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

Rechenzentrumsnetze 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

Aktueller Kongress

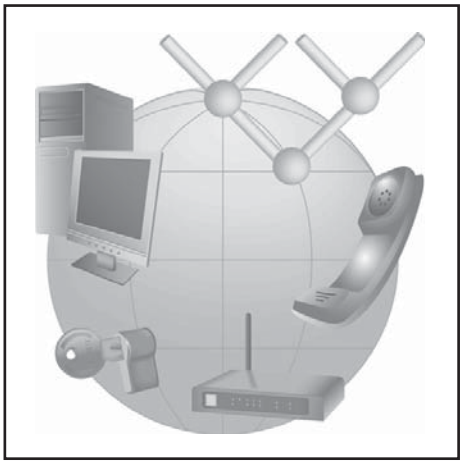
Netzwerk-Redesign Forum 2008

Die ComConsult Akademie veranstaltet vom 14. - 17. April 2008 das „Netzwerk-Redesign Forum 2008“ in Königswinter.

Netzwerke sind der Lebensnerv der IT. Sie unterliegen einer permanenten Weiterentwicklung, wobei sich die Anforderungen nahezu permanent verändern. Parallel verändern sich die Möglichkeiten, die neue Netzwerk-Technologien liefern. Aus diesem Mix aus Bedarf und Potenzial muss das wirtschaftliche und technische Optimum gefunden werden. Da Netzwerke bereits vorhanden sein müssen bevor entsprechende Projekte umgesetzt werden können, muss das Netzwerk-Design grundsätzlich an der Zukunft orientiert sein.

Hier setzt das ComConsult Netzwerk-Redesign Forum 2008 an. Es analysiert die wichtigsten Bedarfsentwicklungen, stellt diesen die neuesten Netzwerk-Technologien gegenüber und erarbeitet Empfehlungen für ein erfolgreiches Netzwerk-Design und einen stabilen und zuverlässigen Betrieb.

Das ComConsult Netzwerk-Redesign Forum ist traditionell der Treffpunkt der deutschen Netzwerk-Branche. Es bildet die



ideale Basis, um sich technisch auf dem Laufenden zu halten und zu sehen, was im Markt passiert.

Die Schwerpunktthemen des ComConsult Netzwerk-Redesign-Forums 2008 sind:

- Applikations-bewusste Netzwerke
- WAN-Redesign
- Rechenzentrum und Server-Konsolidierung
- Integration mobiler Mitarbeiter / Fixed-Mobile-Konvergenz
- Video
- Voice-over-IP und Kollaboration
- Ethernet in der Produktion
- Wireless-Netzwerke
- Sicherheit

Moderiert wird der Kongress von Dr. Jürgen Suppan, der als einer der führenden Berater für Kommunikationstechnik und verteilte Architekturen gilt. Unter seiner Leitung wurden in den letzten 25 Jahren diverse Projekte aller Größenordnungen erfolgreich umgesetzt. Sein Arbeitsschwerpunkt ist die Analyse neuer Technologien und deren Nutzen für Unternehmen. Er leitet das internationale Labor von ComConsult-Research in Christchurch, das die Technologieentwicklung in Asien, Australien, den USA und Europa analysiert und für Kunden bewertet.

Das ComConsult Netzwerk-Redesign Forum 2008 ist die zentrale Netzwerk-Veranstaltung des Jahres 2008. Sie ist für jeden Entscheider, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk-Redesign Forum 2008

☐ Ich buche den Kongress
Netzwerk-Redesign Forum 2008
14.04. - 17.04.08 in Königswinter

mit Intensiv-Training am letzten Tag
☐ Thema 1: Voice-Readiness
☐ Thema 2: Zukunft der Weitverkehrstechnik: wohin geht der Weg?
☐ Thema 3: Tools für den erfolgreichen Netzwerk-Betrieb
zum Preis von € 2.190,- zzgl. MwSt.

☐ **ohne Intensiv-Training am letzten Tag**
zum Preis von € 1.790,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____08

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname
_____ Nachname
_____ Firma
_____ Telefon/Fax
_____ Straße
_____ PLZ,Ort
_____ eMail
_____ Unterschrift

Programmübersicht Netzwerk-Redesign Forum 2008

Montag, den 14.04.2008

9:30 - 11:00 Uhr
Applikations-bewusste Netzwerke: wo liegt die Zukunft der Netzwerke? Analyse unseres internationalen Labors in Christchurch
- Trendanalyse: IT- und Netzwerk-Architekturen
- Applikationen im Netzwerk:
  wie weit nehmen sie Einfluss auf Design und Betrieb?
  - Anforderungen an Netzwerke
  - Applikations-spezifische Umsetzungen
- Ausgwählte Applikationen: SOA, Voice, Kollaboration
- Wer treibt den Markt:
  Netzwerk-Hersteller kontra IT-Hersteller kontra TK-Hersteller

Dr. Jürgen Suppan, ComConsult Research

11:30 - 12:30 Uhr
Unified Communications:
Probleme und Anforderungen aus der Sicht großer Unternehmen
- Unternehmensweite TK-Architektur
- SIP als Kommunikationsplattform
- Bedeutung der UC/OCS-Lösung von Microsoft
- Zusammenarbeit von Siemens und IBM

Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause
ab 18:00 Uhr Happy Hour

14:00 - 15:30 Uhr
Data-Centre-Networks:
wie die Herausforderungen zu meistern sind
- Welche Verkabelungsstruktur: einstufig oder mehrstufig?
- Wie sind die aktiven Komponenten auf die RZ-Fläche zu verteilen: nah bei den Servern oder separat?
- Welchen Kabelstandard für LWL und Kupfer nehmen?
- Aktives Netzdesign für Data Centre:
  Layer 2, Layer 3 oder Kombinationen davon?
- Die Rolle verschiedener Redundanzmechanismen:
  Spanning Tree, Routing, VRRP, Virtuelles Switching
- Blade Switches: nutzen oder nicht?
  Wie sind Blade-Switches in die Netzstruktur zu integrieren?
- Rolle von Load Balancing: Alternativen und was davon zu halten ist
- Cisco Nexus: wie ist das neue Produkt einzuschätzen?

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

16:00 - 17:30 Uhr
LAN-Designs 2008:
aktuelle Trends für Design und Komponentenauswahl
- 10 Gigabit-Ethernet auf dem Weg in die Normalität, 10 GBaseT in der praktischen Nutzung
- PoE: wie viel Power brauchen wir, wie viel haben wir, wohin geht der internationale Standard?
- LLDP /LLDP-MED
- Automatisierte VLAN-Zuweisung
- NAC • VRF / Virtueller-Router
- Ausgewählte aktuelle Komponenten in der Analyse

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

Dienstag, den 15.04.2007

9:00 - 9:45 Uhr
10Gbit, 40Gigabit und 100Gigabit Ethernet
- Wo und warum wird mehr Leistung benötigt?
- Wird 10Gigabit Ethernet bezahlbar?
- Welche Festlegungen sind bereits für 40Gigabit und 100Gigabit Ethernet getroffen?

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

9:45 - 10:30 Uhr
Ethernet der nächsten Generation: wohin geht der Weg?
- Server, Speicher, Endgeräte, Applikationen:
  auf dem Weg in eine gemeinsame Infrastruktur
- Vom Etagenverteiler zum Data Centre:
  Netzwerk-Trends in der Analyse
- Sicher und verfügbar: aber wie?
- Detailthemen: I/O-Konsolidierung, 10GE-Server-Aggregierung, Top-of-Rack, Mid-of-Row, Blade-Server-Anbindung
- Ausblick und Empfehlungen

Ulrich Hamm, Gerd Pflueger, Cisco Systems Deutschland GmbH

11:00 - 11:45 Uhr
RZ-Netzwerke: Planung, Auslegung, Betrieb
- Besondere Anforderungen typischer RZ-Netzwerke
- Wie viel Leistung wird benötigt?
- Integration von Speicher-Systemen
- Redundanz: aber wie?
- Anbindung an den Backbone
- Beispiele • Trend: 40/100G: Bedarf im RZ?
- Load-Balancer: Einsatz-Szenarien und Vorteile

Reinhard Lichte, Foundry Networks GmbH

11:45 - 12:30 Uhr
GreenIT: Auswirkungen auf Infrastruktur-Design
- Kollaborations-Technologien: Reisevermeidung und Effizienzsteigerung, was bedeutet das für das Netzwerk-Design?
- Stromverbrauch
  - Höhe der Kosten
  - Welche Komponenten verbrauchen weniger Strom
  - Wie kann man dem Klimatisierungszwang entgehen
  - Netzdesign und Stromverbrauch
- Materialverbrauch
  - Welche Auswirkungen haben Datenmengen auf den Materialverbrauch
  - Materialverbrauch und Datenhygiene
  - Maximierung der Lebensdauer von Komponenten
  - Zusammenhang IT-Architektur und Matrialverbrauch
- Entsorgung
  - Auswahl von umweltfreundlichen Materialien
  - Ausschreibungsrichtlinien

Dr.-Ing. Behrooz Moayeri, Dipl.-Inform. Mathhias Egerland, ComConsult Beratung und Planung GmbH

14:00 - 14:50 Uhr
Maschen-Netzwerke MESH:
Ausfallsicher, skalierbar, adaptierend, ist das die Zukunft?
- MESH-Netzwerke: Aufbau von Wireless Distribution Netzwerken
- Die Idee des Wireless Maschenetzwerkes
- Von der Evolution zur Revolution:
  eine neue Architektur für Netzwerke
- Anwendungsbeispiele
- Schlüsselfragen: Was leistet das Routing?
  Wo liegen die Leistungsgrenzen?
- Diskussion: Bedarf, Zeitskala

Dr. Franz-Joachim Kauffels, unabhängiger Unternehmensberater

14:50 - 15:40 Uhr
WLAN-Technologie im Einfluss von 11n:
Wohin geht der Weg?
- Leistungsspektrum und Funktionsweise der Übertragungstechniken in IEEE 802.11n
- Strategien der Hersteller und Positionierung von IEEE 802.11n im Enterprise-Bereich
- Sonderrolle des 5-GHz-Bereichs
- Was werden IEEE 802.11k/r/v leisten?
- Evolution im Controller-basierten Design
- Planungs- und Migration zu IEEE 802.11n

