Übung 2

Shehata Abd El Rahaman

Inhaltsverzeichnis

1 VLANs

1.1 Konfiguration von VLANs

1.1.1 Verbindungen zu Endsysteme einstellen

VLAN 10 Verbindungen

```
child1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
child1(config)#interface FastEthernet0/1
child1(config-if)#switchport mode access?
access
child1(config-if)#switchport mode access
child1(config-if)#switchport access vlan 10
child1(config-if)#end
child1#
%SYS-5-CONFIG_I: Configured from console by console
```

(a) Access1/child1

```
child2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
child2(config)#inte
child2(config)#interface fa
child2(config)#interface fastEthernet0/1
child2(config-if)#s
child2(config-if)#switchport mode access
child2(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
child2(config-if)#end
```

(b) Access2/child2

VLAN 20 Verbindungen

```
child1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
child1(config)#interface f
child1(config)#interface fastEthernet0/2
child1(config-if)#switchport mode access
child1(config-if)#switchport a
child1(config-if)#switchport access vlan 20
child1(config-if)#end
child1#
%SYS-5-CONFIG_I: Configured from console by console

child1#show vlan admins
                ^
% Invalid input detected at '^' marker.

child1#show vlan name admins

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
20   admins                           active    Fa0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

child1#
```

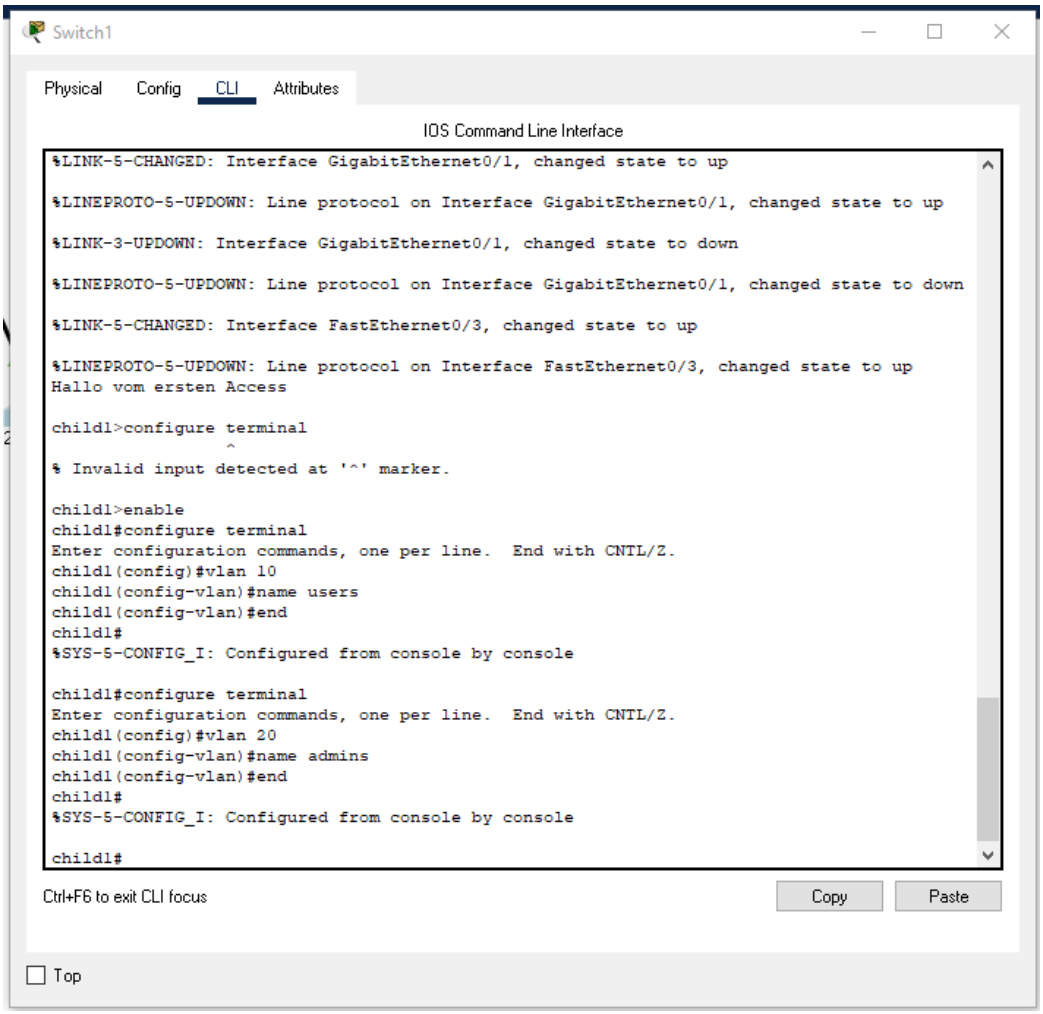
(a) Access1/child1

```
child2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
child2(config)#interface fast
child2(config)#interface fastEthernet0/2
child2(config-if)#switchport mode access
child2(config-if)#switchport access vlan 20
child2(config-if)#end
child2#
%SYS-5-CONFIG_I: Configured from console by console
```

