

Cisco commands

CCNA1 & CCNA2 (CH1 – 7 + 11)

Brecht Van Eeckhoudt

10-01-2016 06:46

1 Important stuff

IP-adres instellen op PC!

Default gateway = dichtstbijzijnde router (ook voor switch)

Meeste commando's schrijven elkaar over (bv ip address), tweede outhouden

DNS-servers Odisee Gent: 10.132.1.5 & 10.135.1.0

"?" na commando (bv.: "show ?", "smd prefer ?" "v?", "?") (bij output:
<cr> = carriage return, "enter")

Router – Router = cross-over

Switch – Switch = cross-over

- **Speed(baud):** 9600
- **Data bits:** 8
- **Stop bit:** 1
- **Parity:** None
- **Flow control:** None

2 Router resetten

```
Router> enable (= en)
Route\# erase startup-config
Router# reload
```

3 Router instellen

```
Router> enable
Router# configure terminal (=conf t)
Router(config)# hostname R1
      (NO hostname (of ip address) om ongedaan te maken!)
R1(config)# no ip domain-lookup
      (opzoeken DNS uitschakelen, voorkomt lange wachttijden bij
      tikfouten)
R1(config)# interface fastEthernet0/0 (=f0/0)
      (of "loopback 0") (gigabit g, serial s)
R1(config-if)# ip address 192.168.0.1 255.255.255.0 (= /24)
R1(config-if)# description link to lan-10 (240 character limit)
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface fastEthernet0/1 (=f0/1)
R1(config-if# (ga verder met zelfde als hierboven)
```

4 Switch resetten

```
Switch> enable
Switch# erase startup-config
Switch# delete flash:vlan.dat
      (= delete vlan.dat if the location hasn't changed)
Switch# reload
```

5 Switch instellen

IP address is configured on a virtual interface: Switched Virtual Interface (SVI)

```
Switch> enable
Switch# config t
Switch(config)# hostname S1
S1(config)# no ip domain-lookup
S1(config)# interface vlan1
S1(config-if)# ip address 192.168.1.4 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# ip default-gateway 192.168.1.1
      (voor remote management)
```

6 Beveiligen

```
R1(Config)# enable secret class
      (PRIVILEGED MODE password = class)
R1(Config)# line console 0 (= line con 0)
      (password CONSOLE instellen)
R1(Config-line)# password cisco
R1(Config-line)# login
      ("er moet ingelogd worden")
R1(Config-line)# login synchronous
      (prevent console messages from interrupting cmd's)
R1(Config-line)# exit
R1(Config)# line vty 0 4
      (5 connecties tegelijkertijd (switch: 0 -> 15 (hoe zien: sh
      run, spatie, helemaal van onder)) TELNET password = cisco)
R1(Config-line)# password cisco
R1(Config-line)# login
R1(Config-line)# login synchronous
R1(Config-line)# exit
R1(Config)# service password-encryption
      (prevent password from displaying)
```

7 SSH instellen

```
R1(Config)# ip domain-name ikdoeict.be
R1(Config)# crypto key generate RSA general-keys modulus 1024
R1(Config)# line vty 0 4 (switch: 0 -> 15)
R1(Config-line)# transport input ssh telnet (welke toelaten?)
R1(Config-line)# login local (lokale database)
R1(Config-line)# username admin privilege 15 secret adminpass
R1(Config-line)# exit
```

```

R1(Config)# ip ssh version 2
R1(Config)# ip ssh time-out 75
R1(Config)# ip ssh authentication-retries 2

R1(Config)# crypto key zeroize rsa (delete RSA key pair)

```

8 Verder beveiligen

```

R1(Config)# line console 0
R1(Config-line)# exec-timeout 10
    (automatisch afsluiten na 10 min, 0: voor het gemak, geen
    timeout, of: "5 10" (5min 10sec))
R1(Config-line)# exit
R1(Config)# line vty 0 4 (switch: 0 -> 15)
R1(Config-line)# exec-timeout 10
R1(Config-line)# exit
R1(Config)# login block-for 120 attempts 3 within 60
    (120 seconden, 2 within 2 = 2 verkeerde pogingen)
R1(Config)# security password min-length 8