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

16:10 - 17:10 Uhr
Standard für Controller-Architekturen in Wireless LANs:
CAPWAP in der Analyse
- Controller-basierte Lösungen: Control Plane, Data Plane, Client
- Offene Lösungen: CAPWAP, LWAPP, SLAPP
- CAPWAP-Leistungsumfang
- Standpunkte der Hersteller
- Wohin geht der Weg? Ausblick und Empfehlung

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:40 - 16:10 Uhr Kaffeepause

Programmübersicht Netzwerk-Redesign Forum 2008

Mittwoch, den 16.04.2008

9:00 - 9:30 Uhr
Ethernet in der Produktion
- Unterschiede zwischen Office-LAN und Produktions-LAN
- Ethernet unter extremen Bedingungen
- Beispielapplikationen aus dem Produktionsumfeld
- Neue standardisierte Redundanzmechanismen aus dem IEC
- Kurze Übersicht über die Ethernet Normierung im IEEE802.3

Thomas Schramm, Hirschmann Automation und Control GmbH

9:30 -10:15 Uhr
Netztrennung und mandantenfähige Strukturen: reicht IEEE 802.1X wirklich aus?
- Mandantenfähige LANs und Port-based Authentication gemäß IEEE 802.1X: untrennbar verbunden?
- Warum IEEE 802.1X nicht konsequent genug ist
- Ausblick auf MAC Security: IEEE 802.1AE und IEEE 802.1af
- Netzzugangskontrolle und die Konsequenzen für das Netzwerk-Design
- Warum reine VLAN-Trennung nicht ausreicht: Rolle von VRF und MPLS
- Ist eine Trennung zwischen Voice und Data auf Dauer haltbar?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:15 -11:00 Uhr
NAC - Network Access Control, Anspruch, Erwartungen und die Realität
- Anforderungen, die zu einem NAC Projekt führen (können)
- Stolpersteine auf dem Weg zu NAC
- Der NAC Markt - Europa vs. US, technische Ansätze mit ihren Vor- und Nachteilen, Stand der Standardisierung
- Entscheidungsmatrix - welche Lösung ist die richtige für meine Anforderungen
- CNAC - Cost of NAC, wie kann ich den Betrieb einer NAC Lösung optimieren
- Kurze Live Vorführung einer NAC Lösung

Markus Nispel, Enterasys Networks Deutschland GmbH

11:30 -12:15 Uhr
Video im Trend: was passiert und Markt und was bedeutet das für unsere Netzwerke
- Entwicklung im Videomarkt
- Analyse der Hersteller-Strategien
- Auswirkungen auf den Anwender
- Anforderungen an LAN und WAN • Empfehlungen

Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH

13:45 -14:30 Uhr
Fixed-Mobile-Convergence: wohin geht der Weg?
- Kommt das Skandinavische Modell?
- Unterschiede zwischen den Herstellern
- Einfluss von 802.11a/n auf FMC
- Kostengegenüberstellung FMC/WLAN/GSM/Festnetz
- Technische Einflüsse

Dr. Frank Imhoff, Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH

14:30 - 15:15 Uhr
SOA-bewusste Netzwerke
- SOA: vom Design zur Architektur
- Funktionale Elemente einer SOA-Lösung
- Kommunikation in einer SOA-Lösung: worauf kommt es an
- SOA-bewusste Netzwerke: was bedeutet das?

Dr. Frank Imhoff, Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH

15:45 - 16:30 Uhr
WAN: mit Ethernet in die Gigabit-Weitverkehrsnetze?
- Neue Angebote der Service Provider
- Warum Ethernet im WAN Vorteile für die Service Provider und die Kunden bringt
- Neue Standards der ITU und des IEEE und ihre Rolle
- Wird das Layer-2-WAN zum Standard?

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:00- 11:30 Uhr Kaffeepause
12:15- 13:45 Uhr Mittagspause
15:15- 15:45 Uhr Kaffeepause

Donnerstag, den 17.04.2008 - Workshops - Beginn 09:00 Uhr - Bitte ein Thema ankreuzen!!

☐ **Workshop 1:**
Voice-Readiness

Voice-Ready Design
- Bedarfbewertung aus der Sicht von Unified Communication
- Gestaltungsparameter in LAN und WAN
- Prüfung bestehender Netzwerke • Redesign-Gesichtspunkte

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

Voice-Ready-Spezialaspekte
- Voice over Wireless: Stand der Technik
- Kernproblem Roaming und seine Lösbarkeit
- Ergebnis von Messungen an WLAN-Controller-Systemen
- Voice-Sicherheit • Gefahrenpunkte für Voice-Sicherheit
- Lösungsansätze

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

☐ **Workshop 2: Zukunft der Weitverkehrstechnik: wohin geht der Weg?**
- Ist MPLS auch international überall verfügbar? Was ist der durchschnittliche Kostenfaktor zwischen MPLS und Internet-VPN?
- Welche Technologien werden in den nächsten drei Jahren neben MPLS einen signifikanten Anteil am WAN-Markt haben?
- Welcher Anteil der Unternehmen sind über optische Access Links an die WAN-Plattformen der Provider angebunden?
- Welcher Anteil der Unternehmen ist heute schon über Ethernet an die Provider-Plattformen angebunden?
- Welche Rolle spielt Ethernet im Backbone der Provider?
- Welche Rolle spielen in den nächsten drei Jahren SIP Trunks und wie werden sie weiter entwickelt? Werden SIP Trunks in diesem Zeitraum mehr Leistungsmerkmale der Telefonie bieten als ISDN?