(b) Access2/child2

1.1.2 Ports einstellen

Access1



(a) Vlans registrieren

```
childl>enable
childl#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
childl(config)#interfa
childl(config)#interface f
childl(config)#interface fastEthernet 0/3
childl(config-if)#switchport mode trunk
childl(config-if)#switchport trunk allowed vlan 10,20
childl(config-if)#end
childl#
%SYS-5-CONFIG_I: Configured from console by console
show interfaces fastEthernet0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20
```

(b) Trunk Port einstellen

Access2

```
child2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
child2(config)#vlan 10
child2(config-vlan)#name users
child2(config-vlan)#end
child2#
%SYS-5-CONFIG_I: Configured from console by console

child2#show vlan name users

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
10   users                            active    Fa0/1

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
10   enet  100010     1500  -      -      -        -    -        0      0
```

(a) Vlan 10 registrieren

```
child2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
child2(config)#vlan 20
child2(config-vlan)#name admins
child2(config-vlan)#end
child2#
%SYS-5-CONFIG_I: Configured from console by console
show vlan name admins

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
20   admins                           active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0
```

(b) Vlan 20 registrieren

```
child2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
child2(config)#interface fastEthernet0/3
child2(config-if)#switchport mode trunk
child2(config-if)#switchport trunk allowed vlan 10,20
child2(config-if)#end
child2#
%SYS-5-CONFIG_I: Configured from console by console
show interfaces fastEthernet0/3
FastEthernet0/3 is up, line protocol is up (connected)
  Hardware is Lance, address is 0090.2bad.a00b (bia 0090.2bad.a00b)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns

child2#show interfaces fastEthernet0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20
```

(c) Trunk Port einstellen

Backbone

```
backbone>enable
backbone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
backbone(config)#vlan 10
backbone(config-vlan)#name users
backbone(config-vlan)#end
backbone#
%SYS-5-CONFIG_I: Configured from console by console
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
backbone(config)#vlan 20
backbone(config-vlan)#name admins
backbone(config-vlan)#end
backbone#
%SYS-5-CONFIG_I: Configured from console by console
```

(a) Vlans registrieren

```
backbone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
backbone(config)#interace fastEthernet0/1
                     ^
% Invalid input detected at '^' marker.

backbone(config)#interface fastEthernet0/1
backbone(config-if)#switchport trunk allowed vlan 10,20
backbone(config-if)#end
backbone#
%SYS-5-CONFIG_I: Configured from console by console

backbone#show interfaces FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20
```

(b) Verbindung zu Access1 einstellen

```
backbone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
backbone(config)#interface fastEthernet0/2
backbone(config-if)#switchport mode trunk

backbone(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
switchport trunk allowed vlan 10,20
backbone(config-if)#show interfaces FastEthernet 0/2 switchport
                    ^
% Invalid input detected at '^' marker.

backbone(config-if)#end
backbone#
%SYS-5-CONFIG_I: Configured from console by console
show interfaces FastEthernet 0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20
```

(c) Verbindung zu Access2 einstellen

1.2 Testen der Konfiguration

1.2.1 Ping Test

1.2.2 Frage 1

Frage

Wie kann von einem User PC auf einen Admin PC zugegriffen werden?

Antwort

Lösung 1: Da VLAN die Ports auf Layer 2 separiert, könnte man ein Layer 3 Gerät, wie ein Router einfügen und den Default Gateway konfigurieren. Damit sollten Systeme auf beiden VLANs in der Lage sein, miteinander zu kommunizieren.
Lösung 2: Eine weitere Lösung wäre die Ports an den Endsystem auf trunk mode zu ändern und sie für vlan 10 und 20 zu konfigurieren und den native trunk auf 10 oder 20 zu ändern.

Test für Lösung 1

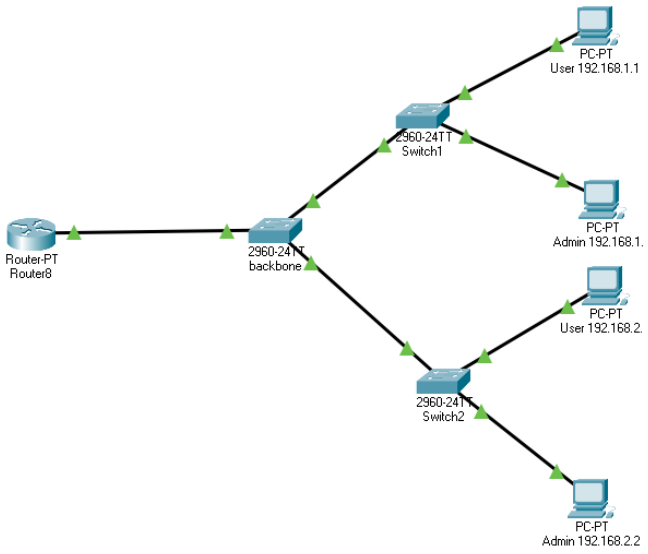


Abbildung 6: Netz

```
interface FastEthernet0/1
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode trunk
!
```

