06 Virtual LAN

1 Thema des Praktikums

Die Schwerpunkte des Praktikums sind:

- Virtual Local Area Network (VLAN – IEEE 802.1Q)
- Priorisierung von Frames (IEEE 802.1p)

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 werden zwei virtuelle Netzwerke aufgebaut, die eine gemeinsame Backbone-Verbindung nutzen. In einem ersten Teil werden die durch den VLAN-Tag geschaffenen Eigenschaften von Ethernet Switches untersucht. Im zweiten Teil werden Frames auf verschiedene Arten priorisiert, deren Abbildung auf Verkehrsklassen und die Auswirkung auf den Durchsatz untersucht. Dazu werden manuelle Port-Konfiguration und Port Mirror für das Monitoring verwendet.

2 Vorbereitung

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

Vorbereitung zu Virtual Local Area Network

Welche Vorteile von VLAN werden im Anwenderhandbuch von Hirschmann genannt?

Netzlastbelastung: Broadcastnachrichten nur innerhalb VLAN

Flexibilität: Arbeitsgruppen erstellen

Übersichtlichkeit: Einfache Wartung

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

zwischen Source Adresse und length

Wie viele VLANs wären theoretisch möglich?

4'094 da VLAN-ID 12Bit sind

Wozu dient beim Switch RS20 das VLAN mit der ID 1? Warum darf es nicht entfernt werden?

Uplink (VLANS kommunizieren darüber)

- Geben Sie Abbildung 1 mit «U» oder «T» an, welche Switch-Ports tagged Frames (T) verschicken müssen und an welchen untaged Frames (U) genügen.
- Wozu dient die Egress-Tabelle? Egress = Ausgang

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):

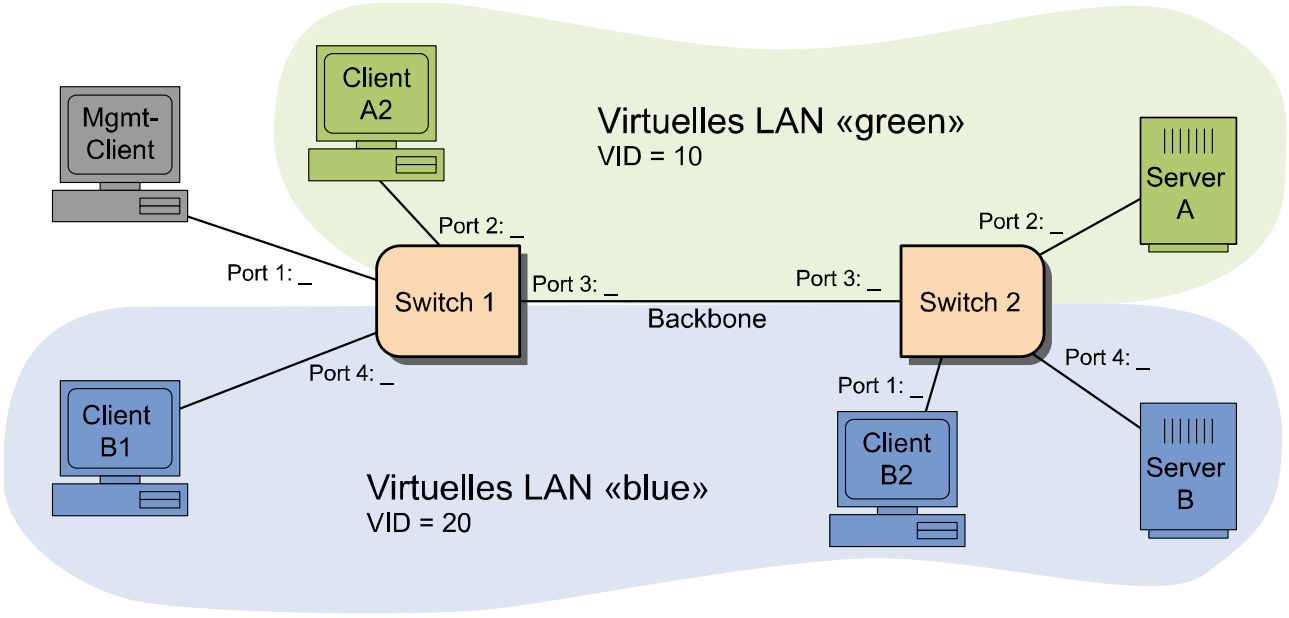

Abbildung 1

- Ergänzen Sie in Tabelle 1: Egress-Konfiguration von Switch 1 mit den folgenden Angaben:

  «-» = Momentan kein Mitglied in diesem VLAN

  «T» = Mitglied im VLAN, Datenpakete mit Tag versenden

  «U» = Mitglied im VLAN, Datenpakete ohne Tag versenden

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

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

Tabelle 1: Egress-Konfiguration von Switch 1

- Ergänzen Sie in Tabelle 2: Egress-Konfiguration von Switch 2 die Angaben «-», «U» oder «T». 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	T	T	T	T
10	green	-	U	T	-
20	blue	U	-	T	U

Tabelle 2: Egress-Konfiguration von Switch 2

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.

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

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

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

Tabelle 3: Ingress-Konfiguration

Vorbereitung zur Priorisierung von Frames

Der VLAN-Tag erweitert das Ethernet Frame nicht nur durch einen VLAN-Identifier sondern auch durch ein Prioritätsfeld.

Wie viele Bits umfasst das Prioritätsfeld im VLAN-Tag und viele Prioritäten sind möglich?

3 Bit, Priorität 0-7 ist möglich

Mit der Priorität kann man die Frame-Weiterleitung im Switch beeinflussen. Ein Switch stellt dazu an jedem Ausgang n Warteschlangen für die verschiedenen Verkehrsklassen bereit.

Wie viele Verkehrsklassen / Priority Queues unterstützt der RS20 Switch?

Das Gerät unterstützt 4 Priority Queues (Traffic Classes nach IEEE 802.1D)

Die VLAN-Prioritäten werden durch den Switch den Verkehrsklassen zugeordnet.

Welche Prioritäten sollten für zeitkritische Anwendungen verwendet werden (hohe oder tiefe)?

hohe

Welche Verkehrsklasse wird für Frames verwendet, die keine Priorität haben (Default)?

traffic class 1 = best effort

Was bedeutet die Betriebsart „Strict Priority“?

Bei Strict-Priority vermittelt das Gerät zuerst alle Datenpakete mit höherer Verkehrsklasse (höherer Priorität), bevor es ein Datenpaket mit der nächst niedrigeren Verkehrsklasse vermittelt.

Zeigen Sie die Vorbereitungen dem Laborbetreuer!

3 Versuchsdurchführung: Virtual Local Area Network

Im folgenden Versuch werden zwei virtuelle Netzwerke aufgebaut, die eine gemeinsame Trunk-Verbindung benutzen (Abbildung 2). Das VLAN *blue* nutzt dabei die VLAN Identifikation 10 und verbindet die „Embedded Linux Box“ (ELB A) mit dem Rechner A. Das VLAN *green* mit der ID 20 verbindet ELB B mit dem Rechner B. Der Rechner C wird für die Konfiguration der Switches und zum Aufzeichnen des Verkehrs auf dem Trunk verwendet.