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

☐ **Workshop 3:**
Tools für den erfolgreichen Netzwerk-Betrieb

Einleitung: Netzwerk-Betrieb 2008
- Anforderungen an den Netzwerk-Betrieb
- Netzwerk-Leistung: Parameter und Messbarkeit
- Applikationen im Netzwerk: Komplexität der Messung
- Störungserkennung: wer erkennt die Störung vor dem Benutzer?
- 24/7-Operating: was bedeutet das?

Dr. Jürgen Suppan, ComConsult Research

Wireless Tools, Stand der Dinge
- Die Tool-basierte WLAN-Planung wird erwachsen: Nutzen und Anwendungshinweise
- Aktuelle Planungstools und Features
- Planungstools für die „11n-Installation“, braucht man etwas Neues?
- Management von Wireless Netze, herstellerspezifisch oder Standard-basiert?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Netzmanagement Update 2008
- Ein Klassiker entwickelt sich weiter - typische Anforderungen heute
- Die Hersteller reagieren - optische Aufbereitung, intelligentere Event-Auswertung • Leider auch ein Klassiker: das Management-System als Investruine - was tun?
- Neue Anwendungen im Netz, z.B. VoIP - und das Netzwerk-Management?
- Die Security-Sicht: Netzwerk-Management?! Aber sicher!
- Netzwerk-Management und Open Source - wie sieht es da aus, wie verhalten sich ComConsult-Kunden?

Dipl.-Inform. Oliver Flüs, ComConsult Beratung und Planung GmbH

LAN-Analyse, aktuelle Trends
- „Domino“, „Sniffer“ und „Advisor“ sind in die Jahre gekommen: Wie sieht der moderne Werkzeugkasten aus?
- Einsatzbereiche tragbarer Analysatoren heute
- LAN-Analyse ist Ende-zu-Ende-Analyse: Welche Tools werden benötigt und welche Ergebnisse kann man erwarten?
- Stand der Dinge bei den „Capture Engines“
- Wofür kann man Open Source Tools einsetzen?
- TAPs mit Mehrwert - Merkmale und Einsatzmöglichkeiten
- NetFlow und IPFIX, Datenwust oder nützliche Statistik?

Hersteller/Händler kommen zu Wort

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause
13:00 - 14:00 Uhr Mittagspause
15:30 Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor!

Kongress

ComConsult SIP- und Unified Communication Forum 2008

Die ComConsult Akademie veranstaltet vom 21. - 22. April 2008 das „ComConsult SIP- und Unified Communication Forum 2008“ in Frankfurt.

Siemens hat mit seinen Ankündigungen eine Lawine losgetreten, die spätestens seit dem Markteintritt von Microsoft absehbar war:

- die Zeit der Hardware-basierten Kommunikations-Lösungen neigt sich dem Ende zu, die Hardware kann die Preise von Software-Lösungen nicht mehr kontern
- mit dem Wechsel zur Software kommt aber gleichzeitig auch der Wechsel zu einer offenen Infrastruktur im Kern, die um spezielle Applikationen der Hersteller erweitert wird
- TK-Hersteller werden Applikations-Programmierer und Endgeräte-Entwickler auf der Basis einer offenen Software-Plattform

SIP und Unified Communication sind die zentralen Themen und werden den Markt für Kommunikations-Lösungen in den nächsten Jahren bestimmen:

- SIP liefert die Infrastruktur für die Kommunikation mit beliebigen Medien (Sprache, Video, Webkonferenz, Grafik, ...)
- SIP ist bewusst für Erweiterungen offen, im Gegensatz zu traditionellen Lösungen ist die Architektur konsequent auf Erweiterbarkeit und Skalierbarkeit ausgelegt

- Die Besonderheiten der SIP-Architektur führen dazu, dass SIP zwar eine Vielzahl von Leistungsmerkmalen realisiert, aber damit nicht zu traditionellen Lösungen vergleichbar ist
- SIP sieht viele High-End-Leistungsmerkmale eher als Applikation, die außerhalb der Kerninfrastruktur angesiedelt sind

Unified Communication ist das technische Element, das die SIP-Kerninfrastruktur nach „Oben“ abrundet:

- UC liefert die komplette Funktionalität in einem Klienten
- Es entsteht eine Benutzerschnittstelle, die wichtige Kommunikations-Funktionen für alle Benutzer intuitiv nutzbar macht
- UC hat ein völlig anderes Funktionsverständnis als traditionelle Lösungen
- Im Mittelpunkt aller UC-Lösungen steht der Arbeitsprozess, der zu unterstützen ist. Ein typisches Beispiel ist die Integration von UC und ERP. Es geht darum in einem Arbeitsprozess alle Kommunikationspartner mit den besten und effizientesten Medien jederzeit und an jedem Ort erreichen zu können

Mit SIP und Unified Communication wachsen IT und TK zusammen. Die lang diskutierte Integration von Kommunikation in IT-Applikationen wird Wirklichkeit.