(a) Backbone

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 10
 ip address 192.168.1.254 255.255.255.0
!
interface FastEthernet0/0.2
 encapsulation dot1Q 20
 ip address 192.168.2.254 255.255.255.0
!
```

(b) Router

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2E0:8FFF:FE27:5D9D
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.1
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: ::
                                 192.168.1.254
```

(c) User 192.168.1.1

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:42FF:FE04:C8EE
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.2.1
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: ::
                                 192.168.1.254
```

(d) User 192.168.1.2

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::240:BFF:FE8E:A75C
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.2
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: ::
                                 192.168.2.254
```

(e) Admin 192.168.2.1

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::240:BFF:FE8E:A75C
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.2
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: ::
                                 192.168.2.254
```

(f) Admin 192.168.2.2

Abbildung 7: Konfiguration der Systeme

Resulate

Dadurch das die Endsysteme eine /16 Maske haben und das gesamte Netz eigentlich eins ist. Kann man mit dem System, welches am gleichen Switch liegt nicht kommunizieren, aber mit den anderen Endsystemen schon. Dies liegt daran, dass der Router eine /24 Maske hat. Würde der Router auch eine /16 haben, würde auch hier keine Kommunikation zwischen den VLANs zustande kommen.

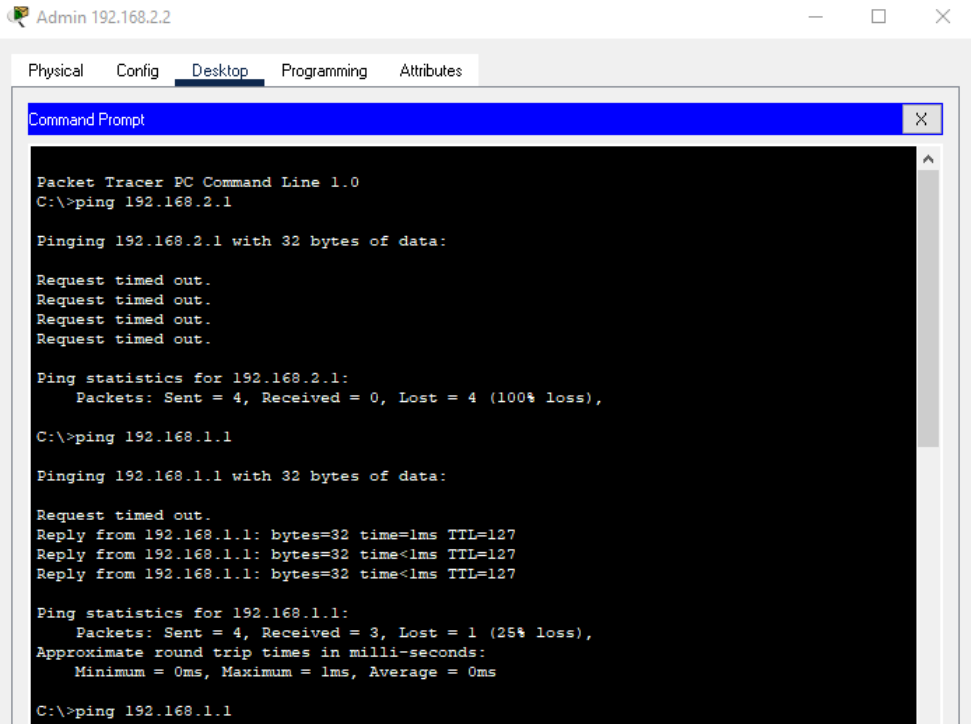


Abbildung 8: Admin kann mit User im anderen Netz kommunizieren,aber nicht im gleichen

Test für Lösung 2

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport trunk native vlan 10
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport trunk native vlan 10
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
```

