LAN-Switching und Wireless

CCNA Exploration Companion Guide

Wayne Lewis, Ph.D.

ADDISON-WESLEY

Cisco | Networking Academy
Mind Wide Open

Lernziele

Wenn Sie dieses Kapitel gelesen haben, sollten Sie in der Lage sein, die folgenden Fragen zu beantworten:

- Welche Rolle spielt ein VLAN in einem geswitchten LAN?
- Welche Rolle spielt ein VLAN-Trunk in einem geswitchten LAN?
- Wie konfigurieren Sie VLANs auf Switches in einem geswitchten LAN?
- Wie überprüfen Sie Probleme bei der Software- und Hardwarekonfiguration in Verbindung mit VLANs in einem geswitchten LAN?

Schlüsselbegriffe

In diesem Kapitel werden die folgenden Schlüsselbegriffe vorgestellt.
Die entsprechenden Definitionen finden Sie im Glossar.

vlan.dat ▪ Flash ▪ VTP ▪ Daten-VLAN ▪ Default-VLAN ▪ Black-Hole-VLAN ▪ natives VLAN ▪ IEEE 802.1Q ▪ Management-VLAN ▪ Sprach-VLAN ▪ Signalisierungsdaten ▪ statisches VLAN ▪ dynamisches VLAN ▪ SVI ▪ VLAN-Trunk ▪ IEEE 802.1p ▪ CFI ▪ VLAN-ID ▪ ungetaggte Frames ▪ ISL ▪ DTP ▪ Trunking-Modi ▪ Nonegotiate ▪ Dynamic Auto ▪ Dynamic Desirable ▪ zugelassene VLANs

Kapitel 3

VLANs

Die Leistungsfähigkeit eines Netzwerks kann einen Faktor für die Produktivität einer Organisation und ihren Ruf darstellen. Eine der Technologien, die zu einer exzellenten Netzwerkleistung betragen, ist die Trennung großer Broadcast-Domänen in kleinere mithilfe von VLANs. Kleinere Broadcast-Domänen beschränken die Anzahl der Geräte, die an Broadcasts beteiligt sind, und gestatten die Unterteilung der Geräte in Funktionsgruppen, zum Beispiel Datenbankdienste für eine Buchhaltungsabteilung oder Highspeed-Datenübertragung für die Entwicklungsabteilung. In diesem Kapitel erfahren Sie, wie Sie VLANs und Ethernet-Trunk-Verbindungen konfigurieren und verwalten und das Troubleshooting durchführen.

3.1 Einführung in VLANs

Switches und VLANs gehören zusammen: Das eine gibt es nicht ohne das andere. Auch wenn es möglich ist, einen modernen Switch mit nur einem VLAN zu betreiben, werden Switches normalerweise mit mindestens zwei VLANs konfiguriert. VLANs bieten Netzwerkadministratoren Flexibilität beim LAN-Design. Sie erweitern den traditionellen Begriff der durch Router beschränkten Broadcast-Domäne auf eine VLAN-begrenzte Variante, denn VLANs ermöglichen das Gestalten von Broadcast-Domänen in beliebige Formen, die durch die Switches im Netzwerk definiert und abgegrenzt werden. In diesem Abschnitt erfahren Sie, was die verschiedenen VLAN-Typen tun und wie man sie konfiguriert und mithilfe von Ethernet-Trunks erweitert. Zunächst jedoch wollen wir die herkömmliche Implementierung von VLANs mit dem aktuellen Einsatz dieser Technik vergleichen.

3.1.1 Definition von VLANs

Um einschätzen zu können, warum VLANs heutzutage fast immer eingesetzt werden, wollen wir uns exemplarisch eine kleine Hochschule ansehen, bei der sich das Studentenwohnheim im selben Gebäude befindet wie die Büros der Hochschulverwaltung. Abbildung 3.1 zeigt die Computer der Studierenden in einem LAN und die Rechner der Verwaltung in einem zweiten. Dies funktioniert sehr gut, weil alle Abteilungen physisch aneinander angrenzen, was die Bereitstellung von Netzwerkressourcen vereinfacht.

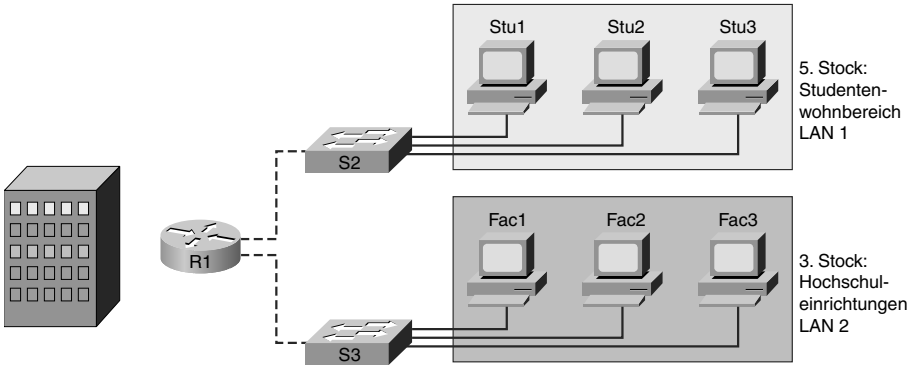

Abbildung 3.1: Ohne VLANs im selben Gebäude

Ein Jahr später wird die Universität vergrößert und umfasst nun drei Gebäude. In Abbildung 3.2 ist das ursprüngliche Netzwerk identisch, doch erstrecken sich die Netze von Studierenden und Hochschule über drei Gebäude. Der Wohnbereich der Studierenden befindet sich weiterhin im fünften, die Büros der Hochschule im dritten Stock. Allerdings möchte die IT-Abteilung nun sicherstellen, dass für alle Computer der Studierenden dieselbe Sicherheitsrichtlinie und Bandbreitenbeschränkung gilt. Wie nun kann das Netzwerk die gemeinsamen Anforderungen logisch zusammengehörender, aber räumlich getrennter Bereiche erfüllen? Müssen Sie ein großes LAN erstellen und jeden Bereich jeweils separat verkabeln? Und wäre es dann unproblematisch, Änderungen an diesem Netzwerk vorzunehmen? Schön wäre es, wenn man den Benutzern die von ihnen verwendeten Ressourcen unabhängig von ihrem physischen Standort zuordnen könnte; dies würde die Administration spezifischer Sicherheits- und Bandbreitenanforderungen vereinfachen.

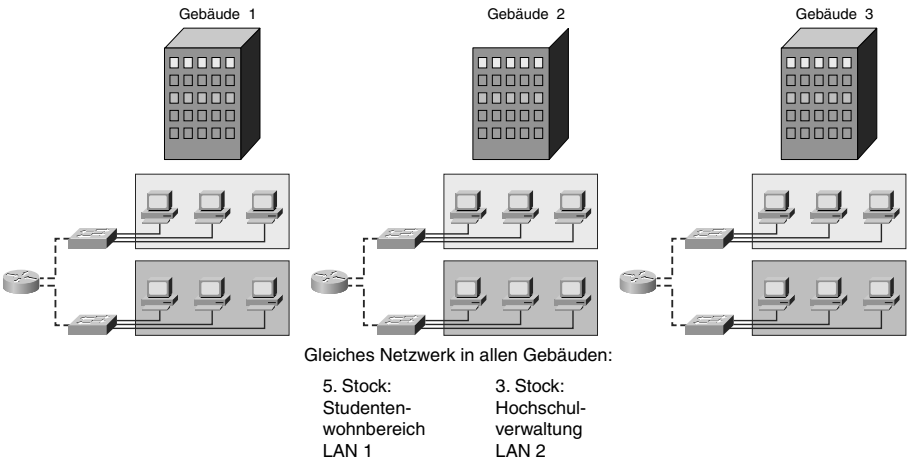

Abbildung 3.2: Ohne VLANs in drei Gebäuden

Die Lösung der Hochschule besteht in der Verwendung einer Netzwerktechnologie, die als VLAN (Virtual LAN) bezeichnet wird. Ein VLAN ermöglicht es dem Netzwerkadministrator, Gruppen logisch zusammenhängender Netzwerkgeräte zu erstellen, die sich so verhalten, als ob es sich um jeweils eigene, unabhängige Netzwerke handelt – und zwar auch dann, wenn sie eine gemeinsame Infrastruktur mit anderen VLANs teilen. Wenn Sie ein VLAN konfigurieren, können Sie ihm einen Namen zuweisen, der die hauptsächliche Rolle der Benutzer dieses VLANs beschreibt. Noch ein Beispiel: Alle Computer in den Wohnbereichen der Hochschule ließen sich in einem »Studierenden-VLAN« zusammenfassen. Mithilfe von VLANs können Sie geswitchte Netzwerke basierend auf Funktionen, Abteilungen oder Projektteams logisch segmentieren. Sie können Ihr Netzwerk mit VLANs aber auch geografisch strukturieren, um die zunehmende Abhängigkeit von Unternehmen von Heimarbeitern zu unterstützen. In Abbildung 3.3 wird ein VLAN für die Studierenden und ein zweites für die Hochschulverwaltung erstellt. Diese VLANs ermöglichen es dem Netzwerkadministrator, andere Zugriffs- und Sicherheitsrichtlinien für diese Benutzergruppe zu implementieren. So dürfen beispielsweise die Mitarbeiter der Universität – nicht jedoch die Studierenden – zum Zweck der Entwicklung neuer Kursmaterialien auf E-Learning-Server zugreifen.

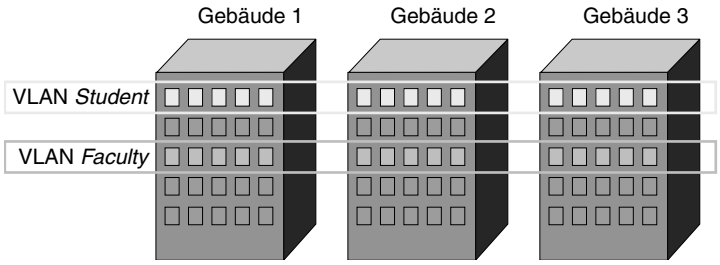

Abbildung 3.3: Mit VLANs in drei Gebäuden

Ein VLAN ist ein logisch unabhängiges IP-Subnetz. VLANs ermöglichen das Vorhandensein mehrerer IP-Netzwerke und -Subnetze im selben geswitchten Netzwerk. Abbildung 3.4 zeigt ein Netzwerk mit drei Computern. Damit diese Computer im selben VLAN miteinander kommunizieren können, benötigen sie jeweils eine IP-Adresse und eine Subnetzmaske, die für dieses VLAN eindeutig sind und zu einem IP-Netzwerk gehören. Das VLAN muss auf dem Switch konfiguriert sein, und jeder Port im VLAN muss diesem explizit zugeordnet werden. Ein Switch-Port, auf dem genau ein VLAN konfiguriert ist, heißt Access-Port. Wie Sie wissen, bedeutet die physische Verbindung zweier Computer nicht zwingend, dass diese auch miteinander kommunizieren können. Geräte in zwei getrennten (Sub-)Netzen müssen unabhängig davon, ob VLANs verwendet werden oder nicht, über einen Router (Schicht 3) miteinander kommunizieren. Um mehrere Subnetze in einem geswitchten Netzwerk einzurichten, benötigen Sie zwar keine VLANs, doch bietet deren Verwendung in jedem Fall Vorteile.

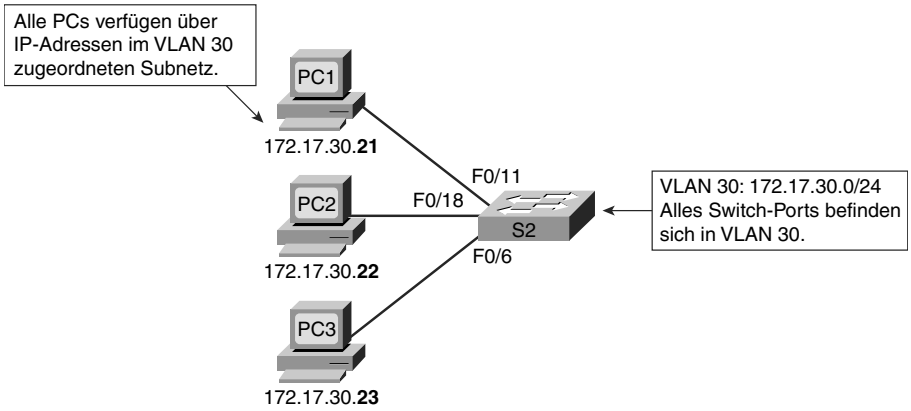

Abbildung 3.4: Switches definieren VLANs

3.1.2 Vorteile von VLANs

Leistungsfähigkeit und die Anpassungsfähigkeit des Netzwerks sind wesentliche Grundlagen für das Wachstum und den Erfolg eines Unternehmens. Die Implementierung von VLAN-Technologien bietet einem Netzwerk mehr Flexibilität bei der Unterstützung der Unternehmensziele. Die primären Vorteile der Verwendung von VLANs sind folgende:

- **Sicherheit.** Arbeitsgruppen, in denen sensible Daten verarbeitet werden, werden vom Rest des Netzwerks getrennt. Hierdurch verringert sich das Risiko eines Missbrauchs vertraulicher Informationen. Die Computer der Hochschulverwaltung befinden sich in VLAN 10 und sind vom Datenverkehr der Studierenden und Gäste vollständig getrennt.
- **Kostensenkung.** Eine Kostensenkung ergibt sich aus dem verringerten Bedarf an teuren Netzwerkerweiterungen und der effizienteren Verwendung der vorhandenen Bandbreite und der Uplinks.
- **Höhere Leistungsfähigkeit.** Durch Unterteilung flacher Schicht-2-Netzwerke in mehrere logische Arbeitsgruppen (Broadcast-Domänen) wird unnötiger Datenaustausch im Netzwerk reduziert und die Leistung erhöht.
- **Begrenzung von Broadcast-Stürmen.** Durch Unterteilung eines Netzwerks in VLANs verringert sich die Anzahl der Geräte, die an einem möglichen Broadcast-Sturm beteiligt sind. Die LAN-Segmentierung verhindert das Ausbreiten von Broadcast-Stürmen im gesamten Netzwerk. In Abbildung 3.5 sehen Sie drei Broadcast-Domänen: *Faculty*, *Student* und *Guest*.
- **Erhöhte Effizienz der IT-Mitarbeiter.** VLANs vereinfachen die Administration des Netzwerks, weil Benutzer mit ähnlichen Anforderungen an das Netzwerk dasselbe VLAN benutzen. Wenn Sie einen neuen Switch einbringen, werden alle für das betreffende VLAN bereits eingerichteten Richtlinien und Prozeduren einfach bei der Zuweisung der Ports erneut verwendet. Außerdem kann die Funktion eines VLAN normalerweise seinem Namen entnommen werden. In Abbildung 3.5 ist dies möglich: Das VLAN 10 heißt *Faculty*, VLAN 20 *Student* und VLAN 30 *Guest*.
- **Einfachere Projekt- oder Anwendungsverwaltung.** VLANs fassen Benutzer und Netzwerkgeräte zusammen, um geschäftliche oder geografische Anforderungen zu realisieren. Die Trennung nach Funktionen macht die Verwaltung eines Projekts oder das Arbeiten mit einer Spezialanwendung einfacher (z. B. die Entwicklung von E-Learning-Software für die Hochschuleinrichtung). Außerdem erleichtern VLANs die Feststellung von Auswirkungen der Erweiterung von Netzwerkdiensten.

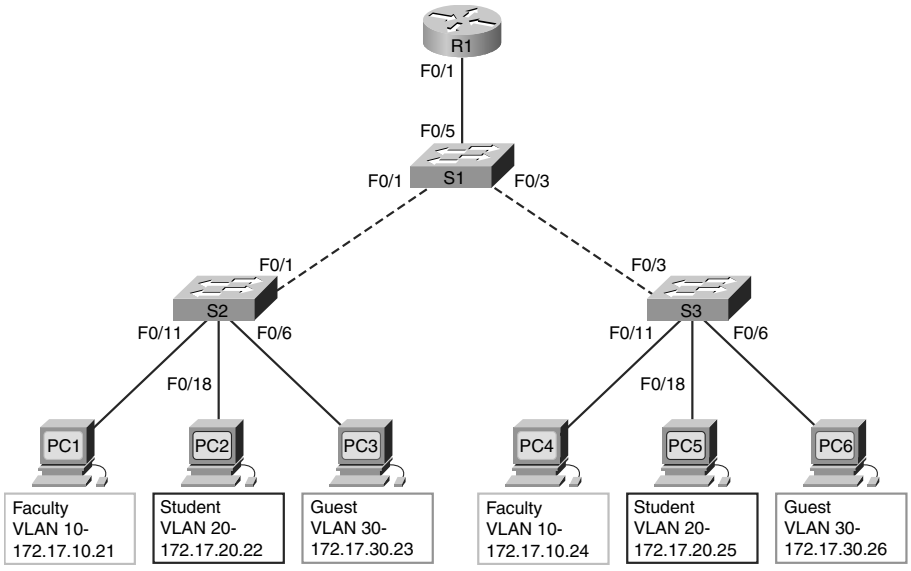

Abbildung 3.5: VLANs benennen

3.1.3 ID-Bereiche bei VLANs

VLANs sind numerisch in einen normalen und einen erweiterten Bereich unterteilt. VLANs im normalen Bereich lassen sich wie folgt kennzeichnen:

- Sie werden gleichermaßen in KMU- wie auch in Netzwerken von Großunternehmen verwendet.
- Sie haben eine VLAN-ID zwischen 1 und 1005.
- Die IDs 1002 bis 1005 sind für Token Ring- und FDDI-VLANs reserviert.
- VLAN 1 sowie die VLANs 1002–1005 werden automatisch erstellt und können nicht gelöscht werden. Mehr zu VLAN 1 erfahren Sie im weiteren Verlauf dieses Kapitels.
- Die Konfigurationen werden in einer VLAN-Datenbankdatei namens *vlan.dat* gespeichert. Diese Datei befindet sich im Flashspeicher des Switchs.
- Das VTP-Protokoll (VLAN Trunking Protocol) erleichtert die Switch-übergreifende Administration von VLAN-Konfigurationen; es kann nur VLANs aus dem normalen Bereich erlernen und speichert diese in der VLAN-Datenbankdatei.

VLANs im erweiterten Bereich lassen sich wie folgt kennzeichnen:

- Sie ermöglichen es Providern, ihre Infrastruktur auf eine größere Anzahl von Kunden auszudehnen. Einige globale Unternehmen sind unter Umständen so groß, dass sie VLAN-IDs aus dem erweiterten Bereich benötigen.
- Sie haben eine VLAN-ID zwischen 1006 und 4094.
- Sie unterstützen weniger VLAN-Funktionen als VLANs aus dem normalen Bereich.
- Sie werden in der Datei *running-config* gespeichert.
- Sie werden von VTP nicht erlernt.

Ein Cisco Catalyst 2960-Switch kann eine Kombination von bis zu 255 VLANs aus dem normalen und dem erweiterten Bereich unterstützen. Die Anzahl der konfigurierten VLANs wirkt sich auf die Leistungsfähigkeit der Switch-Hardware aus. Weil größere Unternehmen unter Umständen Switches mit eine hohen Anzahl Ports benötigen, hat Cisco speziell für solche Netzwerke Switches entwickelt, die mit Clustering arbeiten oder gestapelt werden können und dann eine einzelne logische Switching-Einheit bilden. So lassen sich beispielsweise neun Switches mit je 48 Ports clustern, um als einzelne Switching-Einheit mit 432 Ports zu fungieren. In diesem Fall kann die Beschränkung auf 255 VLANs pro Einzel-Switch für den einen oder anderen Unternehmenskunden eine Limitierung darstellen.

3.1.4 VLAN-Typen

Heutzutage gibt es im Wesentlichen nur eine Art der Implementierung von VLANs: portbasierte VLANs. Hierbei wird dem VLAN eine Anzahl von Switch-Ports zugeordnet, die dann in einer Broadcast-Domäne liegen. Die mit einem portbasierten VLAN verknüpften Ports heißen Access-Ports. In gewisser Hinsicht wird das VLAN durch die Access-Ports definiert, die ihm zugeordnet sind.

Die (portbasierten) VLANs umfassen eine Anzahl von VLAN-Typen. Einige dieser Typen definieren sich auf der Basis des von ihnen unterstützten Datenverkehrs, während andere durch die jeweilige spezielle Funktion bestimmt werden. Zu diesen VLAN-Haupttypen gehören Daten-VLANs, das Default-VLAN, das Black-Hole-VLAN, native VLANs, Management-VLANs und Sprach-VLANs.

Da Switches Daten übertragen, die aus verschiedenen VLANs stammen, müssen die Switches über bestimmte Ports Daten für mehrere VLANs übertragen. Diese Ports heißen Trunk-Ports. Abbildung 3.6 zeigt Trunks zwischen Switches. Eine ausführlichere Abhandlung zu Trunks finden Sie im nächsten Abschnitt.

Ein Daten-VLAN ist ein VLAN, das nur Benutzerdaten überträgt. Normalerweise gibt es in einer geswitchten Infrastruktur mehrere Daten-VLANs. Ein VLAN könnte Sprachdaten oder auch Daten übertragen, mit denen der Switch administriert wird, doch wären diese Daten nicht Teil des Daten-VLAN. Sprach- und Managementdaten vom regulären Datenverkehr zu trennen, ist gängige Praxis. Die Bedeutung der Trennung der Benutzerdaten von Administration und Sprache wird durch die Verwendung eines besonderen Begriffs unterstrichen, mit dem VLANs bezeichnet werden, die nur Benutzerdaten übertragen: das Daten-VLAN eben. Ein Daten-VLAN wird manchmal auch als Benutzer-VLAN bezeichnet. Abbildung 3.6 zeigt den Teil eines Netzwerks, in dem Benutzer-VLANs aktiv sind.

