ComConsult Research

Der Netzwerk Insider

März 2008

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit

Kommunikationssicherheit auf dem Irrweg

von Dr. Behrooz Moayeri

Im Netzwerk Insider vom Juli/August 2007 wies der Autor darauf hin, dass Kommunikationssicherheit letztendlich immer mit Verschlüsselung einhergeht.

Dies leuchtet insbesondere dann ein, wenn man bedenkt, unter welchen Bedingungen man von einem „vertrauenswürdigen“ Netz sprechen kann. Ein IP-Netz ist nur dann vertrauenswürdig, wenn alle an dieses Netz angeschlossenen Systeme als vertrauenswürdig eingestuft werden können. Und dies wiederum setzt voraus, dass alle diejenigen Personen, die auf irgendwelche dieser Systeme uneingeschränkten Zugriff (zum Beispiel Administrationsrechte) haben, vertrauenswürdig sind. Kaum ein IP-Netz würde diese Bedingungen erfüllen.

Also bleibt zum Erreichen der Kommunikationssicherheit kein anderer Weg als Ende-zu-Ende-Verschlüsselung. Wie im genannten Beitrag dargestellt, ist das auch der Weg, den man geht, wenn man zum Beispiel eine Banktransaktionen über das Internet durchführen muss. Es muss eine Ende-zu-Ende-Verschlüsselung geben, und die beiden Enden der Kommunikation müssen vertrauenswürdig sein, d.h. sowohl die involvierten Personen als auch die Endsysteme.

weiter auf Seite 17

Zweitthema

Die nächste Enterprise-WLAN-Generation mit IEEE 802.11n

von Dr. Simon Hoff

Mit IEEE 802.11n soll dieses Jahr ein WLAN-Standard verabschiedet werden, der mit einer neuen Übertragungstechnik Datenraten auf der physikalischen Ebene von bis zu 600 MBit/s brutto erreichen wird. Im Betrieb dieser Systeme wird mit einer tatsächlichen Datenrate von meist 200 MBit/s bis 300 MBit/s zu rechnen sein. Netto (d.h. oberhalb des MAC Layer) ergibt dies eine Datenrate von mehr als 100 MBit/s. Nur zum Vergleich: Systeme nach den Standards IEEE 802.11a bzw. IEEE 802.11g schaffen brutto maximal 54 MBit/s und netto ca. 25 MBit/s.

Aktuell sind diverse Vorstandardprodukte auf dem Markt verfügbar und erste Enterprise-taugliche Geräte werden angeboten. Da die Wi-Fi Alliance inzwischen ein eigenes Zertifizierungsprogramm basierend auf Draft 2.0 von IEEE 802.11n im Programm hat, sind diese Vorstandardprodukte durchaus ernster zu bewerten.

weiter auf Seite 9

Aktuelle Agenda

Netzwerk-Redesign Forum 2008

ab Seite 4

Geleit

Rechen-zentrumsnetze im Redesign: wie virtuell wird die Zukunft?

ab Seite 2

Report des Monats

Leseprobe: Office Communications Server 2007

ab Seite 14

Zum Geleit

Rechenzentrumsnetze im Redesign: wie virtuell wird die Zukunft?

Das Redesign bestehender Rechenzentren steht bei vielen Unternehmen weit oben auf der Prioritätenliste. Häufig motiviert von Platz, Klima, Strom, Gewichts-Problemen, kommt dabei auch das Netzwerk mit auf den Tisch. Und hier hat sich in den letzten Monaten viel getan.