(a) Switch 1

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport trunk native vlan 10
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport trunk native vlan 10
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk allowed vlan 10,20
 switchport mode trunk
'
```

(b) Switch 2

Resulate

Wie erwartet können alle Systeme miteinander kommunizieren

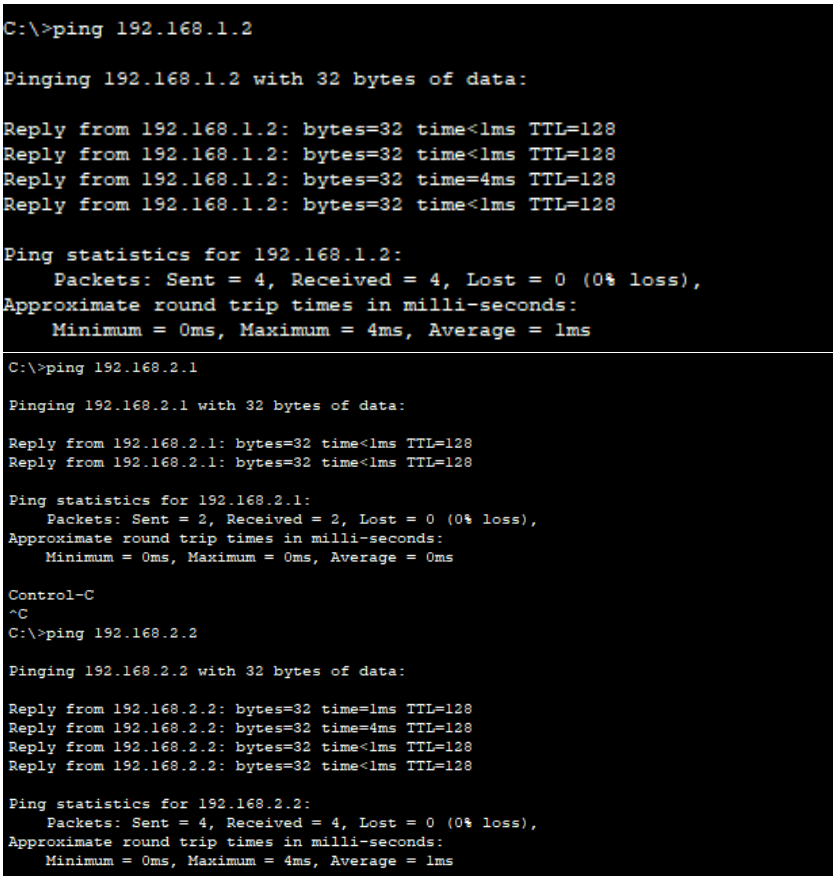


Abbildung 10: 192.168.1.1 kommuniziert mit allen Endsystemen

2 Port Security

2.1 Source Address Tables

2.1.1 SATs der Switches

SATs

```
backbone#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0090.0c1a.7980    DYNAMIC     Fa0/1
   1    0090.2bad.a00b    DYNAMIC     Fa0/2
  10    0001.4204.c8ee    DYNAMIC     Fa0/2
  10    0090.0c1a.7980    DYNAMIC     Fa0/1
  10    00e0.8f27.5d9d    DYNAMIC     Fa0/1
  20    0001.968d.38a6    DYNAMIC     Fa0/2
  20    0030.f238.6804    DYNAMIC     Fa0/1
  20    0090.0c1a.7980    DYNAMIC     Fa0/1
```

Abbildung 11: Backbone

```
child1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0060.2fa7.6788    DYNAMIC     Fa0/3
  10    0001.4204.c8ee    DYNAMIC     Fa0/3
  10    00e0.8f27.5d9d    DYNAMIC     Fa0/1
  20    0001.968d.38a6    DYNAMIC     Fa0/3
  20    0030.f238.6804    DYNAMIC     Fa0/2
```

Abbildung 12: Access 1

```
child2#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.c7c0.90d1    DYNAMIC     Fa0/3
  10    0001.4204.c8ee    DYNAMIC     Fa0/1
  10    0001.c7c0.90d1    DYNAMIC     Fa0/3
  10    00e0.8f27.5d9d    DYNAMIC     Fa0/3
  20    0001.968d.38a6    DYNAMIC     Fa0/2
  20    0001.c7c0.90d1    DYNAMIC     Fa0/3
  20    0030.f238.6804    DYNAMIC     Fa0/3
```

Abbildung 13: Access 2

2.1.2 Änderung der MAC Adresse

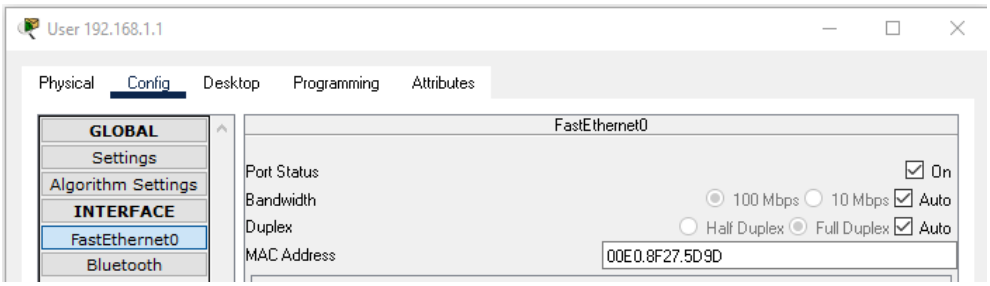


Abbildung 14: Access 1

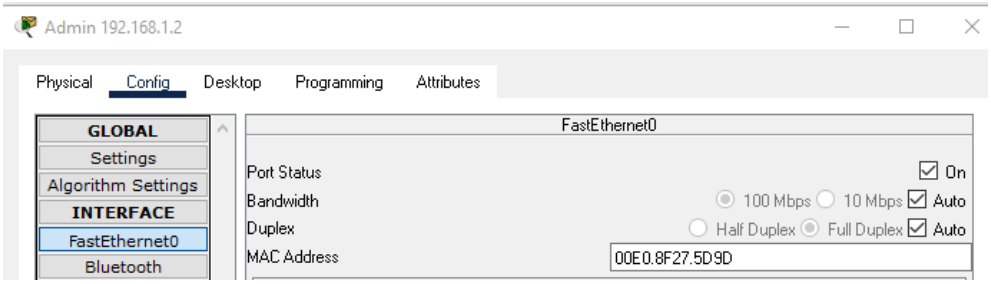


Abbildung 15: Access 2

2.1.3 Frage 2

Frage

Welche MAC Adressen liegen an welchen Ports an, und zu welchen Systemen gehören diese MAC Adresse, wie macht sich die doppelt vergebene MAC-Adresse in der SAT bemerkbar, und wie sind die beiden Systeme mit gleicher MAC-Adresse von anderen Systemen aus erreichbar und warum?

Antwort

Gerät	Adresse	Port
User 192.168.1.1	00E0.8F27.5D9D	Switch 1, Fa0/1
Admin 192.168.1.2	0030.F238.6804	Switch 1, Fa0/2
User 192.168.2.1	0001.4204.C8EE	Switch 2, Fa0/1
Admin 192.168.2.2	0001.968D.38A6	Switch 2, Fa0/2

Resultate nach der Änderung

Auf dem Switch 1, wo das Endsystem anhängt, wurde nur die Mac-Adresse auf dem jeweiligen Port geändert. Auf dem Backbone und dem Switch 2 wurde in der Tabelle die alte Adresse entfernt und die neue Adresse mit den gleichen Parametern hinzugefügt.

Das Systeme mit den gleichen Adressen sind wie zuvor von den zugeordneten Systemen erreichbar. Dies ist möglich, da die 2 Adressen auf 2 getrennten logischen Netzen liegen. Durch die Vlan Tags wissen die Switches wohin die Packets hin müssen.