Bauen Sie das Netzwerk gemäss Abbildung 2 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 und starten Sie das Web-Interface (HiView).
- Öffnen Sie im Web-Interface die Seite: *Switching → VLAN → Global*

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

Wie viele VLAN unterstützt der Switch gleichzeitig?

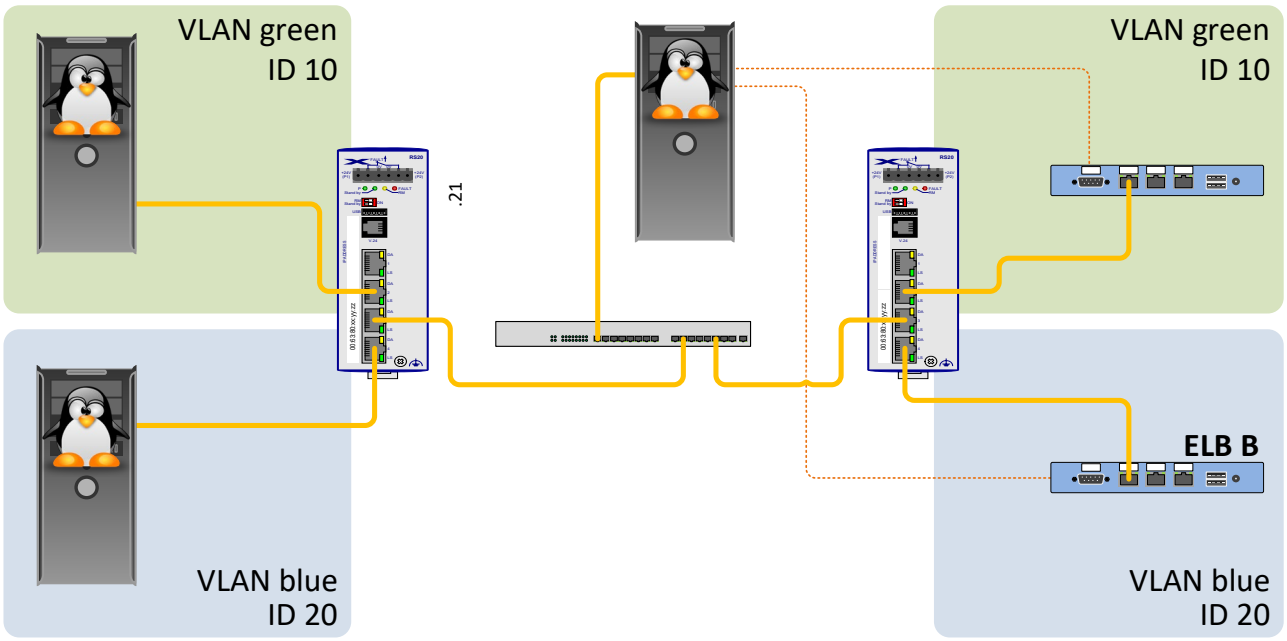

Abbildung 2

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

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

- Öffnen Sie die Egresss-Tabelle unter: *Switching → VLAN → Static*
- Legen Sie die VLAN «green» und «blue» mit **`[Create]`** an. Beachten Sie die Hilfe im Web Interface.
- Tragen Sie in Tabelle 4: Egress-Konfiguration von Switch 1 und Switch 2 pro Switch-Port ein, von welchen VLAN die Frames über dieses Port gesendet werden dürfen und ob die an diesem Port abgehenden Frames ein Tag bekommen.

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

Tabelle 4: Egress-Konfiguration von Switch 1 und Switch 2

- Übertragen Sie die Tabelle 4 auf die Switch und schliessen Sie die Konfiguration mit **`[Set]`** ab.
- Geben Sie in Tabelle 5 an, welchem VLAN die an den Ports eingehenden Frames zugewiesen werden sollen:

Port	VLAN ID
2	
3	
4	

Tabelle 5: Ingress-Konfiguration von Switch 1 und Switch 2

Übertragen Sie Tabelle 5 unter der Menüposition *Switching → VLAN → Port* auf die beiden Switches. Lassen Sie die restlichen Einstellungen unverändert (insbesondere „Ingress Filtering“ deaktiviert).

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.

- Im Anhang A auf Seite 162 steht für eine der unseren vergleichbare Netz-Topologie:

  Konfigurieren Sie den Uplink-Port [hier Port 3] mit ***admit only VLAN tags****. Um die VLAN-Markierung an diesem Port auszuwerten, aktivieren die „Ingress-Filtering" am Uplink-Port.*

Warum ist dies keine gute Idee?

- Zur Beobachtung der Frames aktivieren Sie auf den ELBs den Ethernet-Port eth0 mit dem Befehl

  `ip link set up eth0`

  und zeigen Sie die ankommenden Frames an mit

  `tcpdump -e`

  Auf den Rechnern A, B und C starten Sie Wireshark (Interface eth1).

- Auf Rechner C richten Sie Wireshark so ein, dass die VLAN-IDs angezeigt werden:
  (*Edit →Preferences →Colums* siehe Abbildung 3).
  Achtung: Unter Windows wird im Wireshark die VLAN-ID nicht angezeigt.

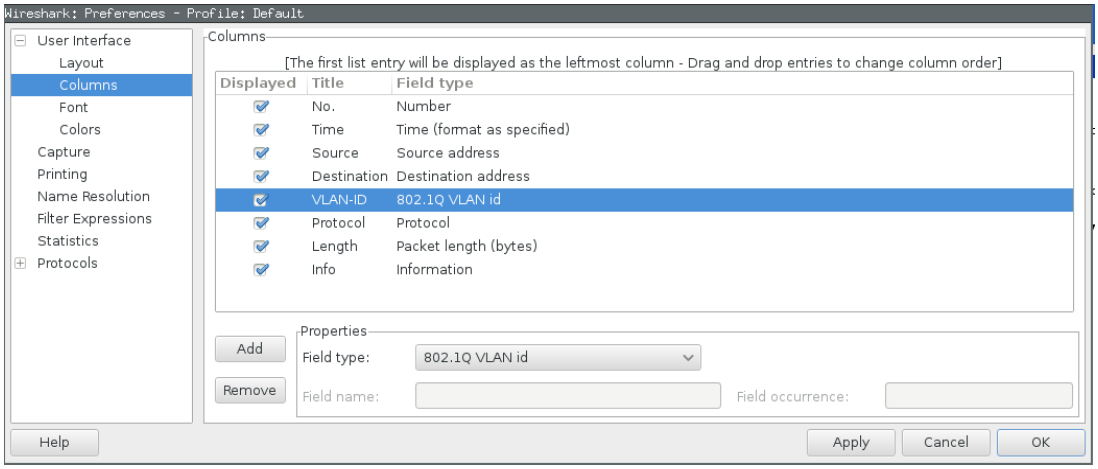

Abbildung 3

- Erzeugen Sie auf den Rechnern Datenverkehr mit Hilfe des `sendframes` Befehls. Der Parameter –t setzt das Type-Feld und vereinfacht die Identifikation des Senders.

  ELB A: **`sendframes eth1 -t 0xAAA -i 1`**
  ELB B: **`sendframes eth1 -t 0xBBB -i 1`**
  Rechner C: **`sendframes eth1 -t 0xCCC -i 1`**

- Tragen Sie in Tabelle 6 für jedes Ziel ein, welche Frames es empfängt (0xAAA, 0xBBB oder 0xCCC).

