# 5. VLAN´s - Virtuelle Netze

## 5.1. Grundlegende Betrachtungen

### 5.1.1. Allgemeine Definition und wesentliche Vorteile sowie nachteilige Aspekte

Bestehende Netzstrukturen sind relativ unflexibel und erfordern einen hohen Verwaltungs- und Wartungsaufwand. Umzüge erfordern immer Rekonfigurationen von Netzadressen in den Endgeräten und der physikalischen Netzstruktur. Zudem besteht heute der Wunsch nach flexibel anpaßbaren Arbeitsgruppen, die über das gesamte Netz verteilt sein können.
Virtuelle LAN´s ermöglichen die logische Definition von Strukturen, welche in klassischen Netzen physikalisch geschaltet werden müßten. Der Anwender kann seine Kommunikationsstrukturen auf logische Art festlegen, ohne auf geographische Verhältnisse Rücksicht nehmen zu müssen.

Wesentliches Merkmal: Trennung von physikalischer und logischer Netzebene
Die logische Topologie wird auf die physikalische Topologie eines Netzes aufgesetzt. (Overlay-Prinzip)

VLAN´s bestehen aus Gruppierungen von Endstationen/Anwendern, basierend auf ihren logischen Zusammengehörigkeiten, Kommunikationsbeziehungen und Funktionen anstelle ihrer physikalischen Lokation. Ein großes physisches Netz ist in unterschiedliche, voneinander unabhängige virtuelle LAN´s aufteilbar. Unabhängig vom Standort kann ein Endbenutzer in das ihm zugewiesene VLAN eingegliedert werden. Einzelne Nutzer können dabei einem oder mehreren (heute noch nicht in allen Fällen möglich) VLAN´s angehören.
VLAN´s stellen eine Möglichkeit der flexiblen Netzgestaltung dar. Die Flexibilität läßt sich u.a. daran nachweisen, daß VLAN´s sich überlappen und überschneiden können (wenn Switches multiple Portkonfigurationen unterstützen / heute meist nur für

Highspeed-Ports umgesetzt), um beispielsweise Ressourcen effektiv zu sharen (Hochleistungs-Server).
Für alle Mitglieder eines VLAN´s erscheint dieses, als wären sie an ein physikalisches LAN angeschlossen.

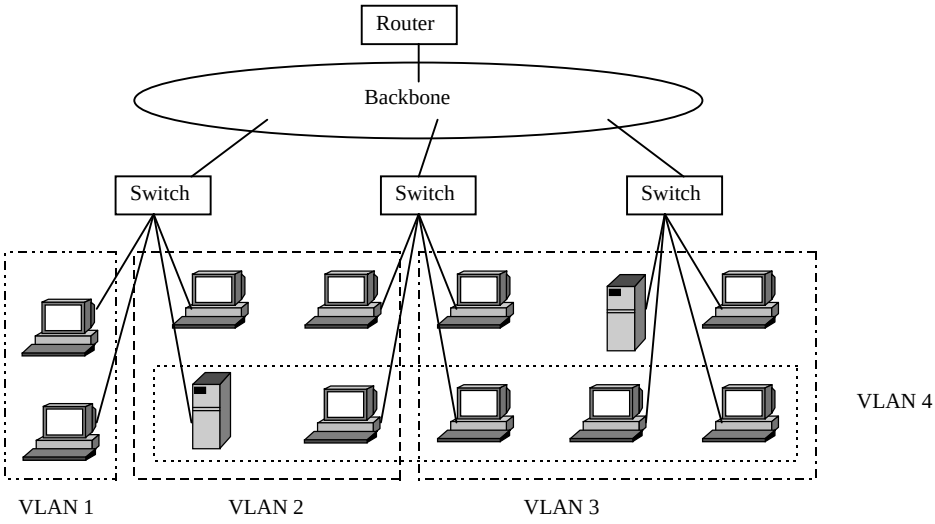



**Abb. 5.1.:** Allgemeines VLAN-Konzept

Die Möglichkeiten, wie ein Endgerät einem VLAN zugeordnet werden kann, sind:

- physikalischer Port
- MAC-Adresse
- Layer-3-Protokoll, -adressen

Ein VLAN bildet eine Broadcast- und Security-Domain, d.h. das Multi-/Broadcastaufkommen bleibt auf das VLAN begrenzt.
VLAN´s dienen dazu, den Zugriff auf Informationen zu regulieren und einzelne Subnetze zu trennen.
VLAN´s bieten Sicherheits- und Filterfunktionen (z.B.: Firewalls durch Restriktionen an die Zugehörigkeit zu bestimmten VLAN´s / Abhängigkeit des Zugangs vom Netztyp, Netzwerkadressen und Ports, usw.), wie bei klassischen Routern geschätzt. Die (nach wie vor erforderlichen) Router wandern an die Außenränder und verbinden einzelne VLAN´s miteinander. Innerhalb eines VLAN wird der Verkehr geswitcht und zwischen einzelnen VLAN´s geroutet. Der Einsatz eines Routers stellt die Filterung, Absicherung

und Verwaltung des Inter-VLAN-Verkehrs auf Netzwerk-Layer-Ebene sicher. Das Routing erfolgt separat, unabhängig von der LAN-Switching-Logik (Routing-Verzögerungen).
Auch der Einsatz von Multilayer-Switches, welche integriertes Bridging und Multiprotokoll-Routing unterstützen, (alternativ zum Router) ist möglich und ermöglicht integrierte „High-Speed-Connectivity".
Die resultierende Netzstruktur aus verschiedenen VLAN´s ist flach, d.h. es werden nur wenige Routerübergänge benötigt, was der Effizienz zugute kommt.

Im Zusammenhang mit ATM ist genau zu klären, was unter einem VLAN zu verstehen ist. Einige Hersteller verstehen das ATM-Backbone (mit LANE) darunter, welches lediglich **ein** LAN emuliert. In den meisten Fällen wird jedoch die durch die LANE unterstützte VLAN-Funktionalität im Sinne zusätzlicher organisationsorientierter Netzpartitionierung darunter verstanden (mehrere unabhängige ELAN´s).

Vorteile:

- Mitgliedschaft in einem VLAN ist weder durch den physikalischen Standort noch durch die Topologie des Netzes begrenzt
- tragen zur logischen Strukturierung des Netzes bei (Lastteilung)
- Unterstützung mehrerer VLAN´s über den Backbone simultan
- VLAN´s ermöglichen effiziente Verkehrstrennung und daher eine optimale Bandbreitenausnutzung, Steigerung der Netzleistung
- durch logische Segmentierung der LAN-Infrastrukturen in verschiedene Subnetze werden die jeweiligen Pakete lediglich innerhalb des VLAN geswitcht (VLAN = Broadcast-Domäne, d.h. Multi- und Broadcast-Traffic bleibt begrenzt)
- zwischen VLAN´s bestehen Sicherheits- und Filterfunktionen
- von zentraler Managementstation konfigurierbar, erleichtern administrative Aufgaben, komfortabel durch grafische Benutzeroberfläche und drag-and-drop-Funktionen
- erhöhte Flexibilität, dynamisch anpaßbares Netzdesign
- Zuordnung durch Management erspart Veränderungen an der physikalischen Netzstruktur (kein Rangieren von Kabeln nötig)

nachteilige Aspekte:

- u.U. hohe Migrationskosten, vor allem Installationskosten, da strukturierte Verkabelung und Switching-Technologien sowie ein leistungsfähiges Management benötigt werden (gegenwärtig höhere Kosten im Switching-Bereich)
- VLAN´s erfordern „wire speed“ über große Entfernungen, um ortsunabhängige Arbeitsgruppen zu realisieren
- mangelnde Standardisierung und daraus resultierende Inkompatibilität

Mit der gesteigerten Flexibilität im Netz erhöht sich i.a. der Aufwand in der Netzverwaltung, welcher nur von einem entsprechend leistungsfähigen, automatischen und intelligenten Netzwerkmanagement bewältigt werden kann.
Die Anforderungen gehen dabei über ein reines Monitoring hinaus, aktive Eingriffe müssen unterstützt und protokolliert werden. Aufgrund der Trennung von logischer und physikalischer Netzstruktur sind VLAN´s nur noch mittels Netzwerkmanagement überblick- und handhabbar. Die gesamte VLAN-Verwaltung wird durch das Management abgedeckt. Als Analysewerkzeug sollte es in der Lage sein, Fehler zu diagnostizieren. Die Bedeutung des Netzwerkadministrators ist gestiegen, er übernimmt zentrale Überwachungs- und Verwaltungsfunktionen. Die Aufgaben im manuellen Bereich haben sich verringert (physikalisches Patchen, usw.).

VLAN´s sind der richtige Ansatz für flexible Netzgestaltung und werden sich zukünftig verstärkt etablieren und erhebliche Vorteile bringen.
Der Haupteinsatzbereich liegt im LAN-Bereich, da durchsatzschwache Weitverkehrsverbindungen oder hohe Weitverkehrsgebühren dem VLAN an der Schwelle zum WAN ein Ende setzen.

[Cis(2)95], [Cis-VLAN], [LL 11/96], [Gat 5/95], [Data 3/96], [Bay 96], [Bad 95], [IBM], [Data 11/95], [Data 5/95], [Data 8/96], [Data 11/96], [Data 7/96]

### 5.1.2. Technischer Hintergrund

Die beiden maßgebenden Faktoren für volle VLAN-Funktionalität stellen Switching und ein schnelles Backbone-Medium dar (z.B.: ATM).

VLAN´s sind nur richtig nutzbar, wenn Switching flächendeckend im Netz eingesetzt wird. Gerade dem Backbone kommt heute eine größere Bedeutung zu, da verteilte, standortweite (z.T.: standortübergreifende) VLAN´s gebildet werden.
„..ohne ATM im Backbone, das die skalierbare Bandbreite zwischen den Switches sicherstellt, sind VLAN´s in der Regel weniger sinnvoll.“ [Data 8/96]
(zudem Multimediafähigkeit von ATM!)
Prinzipiell ist die VLAN-Bildung auch ohne ATM realisierbar, jedoch können die Möglichkeiten nicht in jedem Fall voll ausgeschöpft werden.

Der Wettbewerb um Marktanteile hat im wesentlichen alle Internetworking-Hersteller (z.B.: Cisco, Bay Networks, Cabletron, 3Com, Madge, IBM, Newbridge, UB Networks, Agile,...) in den Prozeß der VLAN-Implementation gestürzt, in einem Stadium, wo keine einheitlichen Standards (abgesehen von der LANE) verfügbar sind. So sind vor allem herstellerspezifische Lösungen zu finden, von einem allgemeinen Internetworking zwischen Komponenten verschiedener Hersteller ist man auf diesem Gebiet weit entfernt.