```
backbone#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0090.0cla.7980    DYNAMIC     Fa0/1
   1    0090.2bad.a00b    DYNAMIC     Fa0/2
  10    0001.4204.c8ee    DYNAMIC     Fa0/2
  10    0090.0cla.7980    DYNAMIC     Fa0/1
  10    00e0.8f27.5d9d    DYNAMIC     Fa0/1
  20    0001.968d.38a6    DYNAMIC     Fa0/2
  20    0090.0cla.7980    DYNAMIC     Fa0/1
  20    00e0.8f27.5d9d    DYNAMIC     Fa0/1
```

Abbildung 16: Backbone

```
child1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0060.2fa7.6788    DYNAMIC     Fa0/3
  10    0001.4204.c8ee    DYNAMIC     Fa0/3
  10    00e0.8f27.5d9d    DYNAMIC     Fa0/1
  20    0001.968d.38a6    DYNAMIC     Fa0/3
  20    00e0.8f27.5d9d    DYNAMIC     Fa0/2
```

Abbildung 17: Access 1

```
child2#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.c7c0.90d1    DYNAMIC     Fa0/3
  10    0001.4204.c8ee    DYNAMIC     Fa0/1
  10    0001.c7c0.90d1    DYNAMIC     Fa0/3
  10    00e0.8f27.5d9d    DYNAMIC     Fa0/3
  20    0001.968d.38a6    DYNAMIC     Fa0/2
  20    0001.c7c0.90d1    DYNAMIC     Fa0/3
  20    00e0.8f27.5d9d    DYNAMIC     Fa0/3
```

Abbildung 18: Access 2

2.2 Port Security Konfiguration

2.2.1 MAC Adressen an Switchports

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address 00E0.8F27.5D9D
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address 0030.F238.6804
!
interface FastEthernet0/3
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
```

Abbildung 19: Switch 1

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address 0001.4204.C8EE
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address 0001.968D.38A6
!
interface FastEthernet0/3
 switchport trunk allowed vlan 10,20
 switchport mode trunk
```

Abbildung 20: Switch 2

2.2.2 Violation Modes

Für die Tests wurde immer Fa0/2 auf Switch 1 konfiguriert. Die Security Adresse ist die default Adresse des Endsystems, welches zuvor eine neue MAC-Adresse zugewiesen bekommen hat, die jedoch nicht zurückgesetzt wurde zum testen.

Protect

Bei Protect bemerkt man nichts außer, dass das System keine anderen Endsysteme erreichen kann und auch von anderen nicht erreicht werden kann, da es Netwerk nicht existiert.

```
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security violation protect
 switchport port-security mac-address 0030.F238.6804
!
```

Abbildung 21: Switch 1 Fa0/2 Config

```
 childl#show port-security interface fa0/2
 Port Security              : Enabled
 Port Status                : Secure-up
 Violation Mode             : Protect
 Aging Time                 : 0 mins
 Aging Type                 : Absolute
 SecureStatic Address Aging : Disabled
 Maximum MAC Addresses      : 1
 Total MAC Addresses        : 1
 Configured MAC Addresses   : 1
 Sticky MAC Addresses       : 0
 Last Source Address:Vlan   : 00E0.8F27.5D9D:20
 Security Violation Count   : 0
```

Abbildung 22: Resultat nach Ping

Restrict

Da die MAC-Adresse des Geräts nicht mit der am Port konfigurierten Adresse übereinstimmt, wird bei einem Ping-Versuch der Violation-Counter erhöht. Da Ping 4x einem echo sendet, wird der Counter um 4 erhöht.