Herausragendes Beispiel ist der neue Nexus-Switch von Cisco, der aus mehreren Gründen spannend ist:

- er verdeutlicht, wie hoch der Bandbreitenbedarf im RZ in Zukunft werden kann. Seine Gesamtkapazität liegt im Terabitbereich, die angestrebten Schnittstellen sind über 10 Gigabit hinaus die zukünftigen 40 und 100 Gigabit-Schnittstellen

- er macht auch klar, dass der bisher mit dem 6500 gepflegte Ansatz der beliebigen Integration von Appliances in Switchgehäuse seine technischen Grenzen hat. Je höher die Datenrate wird, desto weniger könnten diese „Server-Einschübe“ noch auf Wirespeed-Ebene arbeiten

Das Schlüsselthema in der Weiterentwicklung der RZ-Netzwerke ist ohne Frage die Virtualisierung. Dies hat ganz unterschiedliche Facetten:

- virtualisierte Server müssen in Netzwerke eingebunden werden, der Trend geht hier zum virtualisierten Adapter, der ggf. am Hypervisor vorbei direkt auf eine 10 bis 100 Gbit/s-Leitung zum nächsten physikalischen Switch zugreifen kann

- Speicher müssen in Netzwerke integriert werden. Ein wesentlicher Trend ist der virtuelle Fibre Channel, der als Kanal in einem Ethernet läuft und im Server ebenfalls über virtuelle Adapter realisiert wird

- IT- und Server-Virtualisierungstechnik entwickelt sich immer weiter. Die virtualisierten Einheiten werden immer kleiner und gehen runter auf das Niveau von Applikationen. Microsoft ist offenbar sehr an diesem Thema interessiert

- Ablösung der bisherigen Systembusse durch Netzwerke, direkte Verbindung von CPU´s durch Ethernet

Das waren Beispiele, die aber die Kernthemen klar machen:

- Einbindung virtueller Maschinen

- Einbindung von Blade-Servern

- Einbindung von virtuellen Applikationen

- Integration von Speicher- und Datennetzwerken

- Verteilte Architekturen, in denen angefangen von der CPU über den RAM bis hin zum Massenspeicher alles verteilt ist

Damit entsteht auch die Frage nach dem technischen Sinn. Bis auf die hohen Bandbreitenanforderungen erinnert das sehr an das „Ethernet in der Produktion“-Thema. Eine Reihe dieser RZ-Netzwerke vertragen keinen Fehler. Fibre Channel als Beispiel setzt eine fehlerfreie Übertragung voraus. Damit kann Ethernet selber naturgemäß nicht dienen. Also steht wieder einmal zur Diskussion, wie das Basis-Verfahren „Geswitchtes Ethernet“ sinnvoll erweitert werden kann. Ein Kernproblem sind mögliche Überlast-Situationen in Switch-Systemen, die zu einem Puffer-Überlauf führen. Historisch ist dafür die Layer-2-Flusskontrolle mit dem Pause-Kommando geschaffen worden. Diese Lösung verschiebt aber den Endpass nur weiter in Richtung der Sender so lange diese nicht aufhören zu senden (was bei Speicher-Netzwerken nicht zwingend ein gewünschtes Feature ist, dass die Sendung unterbrochen werden muss).

Hier besteht Diskussionsbedarf.

Wohin gehen RZ-Netzwerke, was müssen sie leisten, welche technischen Verfahren fehlen, in wie weit können die Anforderungen moderner Speicher und zukünftiger Virtualisierungsverfahren wirklich abgedeckt werden, welche Bandbreite wird benötigt? Kommt Ethernet verfahrenstechnisch wieder einmal an seine Grenzen, finden wir dazu eine sinnvolle Lösung? 40 und 100 Gigabit-Ethernet, doch mehr als ein Provider-Thema?

Wir greifen dieses Thema als eines der Schwerpunkt-Themen des Netzwerk-Redesign Forums 2008 auf. Dr. Moayeri präsentiert die Analyse des Themas, Cisco stellt sich der Nexus-Diskussion, diverse andere Hersteller präsentieren ihre Position zu diesem brisanten (und durchaus teuren) Thema.

RZ-Netzwerke sind eine Schlüsselinfrastruktur für die Zukunft. Unzureichende Kapazitäten oder Qualitäten können den Einsatz wichtiger IT-Technologien blockieren.

Eine spannende Entwicklung. Ich würde mich freuen, dies mit Ihnen auf dem Forum diskutieren zu können.

Ihr
Dr. Jürgen Suppan

Zweitthema

Die nächste Enterprise-WLAN-Generation mit IEEE 802.11n

Fortsetzung von Seite 1

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung und Betrieb im Bereich lokaler Netze, mobiler Kommunikationssysteme und deren Anwendungen zurück.

