05 Virtual LAN

1 Thema des Praktikums

Die Schwerpunkte des Praktikums sind:

- Virtual Local Area Network (VLAN – IEEE 802.1Q)
- Traffic Monitoring in Switched LANs (Port Mirroring)

Ein physisches Netz kann in mehrere virtuelle LANs aufgeteilt werden. Diese virtuellen LANs sind logisch komplett separiert, als ob sie physisch getrennt wären. Jedes VLAN stellt dabei eine eigene Broadcast Domain dar.

Im folgenden Versuch wird ein Netzwerk aufgebaut und dann in zwei virtuelle Netzwerke aufgeteilt, welche eine gemeinsame Backbone-Verbindung nutzen. In einem ersten Teil werden die durch den VLAN-Tag beeinflussten Eigenschaften von Ethernet Switches untersucht. Im zweiten Teil wird das Verfahren des Port Mirrorings verwendet, um den Verkehr in einem geswitchten LAN beobachten zu können.

2 Vorbereitung

Um die abstrakte Problemlösung von VLANs zu verstehen arbeiten wir mit einem Beispiel:
Sie leiten eine Firma und besitzen das Gebäude, in welchem die Firma tätig ist. Wegen Homeoffice, konnte der Bedarf an Bürofläche reduziert werden. Sie haben eine Firma als Mieter gefunden, die gerne einen Raum im 3. Stock sowie auch einen Raum beim Empfang im EG mieten möchte. Weil Sie ihre Geschäftsgeheimnisse nicht teilen und gleichzeitig aber an der Gebäudeverkabelung nichts ändern möchten, stehen sie vor einem Problem. Dieses lässt sich mit virtuellen LANs lösen, indem Sie auf einem physikalischen Netz mehrere virtuelle, getrennte Netze (VLANs) betreiben.

- Lesen Sie den Anhang A, den gekürzten Auszug des Anwenderhandbuchs:
  Hischmann / Belden: «Grundkonfiguration Industrial ETHERNET (Gigabit-)Switch RS20...»,

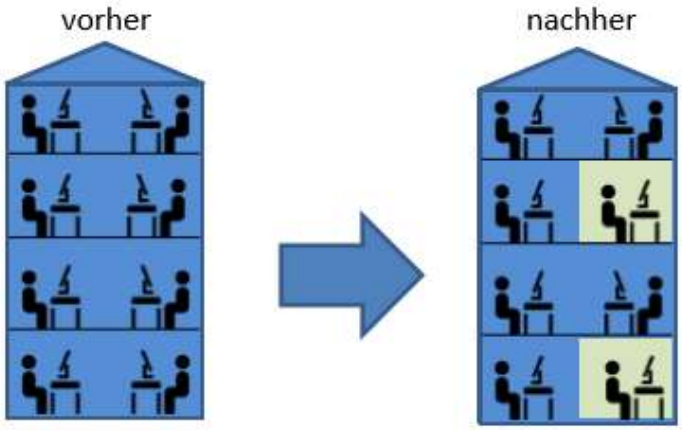
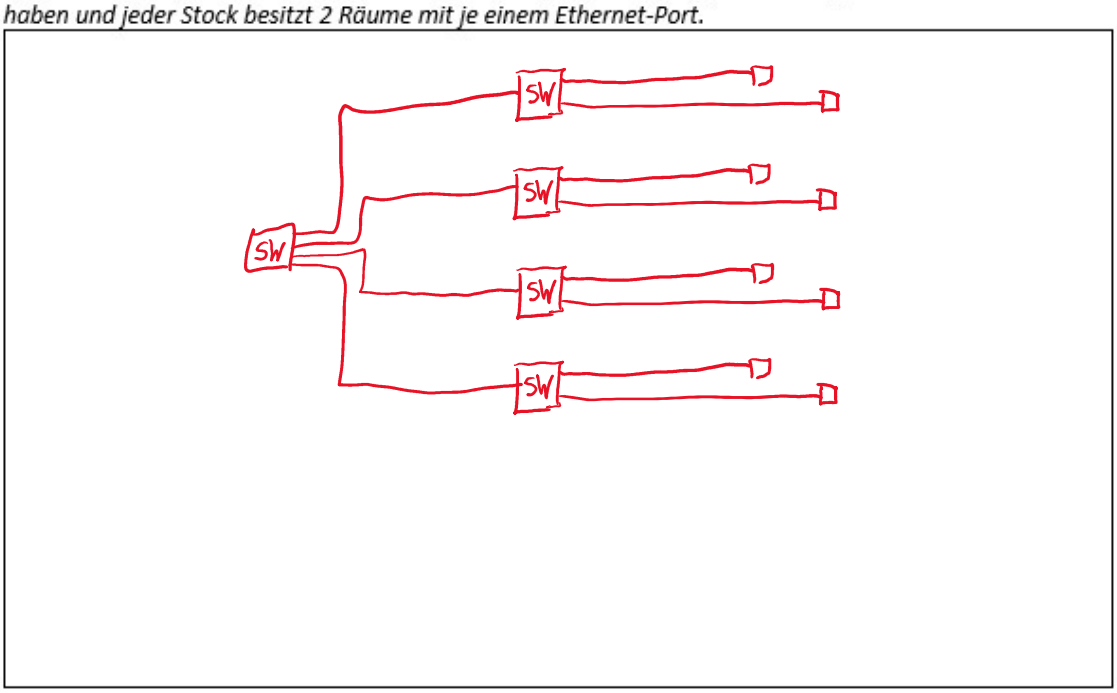