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

Tabelle 6

Warum stimmt die folgende Aussage nicht: «Die Knoten erhalten nur Frames von ihrem eigenen VLAN?»

- Beobachten Sie den Verkehr auf dem Trunk (Wireshark auf Rechner C).

Worin unterscheidet sich ein bestimmtes Frame am Eingangsport (z.B. Port 1 bzw. auf dem Rechner A) und auf den Trunk (Rechner C)?

- Rechner A soll Frames von beiden VLANs («green» und «blue») empfangen.

Was müssen Sie an der Konfiguration ändern?

Zeigen Sie die Resultate dem Laborbetreuer!

4 Versuchsdurchführung: Prioritäten / Durchsatz

Um den Effekt der Priorisierung auf den Durchsatz zu zeigen, wird auf ELB A eine hohe Last mit grossen Frames normaler Priorität erzeugt. ELB B sendet hoch resp. tiefer priorisierte Frames. Eine Durchsatzmessung soll aufzeigen, dass die Priorisierung wirkt. Weil Kollisionen zusätzliche Delays verursachen, wird die unter Aufgabe 3 verwendete Grundkonfiguration leicht modifiziert: der Halb-Duplex-Trunk (Hub) wird durch einen 10 Mbit/s-Full-Duplex-Link ersetzt.

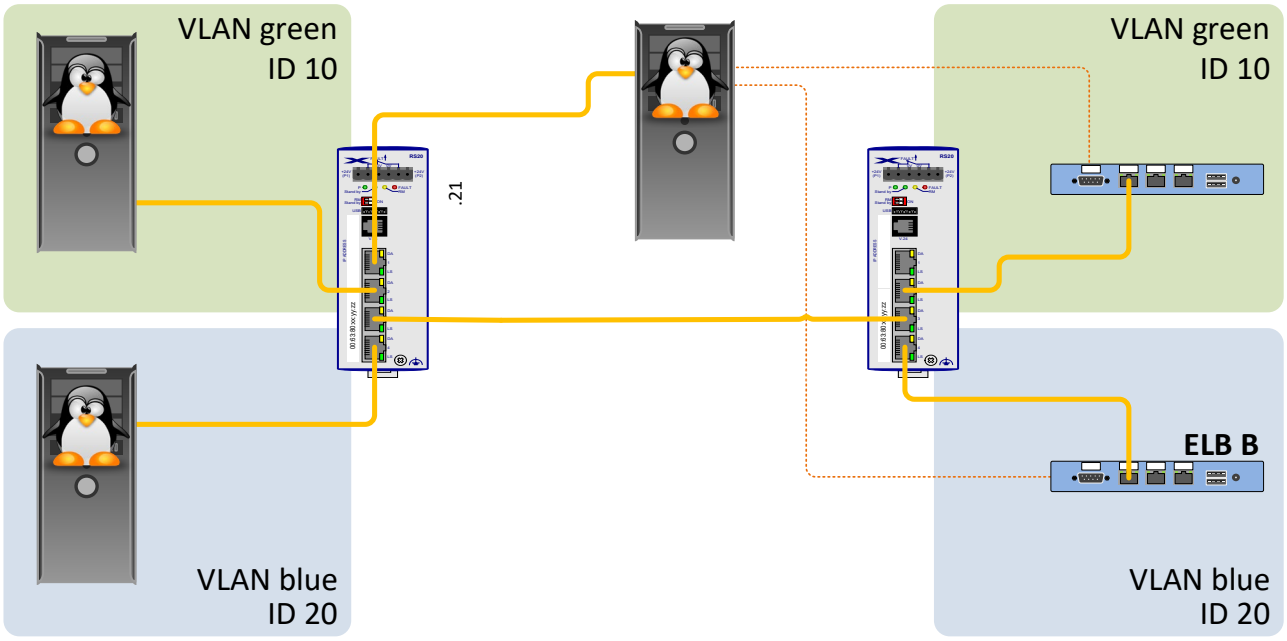

Abbildung 4

- Stellen Sie auf den beiden Switches die Ports 3 manuell auf 10 Mbit/s Full-Duplex ein:
  Basic Settings → Port Configuration
- Ersetzen Sie den Hub zwischen den beiden Switches durch ein Kabel.

Warum würde ein Cross-Over-Kabel benötigt und wie kann das umgangen werden?

- Kontrollieren Sie mit Hilfe der LED-Anzeige, dass die Ports wirklich mit 10 Mbit/s arbeiten.

Um den Verkehr weiterhin beobachten zu können, stellen Sie am linken Switch das Port-Mirroring ein. Damit spiegeln Sie den Verkehr vom einem oder mehreren Ports auf das Port 1 (Rechner C).

- Spiegeln Sie das Port 2 / TX auf Port 1. Die Einstellung erfolgt im Menü *Diagnose → Port Mirroring*.

Gibt es Unterschiede in den Anzeigen von Rechner A und Rechner C?

- Spiegeln Sie zusätzlich Port 2 / TX und Port 3 / RX.

Was, bezogen auf ein bestimmtes Frame, zeigt Wireshark auf Rechner C nun an?

- Spiegeln Sie nur noch Port 3 / RX (Port 2 und Port 3 entfernen).
- In Folgenden generieren wir eine hohe Last. Damit die Managent Frames immer noch durchkommen, erhöhnen Sie deren Priorität auf das Maximum (7). Das machen wir zur Sicherheit an zwei Stellen:

  QoS/Priority → Global → VLAN priority for management packets
  QoS/Priority → Port Configuration → Port priority
- Generieren Sie mit ELB A eine hohe Last mit langen Frames (ohne Tag und Prioritätsangabe):

  ```
  sendframes eth1 –t 0xAAA –i 0 –s 1500
  ```
- Generieren Sie nun mit ELB B eine hohe Last mit kürzeren Frames:

  ```
  sendframes eth1 –t 0xBBB –i 0 –s 500
  ```

Wie verteilt sich der Trunk-Verkehr auf die beiden Quellen? (Wireshark → Statistics → Packet Length)

- Öffnen Sie das Menü: *QoS/Priority → 802.1D/p-Mapping*

Welcher Priorität / Traffic Class wird per Default verwendet?

Nun soll der Effekt der Priorisierung sichtbar gemacht werden, indem durch die Applikation ein VLAN-Tag mit einer Priorität eingefügt wird. Mit dem Parameter –p kann die gewünschte Priorität eingestellt werden.

- Ändern Sie auf dem ELB B die Priorität, so dass Sie gegenüber dem Default die gleiche, eine höhere oder eine tiefere Traffic Class bekommen. und beobachten Sie mit Wireshark die Verkehrsverteilung auf dem Trunk sowie die auf den Rechnern ankommenden Pakete. Starten Sie für jede Messung im Wireshark eine neue Capture-Session, damit die Resultate nicht verfälscht werden.

  Beispiel: **`sendframes eth1 –t 0xBBB –i 0 –s 500 -p 4`**

Bei welchen Prioritäten können Sie Veränderungen feststellen und wie äussern sich diese?

Wie wirkt sich verendete die Betriebsart „Strict Priority“ aus?

- Senden Sie von ELB A mit Priorität 4 und mit ELB B mit Priorität 5 und erklären Sie den Effekt.