In diesem Artikel wird die Technik hinter IEEE 802.11n vorgestellt, die Marktsituation der Vorstandardprodukte analysiert sowie Planungs- und Migrationsaspekte betrachtet.

1. Technische Konzepte

Wesentliche Rahmenbedingung bei der Gestaltung von IEEE 802.11n ist die Forderung der Abwärtskompatibilität zu den aktuell verwendeten Übertragungstechniken IEEE 802.11a und IEEE 802.11g.

Damit die hohe Datenrate erreicht werden kann, spezifiziert IEEE 802.11n eine neue physikalische Übertragung. Dabei wird eine Erweiterung des aus IEEE 802.11a/g bekannten Orthogonal Frequency Division Multiplexing (OFDM) vorgenommen und mehrere dieser Systeme trickreich mit einem als Multiple Input Multiple Output (MIMO) bezeichneten Verfahren gebündelt, wie in Abbildung 1 illustriert. Im Folgenden werden die wesentlichen technischen Aspekte von IEEE 802.11n beschrieben.

1.1 High Throughput OFDM

IEEE 802.11n verwendet eine erweiterte OFDM-Übertragung, die als High Throughput OFDM (HT-OFDM) bezeichnet wird. Die Datenrate für einen OFDM-Kanal berechnet sich allgemein durch die Formel Datenrate = BS * SR * AU * CR, wobei BS die vom Modulationsverfahren abhängige Anzahl der pro Symbol dargestellten Bits ist, SR die Symbolrate, AU die Anzahl der Unterträger und CR die Code-Rate (d.h. das Verhältnis von Nutzdatenbits zu tatsächlich übertragenen mit zusätzlichen Fehlerkorrekturinformationen versehenen Bits) bezeichnet. Die verwendeten Modulationsverfahren entsprechen denen von IEEE 802.11a/g. Die Symbolrate beträgt für ein OFDM-System, wie es bei IEEE 802.11a/g verwendet wird, 0,25 Mega-Symbole pro Sekunde bei 800 ns Abstand zwischen den Symbolen (Guard Intervall, GI). HT-OFDM sieht auch die optionale Verwendung eines GI von 400 ns vor, was die Datenrate entsprechend erhöht. Bei einer Kanalbandbreite von 20 MHz werden (statt 48 Unterträger wie bei IEEE 802.11a/g) 52 Unterträger für die Übertragung von Daten bei IEEE 802.11n verwendet. Bei einer optionalen Kanalbandbreite von 40 MHz sind dies 108 Unterträger. Bei den verwendeten Code-Raten kommt in HT-OFDM zu denen von IEEE 802.11a/g die Rate 5/6 hinzu, was den geringsten Codierungs-Overhead hinzufügt und daher nur bei sehr guten Empfangsbedingungen sinnvoll nutzbar ist.

Tabelle 1 zeigt die sich für HT-OFDM zunächst ergebenden Datenraten im Überblick.

1.2 Multiple Input Multiple Output

Die erhebliche Steigerung der physikalischen Datenrate bei IEEE 802.11n wird durch den Einsatz der Übertragungstechnik Multiple Input Multiple Output (MIMO) erreicht.

Bei einem MIMO-System wird die Übertragung parallel durch mehrere Sendeeinrichtungen mit jeweils eigener Antenne auf der gleichen Frequenz durchgeführt. Zu übertragende Daten werden auf diese (ähnlich zu einer parallelen Schnittstelle an einem PC) aufgeteilt und auf der Empfängerseite durch mehrere Empfangseinrichtungen mit je einer eigenen Antenne parallel empfangen. An jeder dieser Empfangseinrichtungen kommt nun eine eigene Variante der sich überlagernden Signale an. Ein moderner Signalprozessor verarbeitet die Varianten und ermöglicht eine Trennung der überlagerten Signale. Dabei wird die Information genutzt, dass die Signale über verschiedene räum-

