OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Fakultät Informatik und Mathematik

COMLAB
Datenkommunikation und Netzwerke

Prof. Dr. Waas

Praktikum zum Fach

**Kommunikationssysteme/
Rechnernetze**

Übung

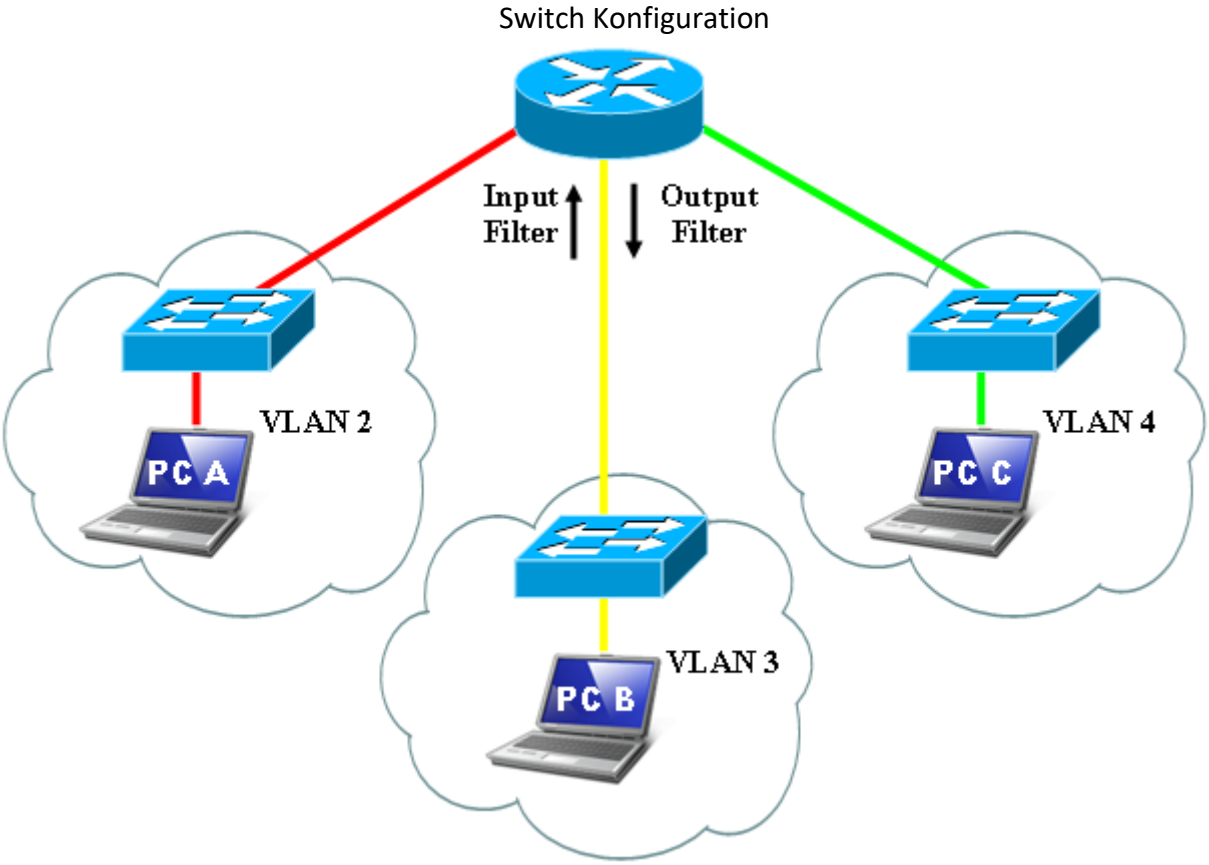
VLANS & LAYER3 SWITCHING MIT CISCO CATALYST 3560

Linux

(Version 02.03.2022 KVM)

1. EINFÜHRUNG

Das Ziel dieser Übung ist es, die Funktionsweise von VLANs und deren Routing kennenzulernen und an geeigneter Hardware auszuprobieren. Das folgende Bild zeigt die Netzwerkumgebung der Übung:



Der Switch fungiert als Router zwischen drei VLANs, wobei Verkehr von/nach VLAN 3 über Filterregeln eingeschränkt werden soll.