Wie kann verhindert werden, dass ein User/eine Applikation die Priorität auf diesem Weg erhöht (2 Wege)?

- Testen Sie die Verfahren.
- Im Menü *QoS/Priorität → Portkonfiguration* lässt sich die Priorität ebenfalls festlegen. Vergleichen Sie den Effekt der port-basierten Prioritätsvergabe mit der applikationsgesteuerten.

Gibt es Unterschiede zwischen port- und applikations-gesteuerter Priorität?

Was sind die Vor-/Nachteile der Verfahren?

Zeigen Sie die Resultate dem Laborbetreuer!

5 Zusatzaufgaben

Um den Effekt der Priorisierung auf den Delay und die Delay-Schwankungen (Jitter) zu zeigen, gehen wir von einer Situation aus, bei welcher der Trunk nicht immer voll ausgelastet ist. Auf Rechner A wird eine hohe Last mit grossen Paketen bei normaler Priorität erzeugt (typische Anwendung z.B. Backup). Rechner B produziert eine relativ kleine Last mit kurzen aber zeitkritischen Frames (typische Anwendung Multimedia-Stream). Eine Delay-Messung soll aufzeigen, wie die Priorisierung wirkt und wo ihre Grenzen liegen.

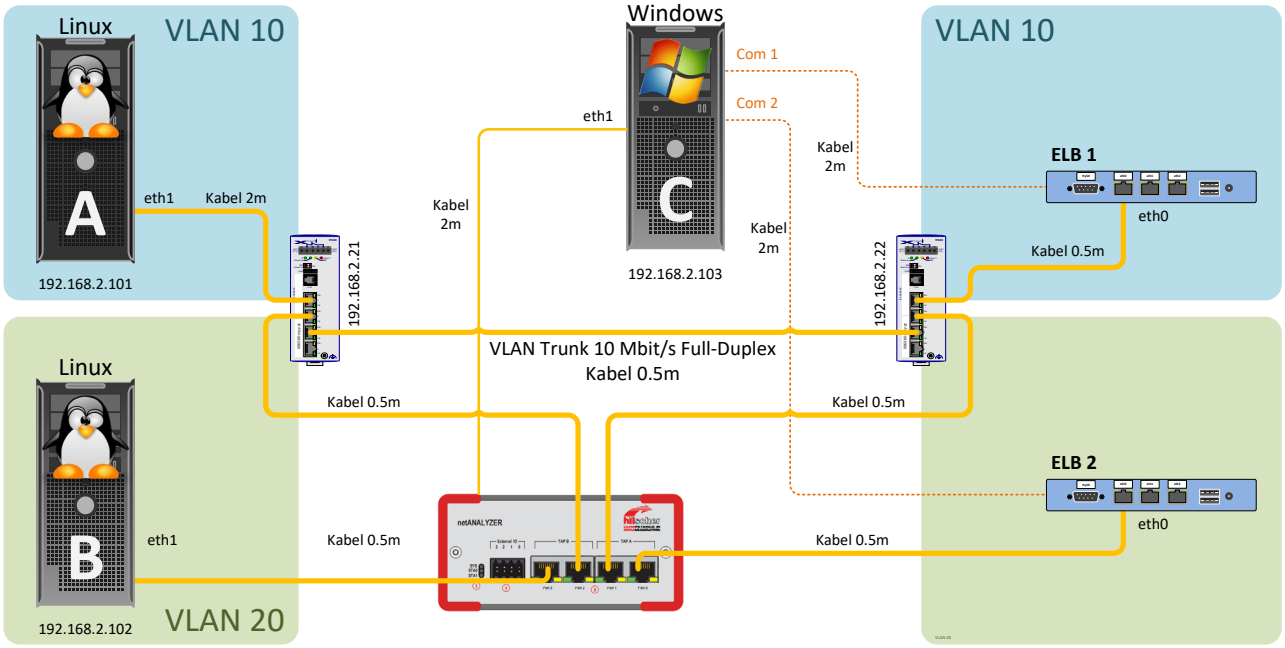

Abbildung 5

- Bauen Sie anschliessend den netANALYZER gemäss Abbildung 5 in die Konfiguration ein.

Sie messen nun 3 Situationen mit und ohne Verwendung von Prioritäten:

- **Messung 1: Leerlauf-Situation**
  Erzeugen Sie auf Rechner B zeitkritischen Verkehr mit 2000 Frames/s (mit je 20 Samples à 16 Bit = 40 Byte).

  ```
  sendframes eth1 -t 0xBBB -s 40 -i 0.0005 -p 0
  ```

  Messen Sie mit dem netANALYZER den Delay von Rechner B zum ELB B für mindestens 1000 Frames und speichern Sie das Histogramm der Verteilung für einen späteren Vergleich als Screenshot ab.

- **Messung 2: Normallast-Situation**
  Erzeugen Sie zusätzlich auf Rechner A breitbandigen Verkehr mit 500 Frames/s.

  ```
  sendframes eth1 -t 0xAAA -s 1500 -i 0.003 -p 0
  ```

  Messen Sie mit dem netANALYZER den Delay von Rechner B zum ELB B für mindestens 1000 Frames und speichern Sie das Histogramm der Verteilung für einen späteren Vergleich als Screenshot ab.

- **Messung 3: Überlast-Situation**
  Erzeugen Sie auf Rechner A breitbandigen Verkehr mit 1000 Frames/s (statt mit 500 Frames/s).

  ```
  sendframes eth1 -t 0xAAA -s 1500 -i 0.001 -p 0
  ```

  Messen Sie mit dem netANALYZER den Delay von Rechner B zum ELB B für mindestens 1000 Frames und speichern Sie das Histogramm der Verteilung für einen späteren Vergleich als Screenshot ab.

ANHANG A

HIRSCHMANN
A BELDEN BRAND

Anwender-Handbuch

Grundkonfiguration
Industrial ETHERNET (Gigabit-)Switch
RS20/RS30/RS40, MS20/MS30

8.6 VLANs

8.6.1 Beschreibung VLAN

Ein virtuelles LAN (VLAN) besteht im einfachsten Fall aus einer Gruppe von Netzteilnehmern in einem Netzsegment, die so miteinander kommunizieren, als bildeten sie ein eigenständiges LAN.

Komplexere VLANs erstrecken sich über mehrere Netzsegmente und basieren zusätzlich auf logischen (statt ausschließlich physikalischen) Verbindungen zwischen Netzteilnehmern. VLANs werden so zu einem Element der flexiblen Netzgestaltung, da Sie logische Verbindungen einfacher zentral umkonfigurieren können als Kabelverbindungen.

Der Standard IEEE 802.1Q definiert die VLAN-Funktion.

Die wichtigsten Vorteile der VLANs sind:

- Netzlastbegrenzung
  VLANs reduzieren die Netzlast erheblich, da die Geräte Broadcast-, Multicast- und Unicast-Pakete mit unbekannten (nicht gelernten) Zieladressen ausschließlich innerhalb des virtuellen LANs vermitteln. Der Rest des Datennetzes übermittelt den Verkehr wie üblich.

- Flexibilität
  Sie haben die Möglichkeit, flexibel Anwender-Arbeitsgruppen zu bilden, die auf der Funktion der Teilnehmer basieren und nicht auf ihrem physikalischen Standort oder Medium.