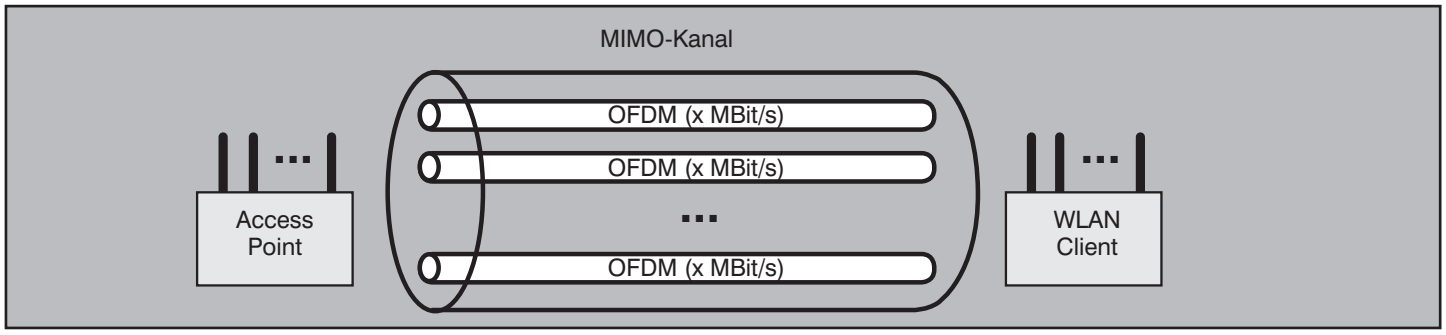

Abbildung 1: Bündelung von OFDM-Kanälen zu einem MIMO-Kanal

		Datenrate [MBits/s]				
		OFDM	**HT-OFDM**			
Modulation	**Coderate**	48 Unterträger, 800 ns GI, 20 MHz Kanalbreite	52 Unterträger, 800 ns GI, 20 MHz Kanalbreite	52 Unterträger, 400 ns GI, 20 MHz Kanalbreite	108 Unterträger, 800 ns GI, 40 MHz Kanalbreite	108 Unterträger, 400 ns GI, 40 MHz Kanalbreite
BPSK	1/2	6	6,5	7,2	13,5	15
QPSK	1/2	12	13	14,4	27	30
QPSK	3/4	18	19,5	21,7	40,5	45
16QAM	1/2	24	26	28,9	54	60
16QAM	3/4	36	39	43,3	81	90
64QAM	2/3	48	52	57,8	108	120
64QAM	3/4	54	58,5	65	121,5	135
64QAM	5/6		65	72,2	135	150

Tabelle 1: Datenraten für OFDM und HT-OFDM

lich getrennte Sende- und Empfangsantennen übertragen werden. Letztendlich wird bei MIMO die Mehrwege-Ausbreitung einer Funkübertragung gezielt für die Erhöhung der Übertragungsleistung genutzt (Abb. 2).

Eine MIMO-Komponente bestehend aus Übertragungs-/Empfangsteil und Antenne wird als Zug (Spatial Stream) bezeichnet. Für MIMO-Systeme im WLAN-Bereich wird von zwei bis vier Sender- und Empfängerzügen ausgegangen. Grundsätzlich sind aber auch mehr als vier Züge nicht ausgeschlossen.

Damit ergeben sich die erreichbaren Datenraten eines MIMO-Systems einfach durch Multiplikation der Datenrate des zugrundeliegenden HT-OFDM-Systems mit der Anzahl der Züge, wie in Tabelle 2 gezeigt. Bei der höchsten Code-Rate 5/6, mit 4 Zügen, 400 ns GI und einer Kanalband-