[Data 11/95], [Data 3/96], [Data 8/96]

### 5.1.3. Kategorisierung

Da ein einheitlicher VLAN-Standard noch nicht verfügbar ist, haben sich unterschiedliche Konzepte bei den Herstellern herausgebildet, die eine logische Kategorisierung komplizieren.
Die Bildung von VLAN´s erfolgt mittels LAN-Switching und/oder mittels virtuellem Routing auf Ebene 2 und/oder Ebene 3 und läßt sich je nach Definition durch Packet-Switching und teilweise zusätzlichem Zellswitching (ATM und LANE) erreichen.

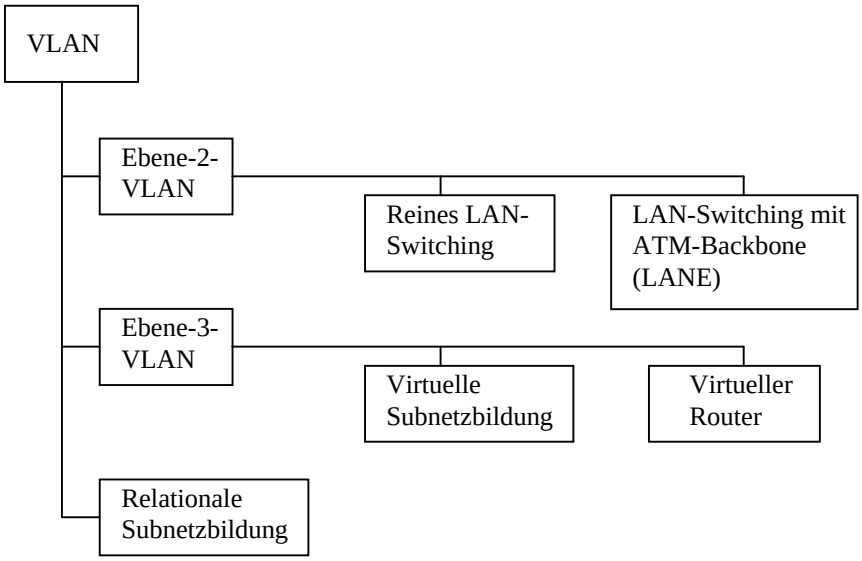



**Abb. 5.2.:** VLAN-Kategorisierung [Data 11/95]

[Data 11/95]

## 5.2. VLAN-Konzepte

### 5.2.1. Layer-2-VLAN´s

Ebene-2-VLAN´s gruppieren Benutzer auf der Basis reiner MAC-Verbindungen, meistenfalls über Adreßtabellen. VLAN´s, die rein durch die Auswertung der MAC-Informationen gebildet werden, sind in folgenden Ansätzen zu finden:

- LAN-Switching,
- ATM-LANE basierte VLAN´s.

#### 5.2.1.1. VLAN´s mit LAN-Switching

Die Bildung von VLAN´s mittels Layer-2-Switching stellt eine reale und problemlose Technik dar und wird heute von allen Hub- und Switch-Herstellern unterstützt.
VLAN-Funktionalität ist bei Cut-Through- als auch bei Store-&-Forward-Switches zu finden, jedoch ist bei Cut-Through-Switches die VLAN-Funktionalität auf Port- und

MAC-Adreßgruppen b eschränkt, d a sie den Frame-Inhalt nicht weiter auswerten können.

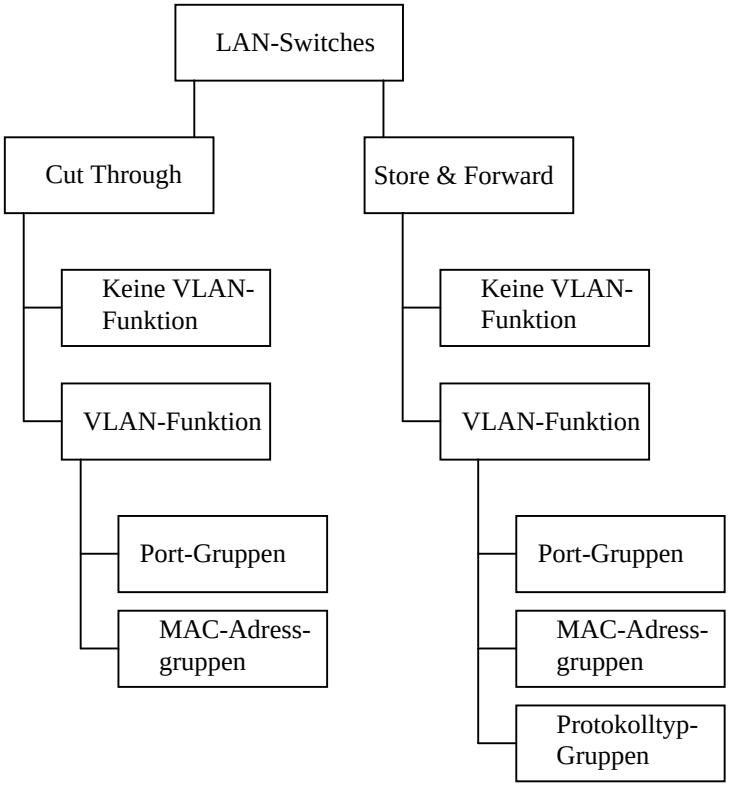



**Abb.5.3.:** Unterstützung von VLAN´s durch Switches [Data 11/95]

Ein Switched Virtual LAN stellt eine Broadcastgruppe hoher Geschwindigkeit und geringer Verzögerung dar, d ie e ine beliebige Sammlung von Endstationen unterschiedlicher LAN-Segmente zu einer logischen Einheit verschmilzt.
Sie a rbeiten auf der Grundlage von Layer-2-Informationen. Für Schicht-3-Verbindungen zwischen den VLAN´s ist ein Router erforderlich.
Für nichtroutbare Protokolle sollte
der Router zudem auch bridgen
können.

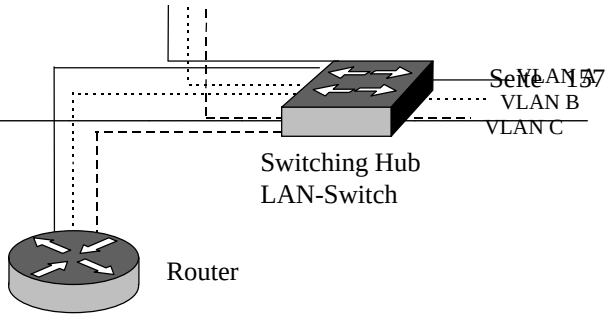



**Abb. 5.4.:** LAN-Switching basierte VLAN-Bildung

Die einzelnen VLAN´s müssen manuell konfiguriert werden. Die Zuordnung zu einem VLAN erfolgt auf der Basis des Ports, über welchen eine Endstation angeschlossen ist, oder auf der Grundlage von MAC-Adressen. In internen Tabellen werden die entsprechenden Konfigurationsinformationen gespeichert.

Portweise Zuordnung:

Wenn ein Port per Netzwerkmanagement einem VLAN zugeordnet wurde, bleibt die Zuordnung auch dann erhalten, wenn sich die angeschlossene Station verändert.

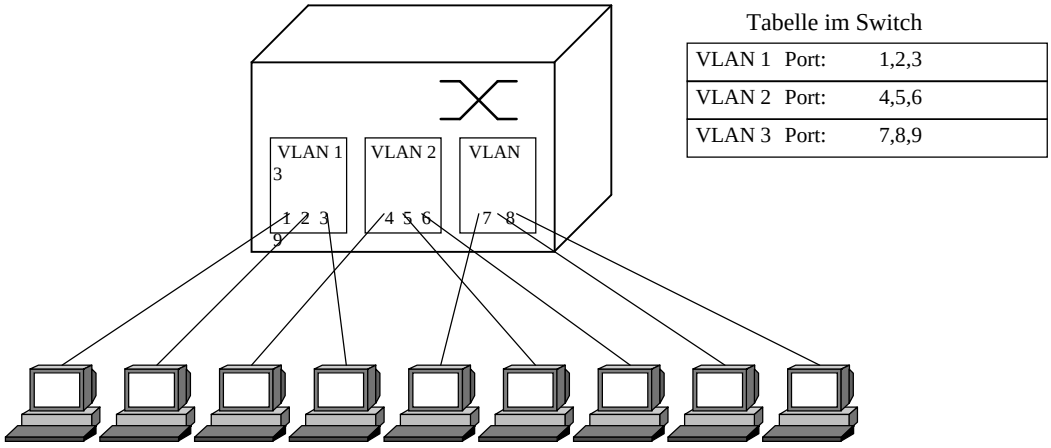



**Abb. 5.5.:** Portweise Zuordnung [nach Data 8/96]

Die portweise Zuordnung ist in den Fällen zu empfehlen, wenn die Örtlichkeit und nicht der Anwender die VLAN-Zugehörigkeit bestimmt, d.h. wenn Port fest für die Vergabe für VLAN-Mitglieder konzipiert sein soll. Eher nachteilig wirkt sich dieses Konzept bei VLAN-internen Umstellungen aus, wenn eine automatische Umkonfiguration gewünscht ist.

MAC-basierte Zuordnung:

Die auf MAC-Adressen basierende Zuordnung bietet eine neue Virtualisierungsqualität und größere Flexibilität, da der Nutzer und nicht die Örtlichkeit die Zugehörigkeit zum VLAN bestimmt. Unabhängig davon, wo der Anwender angeschlossen ist, ist immer ein Zugang zum VLAN möglich, da der Switch die Ebene-2-MAC-Adresse und keinen festen Port mit der VLAN-Kennung assoziiert.

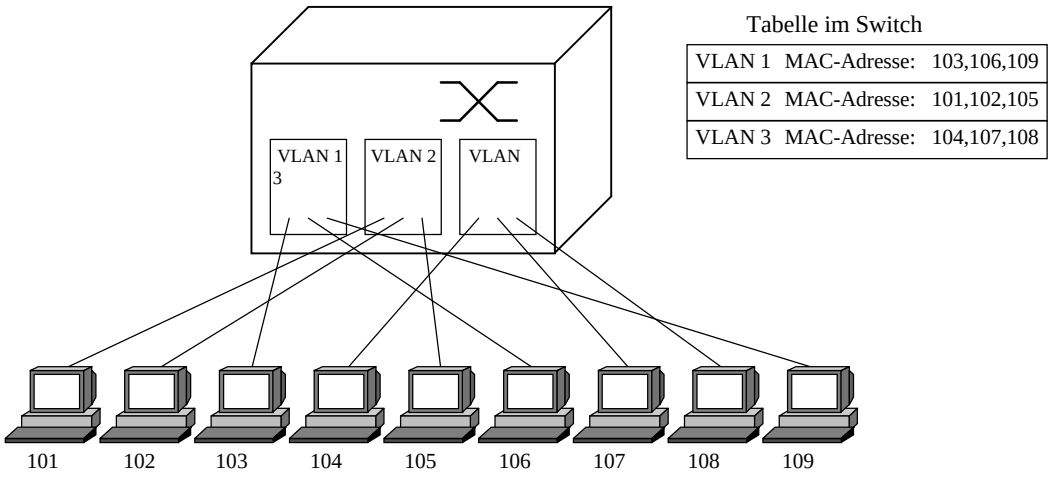



**Abb. 5.6.:** MAC-basierte Zuordnung [nach Data 8/96]

Vorteile der VLAN-Bildung mittels LAN-Switching:

- höhere verfügbare Summenkapazität (verglichen mit traditionellen LAN´s)
- kürzere Verarbeitungszeiten
- Flexibilität gemäß der organisatorischen Struktur

### 5.2.1.2. VLAN´s mit ATM und LANE

Mit zunehmender Durchsetzung von ATM als Backbone-Technologie wurde es notwendig, VLAN´s über das ATM-Netz zu verbinden. Die Basis hierfür bildet die LAN-Emulation (wie bereits beschrieben), welche heute von allen Herstellern mehr oder minder standardkonform implementiert wird.

