

---

# 1 Einleitung

## 1.1.1 Zur Darstellung:

blaue Texte

sind Konfigurationsbefehle welche mit „write memory“ gespeichert werden müssen  
z.B. hostname rombach

rote Texte

sind andere Befehle welche nicht gespeichert werden müssen  
z.B. configure terminal

grüne Texte

sind Befehle welche an einem anderen Gerät ausgeführt werden, z.B. am angeschlossenen PC  
z.B. ping 192.168.179.1

schwarze Texte

sind meldungen des Routers  
z.B. ROMMON 1>

## 1.2 Vorbereitung

Man besorge sich einen Occasionsrouter z.B. einen Cisco 1812, welcher mindestens zwei WAN Interfaces hat und mindestens ein LAN Interface.

## 1.3 Anschliessen

Cisco Geräte haben normalerweise eine Serielle Schnittstelle welche hellblau mit **CONSOLE** bezeichnet ist. Im Lieferumfang enthalten ist jeweils ein hellblaues Kabel, welches man an die Serielle Schnittstelle des Computers anschliessen kann. Sollte der Computer keine serielle Schnittstelle haben gibt es USB Adapter welche mit dem entsprechenden Treiber die selbe Funktion übernehmen.

## 1.4 Verbinden der Konfigurationskonsole

### 1.4.1 Windows

Unter Windows kann man mit dem Programm **PUTTY.exe** eine Verbindung zum Comport (COMx) öffnen. Man kann dies mit der Maus auswählen.

### 1.4.2 Unixoides System wie z.B. Linux oder OSX

Haben standardmässig das Tool **screen** installiert. Um eine Verbindung zu öffnen gibt man an seiner Lieblingshell den Befehl **screen /dev/tty.usb-serial** ein wobei /dev/tty.usb-serial die Serielle Schnittstelle darstellt.

## 1.5 Passwort zurück setzen<sup>1</sup>

Während des Bootens **<BREAK>** drücken, da z.B. auf der Apple Tastatur diese Taste nicht verfügbar ist muss man mit der Befehlskombination von screen **Ctrl-A Ctrl-B** den Break senden. Ctrl-A versetzt Screen in den Modus in dem es Befehle entgegen nimmt und Ctrl-B sendet danach den Break. Mit Ctrl-A ? erhält man eine Liste der Befehle.

```
ROMMON 1> confreg 0x2142 //Starten mit der Standardkonfiguration
ROMMON 2> reset //rebooten im ROMMON
router> enable
router# copy startup-config running-config //lädt die Startkonfiguration ins RAM
router# configure terminal
router# enable secret <neues Passwort>
router# config-register 0x2102 //das richtet die Startkonfig wieder ein
router# write memory
router# reload (und speichern) //rebooten im IOS
```

---

<sup>1</sup> [http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products\\_tech\\_note09186a00802017a1.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_tech_note09186a00802017a1.shtml)