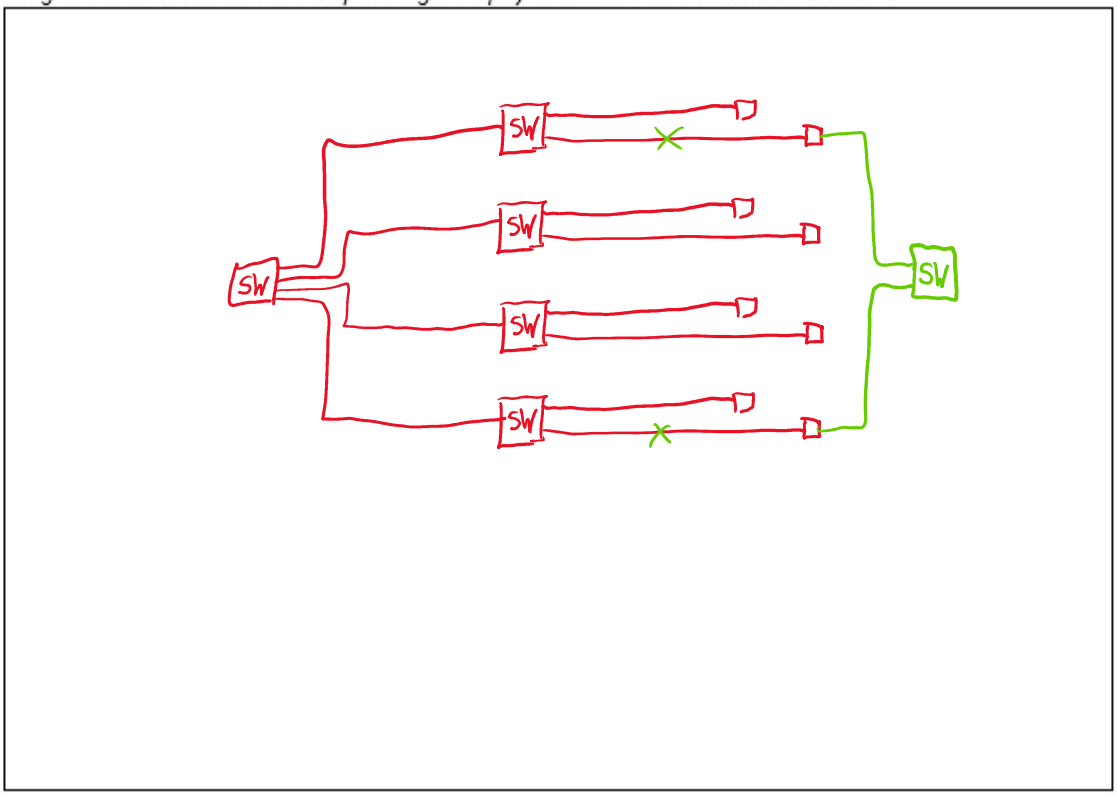
Abbildung 1: Gebäude-Layout vor und nach dem Einzug des Mieters