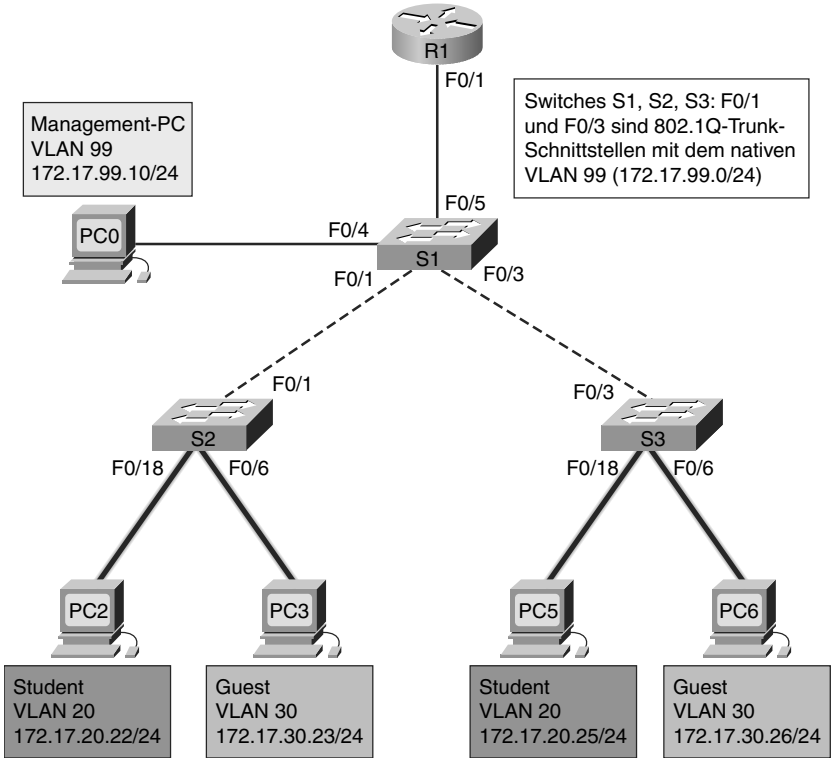

Abbildung 3.6: Daten-VLANs

Das Default-VLAN ist dasjenige VLAN, dem alle Switch-Ports zugeordnet sind, wenn der Switch auf die Werkseinstellungen zurückgesetzt wird. Nach dem Erststart des Switchs sind alle Ports diesem VLAN zugewiesen. Wenn alle Ports Mitglieder dieses VLAN sind, werden sie alle zum Bestandteil derselben Broadcast-Domäne; deswegen kann jedes Gerät, das an einen Switch-Port angeschlossen ist, mit jedem an irgendeinen anderen Port des Switchs angeschlossenen Gerät kommunizieren. Das Default-VLAN bei Cisco-Switches ist VLAN 1. VLAN 1 verhält sich genauso wie alle übrigen normalen VLANs, nur können Sie es weder löschen noch umbenennen. Steuerdaten in Schicht 2 – z. B. CDP- oder STP-Daten – sind grundsätzlich VLAN 1 zugeordnet, was nicht geändert werden kann. Sicherheitstechnisch wird empfohlen, VLAN 1 als »Kanal« ausschließlich von Schicht-2-Steuerdaten zu betrachten, das heißt, andere Daten dort nicht zuzulassen. In Abbildung 3.7 werden Daten aus VLAN 1 über VLAN-Trunks weitergeleitet, die von den Schnittstellen F0/1 und F0/3 auf den Switches S1, S2 und S3 gebildet werden. VLAN-Trunks unterstützen die Übertragung von Daten für mehrere VLANs. Zwar wird das Trunking an dieser Stelle bereits verwendet, doch werden wir uns ihm im Abschnitt »VLAN-Trunking« ausführlich widmen.

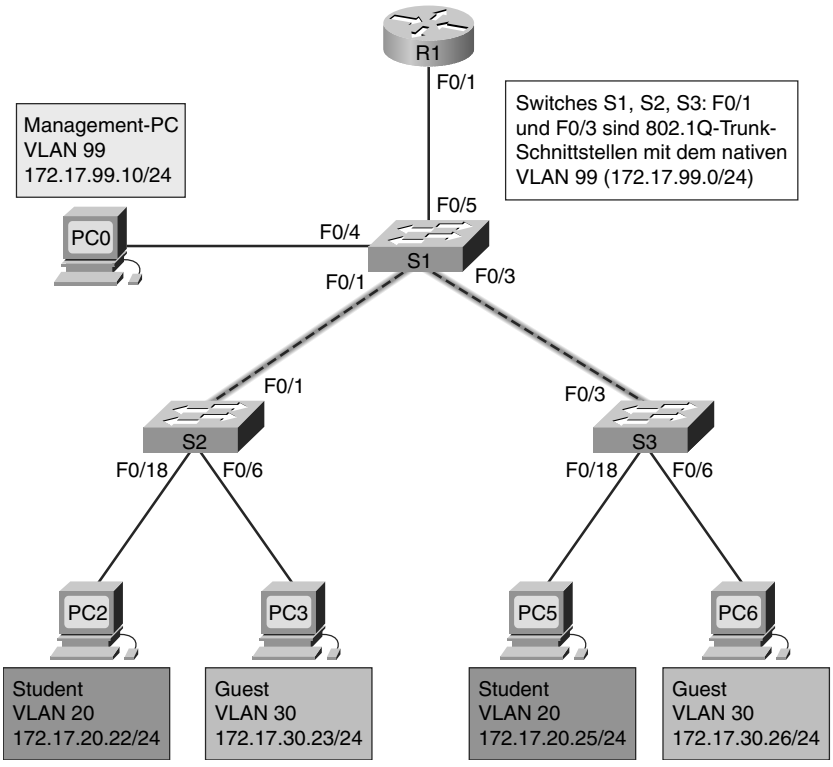

Abbildung 3.7: VLAN 1 (Default-VLAN auf Catalyst-Switches)

Es gibt Netzwerkadministratoren, die mit dem Begriff *Default-VLAN* ein anderes VLAN als VLAN 1 bezeichnen. Es handelt sich um das VLAN, das vom Netzwerkadministrator zur Aufnahme aller Ports verwendet wird, die nicht benutzt werden. Wir führen hierfür an dieser Stelle den Begriff Black-Hole-VLAN ein, um dieses VLAN konzeptionell vom Default-VLAN zu unterscheiden. Das Default-VLAN ist auf dem Switch werksseitig vorhanden; auf Cisco-Switches handelt es sich um VLAN 1. Das Black-Hole-VLAN hingegen wird durch den Switch-Administrator definiert. Es wird empfohlen, ein Black-Hole-VLAN zu definieren, d. h. ein Pseudo-VLAN, das sich von *allen* anderen VLANs unterscheidet, die im geswitchten LAN definiert sind. Alle nicht verwendeten Ports werden dem Black-Hole-VLAN zugewiesen, damit Geräte, die mit einem nicht verwendeten Switch-Port verbunden sind, ebenfalls in diesem VLAN landen. Daten, die in das Black-Hole-VLAN gerichtet sind, sollten auf Trunks nicht transportiert werden. Dies verhindert, dass Geräte, die zum Black-Hole-VLAN gehören, über den Switch, an den sie angeschlossen sind, hinaus kommunizieren können.

Weiter gibt es ein natives VLAN auf einem 802.1Q-Trunk-Port. Ein IEEE 802.1Q-Trunk-Port unterstützt Daten, die aus mehreren VLANs stammen (getaggte Daten), wie auch solche, die nicht aus einem VLAN kommen (ungetaggter Datenverkehr). Der 802.1Q-Trunk-Port weist ungetaggten Datenverkehr dem nativen VLAN zu. In Abbildung 3.8 ist VLAN 99 das native VLAN. Ungetaggter Datenverkehr kommt von einem Computer, der an einen Switch-Port angeschlossen ist, welcher für das native VLAN konfiguriert wurde. Native VLANs wurden in die IEEE 802.1Q-Spezifikation aufgenommen, um Abwärtskompatibilität mit ungetaggten Daten zu ermöglichen, die in herkömmlichen LAN-Szenarien häufig anzutreffen sind. Für unsere Zwecke dient ein natives VLAN als allgemeine Kennung an den gegenüberliegenden Enden einer Trunk-Verbindung. Es wird empfohlen, ein natives VLAN als Pseudo-VLAN zu definieren, das sich von *allen* anderen VLANs unterscheidet, die im geswitchten LAN definiert sind. Das native VLAN wird nur dann für den Datenaustausch im geswitchten Netzwerk verwendet, falls im Netzwerk ein herkömmliches Bridging-Gerät vorhanden ist oder eine Multiaccess-Verbindung zwischen den Switches existiert, die einen Hub beinhaltet (was im modernen Netzwerk eher nicht vorkommt).

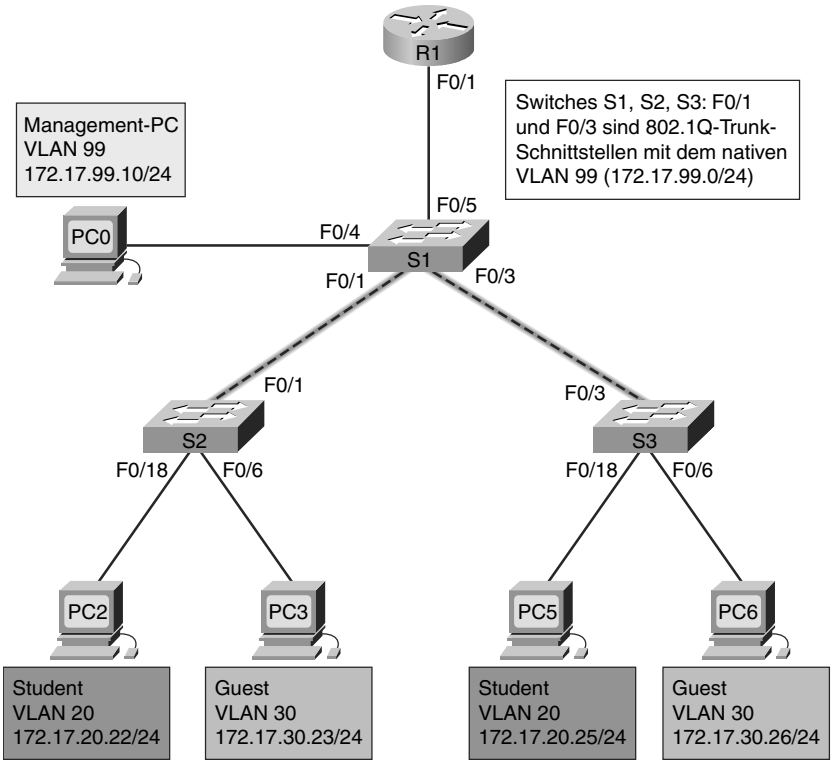

Abbildung 3.8: Natives VLAN

Ein Management-VLAN ist ein VLAN, das vom Switch-Administrator als Möglichkeit definiert wurde, auf die Verwaltungsfunktionen eines Switchs zuzugreifen. VLAN 1 würde als Management-VLAN verwendet, sofern Sie nicht proaktiv ein anderes VLAN für diese Funktion festlegen. Dem Management-VLAN weisen Sie eine IP-Adresse und eine Subnetzmaske zu. Ein Switch kann via HTTP, Telnet, SSH oder SNMP verwaltet werden. Weil die Werkskonfiguration eines Catalyst-Switchs VLAN 1 als Default-VLAN vorsieht, ist verständlich, dass VLAN 1 oder das Black-Hole-VLAN als Management-VLAN eher ungeeignet sind – die Vorstellung, dass irgendein Benutzer sich an einem Switch anmeldet und sofort im Management-VLAN landet, ist abschreckend. Es wird empfohlen, das Management-VLAN als VLAN zu definieren, das sich von *allen* anderen VLANs unterscheidet, die im geswitchten LAN definiert sind. Der Einfachheit halber verwenden wir aufgrund der Begrenzung auf 24 Ports bei Catalyst 2960-Switches, die wir in Packet Tracer-Aktivitäten, Übungen und erläuternden Beispielen verwenden, für unsere Zwecke in diesem Buch VLAN 99 sowohl für das Management-VLAN als auch für das native VLAN. Ein Management-VLAN ist in Abbildung 3.9 gezeigt.

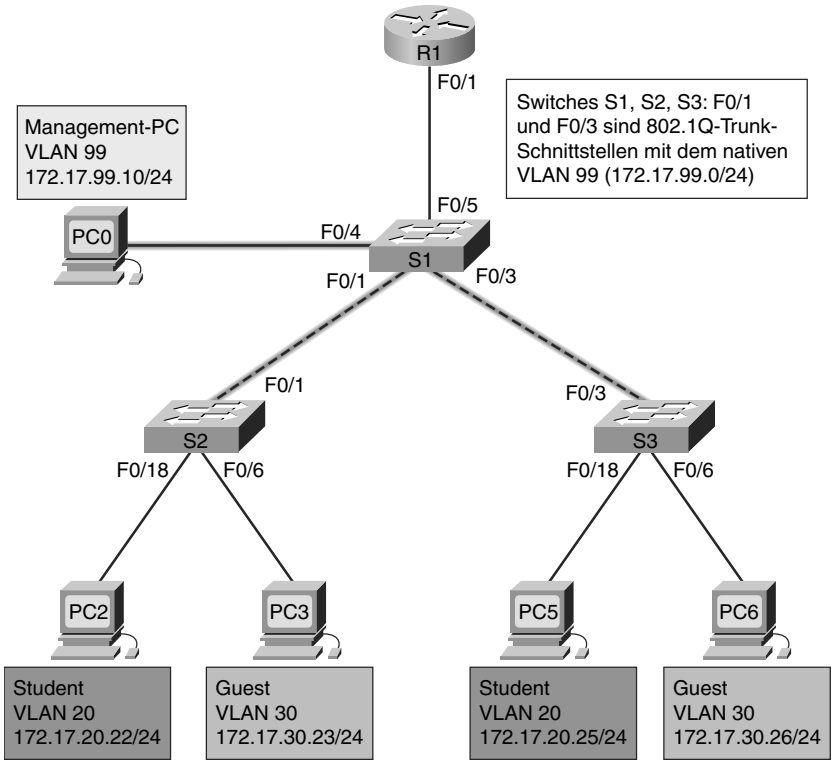

Abbildung 3.9: Management-VLAN

Den letzten verbleibenden VLAN-Typ – die Sprach-VLANs – untersuchen wir im nächsten Abschnitt.

3.1.5 Sprach-VLANs

Es ist wohl leicht nachzuvollziehen, warum zur Unterstützung von VoIP (Voice over IP) ein separates VLAN benötigt wird. Stellen Sie sich vor, Sie empfangen einen Notruf, und plötzlich fällt die Qualität der Übertragung derart ab, dass Sie nicht mehr hören können, was der Anrufer sagt. Für VoIP-Datenverkehr ist Folgendes erforderlich:

- Garantierte Bandbreite zur Sicherstellung der Sprachqualität
- Vorrang der Übertragung vor anderen Datentypen im Netzwerk
- Vermeidung des Routings über überlastete Netzwerkbereiche
- Gesamtlatenz von maximal 150 Millisekunden im Netzwerk

Um diese Anforderungen zu erfüllen, muss das gesamte Netzwerk für die Nutzung von VoIP entworfen werden. Die Details der Konfiguration eines Netzwerks für die VoIP-Unterstützung würden den Rahmen dieses Buches sprengen, doch ist es nützlich aufzuzeigen, wie ein Sprach-VLAN zwischen einem Catalyst-Switch, einem Cisco-IP-Telefon und einem Computer funktioniert.

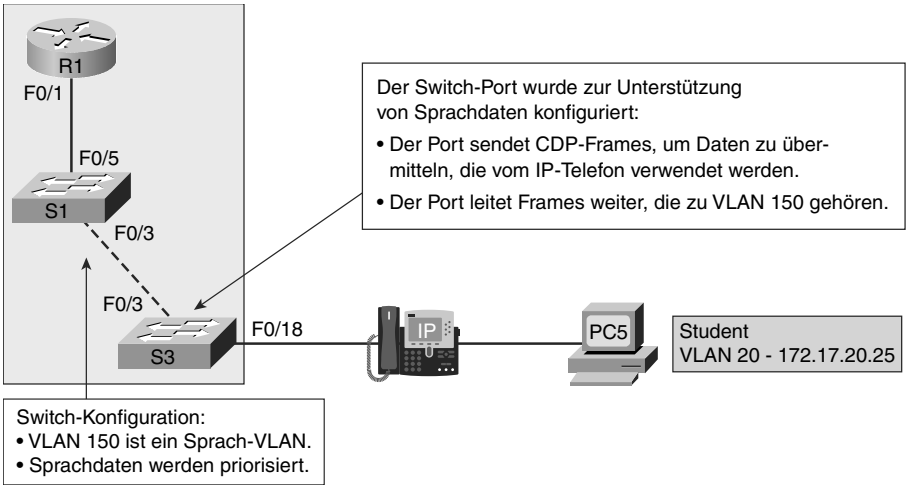

Abbildung 3.10: Sprach-VLANs

In Abbildung 3.10 wurde das VLAN 150 zur Übertragung von Sprachdaten eingerichtet. Der Computer PC5 ist an das Cisco-IP-Telefon angeschlossen, das Telefon wiederum an den Switch S3. PC5 befindet sich in VLAN 20, welches für die Daten der Studierenden verwendet wird. Der Port F0/18 auf S3 ist als Access-Port konfiguriert, wobei die Funktionalität für Sprach-VLANs aktiviert ist. Insofern weist der Switch das Telefon mithilfe von CDP an, Sprach-Frames für das VLAN 150 zu taggen.

ANMERKUNG

Die Kommunikation zwischen dem Switch und dem IP-Telefon wird durch das CDP-Protokoll ermöglicht. Dieses Protokoll wird im CCNA Exploration Companion Guide »Routing-Protokolle und -Konzepte« ausführlich behandelt.

Daten-Frames, die von PC5 kommend über das IP-Telefon übertragen werden, bleiben ungetaggt. Daten, die an PC5 gerichtet sind und über den Port F0/18 laufen, werden mit VLAN 20 getaggt; werden diese Daten vom IP-Telefon empfangen, dann wird das VLAN-Tag entfernt, bevor die Daten

an PC5 weitergeleitet werden. Der Begriff des Taggens beschreibt das Hinzufügen von VLAN-spezifischen Informationen zu einem Feld im Daten-Frame, anhand dessen der Switch feststellt, an welches VLAN die Daten-Frames gesendet werden sollen. Sie werden später erfahren, wie Daten-Frames getaggt werden.

Das Cisco-IP-Telefon enthält einen integrierten 10/100-Switch mit drei Ports (siehe Abbildung 3.11). Die Ports vermitteln dedizierte Verbindungen zu den folgenden Geräten:

- Port 1 ist mit dem Switch oder einem anderen VoIP-Gerät verbunden.
- Port 2 ist eine interne 10/100-Schnittstelle, über die die IP-Telefondaten übertragen werden.
- Port 3 (Access-Port) ist mit einem PC oder einem anderen Gerät verbunden.

Die Sprach-VLAN-Funktionalität ermöglicht es Switch-Ports, Sprachdaten eines IP-Telefons zu übertragen. Wenn der Switch an ein IP-Telefon angeschlossen wird, sendet er CDP-Nachrichten, die das angeschlossene Telefon anweisen, Sprachdaten mit dem Tag für das Sprach-VLAN (ID 150) zu übertragen. Die Daten des an das IP-Telefon angeschlossenen PC werden durch das Telefon nicht mit Tags versehen. Wenn auf dem Switch-Port ein Sprach-VLAN konfiguriert wurde, agiert die Leitung zwischen Switch und IP-Telefon als modifizierter Trunk, über den sowohl getaggte Sprachdaten als auch ungetaggte Daten ausgetauscht werden.

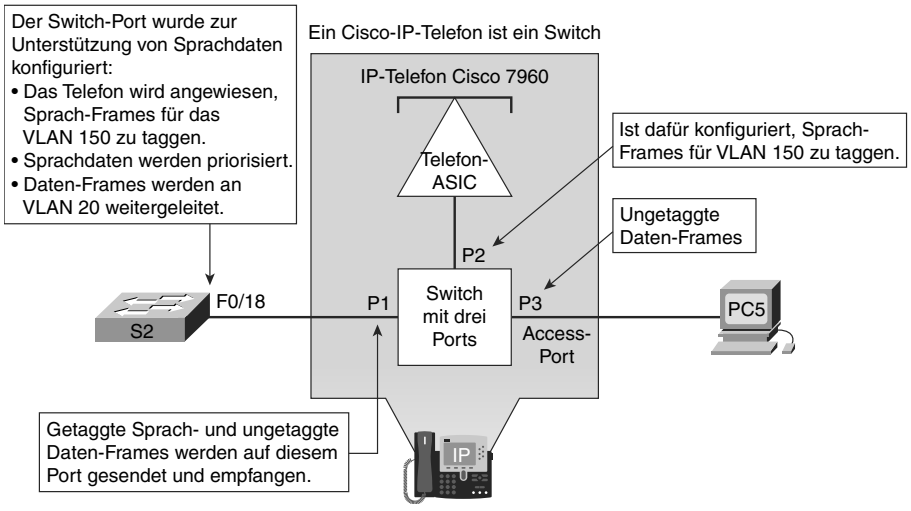

Abbildung 3.11: Ein in das IP-Telefon integrierter Switch

Listing 3.1 zeigt eine Beispielausgabe für den Switch-Port, der mit einem IP-Telefon verbunden ist.