VLAN
Virtual Local Area Network (VLAN) ist eine Technologie, die es möglich macht, ein vorhandenes Local Area Network in mehrere virtuelle Netze zu unterteilen. Voraussetzung dafür sind VLAN-fähige Switches (sogenannte Layer3-Switches). Die Vorteile sind:

- Die einzelnen Netze sind voneinander so getrennt, als ob sie physikalische Teilnetze wären
- Bei Änderungen in der Organisationsstruktur der LANs sind keine Änderung des Hardwareaufbaus/der Verkabelung notwendig
- Alle Einstellungen geschehen über Software auf den Switches

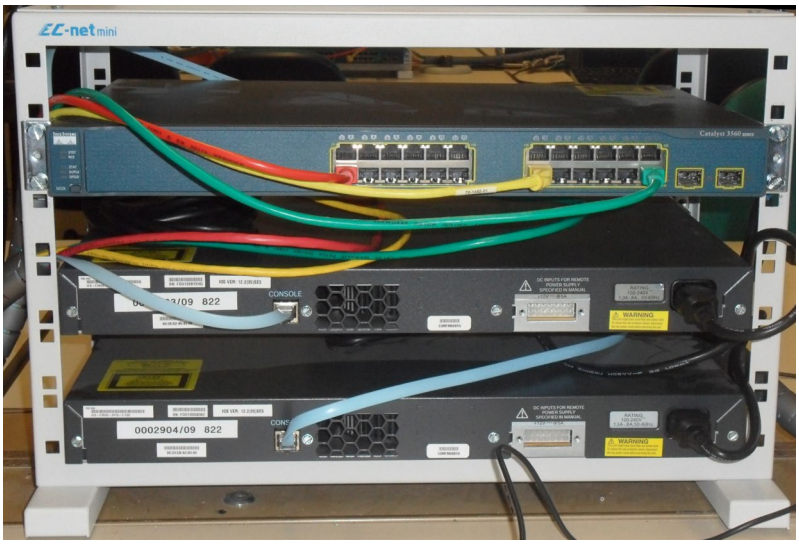
Natürlich ist es in der Regel notwendig, dass verschiedene VLANs wieder miteinander kommunizieren können. Dies erreicht man mittels „Layer3-Switching“.

Layer3-Switching
Layer3-Switching ist eine Erweiterung der VLAN-Technologie um Routing-Fähigkeiten. Einfach gesagt: Ein Layer3-Switch ist ein VLAN-fähiger Switch, der zusätzlich noch fähig ist, Datenverkehr zwischen verschiedenen VLANs zu routen.

2. VORBEREITUNGEN

Alle Switche müssen vor der Übung ausgeschaltet sein. Nur der Kursleiter oder der Laborbetreuer schaltet alle Switche vor Übungsbeginn ein. Beide Einschalter befinden sich auf dem Rack in der Mitte. Dies sollte auch zwischen den Übungsstunden erfolgen.

- Diese Übung kann nur an den PC-Arbeitsplätzen **PC1 bis PC6** durchgeführt werden. Alle Switche sind in sog. Racks eingebaut.
- Die Switche sind mit dem Namen des Arbeitsplatzes beschriftet, zu dem sie zugeordnet sind. Für diese Übung brauchen Sie jeweils nur einen Switch.



- Öffnen Sie auf dem **Desktop** den Ordner **Virtual Machines Links**. Dort befinden sich Verknüpfungen zu den vorbereiteten virtuellen Maschinen.

- Klicken Sie auf die folgenden Verknüpfungen um die damit verlinkten virtuellen Maschinen zu starten: **PC-A, PC-B** und **PC-C**

Hinweis: An PC-B und PC-C befindet sich keine COM Schnittstelle. Eine evtl. beim Start des virtuellen PCs erscheinende Fehlermeldung kann ignoriert werden.