2.1 Vorbereitung zu Virtual Local Area Network (VLAN)

Q01 *Skizzieren sie von Hand das Netzwerk im Gebäude (vor dem Umbau). Es soll auf jedem Stock einen Switch haben und jeder Stock besitzt 2 Räume mit je einem Ethernet-Port.*



Q02 *Zeichnen Sie von Hand das Netzwerk vom Gebäude (nachher). Was ändert sich an der Verkabelung, wenn die grünen Räume in einem komplett eigenen physikalischen Netzwerk sein müssen?.*



Q03 *Was ist der Vorteil einer Lösung mit VLANs statt einer neuenVerkablung?*

physischer Umbau ist aufwendig
man kann beliebig neue VLANs aufsetzen

Q04 *In Anhang wird viel von der VLAN-ID gesprochen. Wo befindet sich diese im Ethernet-Frame?*

Tag-Header

Q05 *Wie viele VLANs wären theoretisch möglich?*

$2^{12\ Bit} = 4096$

Q06 *Wozu dient beim Switch RS20 das VLAN mit der ID 1? Warum darf es nicht entfernt werden? (VLAN 1 wird häufig so verwendet, aber nicht in allen IT Systemen)).*

Management

2.2 Konfiguration des Netzwerks

Abbildung 2 zeigt ein vereinfachtes Bild unseres Gebäudes für den späteren Laboraufbau. Das blaue Netzwerk erhält VLAN-ID 10 und das grüne Netzwerk VLAN-ID 20.

Geben Sie in Abbildung 2 mit «U» oder «T» an, welche Switch-Ports tagged Frames (T) verschicken müssen und an welchen untagged Frames (U) genügen. In Abbildung 2 ist bei jedem Port ein Platzhalter für «T» oder «U» vorgesehen.

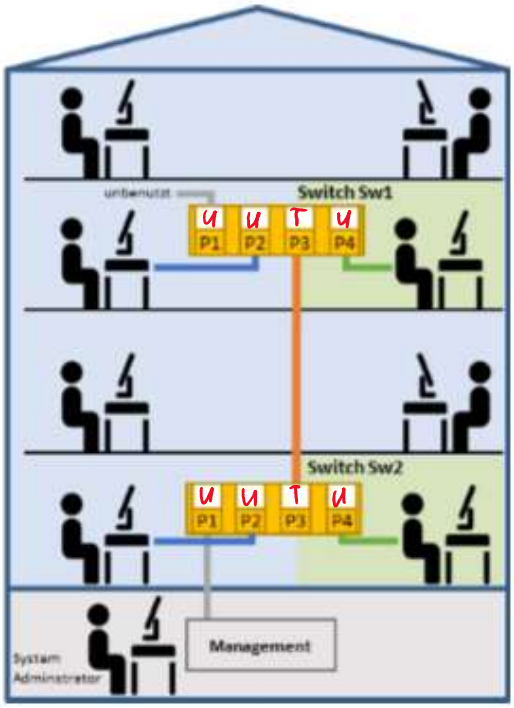


Abbildung 2: Vereinfachtes Netz

2.3 Egress Konfiguration

Q07 *Wozu dient die Egress-Tabelle?*

Die Egress-Tabelle legt fest, an welchen Ports der Switch die Frames aus diesem VLAN senden darf. Mit Ihrem Eintrag definieren Sie zusätzlich, ob der Switch die an diesem Port abgehenden Ethernet-Frames markiert (tagged)

Q08 *Ergänzen Sie Tabelle 1 mit den folgenden Angaben (für Switch Sw1). Sie müssen bei jedem angeschlossenen Port eines der 3 Zeichen(-,U,T) setzen.*

«-» = Momentan kein Mitglied in diesem VLAN

«T» = Mitglied im VLAN, Datenpakete werden mit Tag versendet

«U» = Mitglied im VLAN, Datenpakete werden ohne Tag versendet

Beachten Sie, dass der Management-Client beide Switches konfigurieren können soll.