Listing 3.1: Ausgabe des Sprach-VLAN

```
S3# show interfaces f0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (VLAN0020)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (VLAN0150)
<Ausgabe unterdrückt>
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Eine Abhandlung zu den VoIP Cisco IOS-Befehlen ist zwar nicht Gegenstand dieses Buches, doch können Sie den hervorgehobenen Bereichen im obigen Listing entnehmen, dass für die Schnittstelle F0/18 ein VLAN für Daten (VLAN 20) und ein VLAN für Sprache (VLAN 150) konfiguriert wurden.

3.1.6 Arten von anwendungsgenerierten Netzwerkdaten

Im CCNA Exploration Companion Guide »Netzwerkgrundlagen« haben Sie verschiedene Arten von Daten kennengelernt, die in einem LAN übertragen werden. Weil ein VLAN alle Eigenschaften eines LAN aufweist, muss es folglich auch dieselben Netzwerkdaten wie ein LAN übertragen können. Hierzu gehören Daten zur Netzwerkverwaltung, Steuerdaten, IP-Telefoniedaten, Multicast-Daten, normaler Datenverkehr und Daten der Scavenger-Klasse.

Viele Arten von Netzverwaltungs- und Steuerdaten können im Netzwerk vorhanden sein: CDP-Daten, SNMP-Daten (Simple Network Management Protocol), RMON-Daten (Remote Network Monitoring) usw. Abbildung 3.12 zeigt Daten, die zur Verwaltung eines Netzwerks dienen.

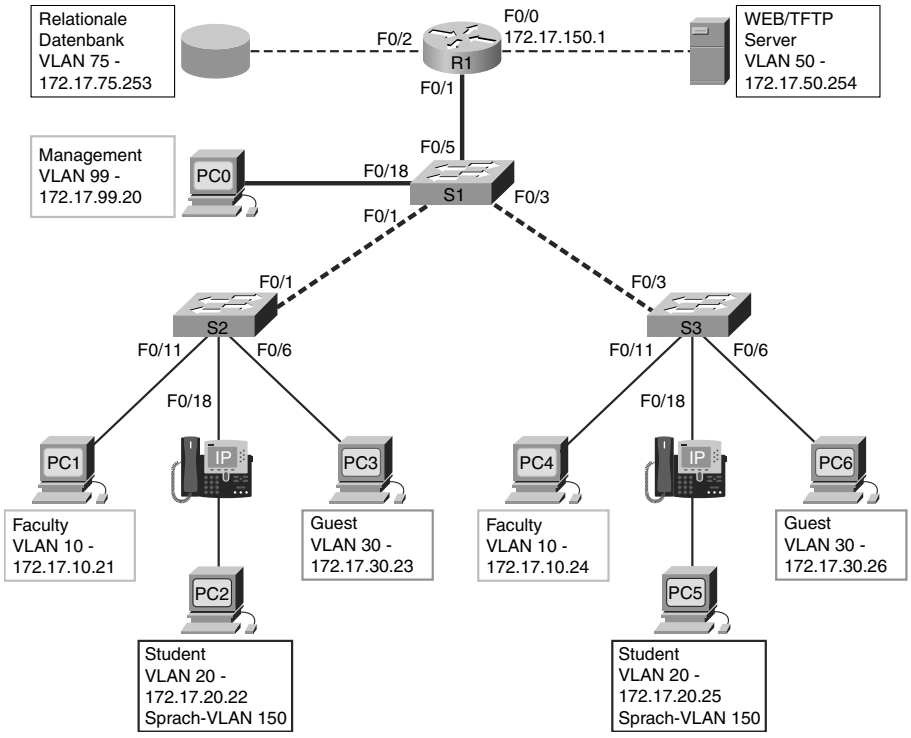

Abbildung 3.12: Netzverwaltungsdaten

IP-Telefoniedaten umfassen Signalisierungsdaten und Sprachdaten. Signalisierungsdaten dienen zum Aufbau, zur Aufrechterhaltung und zum Abbau eines Anrufs. Der zweite Datentyp bei der Telefonie sind die eigentlichen Sprachdaten, die in Abbildung 3.13 gezeigt werden. Wie Sie gerade gelernt haben, wird in Netzwerken, in denen VLANs konfiguriert wurden, dringend empfohlen, als Management-VLAN eines auszuwählen, das für keinerlei andere Aufgabe eingesetzt wird. Normaler Datenverkehr sollte einem Daten-VLAN (außer VLAN 1), Sprachdaten hingegen einem Sprach-VLAN zugeordnet werden.

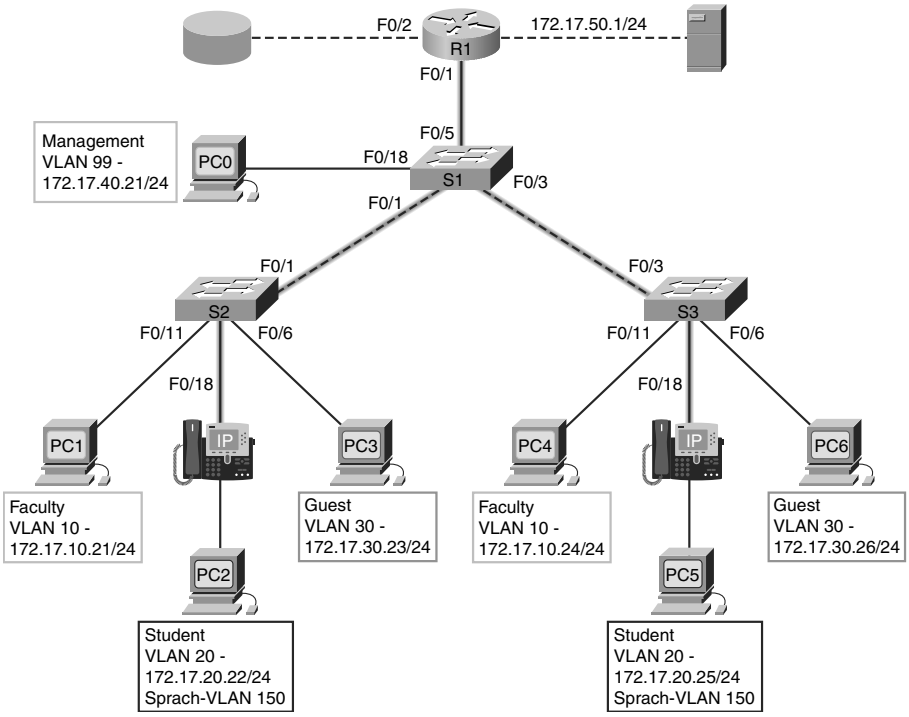

Abbildung 3.13: IP-Telefoniedaten

Multicast-IP-Daten werden von einem bestimmten Absender an eine Multicast-Gruppe gesendet, die durch eine einzelne IP-Adresse angesprochen wird; diese repräsentiert mehrere Empfänger, für die diese Multicast-Adresse konfiguriert wurde. Die Multicast-Theorie erläutert, wie Multicast-MAC-Adressen den Multicast-IP-Adressen zuzuordnen sind. Ein Beispiel für eine Anwendung, die solche Daten generiert, ist eine Cisco-IP/TV-Sendung. Multicast-Daten können umfangreiche Datenströme im gesamten Netzwerk generieren. Wenn das Netzwerk Multicast-Daten unterstützen soll, müssen VLANs konfiguriert werden, um sicherzustellen, dass Multicast-Daten nur an jene Endgeräte gesendet werden, die den bereitgestellten Dienst – z. B. Audio- oder Videoanwendungen – in Anspruch nehmen wollen. Router müssen so konfiguriert werden, dass die Weiterleitung der Multicast-Daten ausschließlich in diejenigen Bereiche erfolgt, in denen sie angefordert wurden. Abbildung 3.14 veranschaulicht den Multicast-Datenfluss exemplarisch.

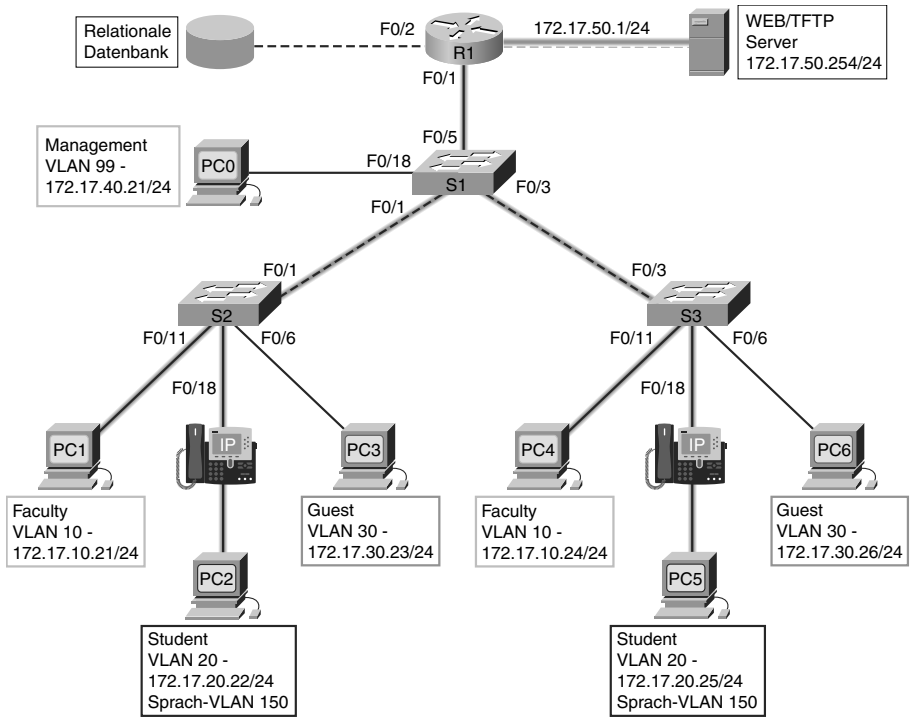

Abbildung 3.14: IP-Multicast-Datenverkehr

Normaler Datenverkehr steht in Zusammenhang mit der Erstellung und der Speicherung von Dateien, der Nutzung von Druckdiensten, dem Zugriff auf eine Maildatenbank und anderen verteilt genutzten Netzwerkanwendungen, wie sie in modernen Unternehmensumgebungen gängig sind. Abbildung 3.15 veranschaulicht den Datenfluss exemplarisch. VLANs stellen eine natürliche Lösung für derartige Daten dar, weil sie Benutzer nach ihren Funktionen oder ihren geografischen Standorten zusammenfassen können, um ihre speziellen Bedürfnisse besser bereitzustellen.

Die Scavenger-Klasse soll sogenannte Less-Than-Best-Effort-Dienste für bestimmte Anwendungen zur Verfügung stellen. Anwendungen, die dieser Klasse zugewiesen sind, tragen nur wenig oder gar nicht zu den Geschäftszielen des Unternehmens bei und sind meistens eher unterhaltender Natur. Hierzu gehören P2P-Anwendungen für den Medienaustausch (Kazaa, Morpheus, Grokster, Napster, iMesh usw.), Spiele (DOOM, Quake, Unreal Tournament u. Ä.) sowie Videoanwendungen mit Unterhaltungscharakter.

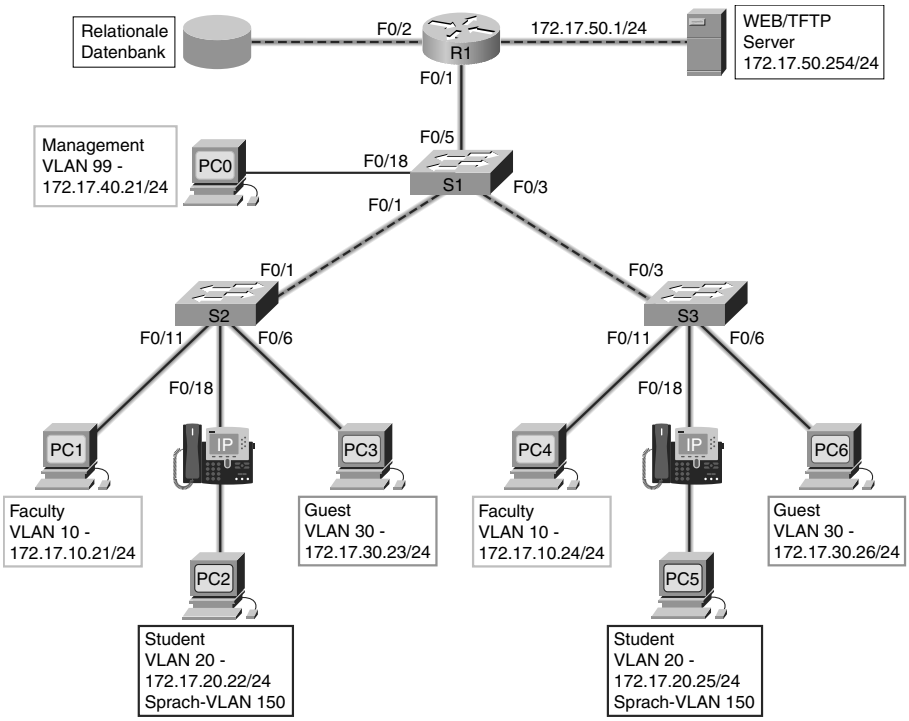

Abbildung 3.15: Normaler Datenverkehr

3.1.7 Mitgliedsmodi für Switch-Ports

Switch-Ports sind Schicht-2-Schnittstellen, die zur Steuerung physischer Schnittstellen und zugehöriger Schicht-2-Protokolle verwendet werden. Routing oder Bridging gehören nicht zu ihren Aufgabenbereichen. Switch-Ports gehören einem oder mehreren VLANs an.

Wenn Sie ein VLAN konfigurieren, müssen Sie ihm eine numerische ID zuweisen; ferner können Sie optional einen Namen konfigurieren. Die Aufgabe einer VLAN-Implementierung besteht darin, Ports sinnvoll bestimmten VLANs zuzuordnen. Sie konfigurieren den Port so, dass ein Frame an ein bestimmtes VLAN weitergeleitet wird. Sie können einen Switch-Port mit aktivierter Sprach-VLAN-Funktion konfigurieren, um sowohl Sprach- als auch normalen Datenverkehr zu unterstützen, der von einem Cisco-IP-Telefon kommt. Zudem können Sie einen Port als einem VLAN zugehörig konfigurieren, indem Sie einen Modus definieren, aus dem hervorgeht, welche Art von Daten der Port überträgt und zu welchen VLANs er gehört.

Auf einem Port kann die Unterstützung der folgenden VLAN-Optionen konfiguriert werden:

- **Statisches VLAN.** Ports auf einem Switch werden einem VLAN manuell zugewiesen. Statische VLANs werden über das Cisco-CLI konfiguriert. Alternativ kann diese Aufgabe auch mit grafischen Administrationsanwendungen wie dem Cisco Network Assistant durchgeführt werden. Ein praktisches Merkmal des CLI besteht darin, dass, wenn Sie eine Schnittstelle einem nicht vorhandenen VLAN zuweisen, dieses neue VLAN automatisch für Sie erstellt wird.
- Listing 3.2 zeigt exemplarisch die Konfiguration eines statischen VLAN.

Listing 3.2: Statisches VLAN konfigurieren

```
S3# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)# interface fastEthernet 0/18
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 20
S3(config-if)# end
```

- **Dynamisches VLAN.** Diese Option wird in Produktionsnetzwerken relativ selten verwendet und in diesem Buch auch nicht ausführlich behandelt. Allerdings ist es durchaus sinnvoll zu wissen, was ein dynamisches VLAN ist. Dieser Mitgliedschaftstyp wird mithilfe eines speziellen Servers – des VMPS (VLAN Membership Policy Server) – konfiguriert. Mit dem VMPS weisen Sie Switch-Ports basierend auf der Absender-MAC-Adresse des an den Port angeschlossenen Geräts dem VLAN dynamisch zu. Der Nutzen wird deutlich, wenn ein Host seinen Anschluss von einem Port eines Switchs zu einem Port an einem anderen Switch im Netzwerk wechselt: Der neue Switch weist den neuen Port dynamisch dem korrekten VLAN für diese Hosts zu. Ein Beispiel für die Implementierung eines dynamischen VLAN zeigt Abbildung 3.16.

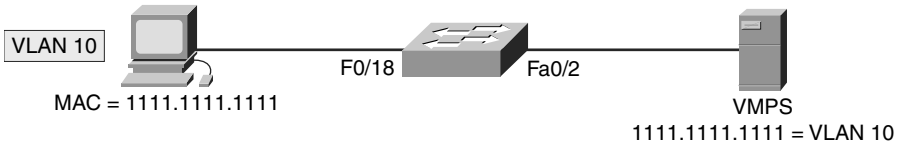

Abbildung 3.16: Dynamische VLANs

- **Sprach-VLANs.** Ein Port wird mit aktivierter Sprach-VLAN-Funktionalität konfiguriert, um an ihm ein angeschlossenes IP-Telefon zu betreiben. Um die Sprachunterstützung des Ports zu konfigurieren, müssen Sie je ein VLAN für Sprache und eines für Daten festlegen. In Listing 3.3 ist VLAN 150 das Sprach-VLAN und VLAN 20 das Daten-VLAN. Nehmen wir an, das Netzwerk sei so konfiguriert worden, dass Sprachdaten

bei der Übertragung Vorrang vor normalen Daten erhalten. Wenn nun ein Telefon an einen Switch mit Sprachunterstützung angeschlossen wird, sendet der Switch-Port Nachrichten an das Telefon und meldet ihm die festgelegte Sprach-VLAN-ID und die Konfiguration. Das IP-Telefon taggt die Sprach-Frames mit der Sprach-VLAN-ID und leitet alle Sprachdaten über das Sprach-VLAN weiter.

Listing 3.3: Sprach-VLAN konfigurieren