ATM mit virtuellen Verbindungen und vermaschter Struktur im Backbone-Bereich ist ein exzellentes Werkzeug für die Beseitigung der Komplexitäts- und Skalierbarkeitsprobleme von VLAN´s.

Das derzeit dominierende Modell für die VLAN-Bildung ist die Benutzung des ATM-Backbones und temporärer SVC´s für die Schaffung hoher Geschwindigkeiten und niedriger Latenz.

Auf dem ATM-Netz können unabhängige ELAN´s gebildet werden, die für die Verbindung von VLAN´s genutzt werden können (durch entsprechende ELAN-VLAN-

Assoziation). Derzeit sind maximal 1024 ELAN´s einrichtbar, da der VLAN-ID in der aktuellen LANE-Version auf 10 Bit beschränkt ist.

ELAN´s müssen per Software-Konfiguration über die Management-Konsole eingerichtet werden. Nach Umzügen innerhalb eines ELAN´s erfolgt eine automatische Neuanmeldung und Initialisierung, ohne daß Adreßkonfigurationen geändert werden müssen. Ein Umzug in ein anderes ELAN ist mit einer manuellen Rekonfiguration verbunden.

Die Verbindung zwischen einzelnen ELAN´s erfolgt über einen Router, der als LEC in jedem ELAN vertreten ist.

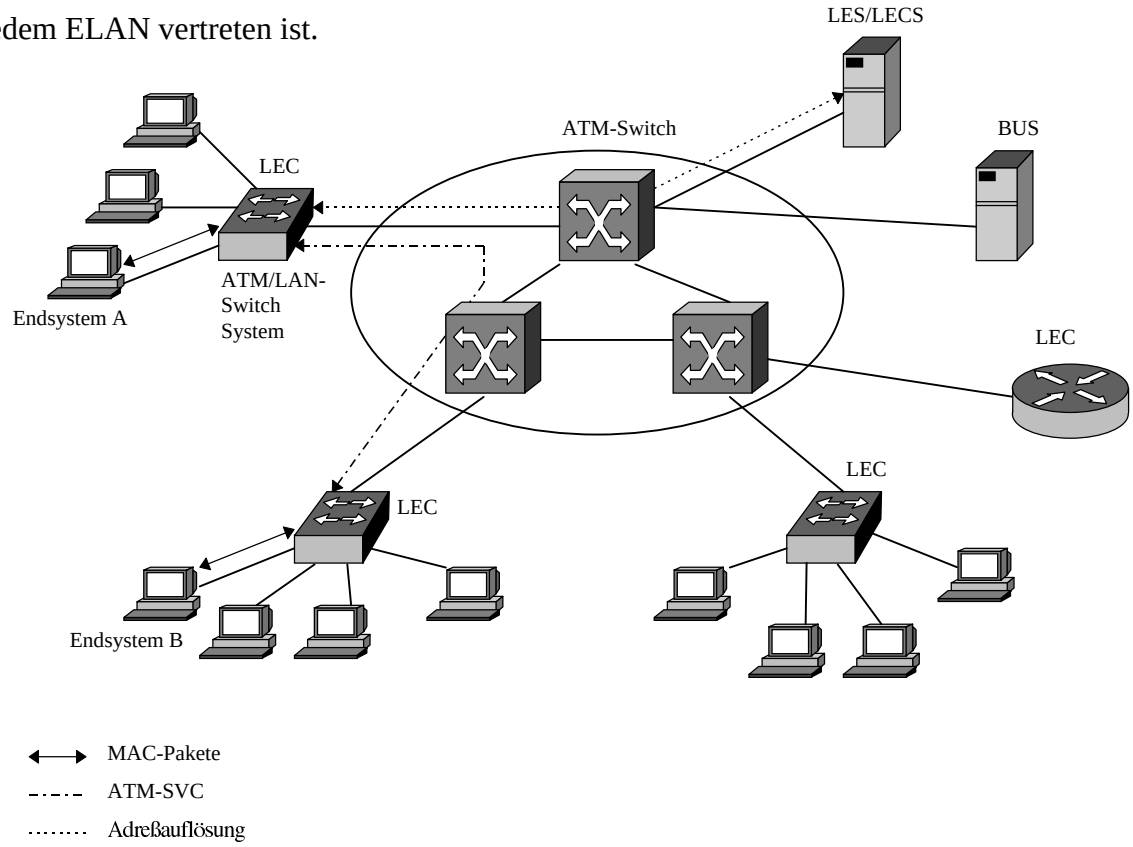



**Abb. 5.7.:** VLAN´s über ATM und LANE [Gat 2/96 ]

Vorteile im Vergleich zum LAN-Switching:

- reduzierter Verkabelungsaufwand, da mehrere virtuelle Verbindungen über ein Kabel unterstützt werden
- ATM-Skalierbarkeit im Backbone
- automatische Integration von Stationen nach Umzügen innerhalb eines logischen Subnetzes
- Konfigurationen lediglich bei Neueinrichtungen oder Löschen von Subnetzen notwendig, sowie bei Umzügen zwischen unterschiedlichen VLAN´s

[Data 8/96], [Data 5/95], [Data 11/95]

## 5.2.2. Layer-3-VLAN´s

Layer-3-/Protocol-VLAN´s stellen eine Gruppierung von Endstationen, basierend auf ihrer Netz-Adresse (OSI-3), die nicht notwendigerweise an physikalische Gegebenheiten gebunden ist, dar.

Im Gegensatz zu Layer-2-VLAN´s (lediglich Port- oder MAC-Level-Virtualisierung) gehen Layer-3-VLAN´s einen Virtualisierungsschritt weiter. Layer-3-Switches lesen die Adreßdaten der Pakete weiter als Layer-2-Switches ein und ermöglichen speziellere Selektion. Entsprechend den Layer-3-Protokollinformationen (z.B.: IP-Adressen 220.1.1.X = VLAN1 und 220.1.2.X = VLAN2) erfolgt die Zuordnung der Stationen zu den Subnetzen, egal an welcher Stelle des Unternehmens bzw. an welchem Switchport die Station angeschlossen ist. (Zuordnung zwischen IP-Subnetzadresse und VLAN ist nicht zwingend, jedoch sinnvoll.)

Ein Layer-3-VLAN kann über mehrere Ports/LAN-Segmente gespannt werden und andererseits kann auch ein Port mit mehreren logischen Subnetzadressen belegt werden.

Auch bei Umzügen bleibt die VLAN-Zugehörigkeit erhalten, wenn eine Station im gleichen VLAN bleibt, da die Endstationen ihre Adressen behalten und nicht rekonfiguriert werden müssen (Umzugsflexibilität).

Die Datenübertragung innerhalb des VLAN´s erfolgt über Switching-Tabellen Für die Kopplung verschiedener, aber protokollgleicher VLAN´s, sind Routingalgorithmen notwendig.

Für den Switch stellt sich die zentrale Frage, woher er die Informationen erhält, über welchen Port (Switchport oder Backbone-Port) er welche Zieladresse erreicht (Routing-Informationen/Routing-Tabellen).

2 Ansätze:

- Virtuelle Subnetzbildung (dezentral, sieht virtuelles Routing in der Zusammenfassung mehrerer physikalischer Interfaces mit Zugangs-Routern zu virtuellen Subnetzen)
- Virtueller Router (zentral, sieht virtuelles Routing in der Erweiterung der Router-Architektur auf den kompletten ATM-Backbone inklusive Route-Server und Multilayer-Switches)

### 5.2.2.1. Virtuelle Subnetzbildung

Die LANE vereinfacht die Schaffung virtueller Workgroups erheblich, ändert jedoch nichts an der zentralen Rolle des Routers im VLAN-Verbund. An ATM angebundene Router müssen daher sehr leistungs-/durchsatzstark sein. High-End-Router (beispielsweise von CISCO und Bay Networks) erreichen diese Leistungen.
Virtuelle Subnetze lassen sich über ein ATM-Backbone und Kantenrouter am Übergang zwischen Subnetz und ATM realisieren. Das Routing wird auf die Endgeräte-Konzentrationspunkte verlegt.
Mit dem Kantenrouter-Konzept wird ein Ansatz verfolgt, der die Integration von Routing, LAN-Switching und ATM bei niedriger Latenz in den Randgeräten ermöglicht (erstes Konzept von Netedge entwickelt). Der Einsatz paralleler Prozessoren für getrennte Aufgaben (Routenverwaltung, High-Speed-Weiterleitung und ATM-Verbindungsmanagement) kann erhebliche Performancesteigerungen erreichen. Kantenrouter können routen und Interfaces per LAN-Switching zu Subnetzen zusammenfassen.
Der Ansatz bietet die Möglichkeit, ein praktisch unbegrenzt skalierbares Netzwerk kleiner modularer Router zu bilden, das mit der enormen Bandbreite und Redundanz des ATM-Backbones weiter wächst.
Jeder Layer-3-Switch arbeitet zugleich als Router ( =Kantenrouter) und versendet Updates über die Netze und gegebenenfalls Endgeräte, die an ihn angebunden sind (z.T. proprietäre Verfahren). Ebenso wertet jeder Layer-3-Switch die Informationen der anderen aus und erstellt eigene Routing-Switching-Tabellen.
Da virtuelle Subnetze backboneübergreifende komplexe Strukturen aufweisen können, muß ein Verfahren implementiert sein, mit dem ein Kantenrouter ein Paket weiterleiten kann, dessen Zielnetz er nicht anhand seiner internen Tabellen erkennt. Dazu ist ein mehrschichtiges Adreßauflösungsschema erforderlich, da Kantenrouter über die Layer-2-Adreßauflösung hinausgeht, indem sowohl MAC- als auch Subnetzadressen aufgelöst werden müssen.
Konzepte, die auf ATM-Backbones aufsetzen, benutzen eine proprietär erweiterte LANE, um die Zieladresse aufzulösen. In diesem Fall wird ein Multilayer-ARP angewendet, welches das Mapping von Netzwerkadressen auf ATM-Adressen ermöglicht. LE-ARP-Requests werden nicht nur für die Auflösung von MAC-Adressen,

sondern auch für gesuchte Layer-3-Adressen verwendet. Die Anfragen werden über einen ATM-Multicast-Kanal an andere Kantenrouter versendet, die diese dann mit der ATM-Adresse beantworten, wenn das angefragtes Zielnetz angebunden ist.