```
childl#show port-security interface fa0/2
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Restrict
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 1
Configured MAC Addresses    : 1
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : 00E0.8F27.5D9D:20
Security Violation Count    : 0
```

Abbildung 23: Switch 1 Fa0/2 Config

```
child1#show port-security interface fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00E0.8F27.5D9D:20
Security Violation Count   : 4
```

Abbildung 24: Resultat nach Ping

Shutdown

Da die MAC-Adresse des Geräts nicht mit der am Port konfigurierten Adresse übereinstimmt, ist die Verbindung bei einem Ping-Versuch ausgeschaltet worden.

```
child1(config)#interface fa0/2
child1(config-if)#switchport port-security violation s
child1(config-if)#switchport port-security violation shutdown
```

Abbildung 25: Switch 1 Fa0/2 Config

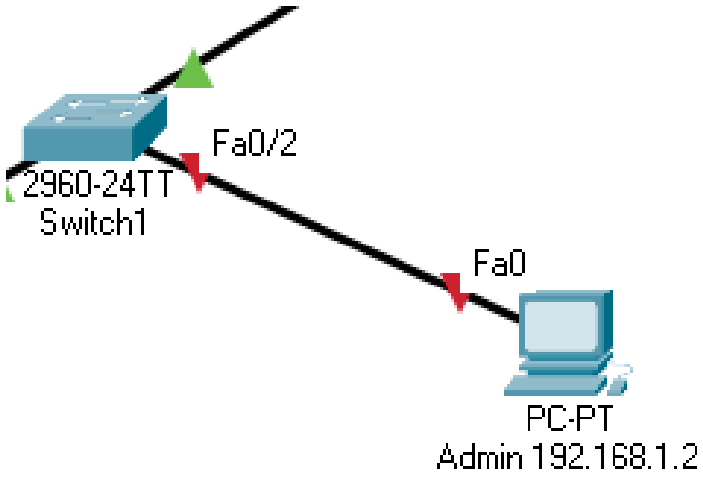


Abbildung 26: Resultat nach Ping

2.2.3 Maximalwerte für die Anzahl an Adressen pro Port

Um die Maximalwerte auprobieren zu können muss an dem Port ein Switch mit weiteren Geräten angehängt werden.Die Test fanden an Switch 1 Fa0/2 statt. Die max Anzahl ist 3.

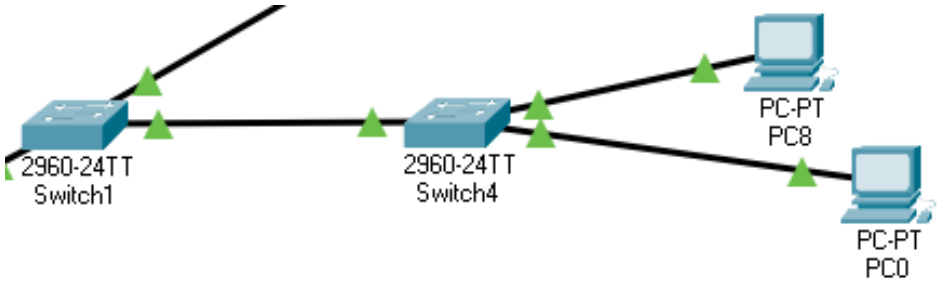


Abbildung 27: Setup für die Test
Der 3.PC der zur Violation führt wurde immer aus- und eingehängt.

Abhängig vom Violation Mode wird die jeweilige Fehlerfunktion ausgeführt.

Protect: Man bemerkt nur, dass man nicht senden kann. Aber als Admin bekommt man keine Violation Meldung.
Restrict: Hier wird der Violation-Counter erhöht und die totalen Addressen bleiben beim Maximum. Man kann mehr Geräte einfügen, aber die Packets werden nicht weitergeleitet und der Counter wird für jedes Packet erhöht. Die registrierten Geräte können ganz normal Daten senden und erhalten ohne, dass der Counter erhöht wird.

```
childl#show port-security interface fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 3
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0001.637D.9D01:1
Security Violation Count   : 4
```

Abbildung 28: Switch 1 Fa0/2 nach Violation

Shutdown: Sobald ein unbekanntes Gerät versucht was zu senden, geht das gesamte Port down und keiner kann was senden und erhalten.

```
child1#show port-security interface fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 3
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0001.637D.9D01:1
Security Violation Count   : 24