Hier setzt unser brisantes und hochaktuelles Forum an, das ComConsult SIP und Unified Communication Forum 2008:

- wir stellen unsere Analyse des Marktes und der aktuellsten Entwicklungen vor
- besonderen Raum wird die Analyse der Situation bei Siemens und die Auswirkung auf den Markt einnehmen
- Cisco, IBM, Microsoft und Siemens präsentieren ihre Strategie und stellen sich der Diskussion
- wir geben Empfehlungen, in welche Richtung Sie Ihre Projekte entwickeln sollten, wohin aus unserer Sicht der Markt geht

Wie immer gilt auch diesmal, dass SIP und UC zwar den Markt bestimmen, aber in den technischen und strategischen Details erheblicher Sprengstoff liegt.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult SIP- und Unified Communication Forum 2008

☐ Ich buche den Kongress
SIP- und Unified Communication Forum 2008
21.04. - 22.04.08 in Frankfurt
zum Preis von € 1.590,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____08

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Programmübersicht ComConsult SIP- und Unified Communication Forum 2008

Montag, den 21.04.2008

Keynote: IP-Telefonie, SIP, Unified Communication: wohin geht der Weg?

- Ausgangslage:
  - Wie ändert sich der Kommunikationsbedarf?
  - Wie ändert sich Benutzerverhalten ?
  - Kommunikation der Zukunft: wie wichtig ist das für die Entscheidung?
- Traditionelle TK kontra IP-Telephonie:
  - Wo sind die Unterschiede in den Architekturen?
- Analyse: Hybrid kontra Softswitch: ist die hybride Lösung am Ende?
- SIP in der Analyse:
  - Wie wird SIP den Herstellermarkt verändern?
  - SIP als Basis-Infrastruktur: was bedeutet das?
  - Präsenz-Dienste: Schlüssel-Infrastruktur, warum?
  - SIP und Applikationen: Integrations-Architektur
- Unified Communication: Kommunikation der Zukunft
  - Funktionalität
  - Integration in IT-Applikationen
  - Zusammenspiel mit traditionellen TK-Lösungen
- Architekturmodell SIP/UC
  - Grenze zwischen Leistungsmerkmal und Applikation
  - Gestaltbarkeit und Offenheit kontra Leistungsmerkmal
  - Der zukünftige Client: der PC im Telefon oder der Softclient?
- Hersteller und Markt:
  - Analyse: Was ändert sich durch den Einstieg von IBM und Microsoft
  - Sind Gewinner und Verlierer erkennbar?
- Analyse: die Siemens-Situation
  - Welche Produkte werden ausgemustert?
  - Wie sieht die Zukunft aus?
  - Wie sicher sind Investitionen?
- Ausblick und Empfehlungen

Dr. Jürgen Suppan, ComConsult Research

Technologie-Analyse: Unified Communication

- Strategisch: Wie wichtig ist das Thema, ein Muss?
- Technisch: Architekturen, Migration, Integration
- Plattform-Situation
- Markt-Situation: Strategien der führenden Hersteller
- Denkbare Strategien für betroffene Unternehmen

Dr. Frank Imhoff, Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH

Session Initiation Protocol SIP: Infrastruktur in der Analyse

- Ergebnisse der SIP-Studie von ComConsult-Research
- SIP-Architektur-Varianten
- Leistungsmerkmale: was ist da, was fehlt?
- SIP, Leistungsmerkmal, Applikation: Abgrenzung
- Markt-Analyse: SIP-Strategie und Produkte führender Hersteller
- Empfehlung zur Einführung von SIP

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

Microsoft OCS im praktischen Test: Ergebnisse aus einer Produktiv-Umgebung

- Ausgangslage • Aufbau der Lösung
- Erfahrung mit Installation und Inbetriebnahme
- Nutzungs-Situation • Reaktion der Benutzer
- Bewertung: Positives, Negatives
- Empfehlungen

Eric Langer, Siemens AG

SIP-Trunking: wohin geht der Weg?

- Was leistet SIP-Trunking heute?
- Über SIP und den Provider ins PSTN: Abschaltung des Primärmultiplex?
- Über SIP mit anderen SIP-Unternehmen kommunizieren: was bedeutet das?
- Leistungsmerkmale, Medienfreiheit in der SIP-zu-SIP-Kommunikation
- Wie werden sich Kosten und Leistung entwickeln?