- Übersichtlichkeit
  VLANs strukturieren Netze überschaubarer und vereinfachen die Wartung.

8.6.2 Beispiele für ein VLAN

Die folgenden Beispiele aus der Praxis vermitteln einen schnellen Einstieg in den Aufbau eines VLANs.

Beispiel 1

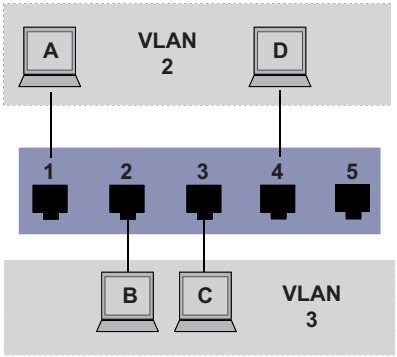

Abb. 32: Beispiel für ein einfaches portbasiertes VLAN

Das Beispiel zeigt eine minimale VLAN-Konfiguration (portbasiertes VLAN). Ein Administrator hat an einem Vermittlungsgerät mehrere Endgeräte angeschlossen und diese 2 VLANs zugeordnet. Dies unterbindet wirksam jeglichen Datenverkehr zwischen verschiedenen VLANs; deren Mitglieder kommunizieren ausschließlich innerhalb ihres eigenen VLANs.
Während der Einrichtung der VLANs erstellen Sie für jeden Port Kommunikationsregeln, die Sie in einer Eingangs- (Ingress-) und einer Ausgangs- (Egress-) Tabelle erfassen.
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.
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):

- `T` = mit Tag-Feld (T = Tagged, markiert)
- `U` = ohne Tag-Feld (U = Untagged, nicht markiert)

Für obiges Beispiel hat der Status des TAG-Feldes der Datenpakete keine Relevanz, setzen Sie es generell auf „U“.

Endgerät	Port	Port VLAN Identifer (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Tab. 12: Eingangstabelle

VLANID	Port				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

Tab. 13: Ausgangstabelle

Verfahren Sie wie folgt, um die Beispielkonfiguration durchzuführen:

☐ VLAN konfigurieren

☐ Öffnen Sie den Dialog `Switching:VLAN:Statisch`.

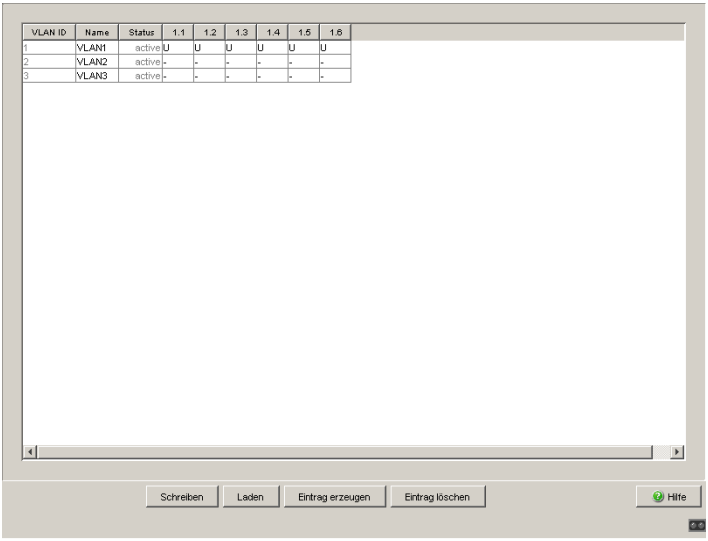

Abb. 33: Neue VLANs erzeugen und benennen

- ☐ Klicken Sie auf „Erzeugen“, um das Eingabefenster für die VLAN-ID zu öffnen.
- ☐ Weisen Sie dem VLAN die VLAN-ID `2` zu.
- ☐ Klicken Sie „OK“.
- ☐ Benennen Sie dieses VLAN mit VLAN2, indem Sie in das Feld klicken und den Namen eintragen. Ändern Sie außerdem die Bezeichnung für VLAN 1 von `Default` in `VLAN1`.
- ☐ Wiederholen Sie die vorherigen Schritte und legen Sie ein weiteres VLAN mit der VLAN-ID `3` und dem Namen `VLAN3` an.

☐ Ports konfigurieren

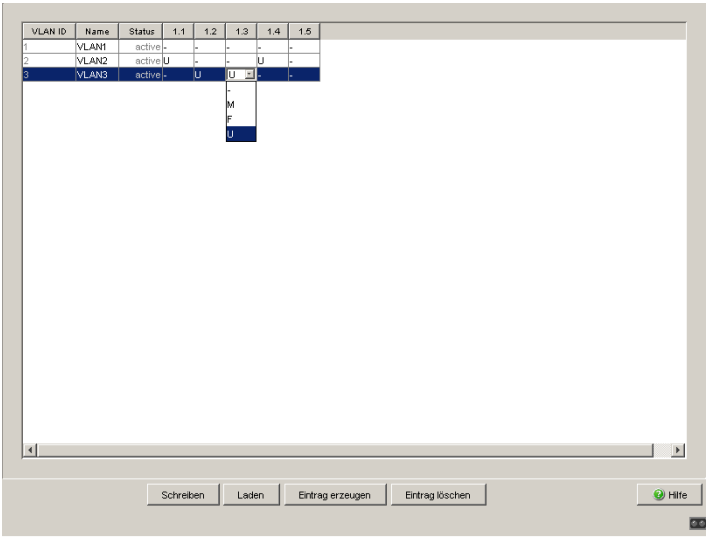

Abb. 34: VLAN-Zugehörigkeit der Ports definieren.

☐ Weisen Sie die Ports des Gerätes den entsprechenden VLANs zu, indem Sie durch einen Klick in die zugehörigen Tabellenzellen das Auswahlmenü öffnen und den Status bestimmen. Entsprechende Wahlmöglichkeiten sind:

- `-` = Momentan kein Mitglied in diesem VLAN (GVRP erlaubt)
- `T` = Mitglied im VLAN, Datenpakete mit Tag versenden
- `U` = Mitglied im VLAN, Datenpakete ohne Tag versenden
- `F` = Kein Mitglied im VLAN (auch für GVRP gesperrt)

Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, wählen Sie hier die Einstellung `U`.

☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
☐ Öffnen Sie den Dialog `Switching:VLAN:Port`.