VLAN ID	Name	Port 1	Port 2	Port 3	Port 4
1	default			U	
10	blue		U	T	
20	green			T	U

Tabelle 1: Egress-Konfiguration von Switch Sw1

Q09 *Ergänzen Sie in Tabelle 2 die Angaben für Switch Sw2.*
Beachten Sie, dass der Management-Client den Switch 2 konfigurieren können soll.

VLAN ID	Name	Port 1	Port 2	Port 3	Port 4
1	default	U		U	
10	blue		U	T	
20	green			T	U

Tabelle 2: Egress-Konfiguration von Switch Sw2

2.4 Ingress Konfiguration

Q10 *Wozu dient die Ingress-Tabelle des Switches?*

Die Ingress-Tabelle legt fest, welche VLAN-ID ein Port den eingehenden Datenpaketen zuweist. Hierbei ordnen Sie das Endgerät über seine Portadresse einem VLAN zu.

Q11 *Ergänzen Sie die fehlenden Angaben in Tabelle 3: Ingress-Konfiguration.*

Switch Sw1	
Port	VLAN ID
1	1
2	10
3	1
4	20

Switch Sw2	
Port	VLAN ID
1	1
2	10
3	1
4	20

Tabelle 3: Ingress-Konfiguration der Switches

Zeigen Sie die Vorbereitungen dem Laborbetreuer!

3 Versuchsdurchführung: Virtual Local Area Network

3.1 Aufbau des Netzes ohne Verwendung von VLANs

Im folgenden Versuch wird ein Netzwerk mit 2 Switches aufgebaut, welches wir bereits aus der Vorbereitung kennen. Wir starten zuerst ohne die Konfiguration von VLANs und prüfen die Sichtbarkeit der Geräte untereinander.

Bauen Sie das Netzwerk gemäss Abbildung 3 auf. Verbinden Sie die seriellen Schnittstellen von ELB A und ELB B mit dem Rechner C und starten Sie die alle Rechner mit Linux. Setzen Sie die Switches mit den USB-Stick zurück (s. Praktikum 04)

- Aktivieren Sie auf ELB A und B den mittleren Ethernet-Port lan2 mit dem Befehl

```
ip link set up lan2
```