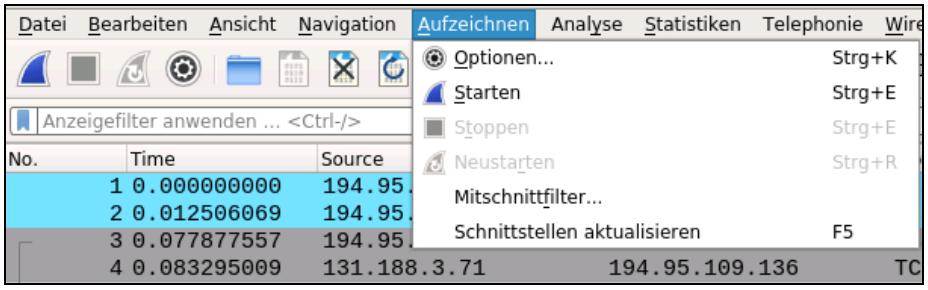
Beachten Sie die folgenden Hinweise:

- Jedem der virtuellen PCs ist das entsprechende Netzwerk (=LAN) aus der Switch Konfiguration zugeordnet:

virtueller PC	Interface am Labor-PC	LAN
PC-A	**IntelPro-oben-rot**	**VLAN2 rot**
PC-B	**IntelPro-unten-gelb**	**VLAN3 gelb**
PC-C	**Dlink-untengrün**	**VLAN4 grün**

- Der Switch wird über den seriellen Port am virtuellen **PC-A** konfiguriert.

- Starten Sie auf dem lokalen Labor-PC das Programm **WireShark**
- Öffnen Sie das **Aufzeichnen Menü** und wählen Sie **Optionen...** aus.



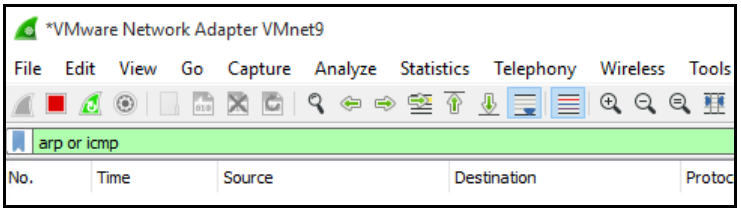
- **MESSUNG VLAN2:** Wählen Sie Interface **IntelPro-oben-rot** aus und klicken Sie auf den **Start**-Button. Damit kann Wireshark auf dem Subnetz 192.168.10.0 alle Datenpakete sehen und aufzeichnen.

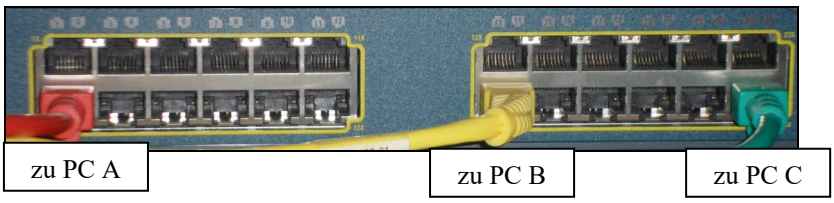
- **MESSUNG VLAN3:** Starten Sie das Programm Wireshark noch einmal. Öffnen Sie dort das **Aufzeichnen** Menü und klicken Sie auf **Optionen**. Wählen Sie diesmal das Interface **IntelPro-unten-gelb** aus und klicken auf den **Start**-Button. Damit kann der zweite Wireshark im Subnetz 192.168.20.0 alle Datenpakete sehen und aufzeichnen.

- **MESSUNG VLAN4:** Starten Sie das Programm Wireshark ein drittes mal. Öffnen Sie dort das **Aufzeichnen** Menü und klicken Sie auf **Optionen**. Wählen Sie diesmal das Interface **Dlink-untengrün** aus und klicken auf den **Start**-Button. Damit kann der zweite Wireshark im Subnetz 192.168.30.0 alle Datenpakete sehen und aufzeichnen.

In der folgenden Übung sollen Sie mit den Wireshark Programmen alle Netzwerke (Subnetze) beobachten und die aufgezeichneten Daten interpretieren.

