
Protokoll

Laborübung 2003-10-08

Accesslisten

Bernhard Mitterer

tm011070

Philipp Reinhartshuber

tm011094

Petra Raab

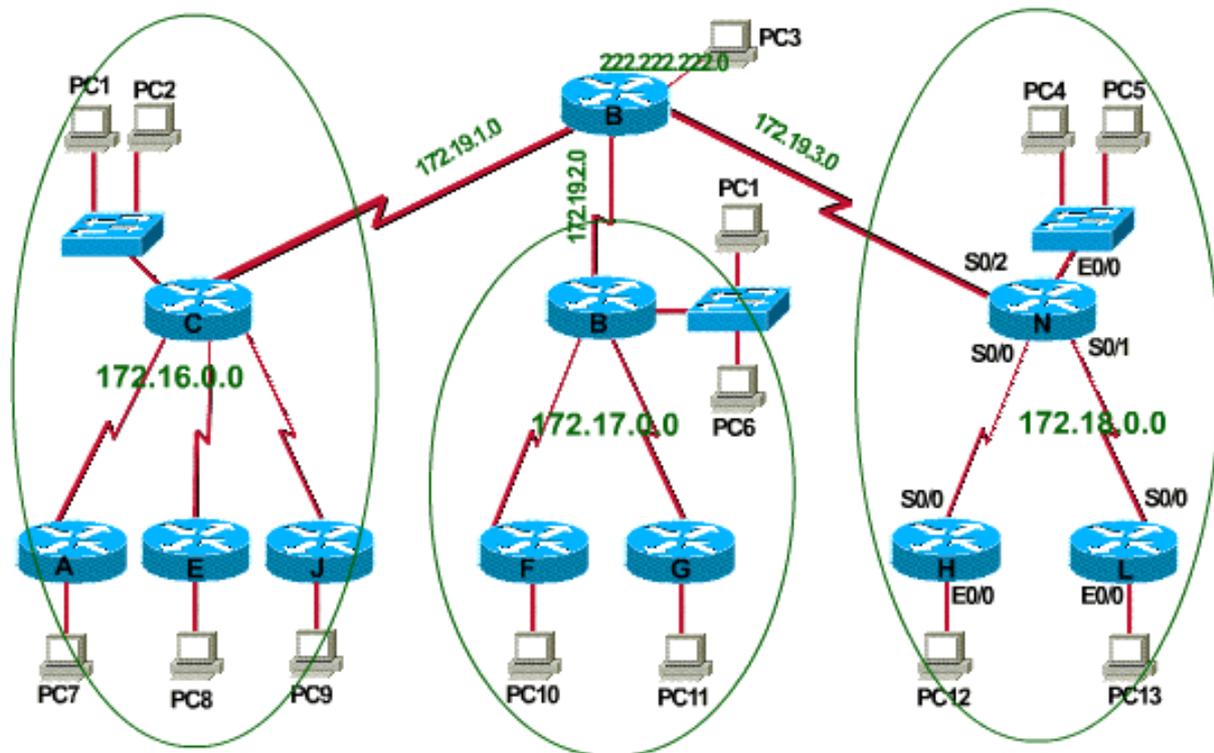
tm011090



Inhaltsverzeichnis/ Aufgabenstellung

Inhaltsverzeichnis/ Aufgabenstellung	2
1) Verkabeln laut Angabe	3
a) Überprüfung der Verkabelung mittels CDP	3
b) Aufnahme der Struktur ins Protokoll	4
2) Routingprotokoll IGRP AS 23 aktivieren	4
a) Konfiguration einer Loopbackadresse	4
b) Überprüfen der Routingtabellen	4
3) Konfiguration von 2 VLAN (Verkauf + Werbung)	5
a) Zuweisen von 2 Ports	5
b) Router/Switch Verbindung konfigurieren (Subinterface)	6
c) Testen	6
4) Standard Access Listen	7
a) Das Ethernetinterface von Router GR1 darf nur von den eigenen Gruppenmitgliedern erreichbar sein.	7
5) Extended Access Listen	7
a) Nach Außen ist http für alle erlaubt	7
b) Nach „Innen“ ist nur ein PING von den anderen Gruppenmitgliedern erlaubt, der Rest ist verboten	7
c) PING nach Außen ist nur von PC von VLAN 300 erlaubt	7
d) Testen der Vorgaben	7

1) Verkabeln laut Angabe



a) Überprüfung der Verkabelung mittels CDP

```
LAB-N#sh cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
```

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
LAB-H	Ser 0/0	134	R S	2620	Ser 0/0
LAB-L	Ser 0/1	131	R S	2610	Ser 0/0

b) Aufnahme der Struktur ins Protokoll

Gerät	Interface	IP-Adresse
N	S 0/0	172.18.1.1/24
	S 0/1	172.18.2.1/24
	S 0/2	172.19.3.1/24
	E 0/0.1	172.18.3.1/24
	E 0/0.2	172.18.4.1/24
H	S 0/0	172.18.1.2/24
	E 0/0	172.18.5.1/24
L	S 0/0	172.18.2.2/24
	E 0/0	172.18.6.1/24
PC04	VLAN 300	172.18.3.13/24
PC05	VLAN 400	172.18.4.13/24
PC12	-----	172.18.5.13/24
PC13	-----	172.18.6.13/24