```

9 IPV6 instellen

- Global unicast address router = default gateway pc
- When a global unicast address is set and it's status is up/up then the ipv6 prefix and prefix length are added to the routing table as a local route (/128 prefix, used by the router to efficiently process packets with the interface address of the router as the destination)

```

R1(Config)# interface f0/0
R1(Config)# ipv6 enable
    (interface generates its own link-local address without having
    a global unicast address)

R1(Config-if)# ipv6 address 2001:db8:acad:1::1/64
    (static global unicast, not required, more than one global
    unicast on the same subnet is allowed)
R1(Config-if)# ipv6 address 2001:db8:acad:1::1/64 eui-64
    (6 byte (48 bit) interface MAC address used to generate
    global unicast IPv6 Address by expanding it into a 64 bit
    interface part (host part))
R1(Config-if)# ipv6 address 2001:db8:acad:1::1 link-local
    (static link-local unicast address (required) instead of the
    automatic link-local IP when global unicast IP is set)
R1(Config-if)# no shutdown
R1(Config-if)# exit

R1(Config)# ipv6 unicast-routing
    (enable ipv6 unicast routing, ICMPv6 router advertisements are
    being
    send (no DHCP server necessary to set IP & default gateway))

```

10 Banner MOTD instellen

```
R1(Config)# banner motd %stuffgoeshere% (% = delimiter)
```

11 Opslaan

```
R1# copy running-config startup-config (= copy run start)
R1# copy running-config tftp (backup & restore using TFTP)
R1# copy running-config usbflash0:/ (save to usb drive)
```

```
R1# copy running-config flash:backup.txt
R1# copy flash:backup.txt running-config
```

12 MAC table

```
S1# show ip arp (= arp)
S1# show mac-address-table (+dynamic, +addresses...)
S1# show mac-address-table interface f0/0
S1# (no) mac address-table static 0050.56BE.6C88 vlan 99 interface
    f0/6

S1(Config)# switchport port-security (enable service)

S1(Config)# switchport port-security mac-address <mac address>
    (only one specific address can connect)

S1(Config)# switchport port-security mac-address sticky
    (dynamisch toevoegen & onthouden)
S1(Config)# switchport port-security maximum 2
    (bij dynamisch enkel eerste 2 onthouden, rest geen verbinding meer)
S1(Config)# switchport port-security violation shutdown
    (bij inbreuk: poort uitschakelen & aantal tellen)
S1(Config)# switchport port-security violation protect
    (bij inbreuk: poort uitschakelen)
S1(Config)# no shutdown ???
```

13 VLAN instellen

- **Native VLAN:** verkeer niet gelabeld
- **Management VLAN:** Switch krijgt hierin IP

```
S1(config)# vlan vlan_id (102, 103, 105 - 107) (no vlan 20: no longer
    ports assigned, if yes: can't communicate anymore)
S1(config-vlan)# name vlan_name
S1(config-vlan)# exit
```

14 VLAN aan interface linken

```
S1(config)# interface interface_id
S1(config-if)# no shutdown
S1(config-if)# switchport mode access (permanent access mode)
S1(config-if)# switchport access vlan vlan_id (no switchport access
    vlan)
```

15 Trunk link instellen

```
S1(Config)# interface f0/1
S1(Config-if)# switchport mode trunk (permanent trunking mode)
(samen met "switchport nonegotiate": no DTP frames)
bij error: S1(Config-if)# sw trunk encap dot1q
S1(Config-if)# switchport trunk native vlan 99
(set native vlan, do this on both ends & make sure vlan exists!)
(no switchport trunk native vlan)
S1(Config-if)# switchport trunk allowed vlan 10,20,30,99
(no switchport trunk allowed vlan)
S1(Config-if)# (no) switchport protected
(Private VLAN Edge, protected ports)
S1(Config-if)# end
```

16 VLAN verder instellen

```
S1(config)# interface vlan 99
S1(config-if)# ip address 172.17.99.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1# copy running-config startup-config
```

17 Snelheid poorten instellen

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# duplex full
S1(config-if)# speed 100
S1(config-if)# end
S1# copy running-config startup-config
```

18 AUTO-MDIX instellen

Medium-Dependent Interface Crossover, straight-through/cross-over

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# duplex auto
S1(config-if)# speed auto
S1(config-if)# mdix auto
S1(config-if)# end
S1# copy running-config startup-config
```