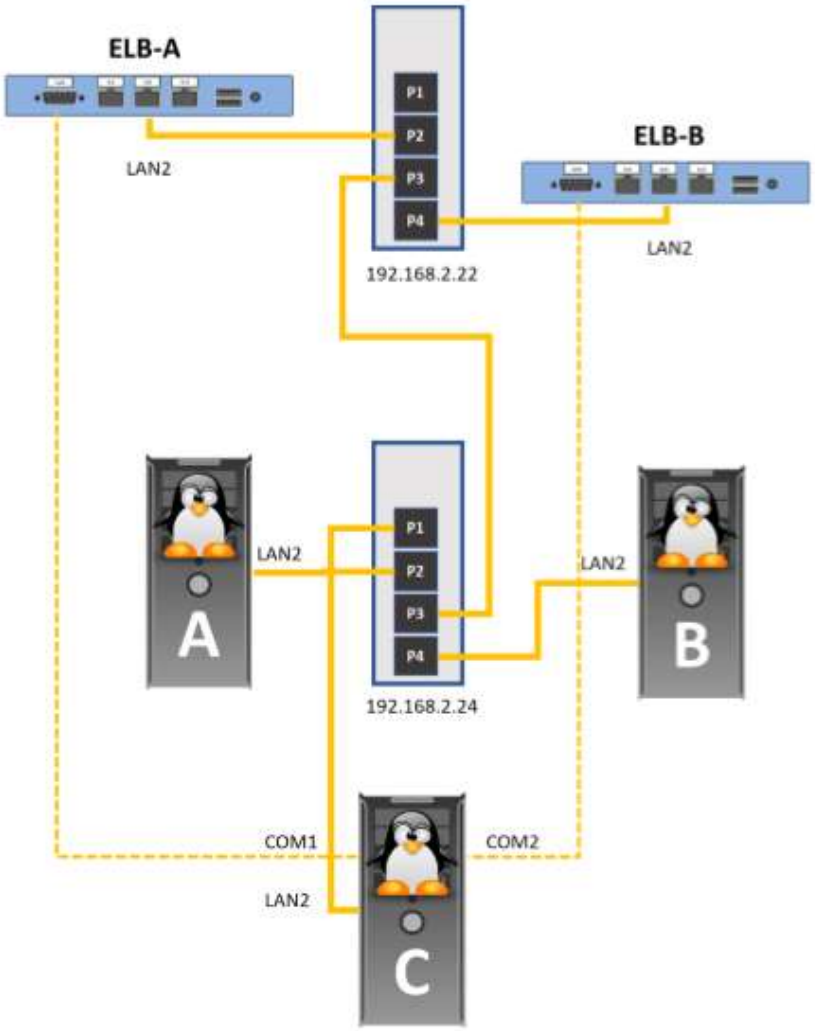


Abbildung 3 Netzwerk ohne VLANs

Erzeugen Sie nacheinander auf ELB A und ELB B Datenverkehr mit Hilfe des **sendframes** Befehls. Der Parameter –t setzt das Type-Feld und vereinfacht die Identifikation des Senders. Der Parameter -i definiert das Sendeintervall in Sekunden. Der Parameter -D setzt die Zieladresse (DA).

- Starten Sie auf allen PCs A, B und C Wireshark und beobachten Sie den Datenverkehr.

ELB A: `sendframes lan2 -D ff:ff:ff:ff:ff:ff -t 0xAAA -i 1`
ELB B: `sendframes lan2 -D ff:ff:ff:ff:ff:ff -t 0xBBB -i 1`

Q12 *Welchen Typ von Datenverkehr können Sie nun beobachten? An welche Adresse sendet `sendframes` die Daten? Können Sie die empfangenen Pakete eindeutig der einen oder der anderen ELB zuordnen?*

Broadcast, aaa bbb

Q13 *Welche PCs sehen die Pakete, welche von ELB A oder ELB B versendet werden?*

alle

Q14 *Wäre das Netzwerk so geeignet für ein Gebäude mit 2 unterschiedlichen Firmen?*

nein

3.2 Einrichten VLAN und Testen der Verbindung

Nun wollen wir das Netzwerk in zwei virutelle Netzwerke trennen, wobei beide Netzwerke eine gemeinsame Trunk-Verbindung nutzen. Das VLAN *blue* mit der ID 10 verbindet die ELB-A mit dem Rechner A. Das VLAN *green* nutzt dabei die VLAN Identifikation 20 und verbindet ELB-B mit dem Rechner B. Der Rechner C wird für die Konfiguration der Switches genutzt.