---

## 1.6 Router resetten wenn das Passwort bekannt ist

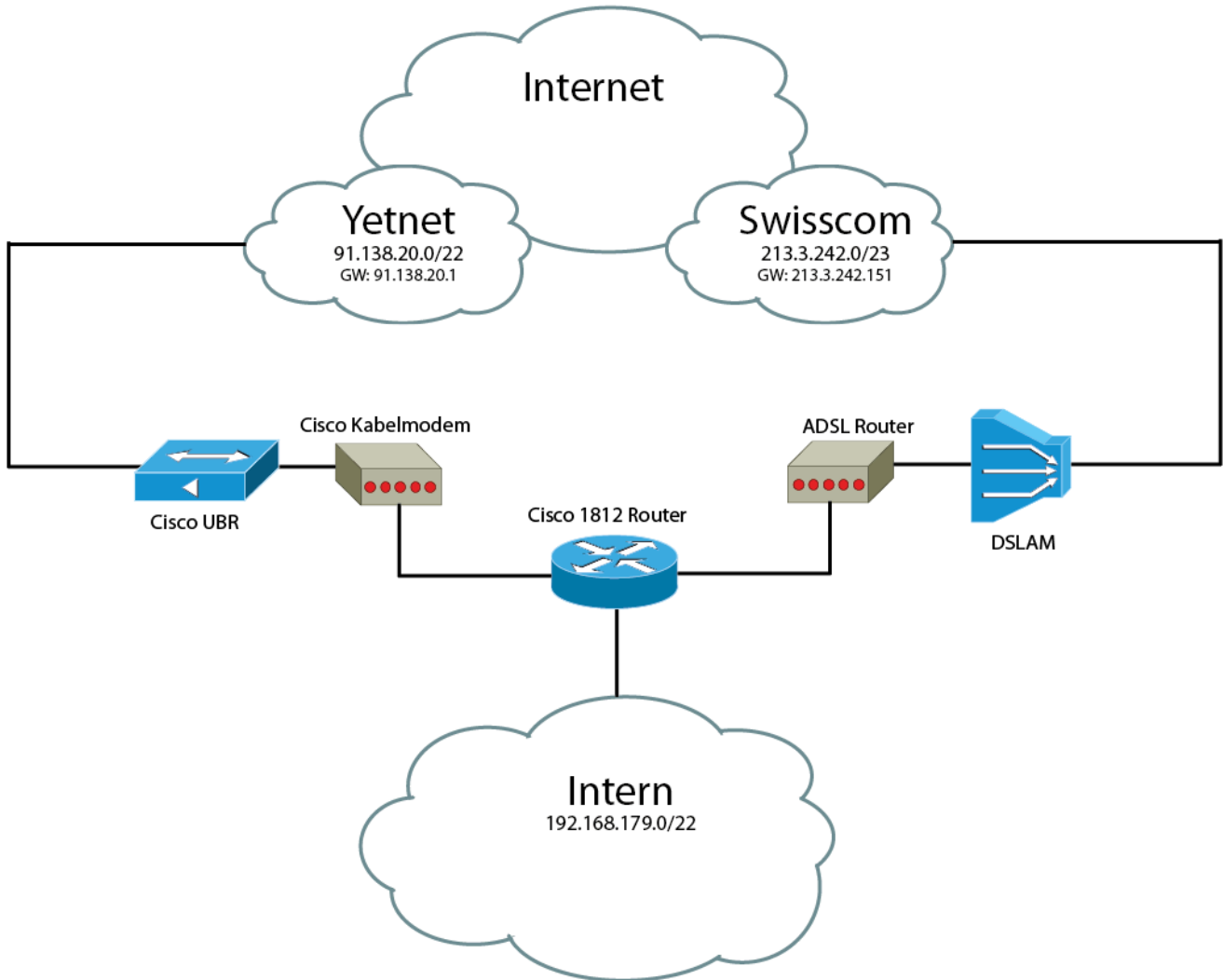
```
router> enable //dies aktiviert den Router so dass Befehle gesendet
//werden können
router# write erase //löscht die Konfiguration
router# reload //Rebootet
```

Would you like to enter the initial configuration dialog? [yes/no]: no

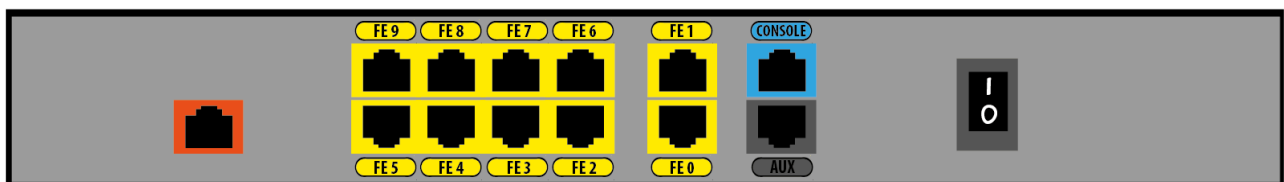
```
router> enable
router# show version //informationen des Routers Anzeigen
router# show running-config //aktuelle Konfiguration anzeigen
router# show interfaces //Interfaces anzeigen
```

## 2 LAN, DHCP, Dual WAN mit NAT, PBR und IP SLA

### 2.1 Netzwerkdiagramm



#### Serieller Anschluss für das Konfigurieren



**ISDN Port**  
Integrated Services  
Digital Network

**Switching Ports**  
Können einem VLAN  
zugeordnet werden

**WAN Ports**  
Kann eine IP haben

---

## 2.2 Einrichtung des Routers (Cisco 1812)

```
configure terminal //in den Konfigurationsmodus wechseln
hostname rombach //Hostnamen vergebe
ip domain name ignored.ch //Domänenname vergeben
ip cef //Cisco Express Forwarding einschalten
//das sorgt dafür, dass Switching Interfaces
//nicht jedes Mal die CPU verwenden müssen und
//nutzt entsprechend spezielle Hardware des Routers

exit //verlässt den Konfigurationsmodus
write memory //schreibt die Konfiguration
reload //rebootet den Router
```

### INTERNES NETZ DEFINIEREN

```
interface FastEthernet 2 //die gewichteten Interfaces
  switchport access vlan 10 // dem VLAN 10 zuweisen

interface FastEthernet 3
  switchport access vlan 10

interface FastEthernet 4...9 //4...9 und das für alle gewichteten Interfaces
  switchport access vlan 10

interface vlan 10 //das VLAN 10 definieren und
  ip address 192.168.179.1 255.255.255.0 //eine IP Adresse vergeben
  ip nat inside //brauchen wir später für das Policy Based
  ip policy route-map PBR //Routing

ping 192.168.179.1 //von einem angeschl. PC z.B. an FastEthernet 2
//und der eine Manuelle IP konfiguriert hat
//z.B. 192.168.179.33/24

exit //den Konfigurationsmodus verlassen
write memory //die Konfiguration speichern
```