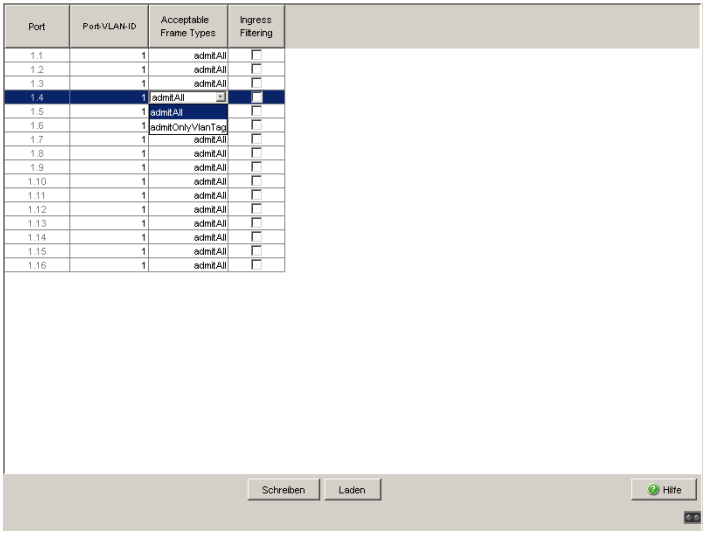

Abb. 35: „Port-VLAN ID“, „Akzeptierte Datenpakete“ und „Ingress-Filtering“ zuweisen und speichern

☐ Weisen Sie den einzelnen Ports die Port-VLAN-ID des zugehörigen VLANs (2 oder 3) zu, siehe Tabelle.
☐ Da Endgeräte Datenpakete in der Regel unmarkiert senden, wählen Sie bei „Akzeptierte Datenpakete“ die Einstellung `admitAll`.
☐ Die Einstellungen von `Ingress-Filtering` hat keinen Einfluss auf die Funktion dieses Beispiels.
☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
☐ Wählen Sie im Rahmen „Speichern“ den Speicherort „auf dem Gerät“ und klicken Sie auf „Sichern“, um die Konfiguration nicht-flüchtig in der aktiven Konfiguration zu speichern.

Beispiel 2

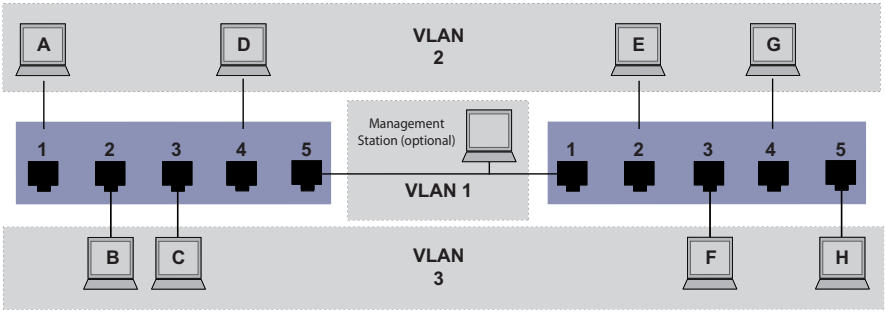

Abb. 36: Beispiel für eine komplexere VLAN-Konfiguration

Das zweite Beispiel zeigt eine komplexere Konfiguration mit 3 VLANs (1 bis 3). Zusätzlich zu dem schon bekannten Switch aus Beispiel 1 setzen Sie einen 2. Switch (im Beispiel rechts gezeichnet) ein.

Die Endgeräte der einzelnen VLANs (A bis H) erstrecken sich über 2 Vermittlungsgeräte (Switch). Derartige VLANs heißen deshalb verteilte VLANs. Zusätzlich ist eine optionale Management Station gezeigt, die bei richtiger VLAN-Konfiguration Zugriff auf alle Netzkomponenten hat.

Anmerkung: Das VLAN 1 hat in diesem Fall keine Bedeutung für die Endgerätekommunikation, ist aber notwendig für die Administration der Vermittlungsgeräte über das sogenannte Management-VLAN.

Ordnen Sie die Ports mit ihren angeschlossenen Endgeräten eindeutig einem VLAN zu (wie im vorherigen Beispiel gezeigt). Bei der direkten Verbindung zwischen den beiden Übertragungsgeräten (Uplink) transportieren die Ports Pakete für beide VLANs. Um diese Uplinks zu unterscheiden, setzen Sie die „VLAN-Markierung" ein, welche für die entsprechende Abwicklung der Frames sorgt. So bleibt die Zuordnung zu den jeweiligen VLANs erhalten.

Verfahren Sie wie folgt, um die Beispielkonfiguration durchzuführen:

Ergänzen Sie die Ingress- und Egress-Tabelle aus Beispiel 1 um den Uplink Port 5. Erfassen Sie für den rechten Switch je eine neue Ingress- und Egress-Tabelle wie im 1. Beispiel beschrieben.

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):

- `T` = mit Tag-Feld (T = Tagged, markiert)
- `U` = ohne Tag-Feld (U = Untagged, nicht markiert)

Markierte (Tagged) Frames kommen in diesem Beispiel in der Kommunikation zwischen den Vermittlungsgeräten (Uplink) zum Einsatz, da an diesen Ports Frames für unterschiedliche VLANs unterschieden werden.

Endgerät	Port	Port VLAN Identifer (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Tab. 14: Ingress-Tabelle Gerät links

Endgerät	Port	Port VLAN Identifer (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

Tab. 15: Ingress-Tabelle Gerät rechts

VLAN-ID	Port				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Tab. 16: Egress Tabelle Gerät links

VLAN-ID	Port				
	1	2	3	4	5
1	U				

Tab. 17: Egress Tabelle Gerät rechts

VLAN-ID	Port					
2	T	U		U		
3	T		U		U	

Tab. 17: Egress Tabelle Gerät rechts

Die Kommunikationsbeziehungen sind hierbei wie folgt:Endgeräte an Port 1 und 4 des linken Gerätes sowie Endgeräte an Port 2 und 4 des rechten Geräts sind Mitglied im VLAN 2 und können somit untereinander kommunizieren. Ebenso verhält es sich mit den Endgeräten an Port 2 und 3 des linken Gerätes sowie Endgeräten an Port 3 und 5 des rechten Gerätes. Diese gehören zu VLAN 3.

Die Endgeräte „sehen“ jeweils ihren Teil des Netzes. Teilnehmer außerhalb dieses VLANs sind unerreichbar. Das Gerät vermittelt auch Broadcast-, Multicast- und Unicast-Pakete mit unbekannter (nicht gelernter) Zieladresse ausschließlich innerhalb der Grenzen eines VLANs.

Dabei kommt innerhalb des VLANs mit der ID 1 (Uplink) das VLAN-Tagging (IEEE 801.1Q) zum Einsatz. Dies erkennen Sie am Buchstaben `T` in der Egress-Tabelle der Ports.

Die Konfiguration des Beispiels erfolgt exemplarisch für das rechte Gerät. Verfahren Sie analog, um das zuvor bereits konfigurierte linke Gerät unter Anwendung der oben erstellten Ingress- und Egress-Tabellen an die neue Umgebung anzupassen.

Verfahren Sie wie folgt, um die Beispielkonfiguration durchzuführen:

☐ VLAN konfigurieren

☐ Öffnen Sie den Dialog `Switching:VLAN:Statisch`.