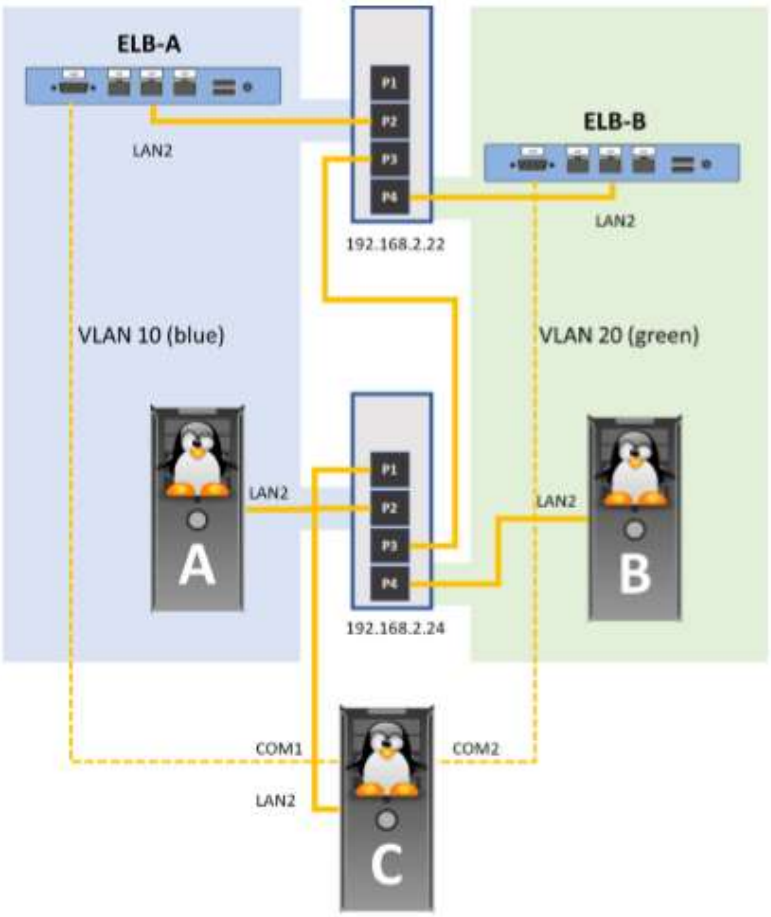


Abbildung 4 Netzwerk mit VLANs

- Starten Sie auf dem Rechner C mit Hilfe des Programms `hiview` das Webinterface des Switches. Hierfür muss im Adressfeld seine IP-Adresse (z.B.: http://192.168.2.22) eingegeben werden.
- Loggen Sie auf dem Switch ein:
  User: `admin`
  Passwort: `private`
- Öffnen Sie im Web-Interface die Seite: *Switching → VLAN → Global*

Q15 *Was ist die grösste VLAN-ID, die der Switch erlaubt? (Vergleichen Sie diese mit der Vorbereitung!)*

4042

Q16 *Wie viele VLANs unterstützt der Switch gleichzeitig?*

255

Q17 *Wenn der Switch nicht die maximale Anzahl VLANs unterstützt, ist er dann Ihrer Meinung nach Standard-Konform?*

ja

- Folgende VLAN-Konfiguration soll auf beiden Switches identisch eingerichtet werden:

Port 1	Management (untagged, VLAN ID = 1)
Port 2	Port im VLAN blue ID=10
Port 3	Trunk Port (VID 10 und 20) sowie Management (untagged)
Port 4	Port im VLAN green ID=20

- Öffnen Sie die Egresss-Tabelle unter: *Switching → VLAN → Static*

Wichtig:
Falls Sie sich vom Switch aussperren, verwenden Sie Port 1, um die Konfiguration zu korrigieren. Verändern Sie daher nichts an der Konfiguration von Port 1.

- Legen Sie die VLAN «blue» und «green» mit `[Create]` an. Beachten Sie die Hilfe im Web Interface.
- Konfigurieren Sie die beiden Switche gemäss den den Tabellen aus Ihrer Vorbereitung. Schliessen Sie die Egress-Konfiguration mit `[Set]` ab. Übertragen Sie die Ingresstabelle unter der Menüposition *Switching → VLAN → Port* auf die beiden Switches. Lassen Sie die restlichen Einstellungen unverändert (insbesondere „Ingress Filtering" deaktiviert).

Q18 *Auf welchem Rechner sehen Sie den Traffic von ELB A und auf welchen Rechnern sehen Sie den Traffic von ELB B*

A A

B B

Zeigen Sie die Ergebnisse dem Laborbetreuer!

3.3 Monitoring

Switches leiten Pakete gezielt weiter. Um Fehler im Netz zu suchen, ist es aber oft nötig, den Verkehr auf dem Backbone (Trunk) zu beobachten. Um das zu ermöglichen, ist in vielen gemanagten Switches die Funktion «Port Mirroring» implementiert.
Rechner C stellt die Management Station dar, daher soll die Beobachtung des Verkehrs auf dem Trunk von diesem Rechner aus erfolgen.