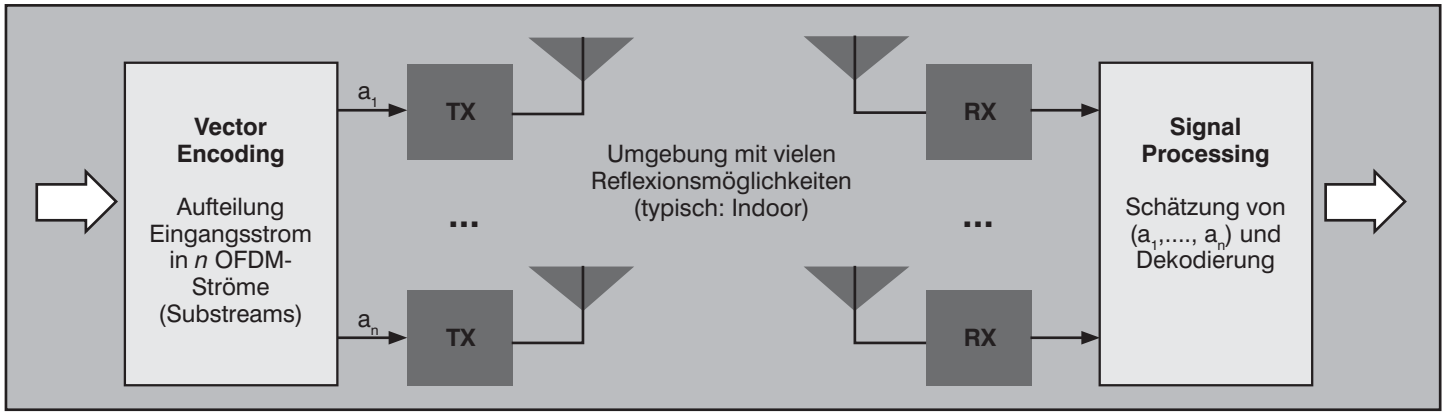

Abbildung 2: Funktionsweise eines MIMO-Systems

		Datenrate [MBits/s]							
		52 Unterträger, 400 ns GI							
		20 MHz Kanalbreite				**40 MHz Kanalbreite**			
Modulation	**Coderate**	1 Zug	2 Züge	3 Züge	4 Züge	1 Zug	2 Züge	3 Züge	4 Züge
BPSK	1/2	7,2	14,4	21,7	28,9	15	30	45	60
QPSK	1/2	14,4	28,9	43,3	57,8	30	60	90	120
QPSK	3/4	21,7	43,3	65	86,7	45	90	135	180
16QAM	1/2	28,9	57,8	86,7	115,6	60	120	180	240
16QAM	3/4	43,3	86,7	130	173,3	90	180	270	360
64QAM	2/3	57,8	115,6	173,3	231,1	120	240	360	480
64QAM	3/4	65	130	195	260	135	270	405	540
64QAM	5/6	72,2	144,4	216,7	288,9	150	300	450	600

Tabelle 2: Datenraten eines MIMO-Systems

Schwerpunktthema

Virtuelle LANs am Arbeitsplatz bringen keine Sicherheit - Kommunikationssicherheit auf dem Irrweg

Fortsetzung von Seite 1

Dr. Behrooz Moayeri gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und beschäftigt sich seit ca. 15 Jahren mit Kommunikationssicherheit.

Der Benutzer muss zu seinem eigenen Endgerät Vertrauen haben, damit auch zu allen Personen mit administrativem Zugriff auf das Endgerät, und er muss sicherstellen können, dass es sich zum Beispiel bei dem anderen Ende des Kommunikationspfades um den Webserver seiner Bank handelt. Dies wird durch Authentifizierung mittels einer Public Key Infrastructure (PKI) erreicht.

Aber diese fundamentalen Erkenntnisse scheinen in der Kommunikationswelt nicht überall angekommen zu sein. Sonst wäre nicht zu erklären, warum statt der Ende-zu-Ende-Verschlüsselung häufig andere Wege zum Erreichen einer sicheren Kommunikation beschritten werden. Dabei handelt es sich teilweise um Irrwege.

Der vorliegende Beitrag geht auf diese Irrwege ein. Konkret wird begründet, warum Virtual Local Area Networks (VLANs) am Arbeitsplatz keine Sicherheit bringen. Genau dieser Weg, nämlich die Bildung verschiedener VLANs am Arbeitsplatz, wird häufig als eine Methode dargestellt, die Sicherheit der einen vor der anderen Anwendung oder des einen Endgeräts vor den anderen zu erreichen.