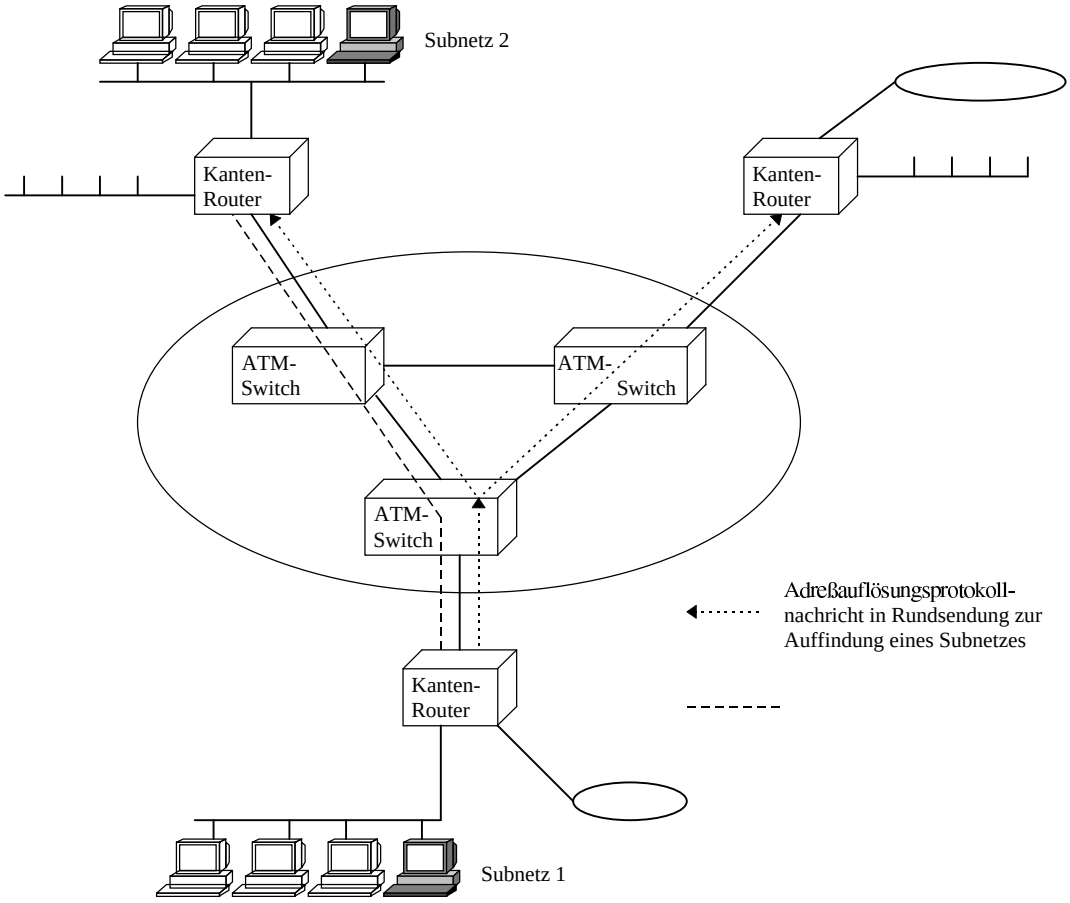



**Abb. 5.8.:** Kanten-Router-Prinzip [nach Data 11/95]

Vorteile:

- Skalierbarkeit der Routing-Performance
- Vermeidung eines Single-Point of Failure (i. Vgl. zu zentralen Routing-Konzepten)

(Das Kanten-Router-Prinzip wird von Bay Networks und Digital verfolgt.)

### 5.2.2.2. Virtuelle Router

Der Ansatz des virtuellen Routers unterscheidet sich vom Kantenroutermodell, vereint jedoch die gleichen Eigenschaften (geringe Verzögerungen, skalierbare ATM-

Backbones, Routing und Switching). Die Aufgabentrennung ist weiter fortgeschritten (konsequente Trennung von Forwarding und Routenverwaltung).
Die Routing-Funktionalität ist auf mehrere Geräte verteilt:

- Route-Server als zentrale Komponente und Layer-2/3-Switches (Multilayerswitches) als untergeordnete Komponenten

Der Route-Server mit Hochkapazitäts-Backbone-Anbindung betreibt dynamische Routing-Protokolle (Tabellen-Updates, Versenden von Update-Informationen) und dient der Wegekalkulation. Er pflegt ständig eine Abbildung der vorliegenden ATM- und Internetztopologie und verteilt zyklisch die Routen-Informationen an alle Multilayer-Switches. Weiterhin kann er als Broadcast-Server agieren und Adreßanfragen beantworten.
Um dem Route-Server die notwendige Informationsbasis zu geben, versorgen die Multilayer-Switches ihn mit Informationen über die jeweils aktuelle Anschlußkonfiguration (angebundene Subnetze oder Endgeräte).
Ein Multilayer-Switch ist ein Layer-2-Switch mit gesteigerter Intelligenz (Layer-3-Funktionalitäten). Multilayer-Switches sind für die Weiterleitung der Pakete zuständig, sie speditieren Pakete auf der Grundlage von Layer 2 und/oder 3 Header-Informationen, d.h. sie bridgen, switchen oder routen die Pakete nach Bedarf. Dazu benötigt er Route-Discovery oder Topologie-Updates vom Route-Server. Ein Multilayer-Switch muß in der Lage sein, Endgeräte desselben logischen Subnetzes an verschiedenen Ports zu bedienen und über den Route-Server zu ermitteln. Desweiteren sollten mehrere Subnetze an einem Port unterstützt werden. Dazu ist es notwendig, entsprechende Tabelleneinträge je angebundenem Endgerät und geroutetem Protokoll zu speichern.

Das Konzept läßt das gesamte ATM-Netz mit Route Server und Multilayer-Switches an den LAN/ATM-Übergangspunkten zum virtuellen Router werden.

| | |
|---|---|
| Multilayer-Switches | = LAN-Interface |
| ATM-Backbone | = Backplane |
| Route Server | = Router-CPU |

Ist ein gesuchtes Ziel nicht im lokalen Cache des Multilayer-Switches auflösbar, kann es über den Route-Server ermittelt werden, welcher mit der entsprechenden Ziel-ATM-Adresse antwortet. Dazu sendet z.B.: eine IP-Station, die sich auf einem Server in einem anderen Subnetz einloggen möchte, erstes Paket an den Route-Server, welcher die Ziel-Endstation und deren Lokalisation und den Weg zwischen Quelle und Ziel ermittelt. An den auslösenden Multilayer-Switch wird die entsprechende ATM-Adresse gesendet, welcher daraufhin eine direkte Verbindung etablieren kann und die erhaltenen Adreßinformationen in seinem lokalen Cache ablegt.
Schicht-3-Pakete reisen mit einem Subnetz-Hop durch den virtuellen Router (geringe Verzögerungen).

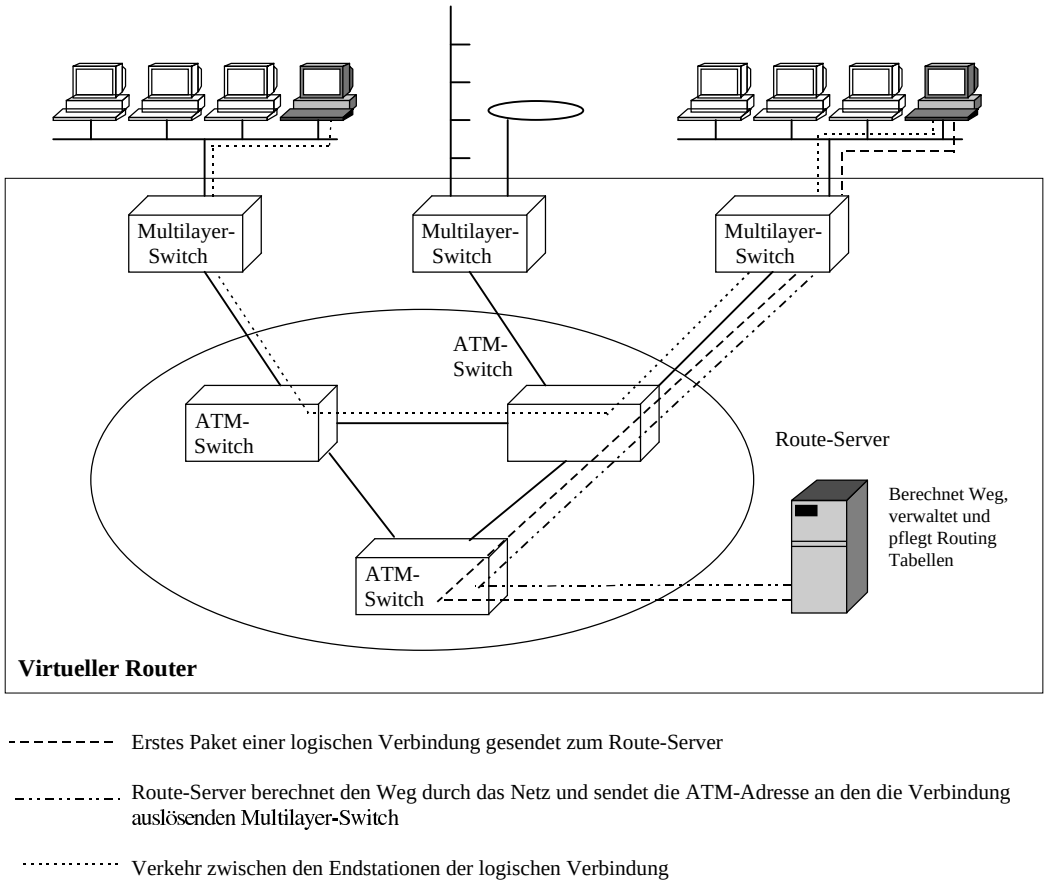



**Abb. 5.9.:** Virtueller Router [nach Data 11/95]

Vorteile:

- klare Funktionstrennung,
- geringerer Synchronisationsaufwand

Nachteilig wirkt sich die Konzentration der Routenkalkulation im Route-Server auf die Systemstabilität aus. Er stellt einen Single-Point-of-Failure dar.

(Konzept wird von Cisco, Cabletron, Newbridge, 3Com unterstützt.)