Für den folgenden Versuch soll geprüft werden, ob der Switch die eingehenden Daten der ELBs korrekt behandelt. Die Hirschmann Switches erlauben es, von einem beliebigen Port Daten auf einen ausgewählten Port zu spielgen. Hierbei kann Receive und Transmit getrennt eingestellt werden.
Die Einstellungen finden Sie im Menü *Diagnose → Port Mirroring N:1*.

Q19 *Von welchen Ports an Switch SW2 (dem unteren Switch) müssen Sie die Daten an den Rechner C weiterleiten?*

3

- Starten Sie auf den Rechnern A, B und C Wireshark (Interface lan2).
- Auf Rechner C richten Sie Wireshark so ein, dass die VLAN-IDs angezeigt werden: (*Edit →Preferences →Colums* siehe
- Abbildung 5).

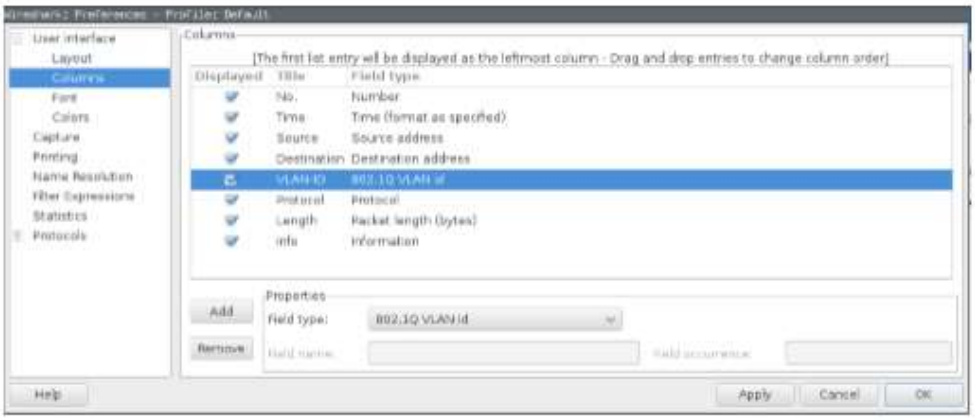


Abbildung 5

- Erzeugen Sie nacheinander auf ELB A und B Datenverkehr mit Hilfe des `sendframes` Befehls.

  ELB A: `sendframes lan2 -D ff:ff:ff:ff:ff:ff -t 0xAAA -i 1`
  ELB B: `sendframes lan2 -D ff:ff:ff:ff:ff:ff -t 0xBBB -i 1`

- Nutzen Sie Wireshark auf Rechner A, Rechner B und Rechner C zur Beobachtung der Frames.

Q20 *Tragen Sie in Tabelle 4 für jedes Ziel ein, welche Frames empfangen werden (0xAAA und/oder 0xBBB).*

Ziel: / Quelle:	Rechner A	Rechner B	Rechner C
ELB A	X		X
ELB B		X	X

Tabelle 4

Q21 *Worin unterscheiden sich die aufgezeichneten Frames auf den unterschiedlichen Rechnen?*

PC A und B: untagged
PC C: tagged

- Starten Sie nun von unserem Management-PC, Rechner C, ebenfalls sendframes.

  Rechner C: `sendframes lan2 -D ff:ff:ff:ff:ff:ff -t 0xCCC -i 1`

- Zur Beobachtung der Frames auf Rechner A, Rechner B sowie auf Rechner C.

Q22 *Auf welchen PCs sehen sie die Pakete vom Management?*

nur C, wegen VLAN 1

- Stoppen sie sendframes auf Rechner C mit «Ctrl+C»

3.4 Überprüfung der Switch-Funktionalität:

Wir wollen vom Management aus die Funktionalität des Switch SW2 überprüfen. Aktivieren Sie daher die Port-Mirroring Funktion von Port 2 (dem Port zu Rechner A).

- Zeigen Sie auf dem Monitoring-PC, dass bei den Paketen zu Rechner A die VLAN Tags korrekt entfernt werden. ✓
- Stoppen sie sendframes auf ELB A und ELB B mit «Ctrl+C»

Zeigen Sie die Resultate dem Laborbetreuer!