Denis Alexeitsev, Deutsche Telekom AG

Dienstag, den 22.04.2008

Microsoft Unfied Communication: Kommunikation auf einem neuen Niveau

- Ziele
- Produktarchitektur
- Skalierbarkeit und Ausfallsicherheit
- Leistungen des Client: das Ende des Hardphones?
- Infrastruktur: Adressbuch, Präsenz: wie realisiert
- Offenheit der Lösung: SIP-Variante, Codec, Schnittstellen
- Integration in Applikationen: Office, Email, Fax, ERP
- Ersatz für eine TK-Lösung oder Ergänzung?
- Mischarchitekturen mit TK-Lösungen: wie realisieren?
- Preisrahmen
- Roadmap: wo will Microsoft in den nächsten 3 Jahren hin?

Vincent James, Microsoft Deutschland GmbH

Mit SIP und UC zur Kollaborations-Plattform

- Zentrale Marktrends
- HiPath 8000 im Kern einer neuen Architektur
- Siemens Antwort auf Unified Communication
- OpenScape: wohin geht der Weg?

Jürgen Brieskorn, Siemens Enterprise Communications GmbH & Co KG

Cisco Unified Communications; Integration, Bedeutung von SIP, Aktuelle Entwicklungen

- Cisco UC, ein Überblick
- Applikationsintegration
- Warum und wo ist SIP wichtig?
- SIP Trunking; Status, Architektur, Herausforderungen
- SIP-Strategie
- Bedeutung von SIP für Sprachqualität nicht nur im Unternehmensnetz

Johannes Krohn, Cisco Systems GmbH

Unified Communication von IBM - die Zukunft der geschäftlichen Kommunikation gestalten

- UC Lösungen von IBM - heute und morgen
- Geschäftsanwendungen und Kommunikation verbinden
- Offene, erweiterbare Kommunikationsplattformen machen den Unterschied
- Flexible Lösungen für individuelle Anforderungen - die Bedeutung der Partnerlösungen für unsere UC Plattform
- Auf sich verändernde Anforderungen reagieren können und bestehende Investitionen schützen

Dirk Schneider, IBM Deutschland GmbH

Podiumsdiskussion

- Wohin geht der Weg?
- Wie weit bringen uns offene Standards?
- Der Markt ist um Umbruch, wie schnell kommt der Wandel?

Sicherheit bei SIP

- Sicherheit bei der internen und externen SIP-Telefonie
- Ende-zu-Ende-Verschlüsselung: Ist das mit SIP überhaupt möglich?
- Welche Hindernisse sind bei der unternehmensübergreifenden SIP-Verschlüsselung zu überwinden?
- Spam over IP-Telefonie (SPIT): ist das eine reale Gefahr und wie wäre sie abzuwehren?

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

Der Veranstalter behält sich Änderungen im Programm vor!

Kongress

ComConsult IT-Sicherheits-Forum 2008

Die ComConsult Akademie veranstaltet in Zusammenarbeit mit der der GAI NetConsult vom 26. - 29. Mai 2008 ihr diesjähriges „IT-Sicherheits-Forum 2008“ in Frankfurt.

Das IT-Sicherheits-Forum wird auch in diesem Jahr wieder einen umfassenden Überblick zu aktuellen Themen der IT-Sicherheit in Theorie und Praxis anbieten. An insgesamt vier Tagen wird mit einführenden Tutorien, technischen Workshops und neutralen Fachvorträgen für jeden Interessierten etwas geboten. Dabei wird äußerst hoher Wert auf sofort verwendbare Informationen gelegt, die Teilnehmer sollen die gewonnenen Erkenntnisse möglichst sofort in der eigenen Umgebung anwenden können. Das Gesamtprogramm umfasst den bewährten Ablauf:

- Aufzeigen aktueller Trends bei Bedrohungen und Schutzmaßnahmen
- Vorstellung und Bewertung neuer Sicherheitstechnologien
- Moderierte Workshops mit Produktvergleichen und Live-Demos
- „Best Practice“ Sessions mit Sicherheitsempfehlungen für den Tagesbetrieb
- Tutorien und Seminare für Anfänger und Fortgeschrittene

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei parallelen Seminaren. Am 2. und 4. Tag werden durch erfahrene Referenten aktuelle Fachthemen analysiert und auch Praxisszenarien vorgestellt. Der 3. Tag ist mehreren Workshops für Produktvergleiche und Fallstudien zu aktuellen Sicherheitsthemen vorbehalten. Da diese in Vor- und Nachmittagssitzungen parallel ablaufen, kann jeder Teilnehmer das für ihn optimale Programm selber zusammenstellen.