```
S3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)# interface fastEthernet 0/18
S3(config-if)# mls qos trust cos
S3(config-if)# switchport voice vlan 150
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 20
S3(config-if)# end
S3# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (VLAN0020)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (VLAN0150)
<Ausgabe unterdrückt>
```

Die Switch-Port-Konfiguration zur Unterstützung von Sprache und Daten hat die folgenden Eigenschaften:

- Der Konfigurationsbefehl `mls qos trust cos` stellt sicher, dass die Sprachdaten priorisiert werden. Denken Sie daran, dass diese Priorisierung im gesamten Netzwerk erfolgen muss; es reicht nicht aus, den Befehl nur auf dem einen Port zu konfigurieren.
- Der Befehl `switchport voice vlan 150` kennzeichnet VLAN 150 als Sprach-VLAN. Dies ist im Listing hervorgehoben: `Voice VLAN: 150 (VLAN0150)`.
- Der Befehl `switchport access vlan 20` konfiguriert VLAN 20 als Daten-VLAN. Dies ist im Listing hervorgehoben: `Access Mode VLAN: 20 (VLAN0020)`.

Weitere Informationen zu Konfiguration von VoIP-VLANs finden Sie auf der Cisco-Website unter *www.cisco.com/en/US/docs/switches/lan/catayst2960/software/release/12.2_46_se/configuration/guide/swvoip.html*.

3.1.8 Broadcast-Domänen mit VLANs steuern

In normalen Betrieb leitet ein Switch, der einen Broadcast-Frame auf einem seiner Ports empfängt, diesen über alle anderen Ports des Switchs weiter. In Abbildung 3.17 wird das gesamte Netzwerk im selben Subnetz (172.17.40.0/24) konfiguriert. Infolgedessen wird ein Broadcast-Frame, der vom Hochschulcomputer PC1 gesendet wird, von Switch S2 über alle Ports weitergeleitet. Schließlich wird der Frame vom gesamten Netzwerk empfangen, denn das Netzwerk ist eine große Broadcast-Domäne.

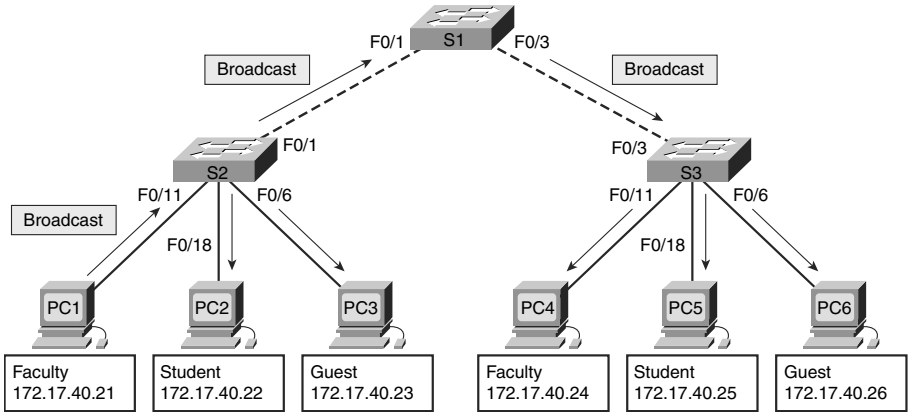

Abbildung 3.17: Einzelnes VLAN

In Abbildung 3.18 wurde das Netzwerk in zwei VLANs segmentiert: VLAN 10 (*Faculty*) und VLAN 20 (*Student*). Wird der Broadcast-Frame von PC1 an Switch S2 gesendet, dann leitet der Switch den Broadcast-Frame nur an diejenigen Switch-Ports weiter, die VLAN 10 unterstützen, da PC1 zu den Computern der Hochschuleinrichtung gehört. Diejenigen Ports in der Abbildung, die die Verbindung zwischen den Switches S2 und S1 bzw. S1 und S3 herstellen (Ports F0/1 bzw. F0/3), wurden für die Weiterleitung aller VLANs im Netzwerk konfiguriert. Eine solche Verbindung bezeichnet man als *Trunk*. Mehr zu Trunks erfahren Sie im weiteren Verlauf dieses Kapitels.

Wenn S1 den Broadcast-Frame auf Port F0/1 empfängt, leitet er ihn über den einzigen Port weiter, der als Mitglied von VLAN 10 konfiguriert ist: F0/3. Empfängt S1 den Broadcast-Frame auf Port F0/3, leitet er ihn über den einzigen Port weiter, der zur Unterstützung von VLAN 10 konfiguriert ist: F0/11. Der Broadcast-Frame landet dann bei PC4 – dem einzigen anderen Computer im Netzwerk, der in VLAN 10 konfiguriert ist.

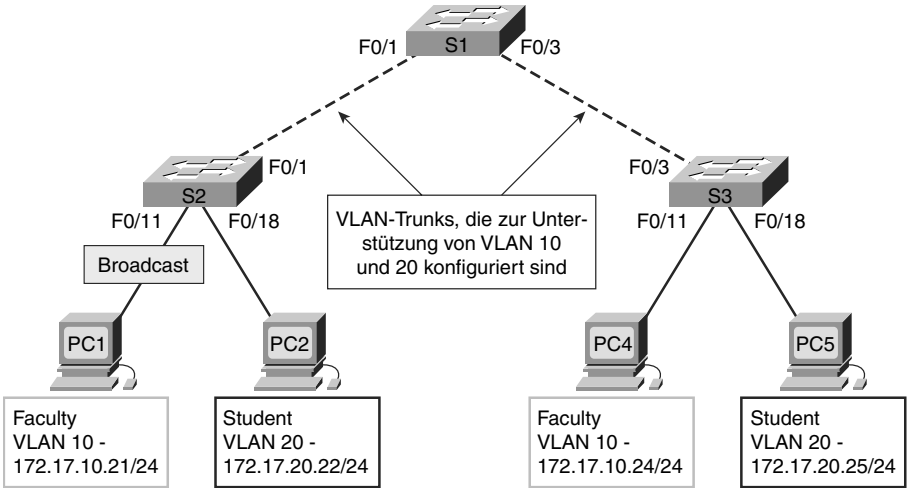

Abbildung 3.18: Zwei VLANs

Wenn VLANs auf einem Switch eingesetzt werden, ist die Übertragung von Unicast-, Multicast- und Broadcast-Daten von einem Host in einem bestimmten VLAN auf die Geräte in diesem VLAN beschränkt.

Die Unterteilung einer großen Broadcast-Domäne in mehrere kleinere Domänen verringert den Broadcast-Datenverkehr und steigert die Leistungsfähigkeit des Netzwerks. Zudem verbessert diese Unterteilung in VLANs den Schutz vertraulicher Daten innerhalb einer Organisation. Die Unterteilung von Broadcast-Domänen kann entweder mit VLANs (auf Switches) oder aber mit Routern erfolgen. Ein Router wird immer dann benötigt, wenn Geräte in verschiedenen Schicht-3-Netzwerken kommunizieren müssen – unabhängig davon, ob VLANs verwendet werden.

In Abbildung 3.19 will PC1 mit PC4 kommunizieren. Beide PCs befinden sich in VLAN 10.

Die Kommunikation mit einem Gerät im selben VLAN heißt VLAN-interne Kommunikation. Nachfolgend wird beschrieben, wie dieser Prozess abläuft:

1. PC1 in VLAN 10 sendet einen ARP-Anfrage-Frame als Broadcast an Switch S2. Switch S2 sendet die ARP-Anfrage über Port F0/1 weiter, Switch S1 über die Ports F0/5 und F0/3.

Anmerkung

Switch S1 ist über zwei Verbindungen mit dem Router verbunden: eine zur Übertragung in VLAN 10 und eine zweite zur Übertragung von Daten in VLAN 20.

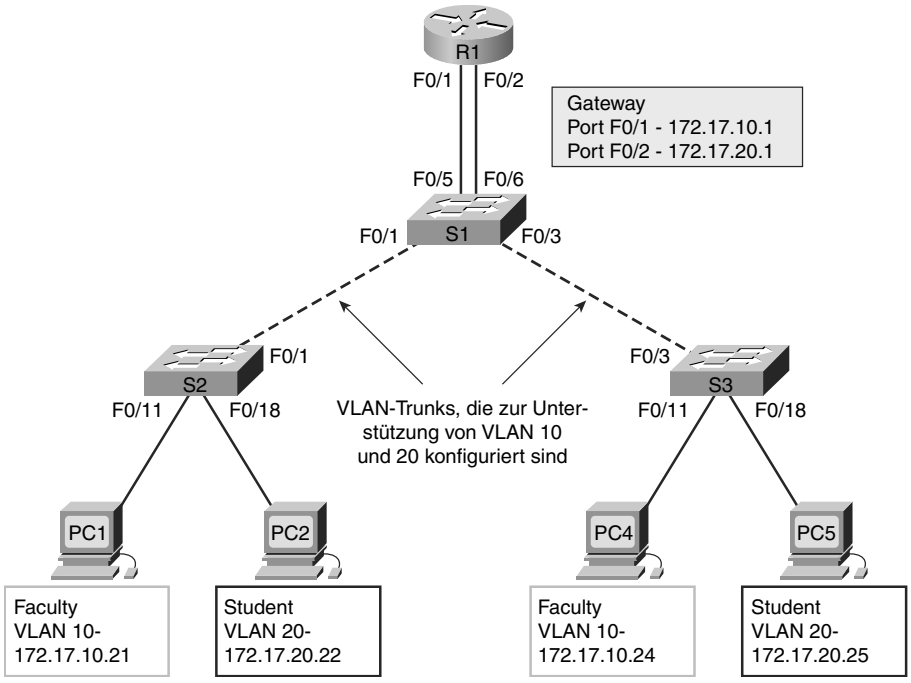

Abbildung 3.19: VLAN-interne Kommunikation

Switch S3 schließlich sendet die Anfrage über den Port F0/11 an PC4 in VLAN 10 weiter.

2. PC4 sendet eine ARP-Antwort an Switch S3, der sie über den Port F0/3 an Switch S1 weiterleitet (der Router R1 antwortet nicht). Switch S1 leitet die Antwort über den Port F0/1 weiter, Switch S2 über den Port F0/11. PC1 erhält die Antwort, die die MAC-Adresse von PC4 enthält.
3. PC1 kennt nun die Ziel-MAC-Adresse von PC4 und erstellt auf dieser Basis einen Unicast-Frame mit der MAC-Adresse von PC4 als Empfängeradresse. Die Switches S2, S1 und S3 leiten den Frame an PC4 weiter.

Ebenfalls in Abbildung 3.19 möchte PC1 in VLAN 10 mit PC5 in VLAN 20 kommunizieren. Die Kommunikation mit einem Gerät in einem anderen VLAN heißt VLAN-übergreifende Kommunikation.

Nachfolgend wird beschrieben, wie dieser Prozess abläuft:

1. PC1 in VLAN 10 möchte mit PC5 in VLAN 20 kommunizieren. Also sendet PC1 einen ARP-Anfrage-Frame für die MAC-Adresse des Default-Gateways R1.
2. Router R1 schickt eine ARP-Antwort über seine in VLAN 10 konfigurierte Schnittstelle zurück. Diese Antwort gelangt über S1 und S2 zu PC1.

3. PC1 erstellt nun einen Ethernet-Frame mit der MAC-Adresse des Default-Gateways. Dieser Frame wird über die Switches S2 und S1 zum Router R1 gesendet.
4. Router R1 sendet einen ARP-Anfrage-Frame in VLAN 20, um die MAC-Adresse von PC5 zu ermitteln. Die Switches S1, S2 und S3 senden die ARP-Anfrage als Broadcast über alle Ports, die in VLAN 20 konfiguriert sind. PC5 in VLAN 20 empfängt den ARP-Anfrage-Frame von Router R1.
5. PC5 in VLAN 20 sendet eine ARP-Antwort über die Switches S3 und S1 an den Router R1 mit der Ziel-MAC-Adresse der Schnittstelle F0/2 auf Router R1.
6. Router R1 sendet den von PC1 erhaltenen Frame über S1 und S3 an PC5 (in VLAN 20).

Als Nächstes wollen wir uns das Schicht-3-Switching ansehen. Abbildung 3.20 zeigt den Catalyst 3750G-24PS-Switch, einen von vielen Cisco Catalyst-Switches, die das Schicht-3-Switching beherrschen. Dargestellt ist auch das Symbol für einen Schicht-3-Switch. Eine vollständige Abhandlung zum Schicht-3-Switching ist nicht Gegenstand dieses Buches, doch ist eine kurze Beschreibung der SVI-Technologie (Switch Virtual Interface), die einem Schicht-3-Switch das VLAN-übergreifende Routing ermöglicht, durchaus sinnvoll.

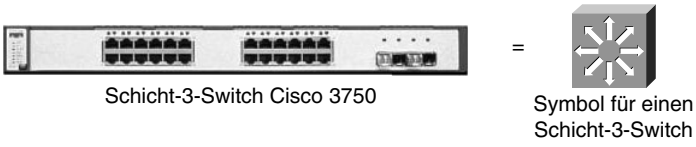

Abbildung 3.20: Schicht-3-Switch

Ein SVI ist eine logische Schicht-3-Schnittstelle, die einem bestimmten VLAN zugeordnet ist. Sie müssen ein SVI für ein VLAN konfigurieren, wenn Sie zwischen VLANs routen oder dem Switch IP-Hostkonnektivität ermöglichen wollen. Standardmäßig wird auf einem Catalyst-Switch ein SVI für VLAN 1 erstellt.

Ein Schicht-3-Switch bietet die Möglichkeit, Übertragungen VLAN-übergreifend zu routen. Die Vorgehensweise entspricht der für die VLAN-übergreifende Kommunikation mit einem separaten Router, nur agieren die SVIs als Router-Schnittstellen zum Routen der Daten zwischen den VLANs. Abbildung 3.21 zeigt den Prozess der VLAN-übergreifenden Kommunikation mithilfe von SVIs.

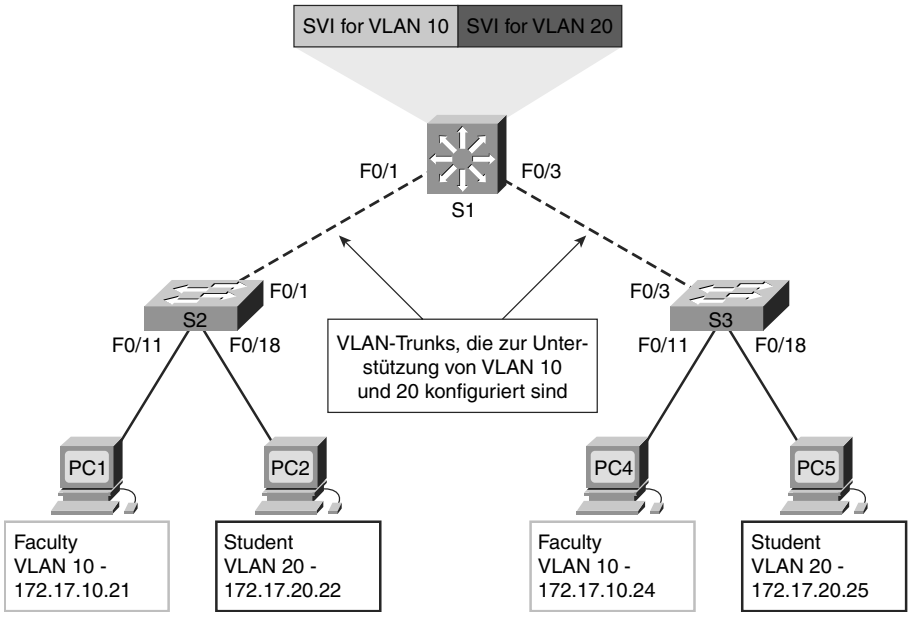

Abbildung 3.21: VLAN-übergreifende Kommunikation mit SVIs

In der Abbildung möchte PC1 mit PC5 kommunizieren. Die folgenden Schritte zeigen die Kommunikation über den Schicht-3-Switch S1:

1. PC1 sendet eine ARP-Anfrage als Broadcast in VLAN 10. S2 leitet die ARP-Anfrage über alle Ports weiter, die für VLAN 10 konfiguriert sind.
2. Switch S1 leitet die ARP-Anfrage über alle Ports weiter, die für VLAN 10 konfiguriert sind; dies betrifft auch das SVI für VLAN 10. Der Switch S3 leitet die ARP-Anfrage über alle Ports weiter, die für VLAN 10 konfiguriert sind.
3. Switch S1 kennt die Position von VLAN 20, da es sich um das direkt angeschlossene Schicht-3-Netzwerk von SVI 20 handelt. Das SVI für VLAN 10 auf dem Switch S1 sendet eine ARP-Antwort zurück an PC1, die seine MAC-Adressangaben enthält.
4. PC1 sendet für PC5 vorgesehene Daten als Unicast-Frame über den Switch S2 an das SVI für VLAN 10 auf den Switch S1.
5. Das SVI für VLAN 20 sendet eine ARP-Anfrage als Broadcast über alle Switch-Ports, die für VLAN 20 konfiguriert sind. Der Switch S3 sendet diesen ARP-Anfrage-Broadcast über alle Ports weiter, die für VLAN 20 konfiguriert sind.
6. PC5 in VLAN 20 sendet eine ARP-Antwort an das SVI für VLAN 20 auf S1.

7. Das SVI für VLAN 20 leitet die von PC1 gesendeten Daten als Unicast-Frame an PC5 weiter und verwendet hierzu die Zieladresse, die es der ARP-Antwort in Schritt 6 entnommen hat.

VLAN-Implementierung untersuchen (3.1.4)

Packet Tracer
Aktivität

In dieser Packet Tracer-Aktivität beobachten Sie, wie Broadcast-Daten von Switches weitergeleitet werden, wenn VLANs konfiguriert bzw. nicht konfiguriert wurden. Zur Durchführung der Aktivität verwenden Sie Packet Tracer und die Datei *e3-3144.pka* auf der Begleit-CD-ROM zu diesem Buch.

3.2 VLAN-Trunking

VLANs und VLAN-Trunks sind untrennbar miteinander verbunden. VLANs in einem modernen geswitchten LAN wären ohne Trunks praktisch nutzlos. Wir wissen, dass VLANs Netzwerk-Broadcasts filtern und dass VLAN-Trunks Daten in verschiedene Teile des Netzwerks innerhalb eines gegebenen VLAN übertragen. In Abbildung 3.22 sind die Verbindungen zwischen den Switches S1 und S2 sowie S1 und S3 so konfiguriert, dass sie Daten aus den VLANs 10, 20, 30 und 99 übertragen. Dieses Netzwerk würde ohne VLAN-Trunks schlichtweg nicht funktionieren. Sie werden feststellen, dass die meisten Netzwerke, auf die Sie stoßen, mit VLAN-Trunks konfiguriert sind. In diesem Abschnitt wollen wir Ihr bereits vorhandenes Wissen zum VLAN-Trunking zusammenfassen und uns mit den Details vertraut machen, die für ein umfassendes Verständnis der Rolle von Trunks in einem geswitchten LAN unentbehrlich sind.

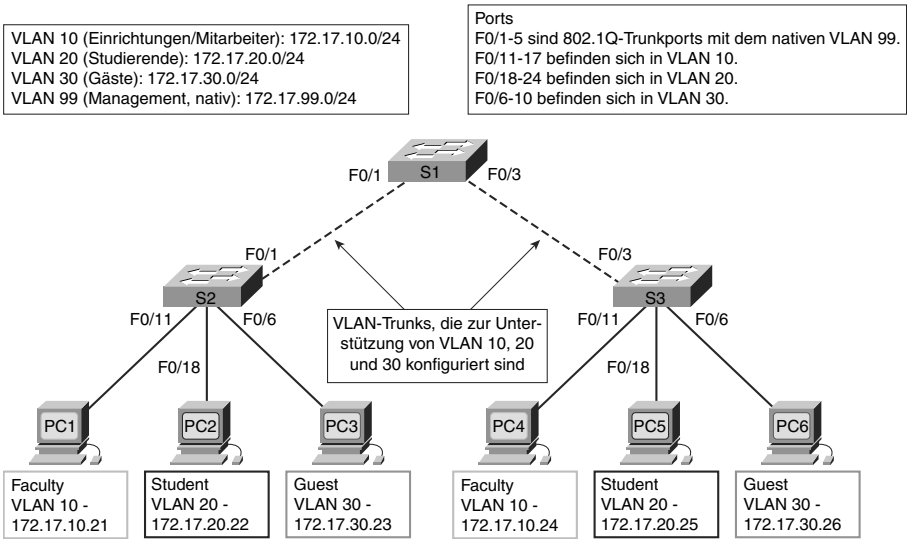

Abbildung 3.22: VLAN-Trunking

3.2.1 VLAN-Trunks

Ein VLAN-Trunk ist eine Point-to-Point-Ethernet-Verbindung zwischen einer Schnittstelle eines Ethernet-Switchs und der Ethernet-Schnittstelle eines anderen Netzwerkgeräts – d. h. eines Routers oder Switchs –, über die Daten mehrerer VLANs gemeinsam übertragen werden. Ein Trunk erlaubt die Ausbreitung von VLANs über das gesamte Netzwerk. Cisco-Switches unterstützen IEEE 802.1Q zur Bildung von Trunks an Fast Ethernet- und Gigabit-Ethernet-Schnittstellen. Mehr zu IEEE 802.1Q erfahren Sie im weiteren Verlauf dieses Abschnitts. Ein VLAN-Trunk gehört keinem bestimmten VLAN an, sondern dient eher als Kanal für mehrere VLANs zwischen Switches.

In Abbildung 3.23 sehen Sie die in diesem Kapitel zugrunde gelegte Standardtopologie, wobei hier allerdings statt des VLAN-Trunks, der sich sonst immer zwischen den Switches S1 und S2 befindet, für jedes Subnetz eine eigene Verbindung vorhanden ist. Die Switches S1 und S2 sind also über vier getrennte Leitungen miteinander verbunden, weswegen drei Ports weniger zur Zuweisung an Endgeräte übrig bleiben. Jedes Mal, wenn ein neues Subnetz benötigt wird, muss eine neue Leitung zwischen allen Switches im Netzwerk verlegt werden.

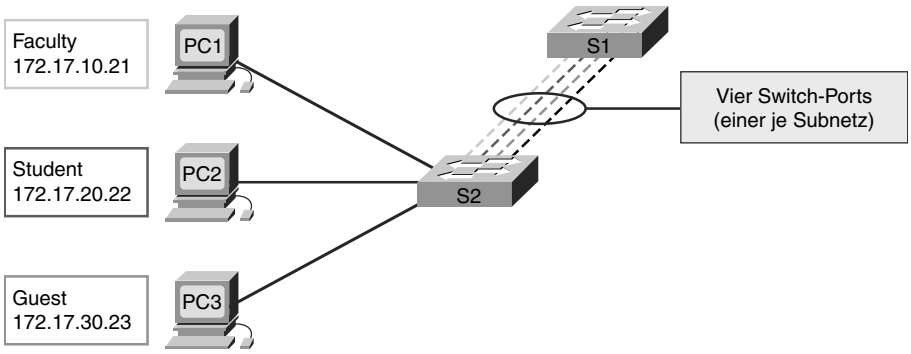

Abbildung 3.23: Keine VLAN-Trunks

In Abbildung 3.24 zeigt die Netzwerktopologie einen VLAN-Trunk, der die Switches S1 und S2 über eine einzige physische Leitung miteinander verbindet. So sollte ein Netzwerk konfiguriert werden: Die vier separaten Leitungen aus Abbildung 3.23 wurden durch eine einzige Trunk-Leitung verbunden.

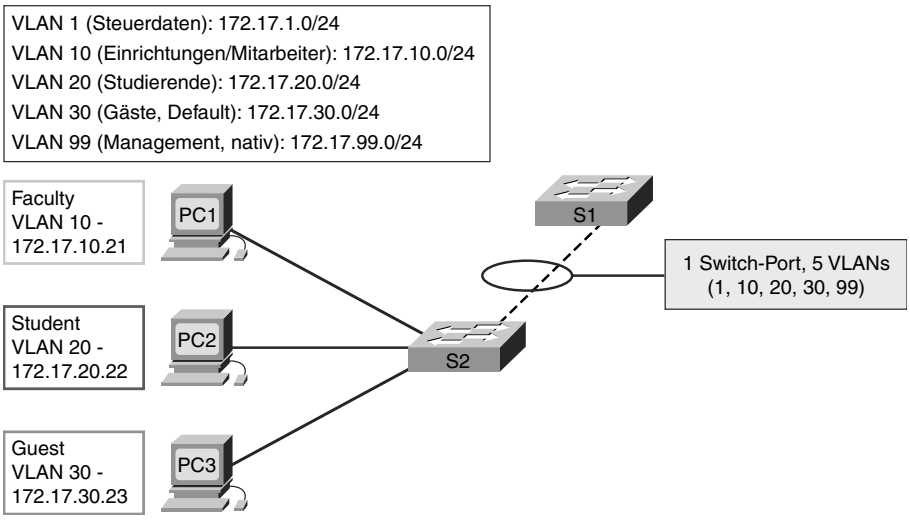

Abbildung 3.24: Mit implementierten VLAN-Trunks

Frame-Tagging nach IEEE 802.1Q

Access-Layer-Switches sind Schicht-2-Geräte. Sie verwenden also zur Frame-Weiterleitung nur die Informationen aus dem Ethernet-Frame-Header. Wenn ein von einem angeschlossenen Gerät stammender Ethernet-Frame von einem Access-Port empfangen wird, enthält dessen Header keine Angaben dazu, aus welchem VLAN der Frame stammt. Insofern müssen Ethernet-Frames, die in einen Trunk eingespeist werden, mit zusätzlichen Angaben zu den VLANs versehen werden, zu denen sie gehören. Dies wird mithilfe des 802.1Q-Frame-Taggings erledigt. Dieser Header fügt ein Tag zum ursprünglichen Ethernet-Frame hinzu, das das VLAN angibt, zu dem der Frame gehört.

Wir haben das Frame-Tagging weiter oben im Zusammenhang mit VoIP-Switch-Ports bereits vorgestellt. Dabei ging es um das Taggen von Sprach-Frames, um diese von Daten-Frames unterscheiden zu können, die an den an das IP-Telefon angeschlossenen Computer gerichtet sind. (Das IP-Telefon selbst war direkt mit dem Access-Port verbunden.) Sie wissen auch bereits, dass zwischen VLAN-IDs im normalen Bereich (1–1005) und solchen im erweiterten Bereich (1006–4094) unterschieden wird. Wie aber fügt man VLAN-IDs in einen Ethernet-Frame ein?

Bevor wir uns den Einzelheiten zu den Tag-Feldern nach IEEE 802.1Q widmen, wollen wir uns zunächst vergegenwärtigen, was ein Switch tut, wenn er einen Frame über eine Trunk-Verbindung weiterleitet. Grob gesagt, analysiert ein Switch, der einen an ein über eine Trunk-Verbindung erreichbares

Remote-Gerät gerichteten Frame auf einem im Access-Modus konfigurierten Port (statisches VLAN) empfängt, diesen Frame erst einmal und fügt ein VLAN-Tag ein. Dann berechnet er die FCS neu und sendet den getaggten Frame über den Trunk-Port weiter.

Das Tag-Feld umfasst ein EtherType-Feld und ein Feld mit Informationen zur Tag-Steuerung.

Das EtherType-Feld ist auf den Hexadezimalwert 0x8100 festgelegt. Dieser Wert heißt TPID (Tag Protocol ID). Wenn das EtherType-Feld auf den TPID-Wert gesetzt ist, weiß der empfangende Switch, dass er im Steuerdatenfeld nach entsprechenden Angaben suchen muss.

Dieses in Abbildung 3.25 gezeigte Feld umfasst die folgenden Angaben:

- **Benutzerpriorität (3 Bits).** Wird vom Standard IEEE 802.1p verwendet, der angibt, wie die beschleunigte Übertragung von Schicht-2-Frames erfolgt. Eine Beschreibung von IEEE 802.1p ist nicht Gegenstand dieses Buches, doch haben Sie bereits weiter oben bei der Erläuterung der Sprach-VLANs ein wenig dazu erfahren.
- **CFI (1 Bit).** CFI (Canonical Format Identifier) ermöglicht die unkomplizierte Übertragung von Token Ring-Frames über Ethernet-Leitungen.
- **VLAN-ID (12 Bits).** VLAN-IDs unterstützen bis zu 4096 VLANs.

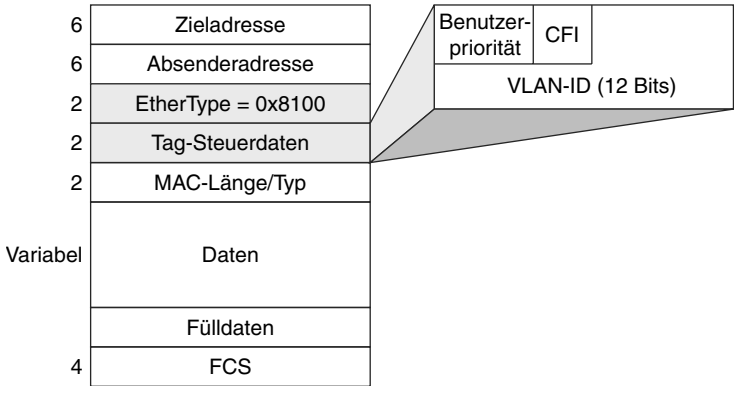

Abbildung 3.25: VLAN-Tag-Felder nach IEEE 802.1Q

Nachdem der Switch die EtherType- und Steuerinformationsfelder eingefügt hat, berechnet er die FCS-Werte neu und fügt diese in den Frame ein.

Native VLANs

Da Sie nun etwas mehr zu der Frage wissen, wie ein Switch einen Frame mit dem entsprechenden VLAN taggt, wollen wir uns ansehen, wie das native VLAN den Switch im Umgang mit getaggten und ungetaggten Frames unterstützt, die auf einem 802.1Q-Trunk-Port empfangen oder über diesen gesendet werden.

Einige Geräte anderer Hersteller, die auch das Trunking unterstützen, taggen native VLAN-Daten standardmäßig. Wenn ein 802.1Q-Trunk-Port einen getaggten Frame im nativen VLAN empfängt, verwirft er diesen. Das bedeutet, dass Sie, wenn Sie einen Switch-Port auf einem Catalyst-Switch konfigurieren, diese Geräte ermitteln und sie so konfigurieren müssen, dass sie keine getaggten Frames im nativen VLAN versenden. Geräte anderer Hersteller, die getaggte Frames im nativen VLAN unterstützen, sind etwa IP-Telefone, Server und Router sowie Nicht-Cisco-Switches.

Wenn ein Trunk-Port auf einem Cisco-Switch ungetaggte Frames empfängt, leitet er diese an das native VLAN weiter. Wie Sie wissen, ist das native VLAN standardmäßig VLAN 1. Wenn Sie einen 802.1Q-Trunk-Port konfigurieren, wird dem Port eine PVID (Port-VLAN-ID) entsprechend dem Wert der nativen VLAN-ID zugewiesen. Alle ungetaggten Daten, die auf dem 802.1Q-Port empfangen oder von dort gesendet werden, werden basierend auf dem PVID-Wert weitergeleitet. Wenn beispielsweise VLAN 99 als natives VLAN konfiguriert ist, lautet die PVID 99, und alle ungetaggten Daten werden an VLAN 99 weitergeleitet. Wurde hingegen das native VLAN nicht umkonfiguriert, wird der PVID-Wert auf VLAN 1 festgelegt.

In Tabelle 3.1 wird VLAN 99 als natives VLAN auf Port F0/1 von Switch S1 konfiguriert.

Tabelle 3.1: Nativen VLAN-Trunk konfigurieren

Beschreibung	Ein- und Ausgabe
Schaltet Switch S1 in den globalen Konfigurationsmodus.	`S1# configure terminal`
Wechselt in den Schnittstellenkonfigurationsmodus.	`S1(config)# interface f0/1`
Konfiguriert VLAN 99 für den Versand und Empfang ungetaggten Datenverkehrs auf dem Trunk-Port F0/1. Der Bereich für *vlan-id* liegt zwischen 1 und 4094.	`S1(config-if)# switchport trunk native vlan 99`
Kehrt zum privilegierten EXEC-Modus zurück.	`S1(config-if)# end`

Mit dem Befehl `show interfaces` *`interface-id`* `switchport` können Sie schnell kontrollieren, ob Sie das native VLAN korrekt von VLAN 1 auf VLAN 99 umgestellt haben. Aus den hervorgehobenen Passagen in Listing 3.4 geht hervor, dass die Konfiguration erfolgreich war.

Listing 3.4: Sprach-VLAN konfigurieren