[PCN 3/96], [Data 5/95], [Data 8/96], [Data 11/95]

Verteilte Subnetze und virtuelle Router

Beide Ansätze weisen noch Probleme auf. An jedem Multilayer-Switch muß jedes Subnetz konfiguriert werden. Zieht ein Benutzer in ein neues Subnetz, muß dieser u.U. am neuen Switch neu eingerichtet werden. Zieht ein letzter Benutzer aus einem Subnetz aus, muß dieses Subnetz deaktiviert werden.

### 5.2.3. Relationale Netze

Alle bisherigen Ansätze hatten den Nachteil der Notwendigkeit manueller Konfigurationen. Ein weiterer Automatisierungsschritt für VLAN´s wird durch relationale Netze unterstützt.

Im Konzept relationaler Netze (von Agile Networks eingebracht im ATMizer) bildet eine intelligente Softwarekomponente, die die Topologie des Netzes, einschließlich der Subnetzstruktur, Protokoll-Typen und Lage von Servern lernt, das Kernstück.

Zusammengehörige Benutzer werden zu Gruppen zusammengeführt (daher relationale Netze). Ein relationales LAN ist ein automatisch konfiguriertes Subnetz. (Jedoch ist die Möglichkeit der nachträglichen manuellen Konfiguration gegeben.) Relationale Netze können sich über mehrere physische Segmente erstrecken. Alle Mitglieder eines IP-Subnetzes werden automatisch ins gleiche relationale LAN gruppiert, unabhängig von ihrer Lage.

Für jedes Subnetz eines routbaren Protokollstacks wird ein eigenes relationales LAN gebildet. Nichtroutbare Protokollstacks werden insgesamt in einem eigenen relationalen LAN vereint.

Umzüge stellen kein Problem dar. Wie bei anderen VLAN´s können Broadcast- und Schutzzonen definiert werden.

Relationale Switches können trotz hoher Systemintelligenz nicht routen, so daß konventionelle Router notwendig sind (für den Verkehr zwischen den relationalen Netzen).

[Data 11/95], [Data 5/95]

## 5.3. VLAN-Signalisierung

LAN-Switches müssen in der Lage sein, Stationen desselben VLAN´s switchübergreifend zu kennen und Pakete innerhalb eines VLAN´s exakt weiterzuleiten. Ein switchübergreifendes Verfahren ist erforderlich, das es den Switches ermöglicht, ihre Informationen in bezug auf die VLAN´s auszutauschen. Hierzu sind verschiedene Verfahren möglich, jedoch hat keines den Status eines Standards.
Folgende Ansätze sind derzeit implementierbar:

Time Division Multiplexing:
Switchverbindungen wird ein festes Zeitraster auferlegt, in dem bestimmte Zeitschlitze den jeweiligen VLAN´s zugeordnet werden. Zum einen ist das Verfahren nur auf eine kleine Anzahl von VLAN´s limitiert und andererseits erscheint die Zuordnung einer festen Bandbreite zu einem VLAN im ATM-Zeitalter als fraglich, da ungenutzte Zeitslots nicht für andere VLAN´s genutzt werden können. Der einzige Vorteil des Verfahrens liegt darin, daß es ohne zusätzliche Overhead-Informationen auskommt.

Austausch von Adreßtabellen:
Bei der Initialisierung einer neuen Endstation wird deren Adresse vom Switch gelernt und zusammen mit einer korrespondierenden VLAN-Kennung an alle anderen Switches übertragen (Signalling Message).
Intervallmäßig werden zwischen den Switches komplette Adreßtabellen (zur Synchronisierung und zum Updaten der Tabellen / Tabellen unterliegen Aging-Prozeß) ausgetauscht.
Als Folge dieses Verfahrens wird das Netz mit einem erheblichen Overhead belastet.
Die Overheadbelastung steigt mit jedem zusätzlichen Switch.

Tagging:

Das Tagging verfolgt einen völlig anderen Weg. Die Informationen über die VLAN-Zuordnung werden in das Datenpaket integriert (Online-Synchronisierung). Dadurch, daß der notwendige Overhead im Datenpaket selbst übertragen wird (ähnlich Funktion des Zellheaders im ATM), entfällt zusätzlicher Steuerdatenverkehr. Im Vergleich zum Tabellenabgleich kann das Verhältnis zwischen Brutto- und Nettodatenrate prozentual ermittelt werden, da der Overhead lastabhängig ist.

Problem:

Durch das Einfügen zusätzlicher Informationen wird das Datenpaket länger. Dies kann dazu führen, daß u. U. die definierte Maximallänge (welche für jeden Netztyp festgelegt ist) überschritten und das Paket als fehlerhaft detektiert und im ungünstigsten Fall verworfen wird.

IEEE 802.10 stellt ein standardisiertes Verfahren dar, welches jedoch nicht für die VLAN-Signalisierung entworfen wurde und nur von wenigen Herstellern unterstützt wird. In IEEE 802.10 ist zudem ein Verfahren beschrieben, wie überlange Pakete fragmentiert werden und konform gemacht werden können.

Bemerkung: Bei Cisco wird das Tagging ohne zusätzliche Verfahren implementiert.
Werden ausschließlich Cisco-Switches verwendet, treten keine Probleme auf.

[Data 8/96], [Data 11/95]

## 5.4. VLAN-Standardisierungsaktivitäten

VLAN´s haben sich heute bereits weitgehend durchgesetzt. Die prinzipiellen Ansätze der VLAN-Realisierung sind herstellerabhängig, so daß zur Zeit bei der Entscheidung für ein VLAN-Netzwerk auch die Bindung an einen Hersteller mit all den sich ergebenden Konsequenzen erfolgt.

Die Anbieter von Komponenten, die den Aufbau virtueller Netze ermöglichen, konnten sich bislang noch nicht auf einen einheitlichen Standard einigen. Jeder geht seinen eigenen Weg und erstellt proprietäre Lösungen. Eine Normierung auf diesem Gebiet wird immer zwingender. Dieser Trend wurde auch von Herstellern erkannt, die eigenständig versuchten, die Entwicklung durch ihre Angehörigkeit in verschiedenen

Normungsgremien vo ranzutreiben. Cisco un ternahm beispielsweise verschiedene Initiativen zur Förderung der Interoperabilität zwischen p roprietären VLAN-Implementationen v erschiedener Anbieter. Cisco schlug u.a. d ie Nutzung des IEEE 802.10 Standards vor und implementierte diesen in Routern und LAN-Switches.
Den einzigen (für alle Hersteller) verfügbaren Standard stellt die LANE dar, allerdings beschränkt auf ATM-Backbones.

Der VLAN-Bedeutung bewußt, faßte der Arbeitskreis IEEE 802.1, welcher sich mit Fragen d es Internetworkings beschäftigt, d ieses Thema im Herbst 1995 erstmals auf. Mit der Zielsetzung der Verabschiedung eines einheitlichen Industriestandards arbeitet die Arbeitsgruppe 802.1q seitdem an einem Verfahren zur VLAN-Bildung, d as auf einem Tagging-Ansatz beruht. Die Art der VLAN-Kennzeichnung (4 Byte erforderlich), deren Einfügung in d ie Frames und Probleme (Kompatibilitätsprobleme durch Framelängenüberschreitungen) werden diskutiert.

[Data 9/96], [Cis(2)95]

### 5.4.1. IEEE 802.10

Die Nutzung des IEEE 802.10 Verfahrens zur VLAN-Unterstützung ist derzeit das einzige standardbasierte Verfahren. Es enthält einen Mechanismus, wie LAN-Verkehr gekoppelt mit VLAN-ID, welcher ein selektives Switching von Paketen ermöglicht, übertragen werden kann.

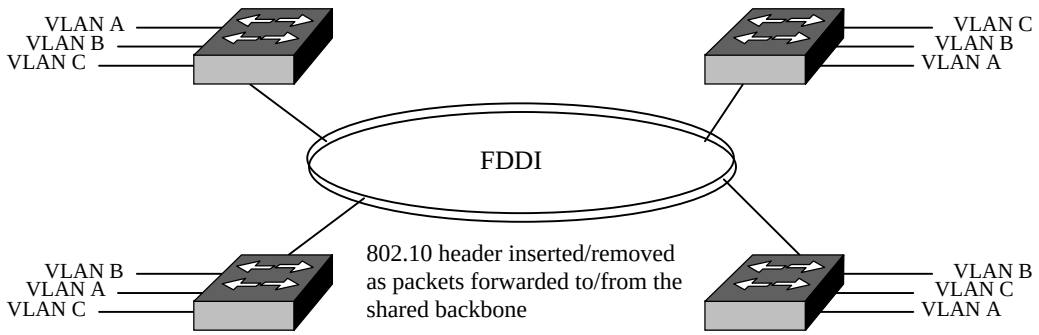



**Abb. 5.10.:** 802.10-Prinzip [Cis-Sem]

IEEE 802.10 wurde eigentlich als IEEE Interoperable LAN/MAN Security Standard verabschiedet (1992), welcher für Sicherheitsaspekte in LAN/MAN-Umgebungen geplant war und Authentikations- und Encryptionstechniken verbindet.
Im Kernpunkt der Spezifikation steht die Definition einzelner PDU´s, bekannt als SDE-PDU (Secure Data Exchange), bestehend aus einem MAC-Layer-Frame mit 802.10 Header, der zwischen MAC-Header und Frame-Daten eingefügt wird. Der 802.10-Header ist zweigeteilt in einen Clear-Header und einen Protected Header.

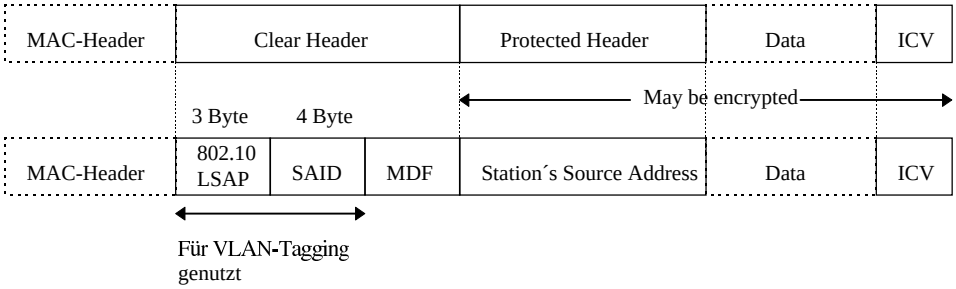



**Abb. 5.11.:** 802.10-Frame Format [Cis-VLAN]

SAID - Security Association Identifier (Einzelstationskennung [erstes Bit=0] oder Gruppenkennung [erstes Bit=1])
MDF - Management Defined Field (optional zu belegen durch Informationen zur Erleichterung der PDU-Übertragung)
Im Protected Header wird die Source-Adresse des MAC-Headers repliziert (zur Adreßbestätigung).
ICV - Integrity Check Value (Schutzmechanismus gegen Datenverfälschungen)

Nutzung für VLAN´s:

Der VLAN-ID stellt den wesentlichen Teil der Headerinformationen dar. Das 802.10 SAID-Feld (4 Byte) wird für die Übertragung des VLAN-ID (Gruppenkennung) genutzt und dient der Identifizierung des zu einem VLAN gehörenden Verkehrs. Internetworking-Devices mit VLAN-Intelligenz können ihre Forwarding-Entscheidungen anhand der Ports, die einem VLAN zugeordnet sind, treffen. High-Throuput-Geräte müssen lediglich den Clear-Header des 802.10-Frames unterstützen.