19 Shutdown unused ports

Or: disable all ports, only enable the necessary ones

```
S1(Config)# interface range F0/1 - 4
S1(Config-if)# shutdown
S1(Config-if)# interface range g0/1 - 2
S1(Config-if)# shutdown
S1(Config-if)# end
```

20 Serial connection

```
R1(Config)# interface serial 0/0/0
R1(Config-if)# description link to R2
R1(Config-if)# ip address 209.165.200.255 255.255.252 (/30)
                (or: ipv6 address 2001:db8:acad:3::1/64)
R1(Config-if)# clock rate 128000 (alleen bij DCE)
                (in packet tracer: serial connection symbool met klokje:
                eerste aangeklikt = DCE) (4MB/s = 4MHz = 4 000 000)
R1(Config-if)# no shutdown
R1(Config-if)# exit
```

21 Loopback interface (IPV4)

```
R1(Config)# interface loopback 0
R1(Config-if)# ip address 192.168.0.2 255.255.255.0 (/24)
R1(Config-if)# exit
```

- Logical interface, not assigned to physical port
- Can be connected to any device
- Testing: at least one interface will always be available (bv.: emulating network behind router)
- Router will use the always available loopback interface address for IDENTIFICATION rather than the IP address assigned to a physical port which may go down (bv.: Open Shortest Path First routing process)
- multiple loopback interfaces are allowed (IPV4 address unique!)

22 Legacy inter-VLAN routing

22.1 Switch

```
S1(config)# vlan 10 (create vlan 10)
S1(config-vlan)# vlan 30 (create vlan 30)
S1(config-vlan)# interface f0/11
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/4 (link to router)
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/6
S1(config-if)# switchport access vlan 30
S1(config-if)# interface f0/5 (link to router)
S1(config-if)# switchport access vlan 10
S1(config-if)# end
```

22.2 Router

```
R1(config)# interface g0/0
R1(config-if)# ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface g0/1
R1(config-if)# ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# end
```

23 Router-on-a-stick Inter-VLAN routing

23.1 Switch

```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
```

23.2 Router

```
R1(config)# interface g0/0.10 (create subinterface)
R1(config-subif)# encapsulation dot1q 10
    (assign vlan to subinterface, can use native keyword to set
    native VLAN (otherwise default native VLAN 1))
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# 172.17.30.1 255.255.255.0
R1(config-subif)# interface g0/0
R1(config-if)# no shutdown
```

24 Static routing

How dest. is specified (one of 3 route types):

- **Next-hop route:** Only next-hop IP address
- **Directly connected static route:** Only router exit interface
- **Fully specified static route:** Next-hop IP address and exit interface

After the command we can put the "Administrative distance", used to create a floating static route (Administrative Distance higher than a dynamically learned route (AD = 90))

IPV4 routing aanzetten (default aan bij ipv4): `ip routing`

IPV6 routing aanzetten (default uit bij ipv6): `ipv6 unicast-routing`

```
R1(config)# ip route 172.16.3.0 255.255.255.0 f0/0
    (dest. ip & mask, exit interface)
R1(config)# ip route 172.16.3.0 255.255.255.0 192.168.2.1
    (dest. ip & mask, next hop ip address (ip next router, searches
    for specific interface in table)) (when connecting to broadcast
    media like ethernet, commonly creates a recursive lookup)
R1(config)# ip route 172.16.3.0 255.255.255.0 s0/0/0 172.16.2.1
    (dest. ip & mask, exit interface & next hop ip address pair)
```

25 Routing Information Protocol

R1(config-router)# ? get the possible commands

25.1 Advertising networks

The "network" command:

- Enables RIP on all interfaces that belong to a specific network. Associated interfaces now both send and receive RIP updates.
- Advertises the specified network in RIP routing updates sent to other routers every 30 seconds.

```
R1(config)# (no) router rip (enable rip)
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.0
```

25.2 Enable RIPv2

RIP versions (default RIPv1):

- **version 1:** sends v1 messages, ignores v2 fields in incoming route entries
- **version 2:** send and receive v2 messages only (includes subnet mask in all updates, classless routing protocol, must be configured on all routers in routing domain)
- **no version:** send v1 updates, listen to both v1 and v2 updates (default?)

```
R1(config)# router rip
R1(config-router)# version 2
```

25.3 Disable auto-summarisation

When disabled: RIPv2 no longer summarizes networks to their classful address at boundary routers. RIPv2 now includes all subnets and their appropriate masks in its routing updates.

```
R1(config)# router rip
R1(config-router)# no auto-summarisation
```

25.4 Configure passive interfaces

RIP updates (send every 30 seconds) only need to be sent out interfaces connecting to other RIP enabled routers.