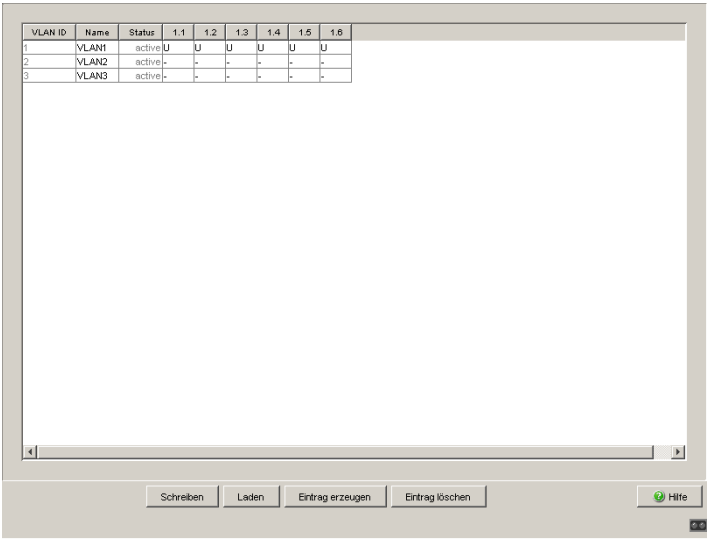

Abb. 37: Neue VLANs erzeugen und benennen

- ☐ Klicken Sie auf „Erzeugen“, um das Eingabefenster für die VLAN-ID zu öffnen.
- ☐ Weisen Sie dem VLAN die VLAN-ID `2` zu.
- ☐ Benennen Sie dieses VLAN mit VLAN2, indem Sie in das Feld klicken und den Namen eintragen. Ändern Sie außerdem die Bezeichnung für VLAN 1 von `Default` in `VLAN1`.
- ☐ Wiederholen Sie die vorherigen Schritte und legen Sie ein weiteres VLAN mit der VLAN-ID 3 und dem Namen `VLAN3` an.

☐ Ports konfigurieren

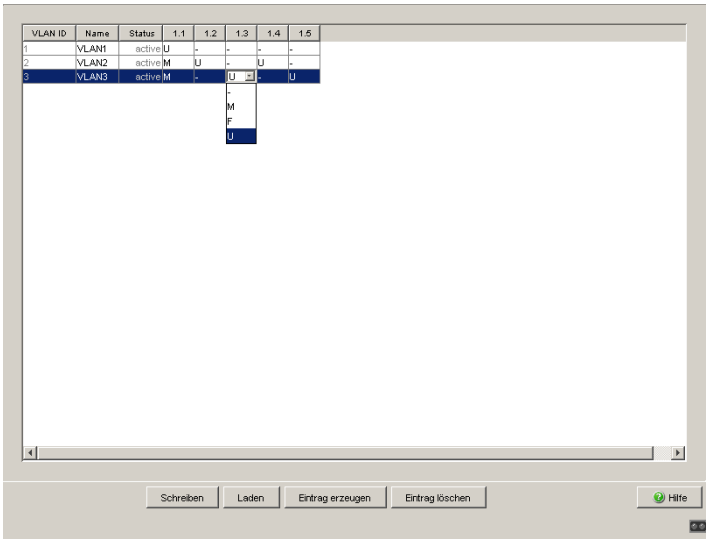

Abb. 38: VLAN-Zugehörigkeit der Ports definieren.

☐ Weisen Sie die Ports des Gerätes den entsprechenden VLANs zu, indem Sie durch einen Klick in die zugehörigen Tabellenzellen das Auswahlmenü öffnen und den Status bestimmen. Entsprechende Wahlmöglichkeiten sind:

- `-` = Momentan kein Mitglied in diesem VLAN (GVRP erlaubt)
- `T` = Mitglied im VLAN, Datenpakete mit Tag versenden
- `U` = Mitglied im VLAN, Datenpakete ohne Tag versenden
- `F` = Kein Mitglied im VLAN (auch für GVRP gesperrt)

Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, wählen Sie die Einstellung `U`. Lediglich am Uplink-Port, an dem die VLANs miteinander kommunizieren, wählen Sie die Einstellung `T`.

☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

☐ Öffnen Sie den Dialog `Switching:VLAN:Port`.

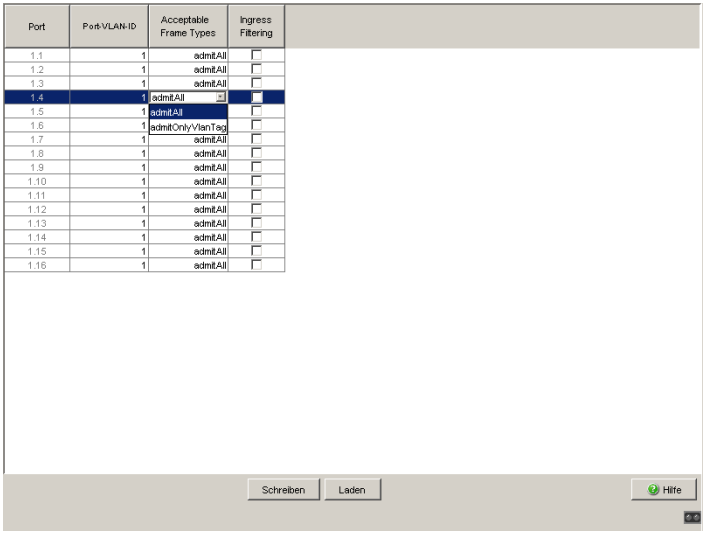

Abb. 39: „Port-VLAN ID“, „Akzeptierte Datenpakete“ und „Ingress-Filtering“ zuweisen und speichern

☐ Weisen Sie den einzelnen Ports die ID des zugehörigen VLANs (1 bis 3) zu.

☐ Da Endgeräte in der Regel keine Datenpakete mit Tag senden, wählen Sie an den Endgeräte-Ports die Einstellung `admitAll`. Konfigurieren Sie den Uplink-Port mit `admit only VLAN tags`.

☐ Um die VLAN-Markierung an diesem Port auszuwerten, aktivieren Sie „Ingress-Filtering“ am Uplink-Port.

- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
- ☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Wählen Sie im Rahmen „Speichern“ den Speicherort „auf dem Gerät“ und klicken Sie auf „Sichern“, um die Konfiguration nicht-flüchtig in der aktiven Konfiguration zu speichern.

8.4 QoS/Priorität

8.4.1 Beschreibung Priorisierung

Diese Funktion hilft zu verhindern, dass zeitkritischer Datenverkehr wie Sprach-/Video- oder Echtzeitdaten in Zeiten starker Verkehrslast durch weniger zeitkritischen Datenverkehr gestört wird. Die Zuweisung von hohen Verkehrsklassen (Traffic Class) für zeitkritische Daten und niedrigen Verkehrsklassen für weniger zeitkritische Daten bietet einen optimierten Datenfluss für zeitkritische Datenverkehr.

Das Gerät unterstützt 4 Priority Queues (Traffic Classes nach IEEE 802.1D). Die Zuordnung von empfangenen Datenpaketen zu diesen Klassen erfolgt durch

- die im VLAN-Tag enthaltene Priorität des Datenpaketes, wenn der Empfangsport auf „trust dot1p“ konfiguriert wurde.
- die Port-Priorität, wenn der Port auf „untrusted" konfiguriert wurde.
- die Port-Priorität beim Empfang von Datenpaketen, die kein VLAN-Tag enthalten und wenn der Port auf „trust dot1p" konfiguriert wurde.

  Voreinstellung: „trust dot1p“.

Das Gerät berücksichtigt die Klassifizierungsmechanismen in der oben dargestellten Reihenfolge.

Datenpakete können Priorisierungs/QoS-Informationen enthalten:

- VLAN-Priorität nach IEEE 802.1Q/ 802.1D (Layer 2)

8.4.2 VLAN-Tagging

Für die Funktionen VLAN und Priorisierung sieht der Standard IEEE 802.1Q vor, dass in einen MAC-Datenrahmen das VLAN-Tag eingebunden wird. Das VLAN-Tag besteht aus 4 Bytes. Es steht zwischen dem Quelladressfeld und dem Typfeld.