Das IT Sicherheits-Forum zählt seit Jahren zu den herausragenden Events im diesem Bereich. Das Programm aus Fachvorträgen hersteller-unabhängiger Referenten und Workshops mit live durchgeführten Produktvergleichen und Praxis-Demos hat seinen hohen praktischen Wert für die Teilnehmer bewiesen. Daneben werden auch neue Entwicklungen aufgezeigt, die sowohl Informationen zu Bedrohungen, als auch zu Schutzmaßnahmen umfassen. Diese eher technischen Informationen werden ergänzt durch Empfehlungen zur Sicherheitsorganisation und zu ihrer Einbettung in die Geschäftsabläufe, da hier noch immer die größten Defizite anzutreffen sind. Damit bietet das IT Sicherheits-Forum für Sicherheitsverantwortliche, aber auch für vorrangig technisch interessierte Teilnehmer eine Fülle wertvoller Informationen.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung ComConsult IT-Sicherheits-Forum 2008

Ich buche den Kongress
ComConsult
IT-Sicherheits-Forum 2008
26.05.08 - 29.05.08 in Frankfurt a.M.
☐ mit Tutorium am ersten Tag
zum Preis von € 1.990,- zzgl. MwSt.*
☐ ohne Tutorium am ersten Tag
zum Preis von € 1.590,- zzgl. MwSt.*

* gültig bis 31.03.08
(dann reguläre Preise € 2.190,- bzw. 1.790,-zzgl. MwSt.

Bitte reservieren Sie für mich ein Hotelzimmer

vom_____bis_____08

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

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-

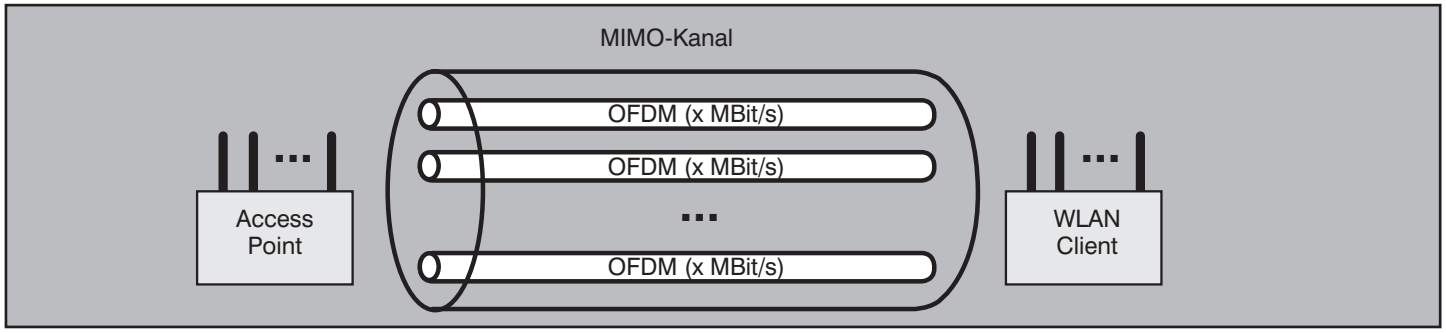


Abbildung 1: Bündelung von OFDM-Kanälen zu einem MIMO-Kanal

Die nächste Enterprise-WLAN-Generation mit IEEE 802.11n

		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-

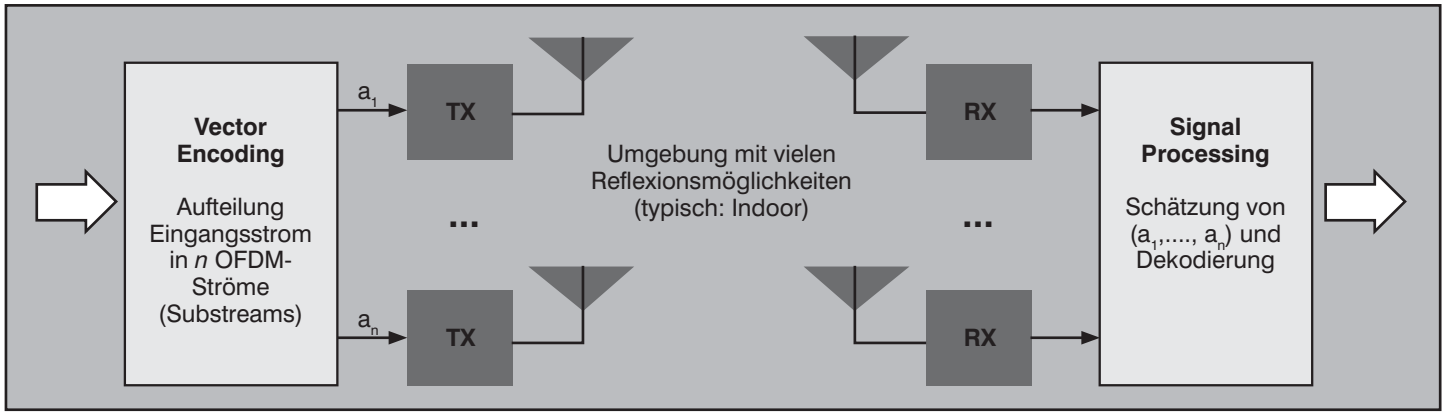


Abbildung 2: Funktionsweise eines MIMO-Systems

		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

breite von 40 MHz schafft man schließlich 600 MBit/s.