```
S1# show interfaces F0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 50
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
<Ausgabe unterdrückt>
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
<Ausgabe unterdrückt>
Trunking VLANs Enabled: ALL
```

3.2.2 Trunking-Betrieb

Sie wissen nun, wie ein Switch ungetaggte Daten auf einer Trunk-Leitung behandelt: Frames auf einer solchen Leitung werden mit der VLAN-ID des Access-Ports getaggt, auf dem sie empfangen wurden, oder sie bleiben ungetaggt, sofern sie zum nativen VLAN gehören. In Abbildung 3.26 senden PC1 in VLAN 10 und PC3 in VLAN 30 Broadcast-Frames an den Switch S2. Switch S2 taggt diese Frames mit der entsprechenden VLAN-ID und leitet sie dann über den Trunk an den Switch S1 weiter. Switch S1 liest die VLAN-ID der Frames aus und sendet sie per Broadcast an die einzelnen Ports, die als Mitglied von VLAN 10 bzw. VLAN 30 konfiguriert sind. Der Switch S3 empfängt diese Frames, entfernt die VLAN-IDs und leitet die nun ungetaggten Frames an PC4 in VLAN 10 bzw. PC6 in VLAN 30 weiter.

3.2.3 Trunking-Modi

Sie wissen mittlerweile, wie das 802.1Q-Trunking auf Ports von Catalyst-Switches funktioniert. Nun ist es an der Zeit, die Konfigurationsschritte für den Trunk-Port-Modus zu untersuchen. Zunächst einmal werden wir ein älteres Trunking-Protokoll namens ISL (Inter-Switch Link) behandeln, da Sie in den Konfigurationshandbüchern zur Switch-Software auf diese Option stoßen werden und diese auch von allen aktuellen Catalyst-Switches mit Ausnahme der 29xx-Serie unterstützt wird.

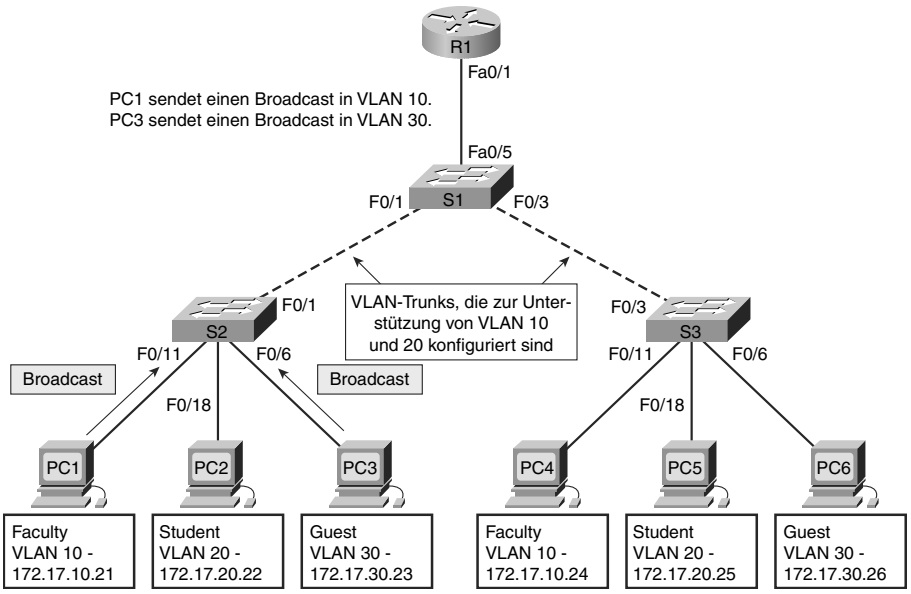

Abbildung 3.26: Trunking-Betrieb

Zwar lassen sich die meisten Cisco Catalyst-Switches so konfigurieren, dass sie zwei Arten von Trunk-Ports unterstützen (nämlich IEEE 802.1Q und ISL), doch wird in der Praxis heute nur noch IEEE 802.1Q eingesetzt. In älteren Netzwerken hingegen könnte ISL tatsächlich zum Einsatz kommen, und es ist durchaus sinnvoll, sich die einzelnen Trunk-Kapselungsoptionen zu vergegenwärtigen:

- Ein IEEE 802.1Q-Trunk-Port unterstützt gleichermaßen getaggte und ungetaggte Daten. Einem solchen Port wird eine Default-PVID zugewiesen, die dem gesamten ungetaggten Datenverkehr auf dem Port zugeordnet wird. Alle Daten mit einer Null-VLAN-ID werden als zur Default-PVID des Ports zugehörig betrachtet. Ein Paket mit einer VLAN-ID, die der Default-PVID des ausgehenden Ports entspricht, wird ungetaggt versendet. Der gesamte andere Datenverkehr wird mit einem VLAN-Tag übertragen.
- Bei ISL-Trunk-Ports wird erwartet, dass alle empfangenen Pakete in einen ISL-Header gekapselt sind, und alle gesendeten Pakete werden mit einem solchen Header versehen. Native (d. h. ungetaggte) Frames, die auf einem ISL-Trunk-Port empfangen werden, werden verworfen. ISL wird als Trunk-Port-Modus nicht mehr empfohlen und von einer Reihe von Cisco Catalyst-Switches bereits nicht mehr unterstützt.

DTP (Dynamic Trunking Protocol) ist ein proprietäres Cisco-Protokoll, das sowohl den Status als auch die Trunk-Kapselung von Trunk-Ports aushan-

delt. Switches anderer Anbieter unterstützen DTP nicht. DTP wird auf einem Switch-Port automatisch aktiviert, wenn bestimmte Trunking-Modi auf ihm konfiguriert sind. DTP steuert die Aushandlung des Trunks, wenn der Port auf dem anderen Switch mit einem Trunk-Modus konfiguriert ist, der DTP unterstützt. DTP unterstützt sowohl ISL- als auch 802.1Q-Trunks. Dieses Buch legt den Schwerpunkt auf die 802.1Q-Implementierung von DTP; eine ausführliche Abhandlung zu DTP würde seinen Rahmen sprengen. Switches müssen DTP nicht unterstützen, um Trunks zu aktivieren, und einige Cisco-Switches und -Router tun dies auch nicht.

Ein Switch-Port auf einem Catalyst-Switch unterstützt eine Reihe von Trunking-Modi. Ein solcher Modus definiert, wie der Port mithilfe von DTP Verhandlungen durchführt, um eine Trunk-Verbindung mit dem gegenüberliegenden Port herzustellen. Nachfolgend erhalten Sie eine kurze Beschreibung der vorhandenen Trunking-Modi und ihre jeweilige DTP-Implementierung.

- **Trunk (*On*).** Der Switch-Port sendet regelmäßig DTP-Frames – sogenannte *Advertisements* – an den Remote-Port. Der verwendete Befehl heißt `switchport mode trunk` und stellt die Default-Konfiguration dar. Der lokale Switch-Port zeigt dem Remote-Port an, dass er dynamisch in den Trunk-Status wechselt. Unmittelbar darauf schaltet der lokale Port unabhängig von den vom Remote-Port als Antwort auf das Advertisement gesendeten DTP-Angaben in den *Trunk*-Status um. Der lokale Port wird nun als in einem unbedingten *Trunk*-Status befindlich betrachtet (d. h. das Trunking ist immer aktiv).
- **Dynamic Auto.** Der Switch-Port sendet regelmäßig DTP-Frames an den Remote-Port. Der verwendete Befehl lautet `switchport mode dynamic auto`. Der lokale Switch-Port zeigt dem Remote-Port an, dass er das Trunking unterstützt, fordert aber keinen Wechsel in den *Trunk*-Status an. Nach einer DTP-Verhandlung wechselt der lokale Port nur dann in den Trunk-Status, wenn auf dem Remote-Port einer der Modi *On* oder *Desirable* konfiguriert wurde. Sind beide Ports auf den Switches auf *Dynamic Auto* festgelegt, dann handeln sie den Wechsel in einen *Trunk*-Status nicht aus, sondern einigen sich vielmehr, den *Access*-Status anzunehmen (der das Gegenteil des *Trunk*-Status ist).
- **Dynamic Desirable.** DTP-Frames werden regelmäßig an den Remote-Port gesendet. Der verwendete Befehl lautet `switchport mode dynamic desirable`. Der lokale Switch-Port zeigt dem Remote-Port an, dass er das Trunking unterstützt, und fordert den Wechsel in den *Trunk*-Status an. Wenn der lokale Port erkennt, dass der Remote-Port in einem der Modi *On*, *Desirable* oder *Auto* konfiguriert wurde, nimmt er selbst den *Trunk*-Status an. Befindet sich der Remote-Port im Modus *Nonegotiate*, so nutzt der lokale Port das Trunking nicht.

- **Nonegotiate.** Sie können DTP für den Trunk deaktivieren, damit der lokale Port keine DTP-Frames an den Remote-Port sendet. Hierzu verwenden Sie den Befehl `switchport nonegotiate`. Der lokale Port wird nun als in einem unbedingten Trunk-Status befindlich betrachtet. Verwenden Sie diese Funktion, wenn Sie einen Trunk mit dem Switch eines anderen Anbieters konfigurieren müssen.

Weitere Informationen zur DTP-Unterstützung auf Cisco-Switches finden Sie auf *http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a008017f86a.shtml*.

Betrachten Sie beispielsweise Abbildung 3.27, in der drei Catalyst 2960-Switches gezeigt sind. Für die Ports F0/1 der Switches S1 und S2 ist der Trunk-Modus *On* (`switchport mode trunk`) konfiguriert. Für die Ports F0/3 der Switches S1 und S2 ist der Trunk-Modus *Dynamic Auto* (`switchport mode dynamic auto`) konfiguriert. Welche Verbindungen werden nun zu aktiven Trunks, sobald die Switch-Konfiguration abgeschlossen ist?

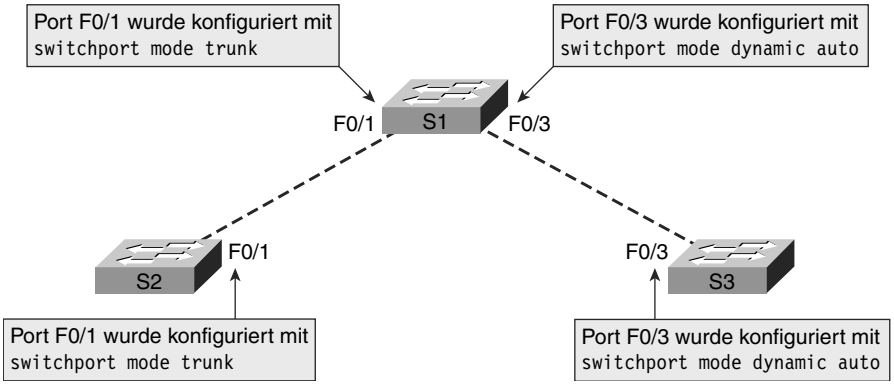

Abbildung 3.27: DTP

Die Verbindung zwischen den Switches S1 und S2 wird zu einem aktiven Trunk, weil die Ports F0/1 auf diesen Switches so konfiguriert sind, dass alle DTP-Advertisements ignoriert werden. Die Ports F0/3 auf den Switches S1 und S3 sind hingegen auf `auto` gesetzt; das Ergebnis ist eine inaktive Trunk-Verbindung, weil die Ports die Verwendung des *Access*-Modus aushandeln.

ANMERKUNG

Der Default-Modus für eine Schnittstelle auf einem Catalyst 2950 ist *Dynamic Desirable*, während bei einem Catalyst 2960 standardmäßig *Dynamic Auto* verwendet wird. Wären S1 und S3 Catalyst 2950-Switches mit der Schnittstelle F0/3 im Default-Modus für Switch-Ports, so würde die Verbindung zwischen S1 und S3 zu einem aktiven Trunk.

Tabelle 3.2 zeigt eine sehr praktische Übersicht, aus der die Ergebnisse des Trunking-Status basierend auf den verschiedenen DTP-Konfigurationsoptionen auf Catalyst 2960-Switches hervorgehen.

Tabelle 3.2: Kombinationen bei der Trunk-Aushandlung

	Dynamic Auto	**Dynamic Desirable**	**Trunk**	**Access**
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	nicht empfohlen
Access	Access	Access	nicht empfohlen	Access

Mit dem in IOS Release 12.2(37)EY auf dem Catalyst 2960 eingeführten Befehl `show dtp interface` bestimmen Sie im privilegierten EXEC-Modus die aktuellen Einstellungen.

Informationen zu Cisco-Switches, die 802.1Q, ISL und DTP unterstützen, finden Sie unter *www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a008017f86a.shtml#topic1*.

Hinweise zur Unterstützung von ISL in Netzwerken finden Sie unter *http://www.cisco.com/en/US/tech/tk389/tk689/tsd_technology_support_troubleshooting_technotes_list.html*.

Packet Tracer Aktivität

VLAN-Trunks untersuchen (3.2.3)

In dieser Packet Tracer-Aktivität üben Sie den Umgang mit VLAN-Trunks. Trunks übertragen die Daten mehrerer VLANs über eine einzelne Leitung und stellen so eine wichtige Komponente der Kommunikation zwischen Switches mit VLANs dar. Diese Aktivität legt den Schwerpunkt auf die Anzeige der Switch- und Trunk-Konfiguration sowie auf VLAN-Tagging-Informationen. Zur Durchführung der Aktivität verwenden Sie Packet Tracer und die Datei *e3-3232.pka* auf der Begleit-CD-ROM zu diesem Buch.

3.3 VLANs und Trunks konfigurieren

Wir haben in diesem Kapitel bereits einige Beispiele für Befehle gesehen, die zur Konfiguration von VLANs und VLAN-Trunks verwendet werden. In diesem Abschnitt lernen Sie die wichtigsten Cisco IOS-Befehle kennen, die zum Erstellen, Löschen und Überprüfen von VLANs und VLAN-Trunks benötigt werden. Häufig weisen diese Befehle zahlreiche optionale Parameter auf, die die Fähigkeiten von VLANs und VLAN-Trunks erweitern. Einige sehr spezielle Befehle sind nicht aufgeführt, doch erhalten Sie Verweise auf andere Quellen, falls Sie die entsprechenden Optionen kennenlernen wollen.

Schwerpunktmäßig soll dieser Abschnitt Ihnen die Fähigkeit vermitteln, VLANs und VLAN-Trunks mit ihren wichtigsten Funktionen sicher zu konfigurieren.

3.3.1 VLAN konfigurieren

In diesem Abschnitt beschreiben wir die Konfiguration statischer VLANs auf Cisco Catalyst-Switches. Zur Konfiguration von VLANs auf einem solchen Switch existieren zwei verschiedene Modi: der Datenbankkonfigurationsmodus und der globale Konfigurationsmodus. Den Datenbankkonfigurationsmodus für VLANs führt die Cisco-Dokumentation zwar noch auf, doch wurde er zugunsten des globalen VLAN-Konfigurationsmodus fallengelassen. Es ist naheliegend, dass der Datenbankkonfigurationsmodus in Kürze nicht mehr verfügbar sein wird; die Absicht dieses Wechsels besteht darin, das Switch-Betriebssystem in eine Richtung zu migrieren, die eher dem eines Cisco-Routers ähnelt. Im Laufe der Jahre wird die Trennung zwischen Cisco-Routern und Catalyst-Switches zunehmen unschärfer werden.

Sie werden VLANs mit IDs im normalen Bereich konfigurieren. Es gibt, wie Sie wissen, bei VLAN-IDs zwei Bereiche: den normalen Bereichen (1–1001) und den erweiterten (1006–4094). Die VLAN-IDs 1 sowie 1002 bis 1005 sind reserviert. Wenn Sie VLANs im normalen Bereich konfigurieren, werden die Konfigurationsangaben automatisch in einer Datei namens *vlan.dat* abgelegt, die sich im Flashspeicher des Switchs befindet. Weil Sie häufig andere Funktionen eines Catalyst-Switchs zur selben Zeit konfigurieren werden, wird empfohlen, Änderungen an der Datei *running-config* in die Datei *startup-config* zu speichern.

Tabelle 3.3 wiederholt die Cisco IOS-Befehle, mit denen ein VLAN einem Switch hinzugefügt wird.

Tabelle 3.3: VLAN hinzufügen

Beschreibung	Ein- und Ausgabe
Wechselt in den globalen Konfigurationsmodus.	`S1# configure terminal`
Erstellt ein VLAN. *vlan-id* ist die VLAN-Nummer, die erstellt werden soll. Das CLI schaltet dann in den VLAN-Konfigurationsmodus für das VLAN *vlan-id* um.	`S1(config)# vlan vlan-id`
Gibt einen eindeutigen VLAN-Namen zur Bezeichnung des VLAN an (optional). Wird kein Name angegeben, wird die Nummer des VLAN – aufgefüllt mit Nullen – an das Wort *VLAN* angehängt (z. B. `VLAN0020`).	`S1(config-vlan)# name vlan-name`

Tabelle 3.3: VLAN hinzufügen (Forts.)

Beschreibung	Ein- und Ausgabe
Kehrt zum privilegierten EXEC-Modus zurück. Sie müssen Ihre Konfigurationssitzung beenden, damit die Konfiguration in der Datei *vlan.dat* gespeichert und übernommen wird.	`S1(config-vlan)# end`

Abbildung 3.28 zeigt eine einfache Topologie, in der das VLAN *Student* (VLAN 20) auf Switch S1 konfiguriert wird.

Abbildung 3.28: Switch-Topologie für die VLAN-Konfiguration

Listing 3.5 zeigt die Befehle zum Hinzufügen von VLAN 20.

Listing 3.5: VLAN hinzufügen