The command stops routing updates out the specified interface. However, the network that the specified interface belongs to is still advertised in routing updates that are sent out other interfaces.

```
R1(config)# router rip
R1(config-router)# passive interface f0/0

R1(config-router)# passive-interface default
(all interfaces become passive)
R1(config-router)# no passive interface f0/0 (re-enable interface)
```


25.5 Default (static) route

```
R1(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.226
      (next hop ip or exit interface)
```

```
R1(config)# ip route ::/0 172.16.2.2 (next hop)
```

25.6 Enable RIPng

```
R1(config)# ip v6 unicast-routing
R1(config)# interface g0/0
R1(config-if)# ipv6 rip RIP-AS enable
```

26 Inter-VLAN routing

Enable routing functionality of 2960 switches (16 static routes):

```
S1(config)# smd prefer lanbase-routing
S1(config)# reload
```

SMD: Cisco Switch Database Manager, provides multiple templates
When the router doesn't support Dynamic Trunking Protocol: no "switchport mode dynamic auto/desirable"

27 Network Address Translation

Don't forget "debug ip nat (+detailed)"

27.1 Configure static NAT

```
R1(config)# ip nat inside source static <inside-local ip>
      <inside-global ip>
R1(config)# interface f0/0 (specify inside interface)
R1(config-if)# ip nat inside
R1(config)# interface f0/1 (specify outside interface)
R1(config-if)# ip nat outside
```

27.2 Configure dynamic NAT

```
R1(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.230
      netmask (or prefix-length) 255.255.255.224
      (define pool, use start & end ip address)
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
      (define which addresses are eligible to be translated)
R1(config)# ip nat inside source list 1 pool NAT-POOL1
      (bind pool with Access Control List)
R1(config)# interface f0/0
R1(config-if)# ip nat inside
R1(config-if)# interface f0/1
R1(config-if)# ip nat outside
```

27.3 Clear dynamic NAT entries

```
R1# ip nat translation timeout <timeout-seconds> (set timeout,
    default: 24h)
R1# clear ip nat translation (clear the dynamic entries before
    timeout has ended)
R1# clear ip nat translation inside <global-ip> <local-ip> (+outside
    <global-ip> <local-ip>) (clear a specific entry)
R1# clear ip nat translation * (clear all dynamic translations)
```

27.4 Configure PAT for pool of addresses

NAT overload, conserves addresses in the inside global address pool by allowing the router to use one inside global address for many inside local addresses. A single public IPv4 address can thus be used for hundreds of internal private IPv4 addresses. When multiple inside local addresses map to one inside global address, the TCP or UDP port numbers of each inside host distinguish between the local addresses.

```
R1(config)# ip nat pool NAT-P00L2 209.165.200.226 209.165.200.230
    netmask 255.255.255.224
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)# ip nat inside source list 1 pool NAT-P00L2 overload
R1(config)# interface f0/0
R1(config-if)# ip nat inside
R1(config-if)# interface f0/1
R1(config-if)# ip nat outside
```

27.5 Configure PAT for single address

```
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)# ip nat inside source list 1 interface serial 0/1/0
    overload
R1(config)# interface s0/0/0
R1(config-if)# ip nat inside
R1(config-if)# interface s0/1/0 (same as in source translation)
R1(config-if)# ip nat outside
```