child1#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
```

Abbildung 29: Switch 1 Fa0/2 nach Shutdown

2.2.4 Frage 3

Frage

Wie unterscheiden sich die Violation-Modes (Vor-/Nachteile), wie ändern sich die Source Address Tables der Switches durch die unterschiedlichen Konfigurationen, und wie kann Port Security umgangen werden?

Antwort

Violation Modes

Mode	Vorteile	Nachteile
protect	Das System bleibt immer aktiv. Ist gut geeignet für Netze, wo man einfach nur die Menge an parallen Verbindungen reduzieren will.	Gegen Angriffe nicht wirklich geschützt. Nicht für Netzwerke die sensible Daten übertragen sollen geeignet.
restrict	Ist gut geeignet für Gruppierungen und wenn das Netz bei Angriffen bzw. Violations nicht gleich abgedreht werden muss, aber man das Netz Monitoren will.	Wie protectnicht wirklich gegen Angriffe geschützt. Nicht für Netzwerke die sensible Daten übertragen sollen geeignet.
shutdown	Für spezielle Fälle geeignet, wo nur ganz bestimmte Geräte in der Lage sein sollten sich zu verbinden.	Für Weitervernetzung nicht wirklich geeignet, da dann alle Systeme am Port gleich getrennt werden, sollte es zu einer Violation kommen.

SATs der Switches

Adressen an den Ports nach der Konfiguration einer statischen MAC-Adresse, werden als statisch in der SAT gespeichert. Bis auf die Switch Adressen werden alle anderen nach der aging time gelöscht.

Wege zum umgehen der Port Security

Wenn man die MAC-Adresse des konfigurierten Ports kennt, kann man MAC spoofing anwenden und sich einfach einbinden. Eine weitere Problematik kann sich ergeben, wenn jemand versucht durch "Brute Forcingëinzudringen und die Port Security zb. nicht auf Shutdown eingestellt ist.

2.3 Sticky Learning

2.3.1 Umstellen auf Sticky secure MAC addresses

```
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode trunk
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security mac-address 0030.F238.6804
```

Abbildung 30: Switch 1 Fa0/2 nach Shutdown

2.3.2 Frage 4

Frage

Worin besteht der Unterschied zum Default Verfahren (also ohne Verwendung von „Sticky secure“ Lernen)?

Antwort

Beim Default Verfahren sind die Addressen statisch, aber werden auf dem jeweiligen Interface nicht gespeichert. Beim SSticky secure"wird die Addresse jedoch vom Switch gespeichert und eingetragen.

```
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode trunk
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security mac-address 0030.F238.6804
 switchport port-security mac-address sticky 000A.4173.D1DE
!
```

Abbildung 31: Running Config nach einem Ping

3 Link Aggregation

3.1 Aufbau des virtuellen Netzwerks – Erweiterung

3.1.1 Server und deren Konfiguration

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:63FF:FE7D:A654
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.100.1
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

(a) IP-Config von Server 1

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20A:F3FF:FE26:A4A
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.100.2
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

(b) IP-Config von Server 2

```
hostname backbone
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
!
```

(c) Running Config des Backbone

3.2 Tests der Ausgangssituation

3.2.1 Frage 5

Frage

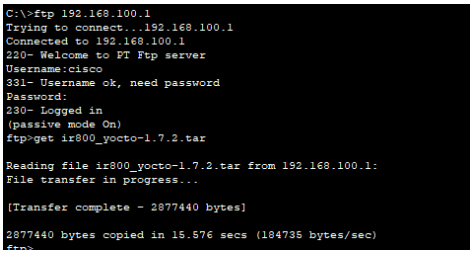
Warum zeigt der Packet Tracer bei dem hinzugefügten Link nicht mehr zwei grüne (also aktive) Ports an?

Antwort

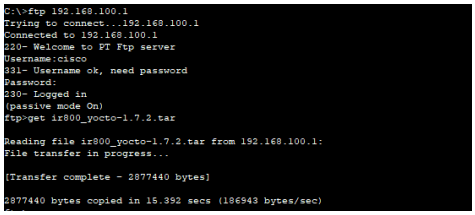
Weil die Switches im STP Mode sind.Die extra Leitung wird erst dann eingeschaltet, wenn die andere Leitung ausfällt, damit keine switching loops enstehen und die MAC-Tabellen(SATs) nicht "corrupted" werden.

3.2.2 FTP Resultat

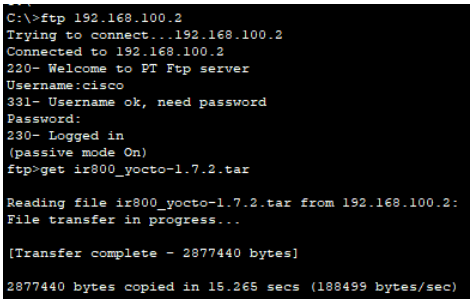
User 192.168.1.1: 15.576 sec
User 192.168.1.2: 15.392 sec
Admin 192.168.2.1: 15.265 sec
Admin 192.168.2.2: 15.265 sec



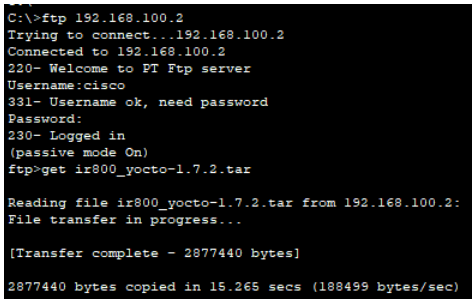
(a) User 192.168.1.1



(b) User 192.168.1.2



(c) Admin 192.168.2.1



(d) Admin 192.168.2.2

3.3 Konfiguration

3.3.1 LACP Config