```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```

Listing 3.6 veranschaulicht die Verwendung des Befehls `show vlan brief` zur Anzeige des Inhalts der Datei *vlan.dat*. Das VLAN *Student* (20) ist hervorgehoben. Auch die Default-VLANs 1 und 1002 bis 1005 sind in der Ausgabe enthalten. Beachten Sie, dass noch keine Ports für VLAN 20 konfiguriert sind.

Listing 3.6: Der Befehl »show vlan brief«

```
S1# show vlan brief

VLAN Name                              Status    Ports
---------------------------------------------------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
```

Listing 3.6: Der Befehl »show vlan brief« (Forts.)

```
20   student                          active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Die Schnittstelle F0/18 ist mit dem Computer des Studenten verbunden und muss zu VLAN 20 hinzugefügt werden. Listing 3.7 zeigt die Konfigurationsbefehle. Ein statischer Access-Port kann nur zu einem VLAN gleichzeitig gehören. Wenn VLAN 20 auf anderen Switches konfiguriert ist, konfiguriert der Switch-Administrator die anderen Computer der Studierenden in dasselbe Subnetz wie PC2: 172.17.20.0/24.

Listing 3.7: Statische VLAN-Schnittstelle konfigurieren

```
S1# configure terminal
S1(config)# interface f0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
```

Nachdem die Schnittstelle F0/18 zu VLAN 20 hinzugefügt wurde, ändert sich die Ausgabe von `show vlan brief` (Listing 3.8).

Listing 3.8: Der Befehl »show vlan brief« (geändert)

```
S1# show vlan brief

VLAN Name                             Status    Ports
---------------------------------------------------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
20   student                          active    Fa0/18
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

ANMERKUNG

Zusätzlich zur Eingabe einer einzelnen VLAN-ID können Sie mit dem Befehl `vlan vlan-id` auch eine kommagetrennte Folge dieser IDs oder – mit einem Bindestrich – einen VLAN-ID-Bereich angeben:

```
switch(config)# vlan 100,102,105-107
```

3.3.2 VLANs administrieren

Nachdem Sie ein VLAN konfiguriert haben, können Sie seine Konfiguration mit den `show`-Befehlen überprüfen, die das Cisco IOS bietet. Die Befehlssyntax für den Befehl `show vlan` lautet:

```
show vlan [brief | id vlan-id | name vlan-name | summary]
```

Tabelle 3.4 erläutert diese Syntax.

Tabelle 3.4: Syntax des Befehls »show vlan«

Erläuterung	Syntax
Zeigt eine Zeile pro VLAN an, die den Namen, den Status und die Ports des VLANs enthält.	`brief`
Zeigt Informationen zu einem einzelnen VLAN an, das durch die VLAN-ID identifiziert wird. Der Bereich für *vlan-id* liegt zwischen 1 und 4094.	`id` *vlan-id*
Zeigt Informationen zu einem einzelnen VLAN an, das durch den VLAN-Namen identifiziert wird. *vlan-name* ist ein ASCII-String mit 1 bis 32 Zeichen.	`name` *vlan-name*
Zeigt zusammenfassende VLAN-Informationen an.	`summary`

Die Befehlssyntax für `show interfaces switchport` lautet wie folgt:

```
show interfaces [interface-id | vlan vlan-id] | switchport
```

Tabelle 3.5 erläutert diese Syntax.

Tabelle 3.5: Syntax des Befehls »show interfaces switchport«

Erläuterung	Syntax
Gültige Schnittstellen sind physische Ports (einschließlich Typ, Modul und Portnummer) sowie Portkanäle. Der Bereich liegt zwischen 1 und 6.	*interface-id*
VLAN-ID. Der Wertebereich liegt zwischen 1 und 4094.	`vlan` *vlan-id*
Zeigt den Administrations- und Betriebsstatus eines Switch-Ports einschließlich der Einstellungen für Portsperre und Portschutz an.	`switchport`

In Listing 3.9 sehen Sie, dass der Befehl `show vlan name student` keine klar unterscheidbare Ausgabe generiert. Sie sollten hier also besser den Befehl `show vlan brief` (Listing 3.8) verwenden.

Listing 3.9: Ausgabe von »show vlan name«

```
S1# show vlan name student

VLAN Name                              Status    Ports
---------------------------------------------------------------------------
20   student                           active    Fa0/18

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

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type            Ports
---------------------------------------------------------------------------
```

Die Ausgabe von `show vlan summary` (Listing 3.10) zeigt die Anzahl aller konfigurierten VLANs an. Enthalten sind hier sechs VLANs: 1, 1002–1005 und das Studierenden-VLAN 20.

Listing 3.10: Ausgabe von »show vlan summary«

```
S1# show vlan summary
Number of existing VLANs              : 6
Number of existing VTP VLANs          : 6
Number of existing extended VLANs     : 0
```

Der Befehl `show interfaces vlan 20` führt Details auf, die den Rahmen dieses Kapitels sprengen würden. Die wichtigsten Angaben erscheinen in der zweiten Zeile der Ausgabe in Listing 3.11 und zeigen an, dass das VLAN aktiv und betriebsbereit ist.

Listing 3.11: Ausgabe des Befehls »show interfaces«

```
S1# show interfaces vlan 20
Vlan20 is up, line protocol is up
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia 001c.573c.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
```

Listing 3.11: Ausgabe des Befehls »show interfaces« (Forts.)

```
  Last input never, output never, 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
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Der Befehl `show interfaces switchport` ist einer der nützlichsten, die es auf einem Catalyst-Switch gibt. Er zeigt relevante Informationen zu der oder den referenzierten Schnittstellen. In Listing 3.12 sehen Sie, dass die Schnittstelle F0/18 VLAN 20 zugewiesen und VLAN 1 das native VLAN ist. Wir haben diesen Befehl bereits früher im Zusammenhang mit Sprach-VLANs verwendet.

Listing 3.12: Ausgabe des Befehls »show interfaces switchport«

```
S1# show interfaces f0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association:10 (VLAN0010) 502 (VLAN0502)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk native VLAN tagging: enabled
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: ALL
Pruning VLANs Enabled: 2-1001
```

Listing 3.12: Ausgabe des Befehls »show interfaces switchport« (Forts.)

```
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Weitere Informationen zu den Feldern in der Ausgabe der Befehle `show vlan` und `show interfaces` finden Sie unter *http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_fx/command/reference/cli2.html*.

VLAN-Mitgliedschaften administrieren

Sie können VLANs und VLAN-Port-Mitgliedschaften auf vielerlei Weise administrieren. Tabelle 3.6 erläutert die Befehle zum Entfernen einer VLAN-Mitgliedschaft.

Tabelle 3.6: VLAN-Mitgliedschaften administrieren

Beschreibung	Ein- und Ausgabe
Wechselt in den globalen Konfigurationsmodus.	`S1# configure terminal`
Wechselt in den Schnittstellenkonfigurationsmodus für die zu konfigurierende Schnittstelle.	`S1(config)# interface` *interface-id*
Entfernt die VLAN-Zuordnung zum Switch-Port und stellt die Default-Mitgliedschaft in VLAN 1 wieder her.	`S1(config-if)# no switchport access vlan`
Kehrt zum privilegierten EXEC-Modus zurück.	`S1(config-if)# end`

Um VLAN 1 einen Port wieder zuzuweisen, verwenden Sie den Befehl `no switchport access vlan` im Schnittstellenkonfigurationsmodus. Nachdem Sie diesen Befehl eingegeben haben, untersuchen Sie die Ausgabe von `show vlan brief` in Listing 3.13. Beachten Sie, das VLAN 20 nach wie vor aktiv ist. Es wurde lediglich F0/18 aus VLAN 20 entfernt. Der Befehl `show interfaces f0/18 switchport` zeigt, dass das Access-VLAN für die Schnittstelle F0/18 auf VLAN 1 zurückgesetzt wurde.

Listing 3.13: Port VLAN 1 neu zuweisen

```
S1(config)# interface f0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show vlan brief
```

Listing 3.13: Port VLAN 1 neu zuweisen (Forts.)

```
VLAN Name                              Status    Ports
---------------------------------------------------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
20   student                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
S1# show interfaces f0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
<Ausgabe unterdrückt>
```

Ein statischer Access-Port kann nur einem VLAN zugeordnet werden. Beim Cisco IOS müssen Sie einen Port nicht zunächst aus einem VLAN entfernen, um seine VLAN-Mitgliedschaft zu ändern. Wenn Sie einen statischen Access-Port einem vorhandenen VLAN zuweisen, wird dieser Port automatisch aus dem vorherigen VLAN entfernt. In Listing 3.14 wird Port F0/11 VLAN 20 neu zugeordnet.

Listing 3.14: Port VLAN 20 neu zuweisen

```
S1# show vlan brief

VLAN Name                              Status    Ports
---------------------------------------------------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
```

Listing 3.14: Port VLAN 20 neu zuweisen (Forts.)

```
20   student                          active    Fa0/11
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Listing 3.15 veranschaulicht das Löschen eines VLAN mit dem globalen Konfigurationsbefehl `no vlan` *`vlan-id`*. Der Befehl `show vlan brief` zeigt, dass VLAN 20 nicht mehr in der Datei *vlan.dat* enthalten ist.

Listing 3.15: VLAN löschen

```
S1# no vlan 20
S1# show vlan brief

VLAN Name                             Status    Ports
---------------------------------------------------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Alternativ lässt sich die gesamte Datei *vlan.dat* mit dem Befehl `delete flash:vlan.dat` im privilegierten EXEC-Modus löschen. Wenn der Switch neu geladen wurde, sind die zuvor konfigurierten VLANs dann nicht mehr vorhanden. Auf diese Weise lässt sich die VLAN-Konfiguration des Switchs quasi in den Werkszustand zurückversetzen.

ANMERKUNG

Bevor Sie ein VLAN löschen, sollten Sie in jedem Fall alle Mitgliedsports einem anderen VLAN zuweisen. Ports, die nicht aus einem aktiven VLAN entfernt werden, bleiben Mitglieder des gelöschten inaktiven VLAN und können nicht mehr mit anderen Systemen kommunizieren, nachdem Sie das VLAN gelöscht haben.

3.3.3 Trunk konfigurieren

Um einen Trunk auf einem Switch-Port zu konfigurieren, verwenden Sie den Befehl `switchport mode trunk`. Wenn Sie diesen Befehl für einen Switch-Port eingeben, wechselt die Schnittstelle in den permanenten Trunking-Modus, und der Port leitet eine DTP-Aushandlung ein, um die Leitung in einen Trunk zu konvertieren, selbst wenn die gegenüberliegende Schnittstelle dieser Umstellung nicht zustimmt. In diesem Buch konfigurieren Sie einen Trunk mit dem Befehl `switchport mode trunk`. Die Cisco IOS-Befehlssyntax zur Angabe eines anderen nativen VLAN als VLAN 1 ist ebenfalls in Tabelle 3.7 gezeigt.

Tabelle 3.7: IEEE 802.1Q-Trunk konfigurieren

Beschreibung	Ein- und Ausgabe
Wechselt in den globalen Konfigurationsmodus.	`S1# configure terminal`
Wechselt in den Schnittstellenkonfigurationsmodus für die definierte Schnittstelle.	`S1(config)# interface` *`interface-id`*
Erzwingt die Umstellung der Leitung, die die Switches miteinander verbindet, zu einem Trunk.	`S1(config-if)# switchport mode trunk`
Gibt ein anderes VLAN als natives VLAN für ungetaggte Frames bei IEEE 802.1Q-Trunks an.	`S1(config-if)# switchport trunk native vlan` *`vlan-id`*
Fügt die VLANs hinzu, die auf diesem Trunk zugelassen sind.	`S1(config-if)# switchport trunk allowed vlan add vlan-list`
Kehrt zum privilegierten EXEC-Modus zurück.	`S1(config-if)# end`

Betrachten Sie Abbildung 3.29. Die VLANs 10, 20 und 30 enthalten die Computer *Faculty*, *Student* und *Guest* (PC1, PC2 und PC3). Der Port F0/1 auf Switch S1 wird als Trunk-Port ausschließlich für die VLANs 1, 10, 20 und 30 konfiguriert. (Zur Erinnerung: VLAN 1 wird in jedem Fall auf einer Trunk-Leitung unterstützt, da alle Steuerdaten in VLAN 1 transportiert werden.) VLAN 99 wird als natives VLAN konfiguriert.

Listing 3.16 zeigt die Konfiguration von Switch S1. Port F0/1 wird als Trunk-Port konfiguriert. Das native VLAN wird von VLAN 1 auf VLAN 99 umkonfiguriert und gemeinsam mit den VLANs 10, 20 und 30 auf den Port F0/1 gelegt.

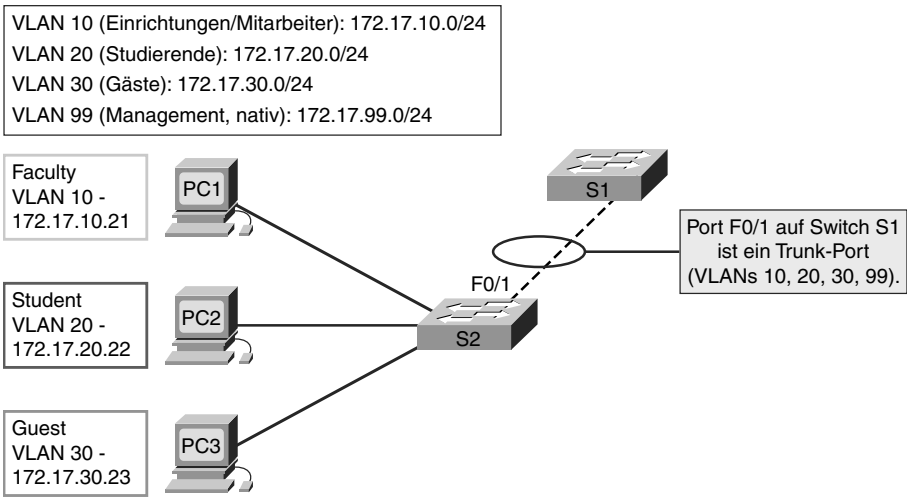

Abbildung 3.29: Trunk-Leitung aktivieren

Listing 3.16: Eingeschränkte Trunk-Leitung aktivieren

```
S1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan add 10,20,30
S1(config-if)# end
```

Zusätzliche Informationen zu allen Parametern des Schnittstellenbefehls `switchport mode` finden Sie auf *http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_37_se/command/reference/cli3.html#wp1948171*.

Listing 3.17 zeigt den Administrations- und Betriebszustand von Switch-Port F0/1 auf dem Switch S1. Der verwendete Befehl heißt `show interfaces` *`interface-ID`* `switchport`.

Listing 3.17: Trunk-Konfiguration überprüfen

```
S1#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management)
```

Listing 3.17: Trunk-Konfiguration überprüfen (Forts.)

```
Administrative Native VLAN tagging: enabled
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 Native VLAN tagging: enabled
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: 10,20,30
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
<Ausgabe unterdrückt>
```

Der erste hervorgehobene Bereich zeigt, das *Trunk* als administrativer Modus für Port F0/1 festgelegt ist, das heißt, der Port bildet in jedem Fall unabhängig von der Konfiguration der gegenüberliegenden Schnittstelle einen Trunk. Die nächste Hervorhebung zeigt, dass VLAN 99 als natives VLAN ausgewählt ist. Laut dem letzten hervorgehobenem Bereich schließlich sind die VLANs 10, 20 und 30 die aktivierten Trunking-VLANs.

Tabelle 3.8 stellt die Befehle da, mit denen sich die zugelassenen VLANs und das native VLAN des Trunks in den Default-Zustand zurückversetzen lassen. Der Befehl zum Zurücksetzen des Switch-Ports auf einen Access-Port und zum Entfernen des Trunks wird ebenfalls gezeigt.

Tabelle 3.8: IEEE 802.1Q-Trunk bearbeiten

Beschreibung	Ein- und Ausgabe
Verwenden Sie diesen Befehl im Schnittstellenkonfigurationsmodus, um alle auf der Trunk-Schnittstelle konfigurierten VLANs zurückzusetzen.	`S1(config-if)# no switchport trunk allowed vlan`
Verwenden Sie diesen Befehl im Schnittstellenkonfigurationsmodus, um das native VLAN auf VLAN 1 zurückzusetzen.	`S1(config-if)# no switchport trunk native vlan`
Verwenden Sie diesen Befehl im Schnittstellenkonfigurationsmodus, um den Trunk-Port auf einen statischen Access-Port zurückzusetzen.	`S1(config-if)# switchport mode access`

Listing 3.18 zeigt die Befehle, mit denen alle Trunking-Merkmale einer Trunking-Schnittstelle auf die Voreinstellungen zurückgesetzt werden. Der Befehl `show interfaces f0/1 switchport` zeigt, dass für den Trunk der Default-Status wiederhergestellt wurde.

Listing 3.18: Trunk zurücksetzen

```
S1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<Ausgabe unterdrückt>
Trunking VLANs Enabled: ALL
```

Die Ausgabe von Listing 3.19 schließlich enthält die Befehle, mit denen der Trunk vom Switch-Port F0/1 auf Switch S1 entfernt wird. Der Befehl `show interfaces f0/1 switchport` zeigt, dass sich die Schnittstelle nun wieder im statischen Access-Modus befindet.

Listing 3.19: Trunk entfernen

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operatioss Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
<Ausgabe unterdrückt>
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Packet Tracer Aktivität

VLANs und Trunks konfigurieren (3.3.4)

In dieser Packet Tracer-Aktivität erweitern Sie Ihre Kenntnisse in Bezug auf die Konfiguration von VLANs und VLAN-Trunks. VLANs sind bei der Administration logischer Gruppen sehr hilfreich, denn sie ermöglichen das einfache Verschieben, Ändern und Hinzufügen von Gruppenmitgliedern. Diese Aktivität legt den Schwerpunkt auf das Erstellen und Benennen von VLANs, das Hinzufügen von Access-Ports zu bestimmten VLANs, das Ändern des nativen VLAN und das Konfigurieren von Trunk-Leitungen. Zur Durchführung der Aktivität verwenden Sie Packet Tracer und die Datei *e3-3344.pka* auf der Begleit-CD-ROM zu diesem Buch.