Lediglich der SDE-Designator (Bezeichner) [IEEE 802.10 LSAP], welcher auf einen 802.10-VLAN-Frame verweist, und der aktuelle VLAN-ID (SAID-Feld) müssen übertragen werden. Es entsteht ein geringer Verarbeitungsoverhead von 7 Byte.
Die ursprünglichen LAN-Datenpakete, wie von den angeschlossenen Endstationen erzeugt, werden mit einem 802.10-Header versehen, welcher den entsprechenden VLAN-ID enthält (notwendig für Weiterleitung im Backbone). Die Verarbeitung der Frames erfolgt nur an Stationen, die demselben VLAN angehören. Empfangene 802.10-Frames, die einen ID enthalten, der von keinem Port unterstützt wird, werden herausgefiltert. Frames mit unterstützten VLAN-ID´s wird der 802.10-Header entfernt und das ursprüngliche Paket an den entsprechenden Port weitergeleitet.
Da 802.10 VLAN-Frames gültige MAC-Frames sind, werden sie transparent durch nicht-802.10-kompatible Geräte übertragen.
802.10 erlaubt die Bildung von VLAN´s, ohne daß die Endgeräte SDE reden können müssen, da VLAN-ID in den Switches vergeben wird (entsprechend der Zugehörigkeit der Ports zu den VLAN´s).

Vorteile:

- funktioniert für alle Standard LAN´s ohne proprietäre Klimmzüge
- Möglichkeit der Kompatibilität gegeben

Der Wurm liegt allerdings oftmals in den Optionen. Cisco nutzt beispielsweise das SAID-Feld für die Übertragung des VLAN-ID´s. Grundsätzlich ist jedoch auch die Verwendung des MDF-Feldes denkbar.

[Data 11/95], [Cis-VLAN], [Cis(2)95]

### 5.4.2. IEEE 802.1q (zukünftig)

Die Entwicklung des IEEE 802.1q Standards wird vor allem durch Aktivitäten von Bay Networks, 3Com und Fore vorangetrieben.
In der derzeitigen Phase werden 2 unterschiedliche Modelle diskutiert.

Gemeinsame Aspekte:

- für jedes LAN-Segment kann nur ein Format verwendet werden, für alle Pakete eines VLAN´s
- Edge Devices übersetzen zwischen untagged und tagged Paketen
- Fabric Switches übertragen tagged Pakete zwischen den LAN-Segmenten anhand der enthaltenen VLAN-ID´s

One-Level-Model:

Im One-Level-Model sind die originalen MAC-Adressen und VLAN-Assoziationen aller Endstationen sichtbar für jeden Packet-Switch, durch welchen das Paket läuft. Zu einem untagged Paket muß ein Distinguishing-Marker ( Unterscheidungsmarkierung [LLC oder Ethertype]), der es als explizit tagged kennzeichnet, und ein VLAN-ID addiert werden.
Die Destination und Source Adressen werden vom originalen untagged Frame abgetrennt und 2 zusätzliche Felder eingefügt, sowie eine neue FCS berechnet.

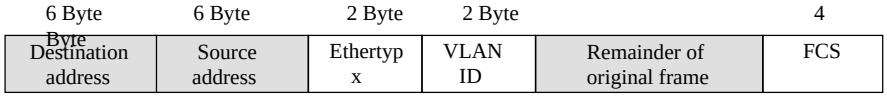



**Abb. 5.12.:** Format des tagged Frame beim One-Level-Model [Cis-802.1q]

Two-Level-Model:

Ein tagged Paket enthält zwei komplette MAC-Layer. Das Originalpaket, wie es von den Endstationen übertragen wird, wird in eine Hülle eingeschlossen, bestehend aus einem zusätzlichen MAC-Header, einem Distinguishing-Marker und einem VLAN-ID. Die äußeren MAC-Adressen stellen dabei keine Endstations-Adressen, sondern Adressen von Packet-Switches oder Multicast-Adressen dar.
In diesem Model wird ein tagged Paket nicht als zugehörig zu einem VLAN, sondern als zugehörig zu einem „Fabric LAN“ betrachtet.

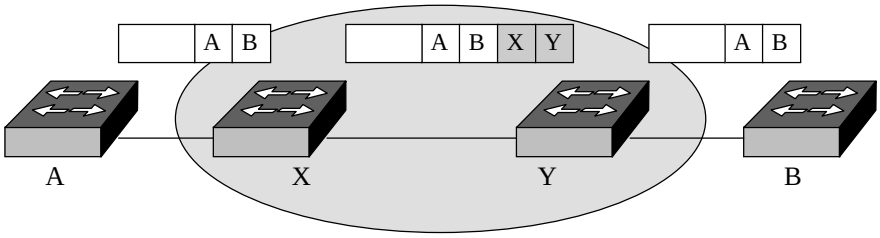



**Abb. 5.13.:** Two-Level-Model [Cis-Sem]

Packet Switches haben MAC-Interfaces zum Fabric-LAN. Der MAC-Adreßraum des Fabric-LAN unterscheidet sich vom MAC-Adreßraum jedes VLAN.

Besonderheiten:
Dem untagged Frame werden 2 völlig neue Adressen hinzugefügt. Der Ethertype-Wert muß sich vom One-Level-Model unterscheiden.
Der vollständig eingehüllte Original-MAC-Frame kann sich vom Typ des tagged Frame hinsichtlich des MAC-Typs (Ethernet, Token Ring, FDDI) unterscheiden.

| 6 Byte Byte | 6 Byte | 2 Byte | 2 Byte | | 4 |
|---|---|---|---|---|---|
| Virtual Dest. address | Virtual Source address | Ethertyp y | VLAN ID | Entire originale frame with FCS | CRC |

**Abb. 5.14.:** Format des tagged Frame beim Two-Level-Model [Cis-802.1q]

[Cis-802.1q], [Data 9/96]

## 5.5. Aktuelle VLAN-Konzepte (anhand ausgewählter Beispiele)

### 5.5.1. Cisco´s VLAN-Strategie

#### 5.5.1.1. VLAN-Development-Roadmap

Die VLAN-Entwicklung ist ein integraler Bestandteil der Cisco Fusion Architektur. Cisco verfolgt damit das Ziel, umfassende Systemlösungen für kosteneffektive, high-performance Switched Internetworks anbieten zu können.

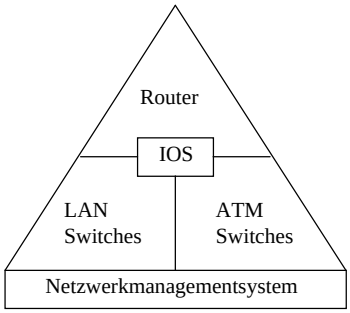



**Abb. 5.15.:** Cisco Fusion Architektur

In Cisco´s VLAN-Development Roadmap werden 5 Entwicklungsphasen aufgezeigt.

| | **Features** | **Benefits** | **Capabilities** |
|---|---|---|---|
| **Phase One (1994)** | VLAN filtering | Performance Management | Address look-up<br>MAC filtering |
| **Phase Two (1995-1997)** | VLAN trunking<br>Inter-VLAN multiprotocol routing<br>VLAN Administration | Bandwidth and change management | Packet Tagging (ISL, IEEE 802.10, LANE)<br>Graphic User Interface based management |
| **Phase Three (1996-1997)** | Multi LAN mapping protocol | Campus-wide VLAN´s | VTP<br>Server integration<br>IEEE 802.1q Tagging |
| **Phase Four (1996-1997)** | Dynamic VLAN´s<br>Automated membership and administration | Automated change management | Virtual configuration server<br>LECS<br>VTP linking |
| **Phase Five (1997-1998)** | Policy driven multi-protocol VLAN´s | Security and application management | Cisco IOS<br>NIC integration |

**Tab. 5.1.:** VLAN-Development Roadmap [Cis(11)96]

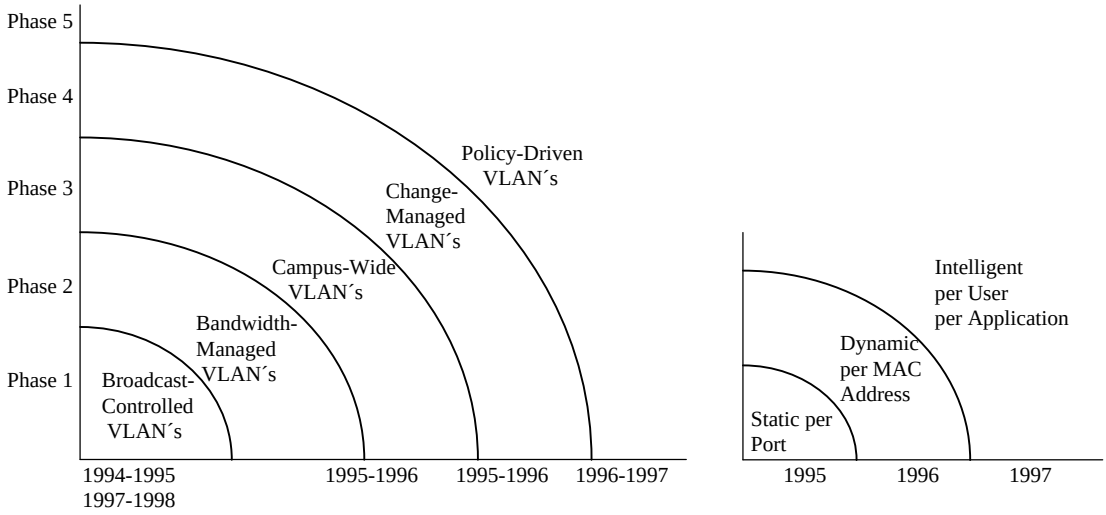



**Abb. 5.16. :** VLAN-Evolution (VLAN-Development-Roadmap/aus Sicht der Flexibilität)

[Cis(11)96 und Cis-Sem]

Charakterisierung der einzelnen Phasen:

Phase 1: Broadcast Controlled VLAN´s (1994)

- Kontrolle des Broadcastaufkommens zwischen Switchports/Nutzern zur Steigerung der Netzleistung
- Grundlage: Filtering-Tabellen (Zuordnung von Ports und MAC-Adressen zu VLAN´s)
- effektive Methode in kleinen Netzen, nicht skalierbar über Campus (Synchronisierungs- und Tabellenaustauschverfahren erforderlich, erhöhter Verwaltungsoverhead)
- Verringerung der Switch-Leistung (Filterfunktionen)