### DHCP DEFINIEREN

```
conf t //ist das selbe wie configuration terminal

ip dhcp excluded-address 192.168.179.1 192.168.179.10
ip dhcp excluded-address 192.168.179.100 192.168.179.255

ip dhcp pool vlan-10 //DHCP Pool mit dem Namen vlan-10 definieren
  import all
  network 192.168.179.0 255.255.255.0 //Subnetz für den DHCP Pool
  default-router 192.168.179.1 //Default Gateway angeben, dieses VLAN
  dns-server 192.168.179.1 //den DNS Server werden wir später starten

ping 192.168.179.1 //auf DHCP umstellen am PC und vlan pingen
exit //den Konfigurationsmodus verlassen
write memory //die Konfiguration speichern
```

### ERSTES WAN KONFIGURIEREN (Kabelmodem mit DHCP)

```
interface FastEthernet 0
  description *** Yetnet ***
  mac-address 0018.4d81.d1ff //weil die „Fixe“ IP per DHCP kommt
  ip address dhcp //die IP beziehen
  ip nat outside //NAT öffentlicher Teil
  no shutdown //wir hätten das Interface gerne aktiviert
  exit

exit //den Konfigurationsmodus verlassen
show dhcp lease //zeigt an ob die IP bezogen wurde
ping www.google.com //zeigt ob die Verbindung nach Aussen steht
```

---

## ZWEITES WAN KONFIGURIEREN (ADSL mit PPPoE)

```
debug ppp negotiation
debug ppp authentication
conf t

interface FastEthernet 1
  description *** Swisscom ***
  mac-address 0050.7fc2.aa8e
  pppoe enable group global
  pppoe-client dial-pool-number 1          //Poolnummer 1 ist in Dialer1
  no shutdown
  exit

interface dialer 0
  bandwidth 20000
  ip address negotiated
  dialer pool 1
  encapsulation ppp
  ppp chap hostname hg5gsx18.226131@swisscomdata.ch
  ppp chap password 0 gfjk5hud
  ppp ipcp route default                  //setzt die default route *S
  ppp ipcp dns request accept            //DNS über das IP Control Protokoll beziehen
  ip nat outside                          //Aussenseite des NAT definieren
  no shutdown
  no cdp enable                           //cisco discovery protokoll deaktivieren

no debug all                             //alle Debug Infos deaktivieren
show ip route                             //S* 0.0.0.0/0 [1/0] via 213.3.242.154
ping www.google.com                       //zeigt ob die Verbindung nach Aussen steht
                                           //natürlich sollte man vorher das Kabelmodem
                                           //ausziehen
```

## TEST NAT Einrichten für ADSL

```
access-list 79 permit 192.168.179.0 0.0.0.255
ip nat inside source list 79 interface dialer 0
(dialer-list 1 protocol ip permit)

ping 173.194.70.105                       //Ping vom PC an FastEthernet 2 (z.B. Google)
                                           //Da der DHCP noch keinen DNS hat

show ip nat translations                   //die NAT Tabelle anschauen
icmp 46.14.243.249:31248 192.168.179.16:31248 173.194.70.105:31248 173.194.70.105:31248

clear ip nat translation *                 //die NAT Tabelle löschen
```

---

## DNS SERVER AKTIVIEREN und im DHCP eintragen

```
debian:~ marc$ nmap 192.168.179.1 //schauen ob da ein DNS ist:
//Nein, keiner

ip dns server //DNS Server auf dem Router aktivieren

debian:~ marc$ nmap 192.168.179.1 | grep 53/tcp // --> 53/tcp open domain
debian:~ marc$ ping www.google.com
```

## TEST NAT Einrichten für Kabelmodem

```
ip nat inside source list 79 interface FastEthernet 0
ping www.google.com //Ping vom PC an FastEthernet 2
//jetzt mit DNS

show hosts //wenn beide WAN angeschlossen sind sollten nun
//vier DNS Server ersichtlich sein
```