- Machen Sie sich klar, welchen Weg ein Ping Request bzw. Ping Reply nimmt. Stellen Sie in allen Wireshark als Display-Filter **arp or icmp** ein





- Prüfen Sie ob die LAN-Kabel am Switch (Bild o.) richtig angeschlossen sind.(*entfällt bei Remote Zugang*)

3. AUFGABENSTELLUNG

Aufgabe 1: Mit dem Switch verbinden und in den Grundzustand bringen

- Starten Sie **Serial port terminal** nur am PC-A Es wird ein Terminalfenster geöffnet. Aktivieren Sie das Terminalfenster und drücken Sie die **ENTER-Taste**, damit der Switch antworten.
  Hinweis: **Cut & Paste** funktioniert im Serial port terminal auch.

Nun sind zwei Fälle **a) und b)** zu unterscheiden:

a) Der Switch ist bereits im Grundzustand

- Falls die folgende Frage erscheint, antworten Sie mit: **yes**

```
Would you like to terminate autoinstall? [yes]:
```

- Dann beantworten Sie die im Terminal angezeigte Frage mit **no**.

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

- Sie können dann bei **Aufgabe 2** weiter machen.

✘ *Falls Sie die obigen **Dialoge falsch** beantwortet haben und Sie sind im „Initial Configuration Dialog" gelandet, können Sie die meisten Dialogfragen mit **STRG C** (bzw. **CTRL C**). Einige Fragen jedoch nicht. Bei den folgenden Fragen müssen Sie eingeben:*

- Enter interface name used to connect to the management network from the above interface summary: **vlan1**
- [0] Go to the IOS command prompt without saving this config.
  [1] Return back to the setup without saving this config.
  [2] Save this configuration to nvram and exit.
  Enter your selection [2]: **0**
- Switch> **enable**
- Switch# **clear startup-config**
  Erasing the nvram … configuration files! Continue? [confirm] **y**
- Switch# **reload**
  Proceed with reload? [confirm] **y**

Dann wird der Switch neu gestartet. Das dauert ca. 2 Minuten.

b) Im Switch befindet sich eine Konfiguration des Vorgängers.

Wenn sofort das **Switch**> Prompt kommt, muss der Switch in den Grundzustand versetzt werden. Die folgende Tabelle gibt die Kommandos an, mit denen das getan werden kann. Beantworten Sie die folgenden Dialogfragen wie in der Tabelle angegeben.

```
Switch> enable
Switch#> erase startup-config
        Erasing the nvram … configuration files! Continue? [confirm]  y
Switch# reload
Switch#> reload
       System configuration has been modified. Save? [yes/no]: no
  Proceed with reload? [confirm] y
```

Der Switch bootet nun. Führen Sie dann den Dialog unter **a)** (siehe oben) weiter.

Die folgende Tabelle enthält eine kurze Erklärung der benötigten Behle am Switch. Nehmen Sie diese kurz zur Kenntnis und gehen Sie dann zu Aufgabe 2 weiter.

Befehl	Beschreibung	Mode
enable	Wechseln vom User Exec Mode in den Privileged Exec Mode, über den der Switch konfiguriert wird	#
disable	Verlassen des Privileged Exec Mode	#
configure terminal	Globaler Konfigurationsmodus	#
exit oder end	Globalen Konfigurationsmodus verlassen Interface-Konfigurationsmodus verlassen	(config) (config-if)
no logging console	Systemmeldungen auf dem Terminal unterdrücken	(config)
interface <interfacename>	Zu einem Port oder ein VLAN wechseln	(config)
ip address <ip address> <subnetmask>	IP Adresse für das vorher angewählte Interface setzen	(config-if)
no ip address <ip address>	Gesetzte IP-Adresse wieder entfernen	(config-if)
no shutdown	Aktivieren der Interfaces	(config-if)
shutdown	Interface deaktivieren	(config-if)
show running-config	Aktuelle Konfiguration zeigen (aus dem RAM)	#
ip route <ip> <mask> <nexthop>	Eintrag in die Routingtabelle	(config)
erase startup-config	Löscht die Startkonfiguration (Inhalt des NVRAM)	#
switchport mode access	setzt ein Interface in den Layer2-*access*-Modus (not-wendig für Zuweisung zu einem VLAN)	config-if)
switchport access vlan *vlan-id*	weist einen Port einem VLAN zu (falls nicht vorhanden, wird das VLAN somit auch angelegt)	(config-if)
ip address *ip_adresse subnetzmaske*	weist einem Interface eine IP-Adresse zu; auf ein VLAN angewandt ergibt sich ein SVI (Switch Virtual Interface), was quasi der Router-Port ist an welchem das VLAN angeschlossen ist	(config-ip)
ip routing	aktiviert die Routing-Funktionalität des Switches	(config)