2. Phase: Bandwidth-Managed VLAN´s (1995)

- Einführung von Catalyst 5000 und Cisco 7000 Routern als Basis für eine revolutionäre Technologie zur VLAN-Bildung
- Packet Tagging: ermöglicht VLAN-Bildung über High-Speed-Uplinks (FDDI, Fast Ethernet, ATM) ohne Einwirkung auf die Switching Performance und die Notwendigkeit komplexer Filtermechanismen
- portbasierte Zuordnung zu VLAN´s
- managebare Broadcast-Domänen
- Bandbreitenmanagement, Funktionen wie Load Distribution usw.
- Einführung grafischer Managementoberflächen zur VLAN-Verwaltung (VLAN-Direktor)

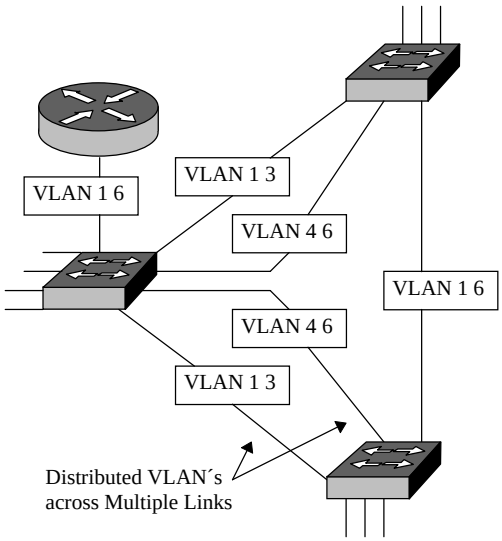



**Abb. 5.17.:** Load Distribution

[Cis(13)95]

Phase 3: Campus-Wide VLAN´s 1996-1997

- Möglichkeit der Abbildung von VLAN´s über unterschiedliche Backbone-Technologien
- Packet Tagging für unterschiedliche Backbone-Technologien

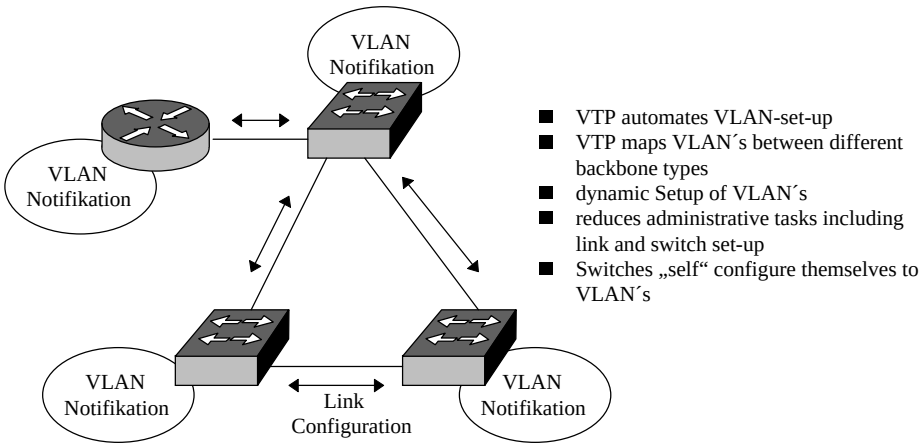



**Abb. 5.18.:** VTP [Cis-Sem]

- Mapping-Protokoll zur automatischen Konfiguration von VLAN´s über den Campus (unabhängig vom Backbonetyp): **Cisco VTP** (Virtual Trunk Protocol)
  - integraler Bestandteil von Cisco IOS
  - Switch-to-Switch-/Switch-to-Router-VLAN-Management-Protocol, welches alle VLAN-Konfigurationsinformationen automatisch (bei Neueinrichtungen, Rekonfigurationen oder Umbenennungen,..) über das Netzwerk verteilt (keine manuelle Konfiguration an jedem Switch nötig)
  - Möglichkeit der zentralen VLAN-Verwaltung

Phase 4: Automated Change Management (1996-1997)

- Ziel: Reduzierung der Verwaltungsaufgaben bei Änderungen der Konfiguration, höhere Flexibilität
- zentrales Management und dynamische VLAN-Konfigurationsarchitektur
- Zuordnung von Nutzern anhand ihrer MAC-Adressen

- Minimierung von Konfigurationsaufgaben bei Umzügen, Switch-Port erkennt umgezogenes Gerät anhand der MAC-Adresse und kann dieses mittels einer zentralen Management-VLAN-Datenbasis (zur Autokonfiguration) zuordnen
- Einführung eines zentralen Konfigurationsserver, dessen Datenbasis vom Netzadministrator verwaltet und gewartet wird (Download bei Änderungen)

**VCS - Virtual Configuration Server**

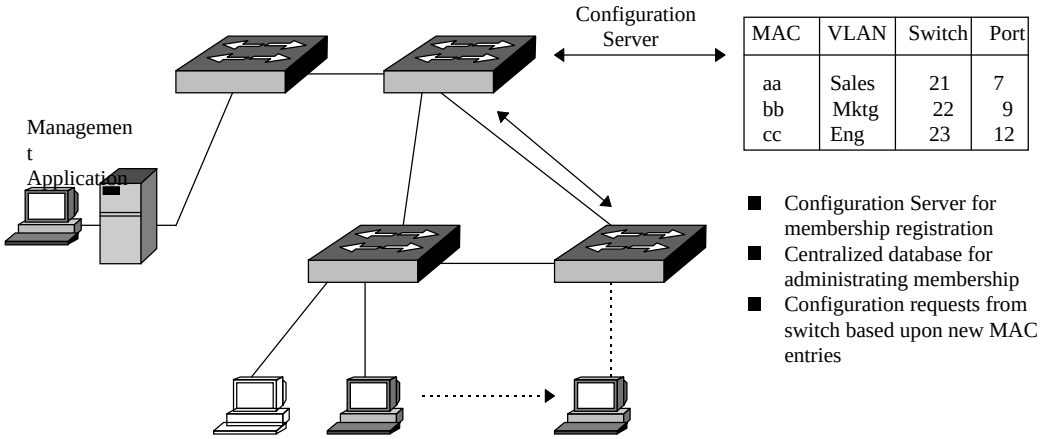



**Abb. 5.19.:** Dynamic VLAN´s [Cis-Sem]

- VCS beantwortet VLAN-Zugehörigkeits-Requests
- Implementierung von VCS, LECS (für ATM-Clients), VTP (automatische Konfiguration übers Netzwerk) und Netzmanagement als Basis dynamischer VLAN´s

Phase 5: Policy Driven VLAN´s (1997-1998)

- zukünftig: VLAN-Zugehörigkeit unabhängig von der physikalischen Lokalisation, erweiterte Sicherheitsmechanismen, neue Dienstklassen und höhere Intelligenz im Netz
- intelligenter VLAN-Konfigurationsmechanismus, welcher über MAC-basierte oder Netzwerk-Layer-Adressen-basierte Zuordnung hinausgeht
- Zuordnung entsprechend der Dienstklassen oder Anwendungen, Einbeziehung höherer Level zur VLAN-Zuordnung
- Möglichkeit der Vergabe unterschiedlicher Prioritätsklassen (optimale Netzressourcenzuordnung zu den Dienstklassen)

- zentrale Intelligenz im Netz erkennt Applikationstypen und VLAN-Prioritäten
- bei Registrierung: 1. VLAN-Membership-Request an VCS (Basis MAC-Adresse)
  2. als Erweiterung: Erkennung der Applikation für Bandbreitenanforderung und Zuordnung zu einer Dienstklasse

[Cis(11)96]

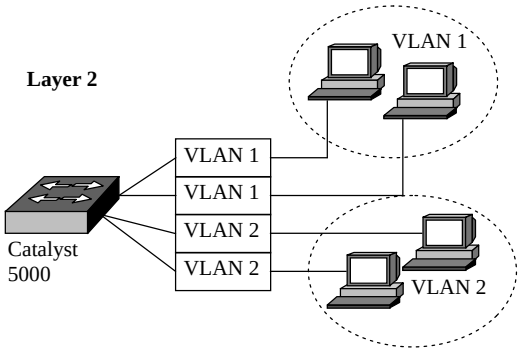
### 5.5.1.2. Derzeitige VLAN-Implementierung

Cisco bietet eine breite Angebotspalette VLAN-fähiger Produkte.

VLAN-Unterstützung in:

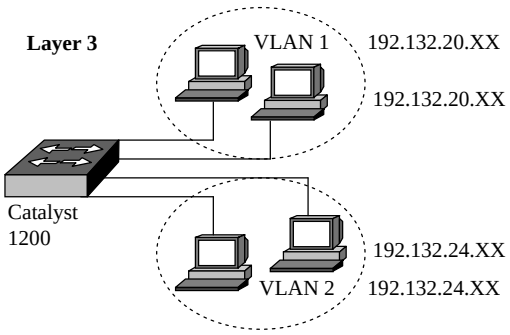
- Catalyst-Produktfamilie (LAN-Switches)
- Lightstream-Produktfamilie (ATM-Switches)
- Cisco Router

In Produkten der Catalyst LAN-Switch Familie werden VLAN´s auf Layer 2 und 3 unterstützt.




Ports Identify VLAN Membership with Unique ID

- portweise Zuordnung
- einfache Konfiguration und Verwaltung
- Verwendung des Packet Tagging (einem an b estimmten Switchport empfangenen Paket wird eigener VLAN-ID im Header zugefügt, weitere Übertragung anhand des VLAN-ID und der MAC-Adresse)




Ports Identify VLAN Membership Based on Network Layer Address

- Catalyst 1200 unterstützt Layer-3- VLAN´s für IP-Subnetze
- Segmentierung basiert auf Subnetz-Adreßmapping
- Integriertes Routing zwischen IP-Subnetzen

**Abb. 5.20.:** Multilayer VLAN´s [Cis(13)95]

[Cis(13)95], [Cis-Cat]