## ROUTE überwachung konfigurieren

```
ip sla 1 //erste überwachung einrichten
icmp-echo 91.138.20.1 source-interface FastEthernet 0
timeout 1000
frequency 1
ip sla schedule 1 life forever start-time now //überwachung starten

ip sla 2 //zweite überwachung einrichten
icmp-echo 213.3.242.151 source-interface Dialer 0
timeout 1000
frequency 1
ip sla schedule 2 life forever start-time now

track 10 rtr 1 reachability
delay down 1 up 1

track 20 rtr 2 reachability
delay down 1 up 1

ip route 0.0.0.0 0.0.0.0 91.138.20.1 track 10 //Route wenn FastEthernet 0
//erreichbar
ip route 0.0.0.0 0.0.0.0 213.3.242.151 track 20 //Route wenn ADSL erreichbar
```

---

## ROUTE MAPS für NAT

```
route-map Yetnet permit 79 //Route-Map für Kabelmodem
  match ip address 79
  match interface FastEthernet 0

route-map Swisscom permit 79 //Route-Map für ADSL
  match ip address 79
  match interface dialer 0

ip nat inside source route-map Yetnet interface FastEthernet 0 //NAT Regel für Kabelmodem
ip nat inside source route-map Swisscom interface Dialer 0 //NAT Regel für ADSL
```

## Policy Based Routing<sup>2</sup> (Damit das Nat weiss über welches Interface)

```
route-map PBR permit 10
  match ip address 10
  set ip next-hop verify-availability 91.138.20.1 1 track 10

route-map PBR permit 10
  match ip address 10
  set ip next-hop verify-availability 213.3.242.151 2 track 20
```

3

---

<sup>2</sup> <https://supportforums.cisco.com/docs/DOC-8313>

<sup>3</sup> [http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_configuration\\_example09186a00808d2b72.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_configuration_example09186a00808d2b72.shtml)

## Gesamte Konfiguration

```
rombach#show running-config
Building configuration...

Current configuration : 3047 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname rombach
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 15
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.179.1 192.168.179.15
ip dhcp excluded-address 192.168.179.100
192.168.179.255
!
ip dhcp pool vlan-10
import all
network 192.168.179.0 255.255.255.0
default-router 192.168.179.1
dns-server 192.168.179.1
!
!
ip domain name ignored.ch
!
multilink bundle-name authenticated
!
!
archive
log config
hidekeys
!
!
track 10 rtr 1 reachability
delay down 1 up 1
!
track 20 rtr 2 reachability
delay down 1 up 1
!
!
interface FastEthernet0
description *** Yetnet (Kabelmodem) ***
mac-address 0018.4d81.d1ff
ip address dhcp
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
!
!
interface FastEthernet1
description *** Swisscom (ADSL) ***
mac-address 0050.7fc2.aa8e
no ip address
duplex auto
speed auto
pppoe enable group global
pppoe-client dial-pool-number 1
!
interface BRI0
no ip address
encapsulation hdlc
shutdown
!
interface FastEthernet2
switchport access vlan 10
!
interface FastEthernet3
switchport access vlan 10
!
interface FastEthernet4
switchport access vlan 10
!
interface FastEthernet5
switchport access vlan 10
!
interface FastEthernet6
switchport access vlan 10
!
interface FastEthernet7
switchport access vlan 10
!
interface FastEthernet8
switchport access vlan 10
!
interface FastEthernet9
switchport access vlan 10
!
interface Vlan1
no ip address
!
interface Vlan10
ip address 192.168.179.1 255.255.255.0
ip nat inside
ip virtual-reassembly
ip policy route-map PBR
!
interface Dialer0
bandwidth 20000
ip address negotiated
ip nat outside
ip virtual-reassembly
encapsulation ppp
dialer pool 1
no cdp enable
ppp chap hostname hg5gsx18.226131@swisscomdata.ch
ppp chap password 0 gfjk5hud
ppp ipcp dns request accept
ppp ipcp route default
!
ip route 0.0.0.0 0.0.0.0 91.138.20.1 track 10
ip route 0.0.0.0 0.0.0.0 213.3.242.151 track 20
!
!
no ip http server
no ip http secure-server
ip dns server
ip nat inside source route-map Swisscom interface
Dialer0 overload
ip nat inside source route-map Yetnet interface
FastEthernet0 overload
!
ip sla 1
icmp-echo 91.138.20.1 source-interface FastEthernet0
timeout 1000
frequency 1
ip sla schedule 1 life forever start-time now
ip sla 2
icmp-echo 213.3.243.154 source-interface Dialer0
timeout 1000
frequency 1
ip sla schedule 2 life forever start-time now
access-list 79 permit 192.168.179.0 0.0.0.255
!
!
route-map Swisscom permit 79
match ip address 79
match interface Dialer0
!
route-map Yetnet permit 79
match ip address 79
match interface FastEthernet0
!
route-map PBR permit 10
match ip address 10
set ip next-hop verify-availability 91.138.20.1 1
track 10
set ip next-hop verify-availability 213.3.242.151 2
track 20
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
login
!
!
webvpn cef
end
```