3.4 Troubleshooting bei VLANs und Trunks

Häufige Probleme bei VLANs und Trunking stehen gewöhnlich mit einer falschen Konfiguration in Verbindung. Wenn Sie VLANs und Trunks in einer geswitchten Infrastruktur konfigurieren, treten diese Konfigurationsfehler (in absteigender Reihenfolge der Häufigkeit) wie folgt auf:

- **Fehlanpassung des nativen VLANs.** Trunk-Ports werden in unterschiedlichen nativen VLANs konfiguriert. Beispielsweise könnte für einen Port VLAN 99, für einen anderen jedoch VLAN 100 als natives VLAN konfiguriert worden sein. Dieser Konfigurationsfehler erzeugt Benachrichtigungen auf der Konsole, bewirkt eine fehlerhafte Weiterleitung von Steuer- und Administrationsdaten und stellt zudem ein Sicherheitsrisiko dar.
- **Ungleiche Trunk-Modi.** So könnte etwa ein Trunk-Port mit dem Modus *Off* und der andere mit dem Modus *On* konfiguriert worden sein. Dieser Fehler hat zur Folge, dass die Trunk-Leitung nicht mehr funktioniert.
- **IP-Subnetze und VLANs.** Unter Umständen wurden auf Benutzercomputern falsche IP-Adressen, Subnetzmasken oder Default-Gateways konfiguriert. Folge ist ein Konnektivitätsverlust.
- **Zugelassene VLANs auf Trunks.** Die Liste der auf einem Trunk zugelassenen VLANs wurde nicht anhand der Trunking-Anforderungen des aktuellen VLAN angepasst. In dieser Situation werden unvorhersehbare oder aber gar keine Daten über den Trunk gesendet.

Wenn Sie ein Problem mit einem VLAN oder Trunk feststellen und nicht wissen, worin dieses besteht, beginnen Sie das Troubleshooting, indem Sie die Trunks auf falsch angegebene VLANs hin überprüfen und dann die Liste weiter nach unten abarbeiten. Die verbleibenden Abschnitte dieses Kapitels untersuchen, wie sich bei Trunks häufig auftretende Probleme beheben lassen.

3.4.1 Häufige Probleme bei Trunks

Betrachten Sie Abbildung 3.30. Sie sind Netzwerkadministrator und erhalten einen Anruf vom Benutzer des Computers PC4, der keine Verbindung mit dem internen Webserver – dem Web-/TFTP-Server – herstellen kann. Bei Ihren Nachforschungen stellen Sie fest, dass ein neuer Netzwerktechniker unlängst Switch S3 konfiguriert hat. Das Topologiediagramm scheint korrekt. Warum also kommt es zu Problemen? Sie beschließen, die Konfiguration von S3 zu überprüfen.

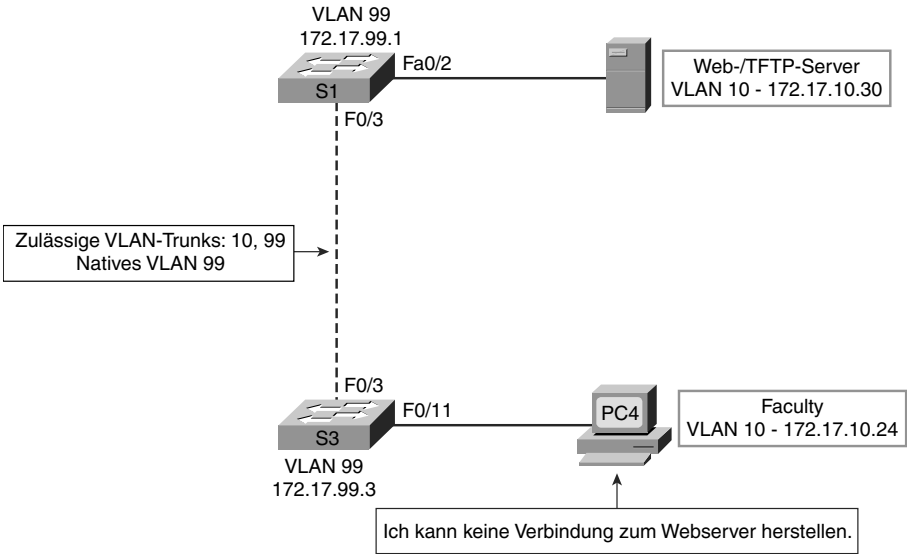

Abbildung 3.30: Probleme beim nativen VLAN

Unmittelbar nach Herstellen der Verbindung mit Switch S3 erscheint die in Listing 3.20 hervorgehobene Fehlermeldung in Ihrem Konsolenfenster. Mit `show interfaces f0/3 switchport` überprüfen Sie die Schnittstelle. Dabei stellen Sie fest, dass das native VLAN – der zweite hervorgehobene Bereich im Listing – auf VLAN 100 gesetzt wurde und inaktiv ist. Beim weiteren Durchsehen der Ausgabe erkennen Sie, dass nur die VLANs 10 und 99 zugelassen sind; dies ist weiter unten in der Ausgabe hervorgehoben.

Listing 3.20: Fehlanpassung des nativen VLAN

```
S3#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3
  (100), with S1 FastEthernet0/1 (99).
S3# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
```

Listing 3.20: Fehlanpassung des nativen VLAN (Forts.)

```
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: 100 (Inactive)
<Ausgabe unterdrückt>
Trunking VLANs Enabled: 10,99
<Ausgabe unterdrückt>
```

Sie müssen das native VLAN auf dem Trunk-Port F0/3 auf VLAN 99 umstellen. In Listing 3.21 zeigt der obere hervorgehobene Bereich den Befehl zur Konfiguration des nativen VLAN als VLAN 99. Die nächsten beiden Hervorhebungen bestätigen, dass das native VLAN für den Trunk-Port F0/3 auf VLAN 99 umgestellt wurde.

Listing 3.21: Korrektur beim nativen VLAN

```
S3# configure terminal
S3(config)# interface f0/3
S3(config-if)# switchport trunk native vlan 99
S3(config-if)# end
S3# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
<Ausgabe unterdrückt>
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management)
<Ausgabe unterdrückt>
Trunking VLANs Enabled: 10,99
<Ausgabe unterdrückt>
```

Die Bildschirmausgabe für Computer PC4 in Listing 3.22 zeigt, dass die Konnektivität mit dem Web-/TFTP-Server unter der Adresse 172.17.10.30 wiederhergestellt werden konnte.

Listing 3.22: Konnektivitätstest

```
PC4> ping 172.17.10.30
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: bytes=32 time=147ms TTL=128
<Ausgabe unterdrückt>
```

Sie haben Trunks manuell mit dem Befehl `switchport mode trunk` konfiguriert. Ferner haben Sie gelernt, dass die Trunk-Ports DTP-Advertisements verwenden, um den Leitungszustand mit dem Remote-Port zu verhandeln. Wenn für einen Port auf einer Trunk-Leitung ein Trunking-Modus konfiguriert wird, der mit dem Modus des Trunk-Ports auf der Gegenseite nicht kompatibel ist, kann zwischen den beiden beteiligten Switches keine Trunk-Leitung gebildet werden.

In Abbildung 3.31 sehen Sie das nächste Szenario.

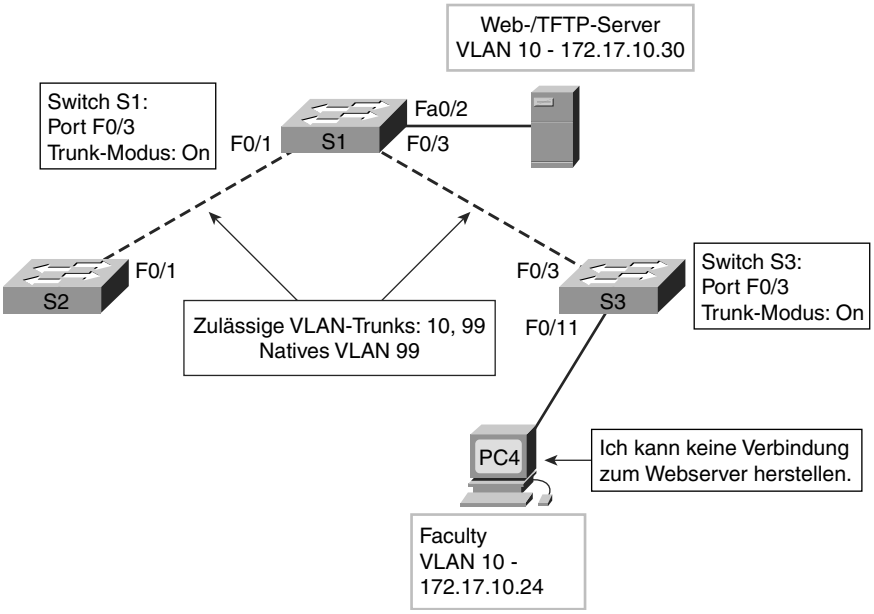

Abbildung 3.31: Probleme mit dem Trunk-Modus

In diesem Szenario kann der Benutzer von Computer PC4 keine Verbindung zum internen Webserver herstellen. Abbildung 3.31 zeigt ein Topologiediagramm mit den aktuellen Konfigurationseinstellungen. Welches Problem liegt vor?

Zunächst müssen Sie den Status der Trunk-Ports auf Switch S1 mit dem Befehl `show interfaces trunk` überprüfen (Listing 3.23). Hierdurch wird enthüllt, dass auf der Schnittstelle F0/3 von Switch S1 gar kein Trunk vorhanden ist. Sie untersuchen die Schnittstelle F0/3 und stellen fest, dass sich der Switch-Port im Modus *Dynamic Auto* befindet (vgl. die erste Hervorhebung im Listing). Eine Untersuchung der Trunks auf Switch S3 fördert zutage, dass keine aktiven Trunk-Ports vorhanden sind. Weitere Überprüfungen zeigen zudem, dass sich auch die Schnittstelle F0/3 im Modus *Dynamic Auto*

befindet (vgl. die erste Hervorhebung in Listing 3.23 unten). Der Trunk ist also ausgefallen, da sich beide Seiten im Modus *Dynamic Auto* befinden.

Listing 3.23: Die Befehle »show interfaces trunk« und »show interfaces switchport

```
S1# show interfaces trunk
Port     Mode    Encapsulation     Status     Native vlan
Fa0/1    on      802.1q            trunking   99
Port   Vlans allowed on trunk
Fa0/1  10,99
Port   Vlans allowed and active in management domain
Fa0/1  10,99
Port   Vlans in spanning tree forwarding state and not pruned
Fa0/1  10,99
S1# show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto

S3# show interfaces trunk

S3#
S3# show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
<Ausgabe unterdrückt>
```

Sie müssen den Trunk-Modus der Ports F0/3 auf den Switches S1 und S3 (zumindest aber auf einem dieser Ports) ändern. Im oberen Teil von Listing 3.24 zeigt die Hervorhebung, dass der Port F0/3 auf dem Switch S1 sich nun im *Trunk*-Modus befindet. Die Ausgabe für Switch S3 zeigt die zur Umkonfigurierung des Ports verwendeten Befehle sowie die Ergebnisse der Befehle `show interfaces switchport` und `show interfaces trunk`. Daraus geht hervor, dass die Schnittstelle F0/3 nun als Trunk konfiguriert wurde. Die Ausgabe auf Computer PC4 zeigt an, dass dieser Computer nun wieder über Konnektivität zum Web-/TFTP-Server unter der Adresse 172.17.10.30 verfügt.

Listing 3.24: Der Befehl »show interfaces trunk«

```
S1# configure terminal
S1(config)# interface f0/3
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1# show interfaces f0/3 switchport
```

Listing 3.24: Der Befehl »show interfaces trunk« (Forts.)

```
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
<Ausgabe unterdrückt>
S1#

S3# configure terminal
S3(config)# interface f0/3
S3(config-if)# switchport mode trunk
S3(config-if)# end
S3# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
<Ausgabe unterdrückt>
S3# show interfaces trunk
Port      Mode      Encapsulation     Status     Native vlan
Fa0/3     on        802.1q            trunking   99
Port   Vlans allowed on trunk
Fa0/3  10,99
Port   Vlans allowed and active in management domain
Fa0/3  10,99
Port   Vlans in spanning tree forwarding state and not pruned
Fa0/3  10,99
S3#

PC4> ping 172.17.10.30
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: bytes=32 time=147ms TTL=128
<Ausgabe unterdrückt>
```

Abbildung 3.32 zeigt das letzte Troubleshooting-Szenario. Sie haben gelernt, dass, damit Daten eines VLAN über einen Trunk übertragen werden können, dieses VLAN auf dem Trunk zugelassen sein muss. Der zu diesem Zweck verwendete Befehl heißt `switchport trunk allowed vlan` *`vlan-list`*. In Abbildung 3.32 wurden VLAN 20 (*Student*) und Computer PC5 zum Netzwerk hinzugefügt. Die Dokumentation wurde mit Angaben dazu aktualisiert, dass die auf dem Trunk zugelassenen VLANs die IDs 10, 20 und 99 haben.

In diesem Szenario kann der Benutzer von Computer PC5 keine Verbindung mit dem Mailserver für Studierende aufnehmen (vgl. Abbildung 3.32).

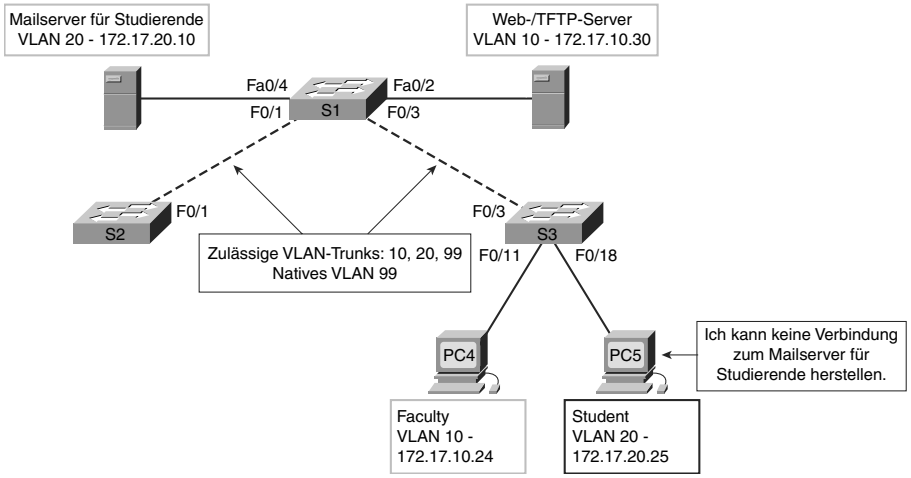

Abbildung 3.32: Probleme mit zugelassenen VLANs

Sie überprüfen zunächst mit `show interfaces trunk` die Trunk-Ports auf Switch S1 (Listing 3.25). Der Befehl enthüllt, dass die Schnittstelle F0/3 auf dem Switch S3 korrekt mit den zugelassenen VLANs 10, 20 und 99 konfiguriert ist. Eine Untersuchung der Schnittstelle F0/3 auf dem Switch S1 zeigt hingegen, dass die Schnittstellen F0/1 und F0/3 nur die VLANs 10 und 99 zulassen. Es hat den Anschein, dass jemand zwar die Dokumentation aktualisiert hat, es aber versäumt hat, die Ports auf dem Switch S1 umzukonfigurieren.

Listing 3.25: Zugelassene VLANs in der Ausgabe von »show interfaces trunk«

```
S3# show interfaces trunk
Port      Mode      Encapsulation      Status      Native vlan
Fa0/3     on        802.1q             trunking    99
Port    Vlans allowed on trunk
Fa0/3   10,20,99
Port    Vlans allowed and active in management domain
Fa0/3   10,20,99
Port    Vlans in spanning tree forwarding state and not pruned
Fa0/3   10,20,99

S1# show interfaces trunk
Port         Mode         Encapsulation  Status        Native vlan
Fa0/1        on           802.1q         trunking      99
Fa0/3        on           802.1q         trunking      99
Port         Vlans allowed on trunk
Fa0/1        10,99
Fa0/3        10,99
<Ausgabe unterdrückt>
S1#
```

Sie müssen die Ports F0/1 und F0/3 auf dem Switch S1 also mit dem Befehl `switchport trunk allowed vlan 10,20,99` umkonfigurieren. Listing 3.26 zeigt, dass die VLANs 10, 20 und 99 nun zu den Ports F0/1 und F0/3 auf dem Switch S1 hinzugefügt wurden. Der Befehl `show interfaces trunk` ist ein herausragendes Tool, wenn es darum geht, häufig auftretende Probleme mit dem Trunking zu enthüllen. Unser letztes Listing 3.26 zeigt, dass PC5 nun wieder über Konnektivität zum Mailserver unter 172.17.20.10 verfügt.

Listing 3.26: Der Befehl »switchport trunk allowed vlan vlan-list«

```
S1# configure terminal
S1(config)# interface f0/3
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1(config-if)# end
S1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/3       on           802.1q         trunking      99
Port        Vlans allowed on trunk
Fa0/1       10,20,99
Fa0/3       10,20,99

PC5> ping 172.17.20.10
Pinging 172.17.20.10 with 32 bytes of data:
Reply from 172.17.20.10: bytes=32 time=147ms TTL=128
<Ausgabe unterdrückt>
```

3.4.2 Ein häufiges Problem bei VLAN-Konfigurationen

In modernen geswitchten LANs entspricht jedes VLAN einem eindeutigen IP-Subnetz. Falls zwei Geräte im selben VLAN unterschiedliche Subnetzadressen aufweisen, können sie nicht miteinander kommunizieren. Eine derartige Fehlkonfiguration ist nicht ungewöhnlich und lässt sich einfach beheben, indem das verursachende Gerät ermittelt und die Subnetzadresse korrigiert wird.

In dem in Abbildung 3.33 gezeigten Szenario kann der Benutzer von PC1 keine Verbindung zum Webserver *Faculty* herstellen.

In Listing 3.27 enthüllt ein Blick auf die IP-Konfigurationseinstellungen von PC1 den meistgemachten Fehler bei der Konfiguration eines VLAN: eine falsch konfigurierter IP-Adresse. Eigentlich müsste PC1 die IP-Adresse 172.17.10.21 aufweisen, doch wurde 172.172.10.21 konfiguriert, weswegen sich PC im falschen Subnetz befindet.

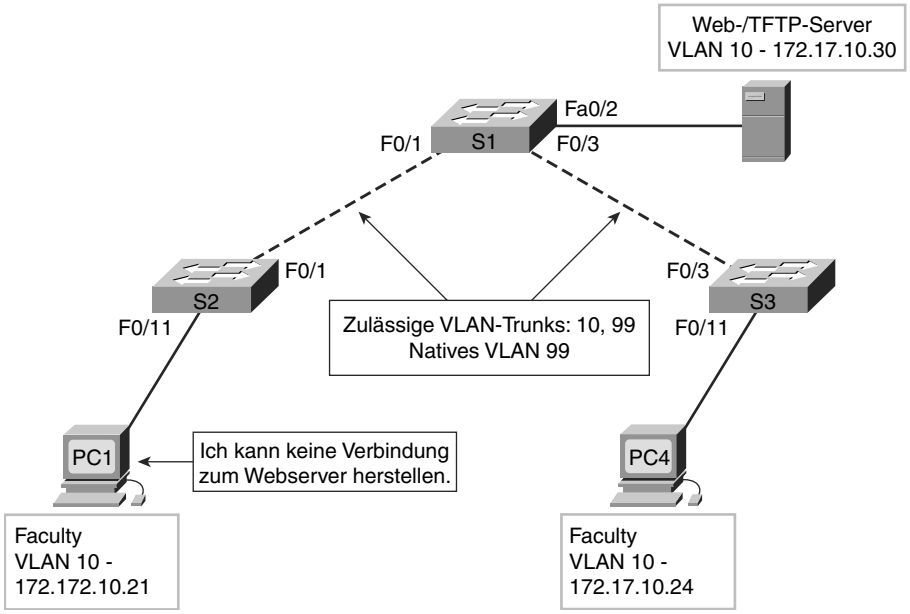

Abbildung 3.33: Probleme mit der VLAN-Konfiguration

Listing 3.27: IP-Adressierung auf einer LAN-Workstation

```
PC1> ipconfig

IP Address.....................: 172.172.10.21
Subnet Mask....................: 255.255.255.0
Default Gateway................: 0.0.0.0

PC1>
```

Nach Umstellung der IP-Adresse von PC1 auf 172.17.10.21 zeigt Listing 3.28, dass PC1 wieder über Konnektivität zum Web-/TFTP-Server unter 172.17.10.30 verfügt.

Listing 3.28: Konnektivitätstest nach Änderung der IP-Adresse

```
PC1> ping 172.17.10.30
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: bytes=32 time=147ms TTL=128
<Ausgabe unterdrückt>
```

Troubleshooting der VLAN-Implementierung (3.4.2)

Packet Tracer Aktivität

In dieser Packet Tracer-Aktivität üben Sie das Troubleshooting bei Konnektivitätsproblemen zwischen PCs im selben VLAN. Zur Durchführung der Aktivität verwenden Sie Packet Tracer und die Datei *e3-3422.pka* auf der Begleit-CD-ROM zu diesem Buch.