Zunächst werden die Konzepte kurz vorgestellt, die mittels VLANs am Arbeitsplatz angeblich für mehr Sicherheit sorgen. Anschließend wird begründet, warum diese Konzepte ohne eine Authentifizierung der Endgeräte im Netz inkonsequent und lückenhaft bleiben. Es folgt eine Darstellung der fundamentalen Schwächen einer reinen Geräteauthentifizierung ohne Verschlüsselung oder zumindest Paketauthentifizierung. Dann wird darauf eingegangen, ob und wie diese Schwächen behoben werden können.

VLAN am Arbeitsplatz: warum und wie?

Virtuelle LANs sind keine neue Erfindung. Sie wurden in den 1990er Jahren dazu erfunden, Broadcast-Domänen in einer Layer-2-Struktur voneinander zu trennen. Die Technik wurde im Rahmen des Standards IEEE 802.1Q standardisiert. Mittels VLANs können mehrere logische Layer-2-Strukturen auf die selbe physikalische Struktur abgebildet werden (siehe Abbildung 1).

Die verschiedenen VLANs sind eigenständige Broadcast-Domänen, die untereinander nicht kommunizieren können, es sei denn, zwei oder mehr VLANs werden außerhalb der Layer-2-Struktur über einen anderen Switch, Router, Gateway, Firewall etc. miteinander verbunden. Aus der Sicht jedes der in der Abbildung 1 dargestellten VLANs handelt es sich bei der Layer-2-Struktur um ein „privates“ Netz; die anderen VLANs sind nicht sichtbar.

Die Voraussetzungen dafür, dass es so bleibt, dass also die verschiedenen VLANs tatsächlich „private“ Netze bleiben und von keinem VLAN aus auf ein anderes VLAN zugegriffen werden kann, sind wie folgt:

- Der Zugriff auf den Layer-2-Switch, der die VLANs voneinander trennt, über den aber Verkehrsströme aller VLANs übertragen werden, bleibt Personen vorenthalten, die aus der Sicht jeder Benutzergruppe vertrauenswürdig sind, ungefähr vergleichbar mit dem Service Provider, der die Daten verschiedener Kunden über die eigene Infrastruktur überträgt und insofern aus der Sicht aller Kunden vertrauenswürdig sein muss.

- Der Layer-2-Switch ist resistent gegen Angriffe, die auf die Aufhebung der Grenzen zwischen den VLANs abzielen, zum Beispiel einen Angriff namens MAC Flooding, der Pakete mit so vielen verschiedenen Source-Adressen an einen Switch sendet, dass dieser gemäß dem Standard IEEE 802.1D Pakete fluten muss. Wenn der Switch diese Paketflutung ohne Rücksicht auf VLAN-Grenzen durchführt, ist der Angreifer am Ziel.

- Die verschiedenen VLANs sind in den beiden Bereichen, in denen nicht vertrauenswürdige Personen präsent sind, auch physikalisch voneinander getrennt. Zum Beispiel darf kein dem

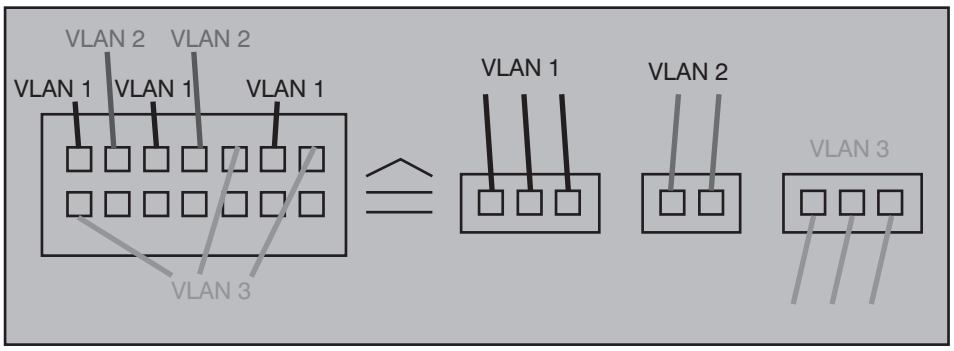

Abbildung 1: Abbildung mehrerer VLANs auf eine Layer-2-Struktur

VLAN 1 zugeordnetes Endgerät bzw. Anwendung durch einfaches Umstecken eines Kabels, Manipulation eines VLAN Tags gemäß IEEE 802.1Q etc. in die Lage versetzt werden können, Zugriff auf VLAN 2 zu erlangen.