access-list *number* permit|deny ip *src-ip src-wildcard dst-ip dst-wildcard*	erstellt eine extended ACL (access-control list), mit der der Datenverkehr anhand von Absender und Empfänger gefiltert werden kann. Die *number* einer extended ACL **muss** zwischen 100 -199 liegen! Die *wildcard* gibt durch 1er-Bits an, welche Stellen der IP variabel sind – z. B. 192.168.1.0 0.0.0.255 => alle IPs aus 192.168.1.x treffen auf diese Regel zu.		(config)
ip access-group *number* in|out	wendet die ACL mit Nummer *number* auf einInterfacean.DieRichtungen *in* und *out* beziehensichaufdieSichtdesRouters!		(config-if)
no *config-command*	macht die meisten Konfigurationsbefehle rückgängig		(config) (config-if)

Aufgabe 2: Stellen Sie die IP-Adresse von PC-B und PC-C so um, dass sie im selben Subnetz wie PC-A sind:

PC-B bekommt: 192.168.10.**20**
PC-C bekommt: 192.168.10.**30**

- Starten Sie dazu auf **PC-B** und **PC-C** das Script: **Netzwerk** am Desktop Mit dem Linux-Editor nano wird eine Konfigurationsdatei geöffnet. Überschreiben Sie die alten IP-Adresse mit der Neuen (verw. Pfeil-Tasten). Speichern Sie mit **Strg-O** und beenden Sie den Editor mit **Strg-X**. Danach wird die aktuelle Einstellung aktiviert und angezeigt. *(Netz-Konfiguration via Linux netplan.)*
- Starten Sie auf **jedem** virtuellen PC die Eingabeaufforderung/Terminal und starten Sie darin **Pings** zu den anderen virtuellen PCs (*ping IP-Adresse*)

  Ergebnis: Pings sollten beantwortet werden. Lässt sich auch mit Wireshark beobachten.

Aufgabe 3: Setzen Sie alle virtuellen PCs wieder in ihre Ausgangsnetze:

- **Beenden** und **starten** Sie die **PC-B** und **PC-C** erneut. Damit werden die IP-Einstellungen zurück gesetzt auf die richtigen Werte.
- Starten Sie auf **jedem** virtuellen PC zwei Eingabeaufforderungs-Fenster und starten Sie darin **Pings** zu den anderen virtuellen PCs (ping *IP-Adresse*). **Beachten Sie, dass die PC's nun wieder andere IP- Adressen haben als bei den Pings vorher**!

  Ergebnis: Alle PCs empfangen ARP-Requests für die MAC-Adressen der Default-Gateways. Lässt sich mit Wireshark beobachten.

Aufgabe 4: Weisen Sie den Switch-Ports folgende VLANs zu:

- Die folgende Tabelle zeigt Ihnen, welche Ports in welchem VLAN zugeordnet sein sollen.

fa0/2	**->**	**VLAN 2**	**(192.168.10.x/24)**
fa0/14	**->**	**VLAN 3**	**(192.168.20.x/24)**
fa0/24	**->**	**VLAN 4**	**(192.168.30.x/24)**

- Nehmen Sie am Switch die notwendigen Konfigurationen vor (siehe Kasten unten, nur das fettgedruckte eingeben) .

```
Switch> enable
Switch# configure terminal
Switch(config)# no logging console

Switch(config)# int fa0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
Switch(config)#

Switch(config)# int fa0/14
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 3
Switch(config-if)# exit
Switch(config)#

Switch(config)# int fa0/24
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 4
Switch(config-if)# exit
Switch(config)#
```

Ergebnis: die Rechner sind nun voneinander getrennt. Keine fremden ARP-Requests werden mehr empfangen. Lässt sich mit Wireshark beobachten.