3.5 Zusammenfassung

Wir haben in diesem Kapitel VLANs kennengelernt. VLANs werden zur Segmentierung von Broadcast-Domänen in einem geswitchten LAN verwendet. Diese Segmentierung optimiert die Leistung und die Administrierbarkeit von LANs. VLANs gestatten Netzwerkadministratoren eine flexible Steuerung der Daten einzelner Geräte im LAN.

Zu den VLAN-Haupttypen gehören Daten-VLANs, das Default-VLAN, das Black-Hole-VLAN, native VLANs, Management-VLANs und Sprach-VLANs.

VLAN-Trunks ermöglichen die Switch-übergreifende Kommunikation mehrerer VLANs. Das IEEE 802.1Q-Frame-Tagging erlaubt dabei die Unterscheidung zwischen Ethernet-Frames, die zu unterschiedlichen VLANs gehören, wenn diese gemeinsam über Trunk-Leitungen übertragen werden.

Wir haben auch die Konfiguration, die Überprüfung sowie das Troubleshooting bei VLANs und VLAN-Trunks über das Cisco IOS-CLI behandelt.

3.6 Übungen

Die Übungen im Begleitbuch »LAN Switching and Wireless, CCNA Exploration Labs and Study Guide« (ISBN 1-58713-202-8) ermöglichen ein praxisbezogenes Üben der folgenden in diesem Kapitel vorgestellten Themen:

Übung 3.1: Grundlegende VLAN-Konfiguration (3.5.1)

Übungen

In dieser Übung lernen Sie, wie Sie die Auswirkungen von Broadcasts im Netzwerk beschränken. Eine Möglichkeit, dies zu tun, besteht darin, ein großes physisches Netzwerk in eine Anzahl kleinerer logischer oder virtueller Netzwerke umzuwandeln. Dies ist eines der Ziele von VLANs. Diese Übung stellt die Grundlagen der VLAN-Konfiguration vor.

Übung 3.2: Fortgeschrittene VLAN-Konfiguration (3.5.2)

In dieser Übung beschränken Sie die Auswirkungen von Broadcasts im Netzwerk, wobei Sie nur eingeschränkte Informationen erhalten. Eine Möglichkeit, dies zu tun, besteht darin, ein großes physisches Netzwerk in eine Anzahl kleinerer logischer oder virtueller Netzwerke umzuwandeln. Dies ist eines der Ziele von VLANs. Diese Übung stellt die Grundlagen der VLAN-Konfiguration vor.

Übung 3.3: Troubleshooting bei VLAN-Konfiguration (3.5.3)

In dieser Übung werden Sie die Ursache für eine fehlkonfigurierte VLAN-Umgebung beheben. Sie oder Ihr Dozent lädt die bereitgestellten Konfigurationen in Ihre Übungsumgebung. Ihr Ziel besteht darin, alle Fehler in den Konfigurationen zu finden und zu beseitigen und eine Ende-zu-Ende-Konnektivität herzustellen. Ihre abschließende Konfiguration sollte dem angegebenen Topologiediagramm und der Adresstabelle entsprechen.

Viele Praxisübungen enthalten Aktivitäten mit Packet Tracer, in denen Sie diese Software zur Simulation der Übung verwenden können. Lesen Sie im »LAN Switching and Wireless, CCNA Exploration Labs and Study Guide« (ISBN 1-58713-202-8) die Praxisübungen mit Packet Tracer.

3.7 Lernzielkontrolle

Beantworten Sie die folgenden Fragen, um Ihren Kenntnisstand bezüglich der in diesem Kapitel beschriebenen Themen und Konzepte zu überprüfen. Die Antworten finden Sie in Anhang A, »Antworten zu den Lernzielkontrollen und weiterführenden Fragen«.

1. Auf den Switches S1 und S2 sind jeweils Ports in den LANs *Marketing*, *Sales*, *Production* und *Admin* konfiguriert. Jedes VLAN umfasst zwölf Benutzer. Wie viele Subnetze werden zur Adressierung der VLANs benötigt?

   a) 1

   b) 2

   c) 4

   d) 8

   e) 12

   f) 24

2. Mit welchem Mechanismus wird die Trennung zwischen verschiedenen VLANs erreicht, die gemeinsam über eine Trunk-Leitung übertragen werden?

   a) VLAN-Tagging unter Verwendung des 802.1Q-Protokolls

   b) VLAN-Tagging unter Verwendung des 802.1p-Protokolls

   c) VLAN-Multiplexing

   d) Festlegung des VLAN als natives VLAN

3. Welche Optionen sind bei der Konfiguration einer Trunk-Verbindung zwischen zwei Switches zu berücksichtigen? Wählen Sie zwei Antworten aus.

   a) Der Befehl `switchport nonegotiate` muss für Trunks konfiguriert werden, die DTP benutzen.

   b) Die Port-Security darf nicht auf Trunk-Schnittstellen konfiguriert werden.

   c) Das native VLAN muss an beiden Enden des Trunks gleich sein.

   d) An beiden Enden der Trunk-Verbindung können verschiedene Kapselungstypen konfiguriert werden.

   e) Trunk-Ports können nur auf Gigabit-Ethernet-Schnittstellen konfiguriert werden.

4. Ein Switch mit zwölf Ports wurde zur Unterstützung dreier VLANs namens *Sales*, *Marketing* und *Finance* konfiguriert. Jedes VLAN erstreckt sich über vier Ports des Switchs. Der Netzwerkadministrator hat das VLAN *Marketing* nun vom Switch gelöscht. Welche Aussagen beschreiben den Status der Ports, die mit diesem VLAN verknüpft waren? Wählen Sie zwei Antworten aus.

   a) Die Ports sind inaktiv.

   b) Die Ports wurden durch den Administrator deaktiviert.

   c) Die Ports werden zu Trunks, um Daten aller anderen VLANs zu übertragen.

   d) Die Ports bleiben Bestandteil des VLAN *Marketing*, bis sie einem anderen VLAN zugewiesen werden.

   e) Die Ports werden automatisch aus dem VLAN *Marketing* entfernt und direkt VLAN 1 zugewiesen.

5. Welche Aussagen zu Hosts, die im selben VLAN konfiguriert sind, sind zutreffend? Wählen Sie drei Antworten aus.

   a) Hosts im selben VLAN müssen sich im selben IP-Subnetz befinden.

   b) Hosts in verschiedenen VLANs können nur mithilfe des Schicht-2-Switchs kommunizieren.

   c) Hosts im gleichen VLAN befinden sich auch in der gleichen Broadcast-Domäne.

   d) Hosts im gleichen VLAN befinden sich auch in der gleichen Kollisions-Domäne.

   e) Hosts im gleichen VLAN gehorchen derselben Sicherheitsrichtlinie.

   f) Hosts im selben VLAN müssen sich im selben physischen Segment befinden.

6. Betrachten Sie Abbildung 3.34. Host C kann keine Daten übertragen, weil er keine MAC-Adresse des Zielhosts kennt. Welche anderen Hosts erhalten die ARP-Anfrage, die Host C daraufhin versendet?

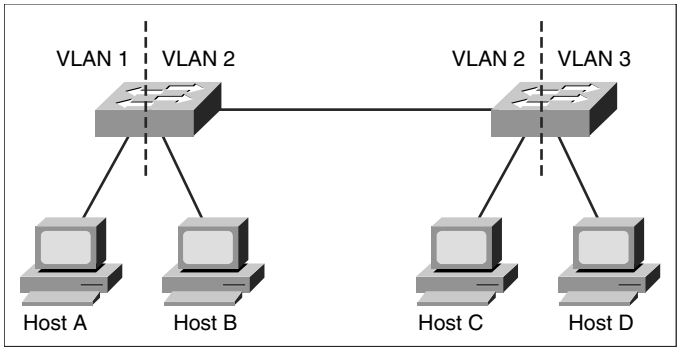

Abbildung 3.34: LAN-Konnektivität

   a) Host A

   b) Host B

   c) Hosts A und B

   d) Hosts A und D

   e) Hosts B und D

   f) Hosts A, B und D

7. Geben Sie für jedes aufgeführte VLAN-Merkmal an, ob es sich um eine Eigenschaft eines statischen oder eines dynamischen VLAN handelt. Kennzeichnen Sie statische Eigenschaften mit *S* und dynamische mit *D*.
   - Jeder Port ist mit dem betreffenden VLAN verknüpft.
   - Eine manuelle Konfiguration der Portzuweisung ist erforderlich.
   - Die Ports bestimmen ihre Konfiguration selbst.
   - Beim Umzug von Benutzern ist der administrative Overhead geringer.
   - Beim Umzug von Benutzern ist ein Eingriff des Administrators erforderlich.
   - Die Konfiguration erfolgt datenbankbasiert.
8. Geben Sie für jedes aufgeführte VLAN-Merkmal an, ob es sich um eine Eigenschaft eines VLAN im normalen oder erweiterten Bereich oder von VLAN 1 handelt. Notieren Sie *N* für VLANs im normalen Bereich, *E* für solche im erweiterten Bereich und *1* für VLAN 1.
   - 1–1001
   - 1006–4094
   - Wird nicht mithilfe von VTP erlernt.
   - Ist in der Datei *vlan.dat* gespeichert.
   - Default-Management-VLAN
   - Natives Default-VLAN
   - Alle Ports sind standardmäßig Mitglied.

9. Betrachten Sie Abbildung 3.35. Fabrikneue Switches mit leeren MAC-Adresstabellen werden über eine Trunk-Leitung miteinander verbunden. Auf allen Hosts auf beiden Switches sind die gezeigten VLAN-Mitgliedschaften konfiguriert. Wie wird ein Frame von Host A an Host B weitergeleitet?

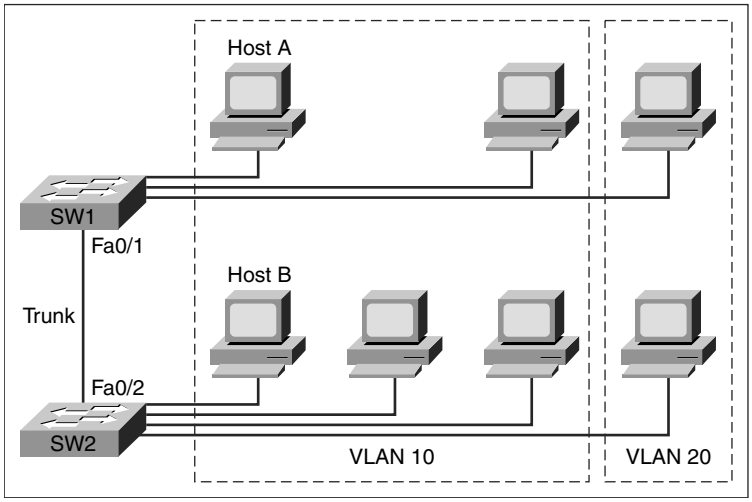

Abbildung 3.35: Fluss der Frames

a) Switch SW1 flutet die Nachricht von Host A an alle an SW1 angeschlossenen Hosts, die Mitglied von VLAN 10 sind.

b) Switch SW1 flutet die Nachricht von Host A an alle an SW1 angeschlossenen Hosts.

c) Switch SW1 flutet die Nachricht von Host A an alle an beide Switches angeschlossenen Hosts.

d) Switch SW1 taggt den Frame mit der VLAN-ID 10. Danach wird er an alle Hosts an Switch SW2 geflutet, die Mitglied von VLAN 10 sind.

e) Switch SW1 taggt den Frame mit der VLAN-ID 10. Danach wird er an alle Hosts an Switch SW2 geflutet.

10. Betrachten Sie Listing 3.29. Host 1 ist mit der Schnittstelle F0/4 mit der IP-Adresse 192.168.1.22/28 verbunden. Host 2 ist mit der Schnittstelle F0/5 mit der IP-Adresse 192.168.1.33/28 verbunden. Host 3 ist mit der Schnittstelle F0/6 mit der IP-Adresse 192.168.1.30/28 verbunden. Nennen Sie die Aussagen, die das Resultat eines `ping`-Befehls von einem Host zu einem anderen beschreiben. Wählen Sie drei Antworten aus.

Listing 3.29: Konnektivität nach der VLAN-Konfiguration

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Accounting
Switch(config-vlan)# vlan 20
Switch(config-vlan)# name Marketing
Switch(config-vlan)# interface range f0/4 , f0/6
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# interface f0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
```

a) Host 1 kann einen `ping`-Befehl an Host 2 senden.

b) Host 1 kann keinen `ping`-Befehl an Host 2 senden.

c) Host 1 kann einen `ping`-Befehl an Host 3 senden.

d) Host 1 kann keinen `ping`-Befehl an Host 3 senden.

e) Host 2 kann einen `ping`-Befehl an Host 3 senden.

f) Host 2 kann keinen `ping`-Befehl an Host 3 senden.

11. Bei welchen Antworten ist der angegebene Befehl mit der korrekten Beschreibung verknüpft? Wählen Sie drei Antworten aus.

a) **`show vlan id vlan-id`.** Zeigt Informationen zu einem bestimmten VLAN an.

b) **`show vlan`.** Zeigt detaillierte Informationen zu allen VLANs auf dem Switch an.

c) **`show vlan brief`.** Zeigt detaillierte Informationen zu allen VLANs auf dem Switch an.

d) **`show interface f0/1 switchport`.** Zeigt Informationen zu einem bestimmten Port an.

e) **`show interface f0/1`.** Zeigt VLAN-Informationen zu einem bestimmten Port an.

12. Ordnen Sie die folgenden Befehle den korrekten Beschreibungen zu.

    - `switchport mode trunk`
    - `switchport mode dynamic desirable`
    - `switchport nonegotiate`
    - `switchport mode access`

    a) Konfiguriert den Port so, dass ein Trunk ausgehandelt wird.

    b) Konfiguriert den Trunk so, dass keine DTP-Pakete gesendet werden.

    c) Konfiguriert den Port als permanenten 802.1Q-Trunk.

    d) Deaktiviert den Trunk-Modus.

13. Ordnen Sie die folgenden Problemdefinitionen den korrekten Beschreibungen zu.

    - Fehlanpassung des nativen VLAN
    - Ungleicher Trunk-Modus
    - Falsche VLAN-Liste
    - VLAN-Subnetzkonflikt

    a) Beide Switches sind im Modus *Dynamic Auto* konfiguriert und handeln keine Verbindung aus.

    b) Nicht alle erforderlichen VLANs dürfen einen Trunk verwenden.

    c) Zwei VLANs verwenden denselben Adressraum.

    d) Das für ungetaggte Frames konfigurierte VLAN ist nicht auf den beiden verbundenen Switches identisch.

14. Bei welchen Antworten sind die Zuordnung der Mitgliedschaft im statischen, dynamischen oder Sprach-VLAN zur Aussage über die Portmitgliedschaft korrekt? Wählen Sie drei Antworten aus.

    a) **Portmitgliedschaft im statischen VLAN.** Ein Port auf einem Switch, der die manuell zugewiesene VLAN-Konfiguration dynamisch ändern kann.

    b) **Portmitgliedschaft im statischen VLAN.** Ein Port auf einem Switch, der seine zugewiesene VLAN-Konfiguration beibehält, bis diese manuell geändert wird.

c) **Portmitgliedschaft im dynamischen VLAN.** Ein Port auf einem Switch, der VMPS verwendet und einem Port in einem VLAN basierend auf der Ziel-MAC-Adresse zugewiesen ist.

d) **Portmitgliedschaft im dynamischen VLAN.** Ein Port auf einem Switch, der VMPS verwendet und einem Port in einem VLAN basierend auf der Absender-MAC-Adresse zugewiesen ist.

e) **Portmitgliedschaft im Sprach-VLAN.** An einem PC angehängter Access-Port, der zur Verwendung eines VLAN für Sprachdaten und eines zweiten für anderen Datenverkehr konfiguriert ist.

f) **Portmitgliedschaft im Sprach-VLAN.** An ein IP-Telefon angehängter Access-Port, der zur Verwendung eines VLAN für Sprachdaten und eines zweiten für übrigen Datenverkehr konfiguriert ist.

3.8 Weiterführende Fragen und Aktivitäten

Die folgenden Fragen setzen ein tieferes Verständnis der in diesem Kapitel behandelten Konzepte voraus. Sie finden die Antworten in Anhang A.

1. Welche der folgenden Definitionen beschreibt die Zuordnung zwischen VLANs und IP-Subnetzen in einem modernen geswitchten Netzwerk am besten?

   a) Ein IP-Subnetz für viele VLANs

   b) Ein VLAN für viele IP-Subnetze

   c) Zwei IP-Subnetze pro VLAN

   d) Zwei VLANs pro IP-Subnetz

   e) Ein IP-Subnetz pro VLAN

   f) Die Zuordnung variiert je nach Switch-Modell.

2. Betrachten Sie Abbildung 3.36. Die gestrichelte Linie deutet eine Trunk-Leitung an. S1 und S2 sind Mitglieder in VLAN 99. Welche der folgenden Aussagen sind zutreffend? Wählen Sie zwei Antworten aus.

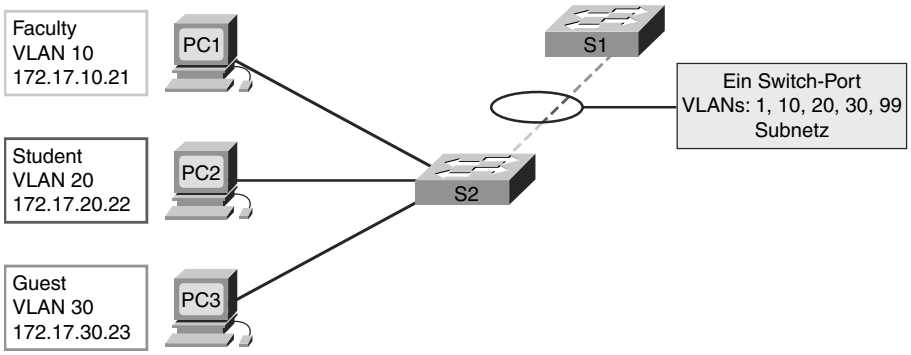

Abbildung 3.36: LAN-Konnektivität

   a) Alle PCs können einander erfolgreich `ping`-Befehle zusenden.

   b) Kein PC kann einem anderen erfolgreich `ping`-Befehle zusenden.

   c) Switch S1 kann erfolgreich `ping`-Befehle an Switch S2 senden.

   d) Alle PCs können erfolgreich `ping`-Befehle an Switch S1 senden.

   e) Alle PCs können erfolgreich `ping`-Befehle an Switch S2 senden.

3. Welche der folgenden Aktionen wird normalerweise am Prompt `Switch(config-vlan)#` durchgeführt?

   a) VLANs hinzufügen

   b) VLANs löschen

   c) VLANs Ports zuweisen

   d) VLANs benennen

   e) Natives VLAN zuordnen

4. Betrachten Sie Abbildung 3.37. Welche potenziellen Gründe liegen für das Ausbleiben der Konnektivität vor?

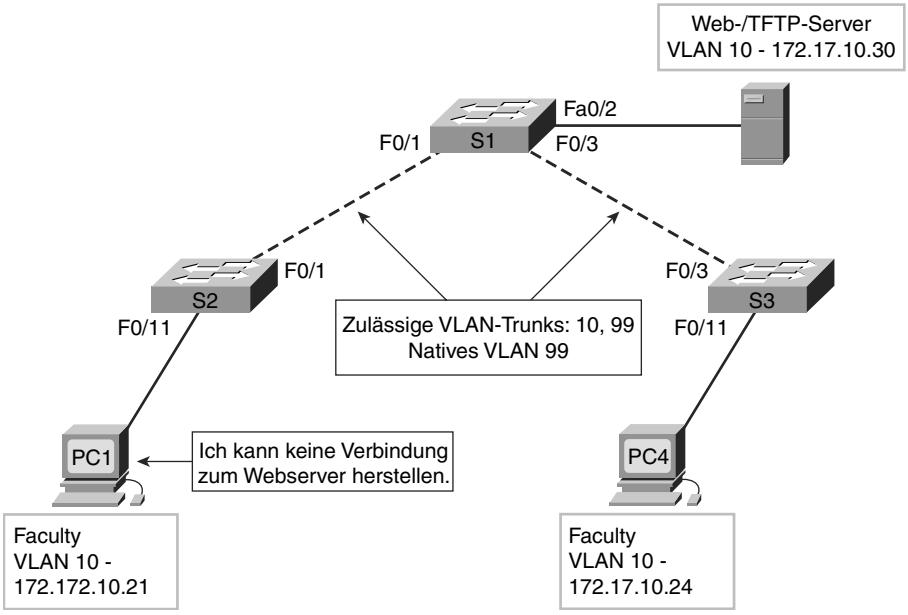

Abbildung 3.37: Fehlende Konnektivität

a) Fehlanpassung des nativen VLAN auf dem Trunk zwischen den Switches S1 und S2

b) Ungleicher Trunk-Modus auf den Switches S1 und S2

c) Ungleiche Angaben zu den zugelassenen VLANs auf dem Trunk zwischen den Switches S1 und S2

d) Fehlkonfigurierte IP-Adressen für VLAN 10

e) Eine Verbindung im Pfad zwischen PC1 und dem Web-/TFTP-Server ist ausgefallen.

Lesen Sie in »LAN Switching and Wireless, CCNA Exploration Labs and Study Guide« (ISBN 1-58713-202-8) die Hinweise zur Durchführung der Packet Tracer Skills Integration Challenge für dieses Kapitel nach.

Packet Tracer Skills