Diese Voraussetzungen sind ungefähr mit den Bedingungen vergleichbar, unter denen Service Provider Virtual Private Networks (VPNs) implementieren und ihren Kunden anbieten. Der Kunde A ist über eine dedizierte Leitung mit einem Provider Edge (PE) Router verbunden, der auch andere Kunden bedient. Administrativen Zugriff auf den PE Router hat nur der Service Provider als vertrauenswürdige Instanz für alle Kunden. Die LANs der Kunden sind physikalisch voneinander getrennt, d.h. kein Kunde hat physikalischen Zugriff auf das LAN eines anderen Kunden. Der PE Router und alle anderen Komponenten, welche gemischte Datenströme verschiedener Kunden übertragen, widersteht Angriffen mit dem Ziel des Durchbruchs durch die Grenzen zwischen den VPN.

Ein Service Provider kann nach dem selben Modell auch VPNs aufbauen, die auf VLAN-Technik basieren: Die beiden Kunden A und B unterhalten getrennte physikalische Infrastrukturen, die aber beide mit einem Layer-2-Switch des Providers verbunden sind, allerdings mit verschiedenen VLANs auf diesem Switch. Wenn die o.g. Voraussetzungen erfüllt sind, gelten die VLANs als VPNs.

Aber in den letzten Jahren ist eine etwas andere Nutzung von VLANs als „Sicherheitsmechanismus“ üblich geworden, vor allem mit der Einführung der IP-Telefonie. Dieses Modell basiert darauf, dass verschiedene VLANs bis zu jedem Arbeitsplatz verlängert werden. Dieses Modell ist in drei verschiedenen Varianten in der Abbildung 2 dargestellt.

In allen dargestellten drei Varianten sind der Computer und das IP-Telefon verschiedenen VLANs zugeordnet. In den meisten Fällen befinden sich ein Computer und ein Telefon im selben Raum und werden von der selben Person genutzt. Insofern wird das Prinzip der physikalischen Trennung zwischen den VLANs nicht mehr eingehalten. Der Benutzer könnte seinen PC an das VLAN 1 (das dem Telefon vorenthaltene VLAN) anschließen und umgekehrt. Unter solchen Bedingungen lassen sich die VLAN-Grenzen technisch nicht erzwingen. Die VLAN-Trennung bringt also keine Sicherheit.

Die drei Szenarien unterscheiden sich in den Details. In dem ersten Szenario, das