28 Show...

Execute user exec or privileged exec cmd's from other router config modes: DO
show vlan brief / ip route / smd prefer / int status

```
ip interface brief (= sh ip int br)
    (summary of all interfaces, addresses & current operational
    status)
ipv6 interface brief / g0/1
    (display global unicast & link-local unicast)
    (link-local unicast: FE80, multicast: FF02)
```

```

ip(v6) route (+static / network)
    (ipv4 routing table in ram)
    (local host route: administrative distance = 0, /32 mask for
    IPV4, /128 for IPV6, for routes on the router owning the
    IP address) (layer 1 (status) / layer 2 (protocol)
    interface status)

ip(v6) protocols

running-config (+ interface f0/0)
    (show commands configured on specific interface)

interfaces (+switchport)
    (interface info, packet flow count)

history
    (terminal history size 200)
    (Ctrl + P / UP arrow, Ctrl + N / DOWN arrow)
    (current terminal session only)

version
ip ssh
ip <id>
ip interface (f0/0 ?) (ipv4 related info)
cdp neighbors (+details)
interface
ipv6 routers

protocols
file systems
startup/running-config (= sh run) (enter to switch pages)
flash
bootvar (= boot) (show current IOS boot file)

port security (+interface interface_id, +address)
controllers

ntp associations
ntp status
ntp master
ip http server status (no ip http server)

vlan(s) (+brief, +summary, +id vlan_id)
vlan name <name> (beter: vlan brief)
interfaces vlan 20 (niet veel gebruikt)
interface f0/18 (+switchport: administrative & operational status)
dtp interface f0/1 (current dtp mode)
interfaces (f0/1) trunk

ip nat translations (+verbose (additional info))
ip nat statistics (clear ip nat statistics)
access-lists

```

29 Filter "show" output

- Show command "pauses" after every 24 lines, press "enter" or "space" after "--more--"
- **terminal length <number>** to set number of lines (zero prevents pausing)
- **Use pipe "|":**
 - **section (bv.: "...line vty")**: shows entire section that starts with the filtering expression
 - **include (bv.: "...up")**: includes all output lines that match the filtering expression
 - **exclude (bv.: "...unassigned")**: excludes all output lines that match the filtering expression
 - **begin (bv.: "...gateway")** show all output lines from a certain point, starting with the line that matches the filtering expression

30 Windows commands

```
ipconfig /all
netstat -r (route tabel)
route print (route tabel)
arp -a
ipconfig /flushdns
ipconfig /displaydns
nslookup (exit)
ping address -t (blijft pingen) (-4: IPV4 forceren)
netstat (open & running TCP connections on networked host)
```

31 Other stuff

tab	autocomplete command
ctrl+C	commando onderbreken of uit config mode komen
ctrl+Z	van overal naar privileged exec
ctrl+shift+6, x?	lopend proces onderbreken vb: lange ping of tracert

- Upload exsisting config (flat text): paste code in "User exec"
- Password recovery: ROMMON interface: startup-config negeren
- Telnet sessie router/switch of console: Hyperterminal i transfer/capture text
- Sessie tijdelijk verlaten: enter om terugkeren te keren naar actieve ssh sessie bij lege CLI prompt
- **clock set 17:00:00 18 Feb 2013** to set the time
- **ssh -l admin 192.168.1.10** to ssh from one router to another

Fouten bij het ingeven (3 soorten):

- Ambiguous: meerdere commandos mogelijk wanneer je een commando afkort vb: show f zal niet werken want er zijn meerdere mogelijkheden die met een f beginnen
- Incomplete: onvolledig commando vb: een ip adres instellen zonder mask
- Invalid: ongeldig commando

R1# ping <ipaddress> (ICMP echo request/reply)

R1# traceroute <ipaddress> (= tracert) (ICMP echo requests with specific time-to-live values defined on the frame, increases after each "hop", defines how many hops the request might take)

R1# boot system (set boot environment variable)

32 Mode switching

enable	user exec → privileged exec
disable	privileged exec → user exec
configure terminal	privileged exec → global configuration
interface g0/0	global configuration → interface configuration
exit	één niveau terug in de hiërarchie
end	global/interface configuration → privileged exec (= ctrl+z)

33 Modes defined

User Exec	Router>	> – teken
Privileged Exec	Router#	# – teken
Global configuration	Router(config)#	sleutelwoord "config"
Interface configuration	Router(config-if)#	sleutelwoord "config-if"

34 Boot loader steps

Operating system missing?

1. Connect PC to serial port
2. Unplug & replug power, within 15s: hold MODE while system LED is still flashing green
3. Keep pressing until system LED briefly turns amber & solid green, then release
4. switch: (dir flash, ...)