```
interface Port-channel1
 switchport mode trunk
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 5
 switchport port-security violation protect
 switchport port-security mac-address 00E0.8F27.5D9D
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address 0030.F238.6804
 switchport port-security mac-address sticky 000A.4173.D1DE
!
interface FastEthernet0/3
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/4
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 channel-group 1 mode active
!
```

(a) Switch 1

```
interface Port-channel2
 switchport mode trunk
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation restrict
 switchport port-security mac-address 0001.4204.C8EE
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address 0001.968D.38A6
!
interface FastEthernet0/3
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/4
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 channel-group 2 mode active
!
```

(b) Switch 2

```
interface Port-channel1
 switchport mode trunk
!
interface Port-channel2
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/2
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/5
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/6
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 channel-group 2 mode active
!
```

(c) Backbone

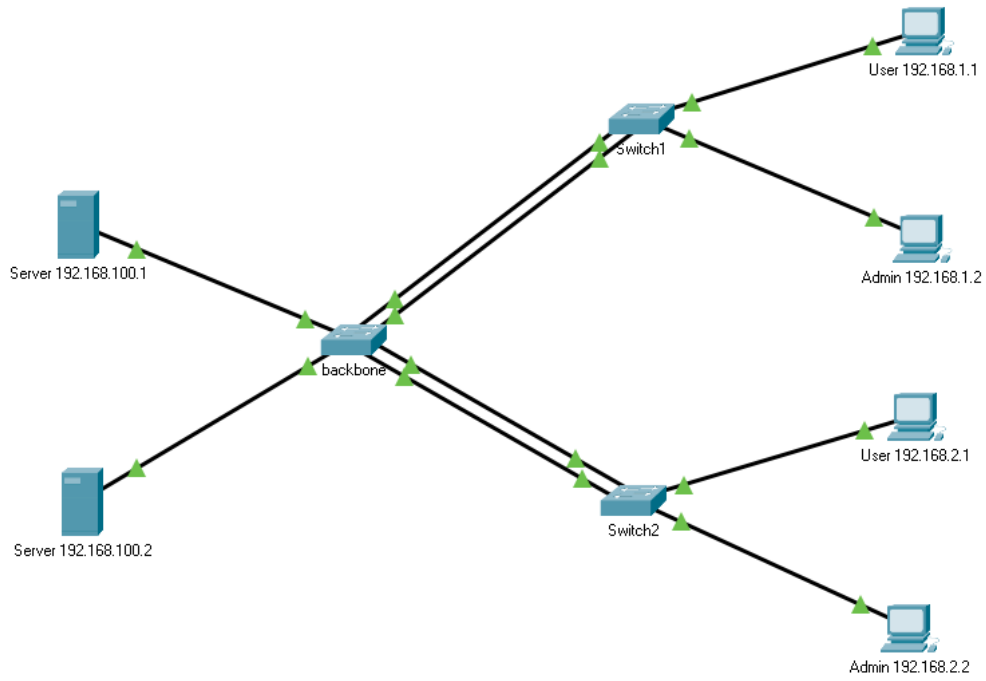


Abbildung 35: Aufgebautes Netz mit LACP

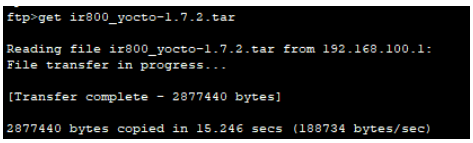
3.3.2 FTP Download Resultate

User 192.168.1.1: 15.246 sec
User 192.168.1.2: 15.546 sec
Admin 192.168.2.1: 15.256 sec
Admin 192.168.2.2: 15.441 sec

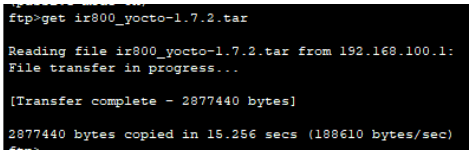
3.3.3 Frage 6

Frage

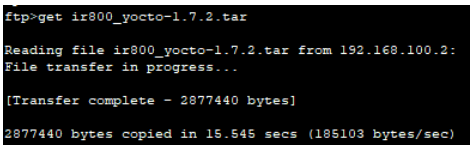
Warum verdoppelt sich die jetzt erreichte Datenrate nicht, wo liegt das „Bottleneck“ (die Stelle mit dem geringsten Durchsatz, die die erreichte Datenrate determiniert)?



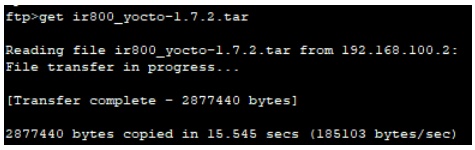
(a) User 192.168.1.1



(b) User 192.168.1.2



(c) Admin 192.168.2.1



(d) Admin 192.168.2.2

Antwort

Der EtherChannel unterstützt mehrere Load Balancing Methoden und die Werkeinstellungen benutzen die ßrc-mac forwardingMethode, was bedeutet, dass Packets von der gleichen Src über den gleichen Port gehen. Damit wirklich die doppelte Datenrate erreicht wird müsste man auf "dest-mac forwardingümstellen