Das Gerät wertet bei Datenpaketen mit VLAN-Tag aus:
- die Prioritäts-Information und
- die VLAN-Information, wenn VLANs eingerichtet sind.

Datenpakete, deren VLAN-Tags eine Prioritäts-Information, aber keine VLAN-Information (VLAN-ID = 0) enthält, heißen „Priority Tagged Frames“.

Eingetragene Priorität	Traffic Class (Voreinstellung)	IEEE 802.1D-Verkehrstyp
0	1	Best Effort (default)
1	0	Background
2	0	Standard
3	1	Excellent Effort (business critical)
4	2	Controlled load (streaming multimedia)
5	2	Video, less than 100 millisconds of latency and jitter
6	3	Voice; less than 10 milliseconds of latency and jitter
7	3	Network Control reserved traffic

Tab. 8: Zuordnung der im Tag eingetragenen Priorität zu den 4 Traffic Classes

Anmerkung: Netzprotokolle und Redundanzmechanismen nutzen die höchste Traffic Class 3. Wählen Sie deshalb andere Traffic Classes für Anwendungsdaten.

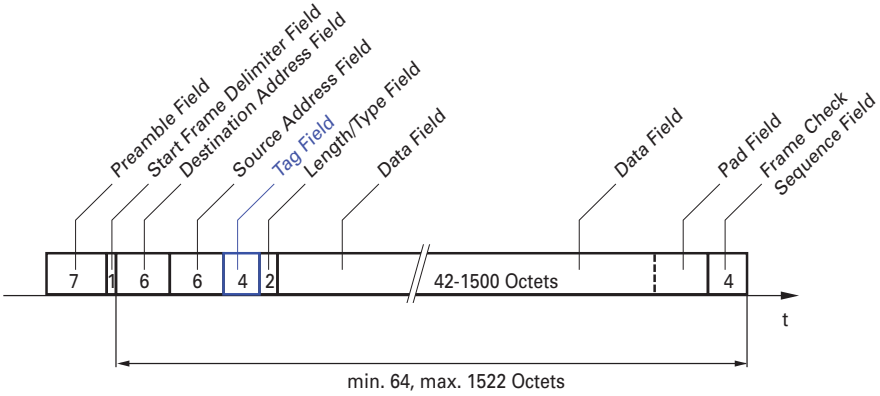

Abb. 28: Ethernet-Datenpaket mit Tag

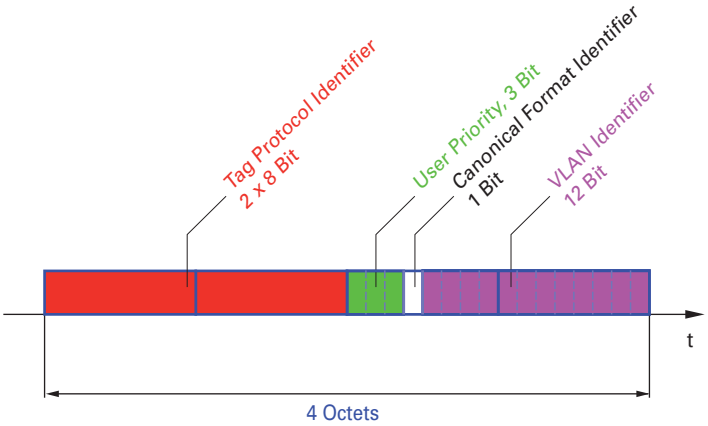

Abb. 29: Tag-Format

8.4.4 Behandlung empfangener Prioritätsinformationen

Das Gerät bietet Ihnen 3 Möglichkeiten, global für alle Ports zu wählen, wie es empfangene Datenpakete behandelt, die eine Prioritätsinformation enthalten.

- trust dot1p
  VLAN-getaggten Paketen ordnet das Gerät entsprechend ihrer VLAN-Priorität den unterschiedlichen Traffic Classes zu. Die Zuordnung erfolgt nach der voreingestellten Tabelle (siehe auf Seite 136 „VLAN-Tagging“). Diese Zuordnung können Sie modifizieren. Paketen, die das Gerät ohne Tag empfängt, ordnet das Gerät die Port-Priorität zu.
- untrusted
  Das Gerät ignoriert die Prioritäts-Informationen im Paket und weist den Paketen immer die Port-Priorität des Empfangsports zu.
- trust ip-dscp
  Das Gerät ordnet IP-Paketen entsprechend des DSCP-Wertes im IP-Header den unterschiedlichen Traffic Classes zu, auch wenn das Paket zusätzlich VLAN-getagged war. (DSCP = Differentiated Services Codepoint)

8.4.5 Handhabung der Verkehrsklassen

Für die Handhabung der Traffic Classes bietet das Gerät:

- Strict Priority

Beschreibung Strict-Priority
Bei Strict-Priority vermittelt das Gerät zuerst alle Datenpakete mit höherer Verkehrsklasse (höherer Priorität), bevor es ein Datenpaket mit der nächst niedrigeren Verkehrsklasse vermittelt. Ein Datenpaket mit der niedrigsten Verkehrsklasse (niedrigsten Priorität) vermittelt das Gerät demnach erst, wenn keine anderen Datenpakete mehr in der Warteschlange stehen. In ungünstigen Fällen sendet das Gerät Pakete mit niedriger Priorität nie, wenn an diesem Port ein hohes Aufkommen von höherpriorem Verkehr zum Senden ansteht.
Bei verzögerungsempfindlichen Anwendungen wie VoIP oder Video ermöglicht Strict-Priority das unmittelbare Senden hochpriorer Daten.

8.4.6 Priorisierung einstellen

Port-Priorität zuweisen

- ☐ Öffnen Sie den Dialog `QoS/Priorität:Portkonfiguration`.
- ☐ In der Spalte „Port Priorität“ haben Sie die Möglichkeit, die Priorität (0-7) festzulegen, mit welcher das Gerät Datenpakete vermittelt, die er an diesem Port ohne VLAN-Tag empfängt.
- ☐ In der Spalte „Trust Mode“ haben Sie die Möglichkeit, festzulegen, nach welchem Kriterium das Gerät empfangenen Datenpakete einer Traffic Class zuordnet (siehe auf Seite 135 „Beschreibung Priorisierung“).

Anmerkung: Falls Sie VLANs eingerichtet haben, beachten Sie den „VLAN 0-Transparent Modus“ (siehe `Switching:VLAN:Global`).

VLAN-Priorität einer Verkehrsklasse zuordnen

- ☐ Wählen Sie den Dialog `QOS/Priorität:802.1D/p-Mapping`.
- ☐ Tragen Sie in der Spalte „Traffic Class“ die gewünschten Werte ein.

Management-Priorität Layer 2 konfigurieren

- ☐ Konfigurieren Sie die VLAN-Ports, an denen das Gerät Management-Pakete verschickt, als Mitglied im VLAN, das Datenpakete mit Tag versendet (siehe auf Seite 151 „Beispiele für ein VLAN“).

- ☐ Öffnen Sie den Dialog `QoS/Priorität:Global`.
- ☐ Im Feld „VLAN-Priorität für Management-Pakete“ geben Sie den Wert der VLAN-Priorität ein.