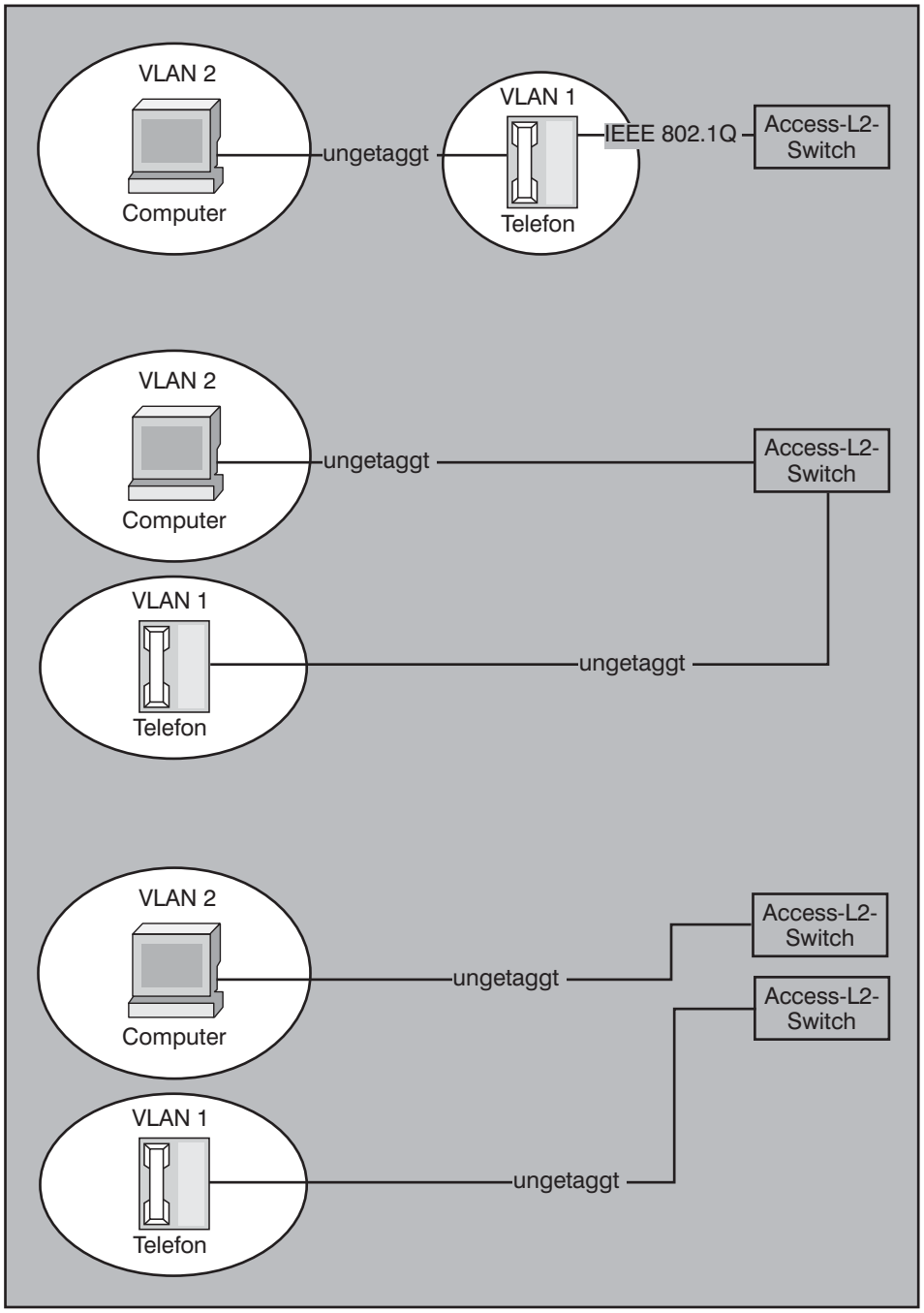

Abbildung 2: VLANs am Arbeitsplatz

im oberen Teil der Abbildung 2 dargestellt ist, und das in den meisten Unternehmen aus Kostengründen (zur Einsparung von Access Switch Ports und Kabeln) angewandt wird, ist der PC an einen Miniswitch im Telefon angeschlossen. Dieser Miniswitch leitet zum Beispiel in einer gängigen Konfiguration die Pakete des PCs ohne einen VLAN Tag gemäß IEEE 802.1Q weiter, während die Pakete des Telefons selbst mit einem IEEE 802.1Q Tag versehen werden, der die VLAN ID für das „Voice VLAN“ enthält (siehe Abbildung 3).

In der anderen Richtung versieht der Access Switch alle für das Telefon bestimmten Pakete mit der VLAN ID für Voice und lässt die Pakete an den PC ungetaggt. Damit diese Konfiguration funktioniert, muss das IP-Telefon die VLAN ID für Voice kennen. Dies kann durch verschiedene Verfahren sichergestellt werden:

- Das aufwändigste Verfahren besteht darin, dass die Voice VLAN ID manuell an jedem IP-Telefon konfiguriert wird. Dies bedeutet, dass bei jenen Umzügen, in denen sich die zu nutzende