interfaec s0/0/0
encapsulation hdlc
```

Verificatie

```
show controllers
```

4.2 PPP

```
int serial 0/0/0
encapsulation ppp
compress preditor|stac
ppp quality 80
```

4.2.1 Multilink PPP

```
ppp multilink
ppp multilink group 1
```

4.2.2 Authentication PAP/CHAP

```
ppp authentication chap/pap
ppp pap sent-username R1 password cisco
```

4.2.3 Verificatie

```
show ppp multilink
debug ppp authentication
```

4.3 PPPoE

```
interface dialer 2
ppp chap hostname Fred
ppp chap password Barney

ip mto 1492
dialer pool 1
no shut

ip g0/1
no ip
pppoe enable
pppoe-client dial-pool-number 1
no shut
```

Verificatie:

```
show pppoe session
debug ppp negotiation
```

4.4 GRE (VPN)

```
int Tunnel10
tunnel mode gre ip
ip add ip sub
tunnel source ip
tunnel destination ip
```

Verificatie:

```
show int tunnel
```

4.5 BGP

```
router bgp AS-num
neighbor ip remote-as as-number
network network-address mask
```