VLAN´s über Backbone-Strukturen

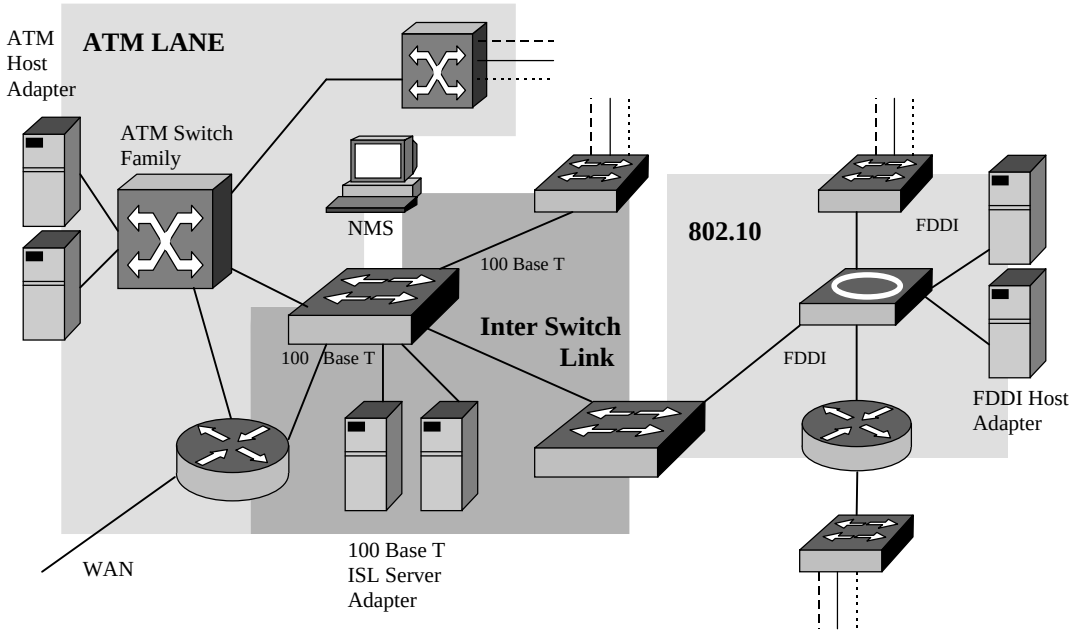



**Abb. 5.21.:** Cisco-VLAN-Architektur [Cis-Sem]

VLAN´s und ATM: - Implementierung der ATM-Forum LANE Spezifikation
- ELAN´s ermöglichen VLAN-Verbindungen übers ATM-Backbone, zudem können ATM-angeschlossene Geräte mit Shared Media angeschlossenen Stationen im VLAN kommunizieren

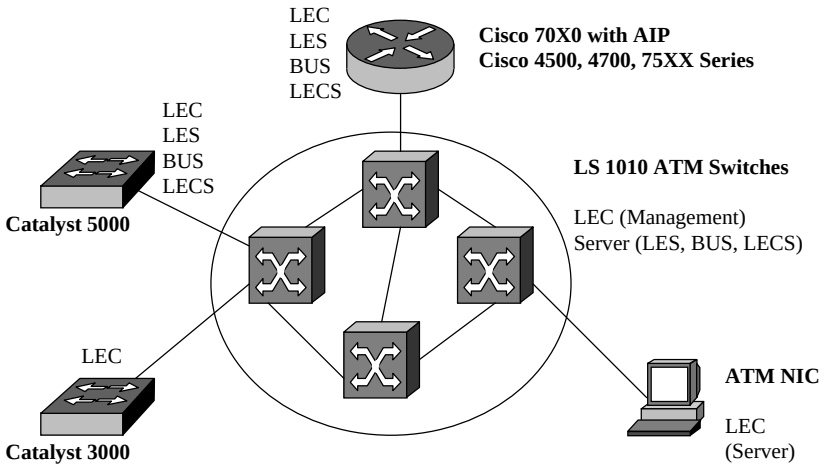



**Abb. 5.22.:** Unterstützung der LAN Emulation in Cisco Produkten

VLAN´s über LAN-Backbone-Technologien:

Cisco entwickelte eine Serie von Interswitch Protokollen für die VLAN-Kommunikation über LAN-Backbone-Technologien. Diese sind unter den Gesichtspunkten einer optimierten Leistung für das jeweils verwendete Backbone-Medium und der Interoperabilität zwischen Cisco-Komponenten entworfen.

- IEEE 802.10:

  Cisco modifizierte das IEEE 802.10 Security Protocol für Interswitch-Verbindungen über FDDI-Backbones. Ein 32 Bit (4 Byte) VLAN-ID wird jedem Paket vorangestellt und dient der Weiterleitung des Paketes an Switches, Router, usw., die dem selben VLAN angehören. Die Switches können anhand des VLAN-ID eine Zuordnung zu den entsprechenden Ports vollziehen.

- ISL (Inter Switch Link)

  Für die Unterstützung der VLAN-Kommunikation über Fast-Ethernet-Backbones entwickelte Cisco das ISL-Protokoll. Diese verwendet eine 10-Bit-Adressierungstechnik, welche jedem Paket angefügt wird. Die Weiterleitung des Paketes erfolgt nur an Switches, die die gleiche 10-Bit-Adresse enthalten. ISL ermöglicht ein kontrolliertes Broadcastaufkommen zwischen den Switches und Routern.

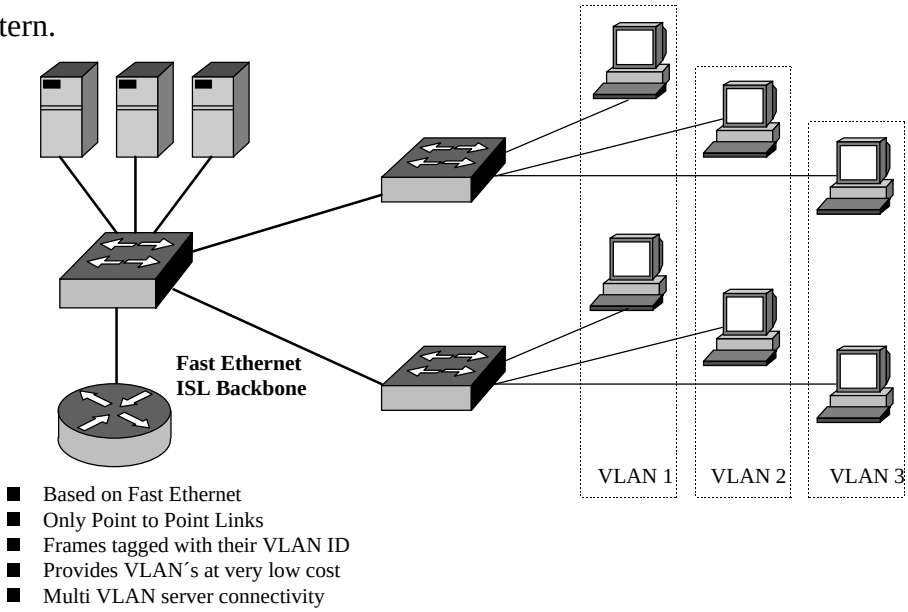



**Abb. 5.23.:** ISL [Cisco-Sem] [Cis-Sem], [Cis(13)95]

## 5.5.2. Vergleich der VLAN-Konzepte von Cisco und 3Com

| | **Cisco** | **3Com** |
|---|---|---|
| **VLAN-fähige Komponenten:** | | |
| ATM-Switches | ■ Lightstream 1010 | ■ Cellplex 7000HD |
| LAN-Switches mit ATM-Uplink | ■ Catalyst 5000<br>■ Catalyst 3000 | ■ LANplex 2500<br>■ LinkSwitch 1000, 3000, 2700 |
| Router | ■ Cisco 7000, 4000 Serie | ■ Netbuilder II |
| **IP over ATM** | ja | ja |
| **PNNI** | Phase 1 | Phase 0 mit funktionalen Erweiterungen |
| **Basis der VLAN-Zuordnung** | ■ Switchport (1 MAC-Adresse je Switch Port)<br>■ (MAC-Adressen zukünftig)<br><br>im Catalyst 5000 kann jeder Port einem VLAN zugeordnet werden, Highspeed-Ports (Fast Ethernet) können Mitglied in mehreren VLAN´s sein | ■ Switchport<br>■ MAC-Adressen<br>■ IP-Adressen, Subnetzadressen<br>■ Layer-3-Protokolle |
| **VLAN-Organisation** | | Einsatz von ASIC´s |
| **VLAN´s über Backbone-technologien via** | 802.10, ISL, LANE 1.0 | LANE 1.0 |
| **LANE-Unterstützung** | (siehe auch Bild 5.22) | |
| Server (LECS, LES, BUS) | ■ Cisco Router 70X0, 75XX, 4500, 4700 Serien<br>■ Lightstream 1010<br>■ Catalyst 5000 | ■ Router (Netbuilder)<br>■ ATM-Switch (Cellplex)<br>■ LAN-Switches |
| LECS | redundant | redundant |
| Clients | ■ Router, Catalyst 5000/3000, ATM-Interfacekarten<br>■ Lightstream 1010 (für Management) | ■ Router, ATM-/LAN-Switches und Interfacekarten |
| Verteilung der LANE-Services | dezentral möglich | dezentral möglich |
| Leistungs-fähigkeit | ■ je ATM-Interface-Processor-Board eines Cisco 75XX: Unterstützung von maximal 256 ELAN´s | ■ je Cellplex 16 ELAN´s<br>■ je LANplex 2500 14 ELAN´s<br>■ je Netbuilder maximal 75 VLAN´s (als sinnvolle Größenordnung ohne Performance-Einschränkungen werden 10 empfohlen) |
| **Internetworking zwischen VLAN´s** | ■ Multiprotokoll im Router | ■ lokal im LANplex 2500 (IP, IPX, Apple Talk) [Reduzierung der Netzlast]<br>■ andere Protokolle im Router, sowie zwischen backbone-übergreifenden VLAN´s |
| **Routing-funktionen** | zentral | dezentral |

| | | |
|---|---|---|
| **Netzlasten aus Routing zwischen VLAN´s** | höher durch zentrales Internetworking | geringer durch dezentrales Internetworking |
| **Firewall-Funktionen zwischen VLAN´s** | ja | ja |
| **Management-software** | Cisco Works | Transcend Enterprise Manager |
| **Verwaltung aller Geräte unter einer Oberfläche** | ja | ja |
| **Tools zur VLAN-Verwaltung** | VLAN Director<br>■ grafisches Benutzerinterface<br>■ Konfiguration von VLAN´s<br>■ VLAN-Monitoring (per Switch/ per Port)<br>■ Topologie-Mapping auf physikalischer und logischer Ebene<br>■ VLAN-Statusinformationen<br>■ VLAN-Fehlermanagement<br>■ drag-&-drop Funktionalität für Nutzerzuordnung<br>■ Anzeige von Statusinformationen für Geräte, Ports<br>■ Verbindungsmanagement | Integraler Bestandteil des Transcend NMS (ATM-, LANE-, VLAN-, Device-Tools)<br>■ Konfiguration von VLAN´s<br>■ grafisches Benutzerinterface<br>■ Darstellung von Strukturen:<br>■ physikalisches Netz<br>■ VLAN´s<br>■ ELAN´s<br>■ IP-Gruppen<br>■ Geräteansichten und Statusanzeigen für Gesamtgeräte, Module, Ports<br>■ Management-Informationen zum Netzstatus |

**Tab. 5.2.:** Vergleich Cisco/3Com hinsichtlich der angewendeten VLAN-Konzepte

Aus dem Vergleich ergibt sich, daß Cisco eine relativ flache VLAN-Architektur anwendet (derzeit lediglich portbasierte Zuordnung möglich).

3Com bietet hinsichtlich der Möglichkeiten der VLAN-Zuordnung eine höhere Flexibilität.