Hinweis: Auf den Switches sind die VLANs 1 sowie 1002-1005 per Default angelegt und haben spezielle Bedeutungen – benutzen Sie diese nicht!

Aufgabe 5: Anlegen eines SVI (Router Port)

- Legen Sie für jedes VLAN ein SVI (Switch Virtual Interface an (quasi der Router-Port an welchem das VLAN angeschlossen ist). Stichwort: Default-Gateway. Damit wird festgelegt, in welchem IP-Subnetz das VLAN betrieben wird. Wählen Sie die Subnetze so, dass sie zu den daran angeschlossenen virtuellen PC passen. Aktivieren Sie das IP-Routing auf dem Switch (nur das fettgedruckte eingeben).

```
Switch(config)# int vlan 2
Switch(config-if)# ip addr 192.168.10.1 255.255.255.0
Switch(config-if)# exit

Switch(config)# int vlan 3
Switch(config-if)# ip addr 192.168.20.1 255.255.255.0
Switch(config-if)# exit

Switch(config)# int vlan 4
Switch(config-if)# ip addr 192.168.30.1 255.255.255.0
Switch(config-if)# exit
Switch(config)#

Switch(config)# ip routing
```

Ergebnis: Pings sollten nun über die Standard-Gateways zu den Zielrechnern gelangen (achten Sie in Wireshark auf die MAC-Adressen der Absender!)

Aufgabe 6: ACL für SVI (VLAN3)

- Lassen Sie Pakete für VLAN3 ausschließlich von VLAN2 zu. Erstellen Sie dazu eine extended ACL (Vorschlag: Nummer 100) und wenden Sie diese in Ausgangsrichtung SVI (Routerport) zum VLAN 3 an.

```
Switch(config)# access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
Switch(config)# int vlan 3
Switch(config-if)# ip access-group 100 out
Switch(config-if)# exit
Switch(config)#
```

Ergebnis: Nur Pings aus VLAN2 kommen in VLAN3 an. Pings von VLAN 4 werden geblockt.

Hinweis: *Jede ACL (Access-Control-List) wird von oben nach unten durchlaufen und enthält stets als letztes die implizite Regel "deny any". Legen Sie deshalb Regeln für das Erlauben von Datenverkehr an, der Rest wird dann automatisch geblockt!*

- Lassen Sie nun zusätzlich Pakete von VLAN3 ausschließlich nach VLAN2 zu. Erstellen Sie dazu Ihre zweite Extended ACL (Vorschlag: Nummer 101) und wenden Sie diese in Eingangsrichtung von VLAN3 zum Router an.

```
Switch(config)# access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
Switch(config)# int vlan 3
Switch(config-if)# ip access-group 101 in
Switch(config-if)# exit
Switch(config)#
```

- Erweitern Sie die ACL, sodass auch Pings von VLAN4 zu VLAN3 und umgekehrt möglich sind. Bitte die bestehenden Listen ergänzen und keine neuen Listen erstellen!

```
Switch(config)# access-list 100 permit ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
Switch(config)# access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
```

Aufgabe 7: Host PC-C zieht um. (beachte folgenden Hinweis!)

Hinweis: Bei betreutem Remote Zugang rufen Sie den/die Kursleiter(in), der/die den Port für Sie umsteckt. Nennen Sie dazu Ihren Arbeitsplatz-PC!

Um die Vorteile von VLANs in Unternehmen zu demonstrieren sei folgende Situation angenommen: Der Mitarbeiter an PC-C zieht in ein anderes Büro um. Dort sei eine andere Netzwerkdose und der Netzanschluss ändert sich. Der PC-C wird jetzt am Switch Port **fa 0/22** angeschlossen. Was ist zu tun, damit der PC-C wieder im Netz funktioniert, ohne am PC selbst Änderungen vornehmen zu müssen?