2) Routingprotokoll IGRP AS 23 aktivieren

```
LAB-H#conf t
Enter configuration commands, one per line. End with CNTL/Z.
LAB-H(config)#router igrp 23
LAB-H(config-router)#network 172.18.0.0
```

Da IGRP nur *classful* routen kann (Netmask wird nicht berücksichtigt) reicht es hier das Class-B-Netz 172.18.0.0 anzugeben.

a) Konfiguration einer Loopbackadresse

```
LAB-N(config)#int loopback 1
LAB-N(config-if)#ip address 172.18.10.1 255.255.255.0
LAB-N(config-if)#no shutdown
```

b) Überprüfen der Routingtabellen

```
LAB-N#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set

I   222.222.222.0/24 [100/80625] via 172.19.3.2, 00:01:02, Serial0/2
I   172.17.0.0/16 [100/82225] via 172.19.3.2, 00:01:02, Serial0/2
I   172.16.0.0/16 [100/84125] via 172.19.3.2, 00:01:02, Serial0/2
    172.19.0.0/24 is subnetted, 3 subnets
C     172.19.3.0 is directly connected, Serial0/2
I     172.19.2.0 [100/82125] via 172.19.3.2, 00:01:02, Serial0/2
I     172.19.1.0 [100/82125] via 172.19.3.2, 00:01:02, Serial0/2
    172.18.0.0/24 is subnetted, 6 subnets
I     172.18.6.0 [100/80225] via 172.18.2.2, 00:00:02, Serial0/1
C     172.18.4.0 is directly connected, Ethernet0/0.4
I     172.18.5.0 [100/80135] via 172.18.1.2, 00:00:39, Serial0/0
C     172.18.2.0 is directly connected, Serial0/1
C     172.18.3.0 is directly connected, Ethernet0/0.3
C     172.18.1.0 is directly connected, Serial0/0
I   222.222.200.0/24 [100/80135] via 172.19.3.2, 00:01:04, Serial0/2
```

3) Konfiguration von 2 VLAN (Verkauf + Werbung)

- Erstellen der VLANs

```
Switch#vlan database
Switch(vlan)#vlan 300 name Verkauf
VLAN 300 added:
  Name: Verkauf

Switch#vlan database
Switch(vlan)#vlan 400 name Werbung
VLAN 400 added:
  Name: Werbung
```

a) Zuweisen von 2 Ports

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 300
Switch(config-if)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 400
Switch(config-if)#int fa0/3
Switch(config-if)#switchport mode trunk
```

b) Router/Switch Verbindung konfigurieren (Subinterface)

```
LAB-N(config)#int e0/0.3
LAB-N(config-subif)#encapsulation dot1Q 300
LAB-N(config-subif)#ip addr 172.18.3.1 255.255.255.0
LAB-N(config-subif)#int e0/0.4
LAB-N(config-subif)#encapsulation dot1Q 400
LAB-N(config-subif)#ip addr 172.18.4.1 255.255.255.0
LAB-N(config-subif)#no shutdown
LAB-N(config-subif)#exit
LAB-N(config)#int e0/0
LAB-N(config-if)#no shutdown
```

c) Testen

```
C:\>ping 192.168.3.13

Ping wird ausgeführt für 192.168.3.13 mit 32 Bytes Daten:

Antwort von 192.168.3.13: Bytes=32 Zeit<1ms TTL=128

Ping-Statistik für 192.168.3.13:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms

C:\>ping 192.168.4.13

Ping wird ausgeführt für 192.168.4.13 mit 32 Bytes Daten:

Antwort von 192.168.4.13: Bytes=32 Zeit<1ms TTL=128

Ping-Statistik für 192.168.4.13:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
```

Durch anpingen der in den unterschiedlichen VLANs befindlichen PCs ermöglicht die Kontrolle der Konfiguration von Router, Switch und PCs.

4) Standard Access Listen

a) Das Ethernetinterface von Router GR1 darf nur von den eigenen Gruppenmitgliedern erreichbar sein.

```
LAB-N(config)#access-list 1 permit 172.18.0.0 0.0.255.255
LAB-N(config)#int e0/0
LAB-N(config-if)#ip access-group 1 out
```

5) Extended Access Listen

Bei längeren ACLs ist es empfehlenswert die Befehle in eine Textdatei zu schreiben und diese dann per Copy&Paste in die Commandline zu kopieren. (Wäre in unserem Fall zwar nicht notwendig gewesen, wurde aber zum Üben trotzdem über die Textdatei gemacht.)

a) Nach Außen ist http für alle erlaubt

```
[ C:\acl.txt ]
!
access-list 100 permit tcp any any eq 80
!
int s0/2
 ip access-group 100 out
!
```

b) Nach „Innen“ ist nur ein PING von den anderen Gruppenmitgliedern erlaubt, der Rest ist verboten

Siehe c)

c) PING nach Außen ist nur von PC von VLAN 300 erlaubt

Da ein Pingen von innen nach außen voraussetzt, dass das angepingte Gerät auch antworten darf (von außen nach innen), widersprechen sich die Angaben b) und c) weshalb diese Punkte gestrichen wurden.

d) Testen der Vorgaben

Getestet wurde die ACL durch Aufrufen einer HTML-Seite von einem auf PC03 konfigurierten HTTP-Server auf Port 80.