- Stecken Sie **V O R S I C H T I G** das **grüne Kabel** von Port 24 auf Port 22 um und achten Sie darauf, dass Sie die Netzwerkbuchse im Switch und den

Halteclip am Kabel nicht beschädigen. Nehmen Sie die nötigen Änderungen im Setup des Switches vor. Testen Sie PC-C im Netz.

Nach der Übung stecken Sie bitte das grüne Kabel V O R S I C H T I G wieder zurück auf Port 24, damit auch die nächste Arbeitsgruppe die richtige Arbeitsumgebung vorfindet.

4 Kontrollfragen

- ☑ Was ist der Sinn und Zweck der VLAN-Technologie bzw. welchen Vorteil haben VLANs gegenüber dem physischen Aufbau?
- ☑ Können zwei Hosts aus verschiedenen VLANs miteinander kommunizieren?
- ☑ Was ist der Unterschied zwischen einem rein VLAN-fähigen Switch und einem Layer3-Switch?
- ☑ Annahme: VM „PC-A“ befindet sich in **VLAN 2** und besitzt die IP 192.168.10.100/24 und VM„PC-B“ befindet sich in **keinerlei VLAN** und besitzt die IP 192.168.10.200/24 Es sind keine Zugriffsbeschränkungen in Form von ACLs o. ä. definiert
  Frage: Kann A B pingen? Kann umgekehrt B A pingen?
- ☑ Annahme: 2 Hosts sind in getrennten VLANs und haben jeweils die IP 192.168.23.42/24
  Frage: Was geschieht, wenn der Port des einen Host auf das VLAN umkonfiguriert wird in dem sich der andere Host befindet?
- ☑ Wie muss eine extended ACL lauten, die sämtlichen Verkehr in ein Netz mit der Adresse 10.12.0.0/16 ausgehend vom Netz 192.168.5.0/24 passieren lässt und den Rest blockt? In welche Richtung muss diese angewandt werden?
- ☑ Was müsste am Switch konfiguriert werden, wenn an Port FA0/4 ein zusätzlicher PC mit der IP-Adresse 192.168.10.20 angeschlossen werden sollte.

4 ENDE DER ÜBUNG

- Beenden Sie alle **Programme** und **virtuelle Maschinen**! Im Rahmen der Übung an Ihrem Arbeitsplatz erzielte Messergebnisse können Sie im Labor auf Ihren Memorystick zur späteren Nachbearbeitung abspeichern. Gewonnene sicherheitsrelevante Informationen insbesondere Passwörter, dürfen nicht weitergegeben oder unbefugt verwendet werden. Geht leider nicht im Remotebetrieb.
- **Loggen** Sie sich aus dem Labor-PC **aus!**
- Lassen Sie den PC weiterlaufen. Er wird automatisch ausgeschaltet.

Bitte hinterlassen Sie Ihren Arbeitsplatz in ordentlichem Zustand!

Entsorgen Sie Mitgebrachtes selbst!

Schieben Sie den Stuhl an den Tisch!

ANHANG: ALLE SWITCH KOMMANDOS

 # Aufgabe 4

```
enable
conf term
no logging console

int fa0/2
switchport mode access
switchport access vlan 2
exit

int fa0/14
switchport mode access
switchport access vlan 3
exit

int fa0/24
switchport mode access
switchport access vlan 4
exit
```

 # Aufgabe 5

```
int vlan 2
ip addr 192.168.10.1 255.255.255.0
exit

int vlan 3
ip addr 192.168.20.1 255.255.255.0
exit

int vlan 4
ip addr 192.168.30.1 255.255.255.0
exit

ip routing
exit

show ip route
```

 # Aufgabe 6

```
conf term
access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 100 permit ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255

int vlan 3
ip addr 192.168.20.1 255.255.255.0
ip access-group 100 out
ip access-group 101 in
exit
exit
```