Bei dem parallelen Empfang über mehrere Antennen ergibt sich ein genereller Vorteil, der als Maximal-Ratio Combining (MRC) bezeichnet wird. Dabei wird das Signal, das von mehreren Antennen empfangen wird, im Prinzip addiert. Durch diese spezielle Form der Diversity erhält man einen Verstärkungseffekt (als Gewinn bezeichnet), der mit der Anzahl der Antennen wächst. Ein MIMO-System kann also beispielsweise nur mit zwei Zügen (Spatial Streams) aber mit drei Antennen arbeiten. Die Datenrate ergibt sich aus den zwei Zügen, die dritte Antenne verbessert die Empfangsqualität.

1.3 Beamforming

Als optionales Element spezifiziert IEEE 802.11n die Verwendung von sogenannten Array-Antennen, die ihre Hauptstrahlrichtung automatisch in die Richtung des Kommunikationspartners lenken. Dieser Mechanismus wird auch als Beamforming bezeichnet. Die Ausrichtung in unterschiedliche Raumrichtungen wird dabei durch eine dynamische Anpassung der Phasenlage der Einzelantennen erreicht, wie in Abbildung 3 gezeigt.

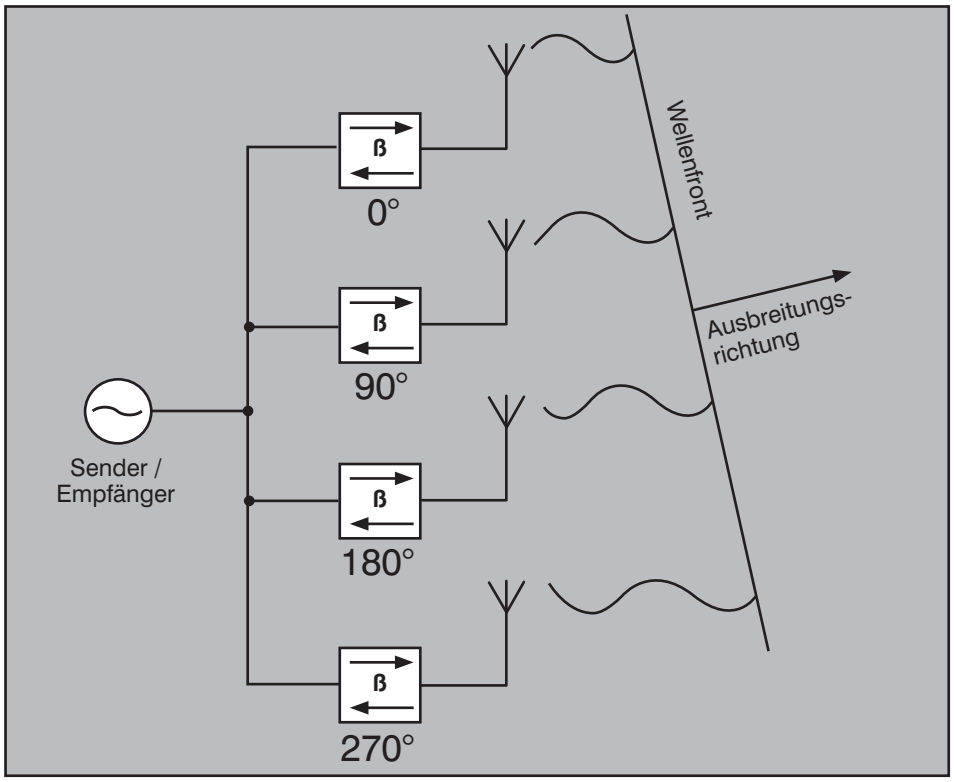


Abbildung 3: Steuerung der Ausrichtung einer Array-Antenne durch unterschiedliche Phasenlagen der Einzelantennen

1.4 Abwärtskompatibilität

Für einen Adapter nach IEEE 802.11n werden drei Betriebsmodi vorgesehen: Legacy Mode, Mixed Mode und Green Field.

Im Legacy Mode werden alle Pakete gemäß IEEE 802.11a/g übertragen. In diesem Modus wirkt lediglich MRC als Diversity und verbessert im Vergleich zu einem konventionellen WLAN-System die Empfangseigenschaften.

Im Mixed Mode werden die Pakete mit einer Präambel, die kompatibel zu IEEE 802.11a/g ist, übertragen. Die Präambel wird also immer mit einer niedrigeren Datenrate (maximal 54 MBit/s) gesendet, auch wenn der Rest des Pakets mit einer hohen Datenrate (z.B. 300 MBit/s) übertragen wird. Auf diese Weise kann eine Station, die IEEE 802.11n nicht unterstützt, feststellen, dass eine andere Station sendet und einen eigenen Sendeversuch zurückstellen. Umgekehrt muss ein Empfänger im Mixed Mode sowohl Mixed-Mode-Pakete als auch Legacy-Pakete dekodieren können. So werden auf eine einfache Weise Kollisionen vermieden und eine Koexistenz mit IEEE 802.11a/g ermöglicht. Bei Verwendung des Mixed Mode ist die Leistung allgemein durch die abwärtskompatible Präambel, die stets mit einer niedrigeren Datenrate übertragen wird, reduziert. Außerdem muss berücksichtigt werden, dass jede Übertragung nach IEEE 802.11a/g das System ausbremst, da für die Dauer der langsameren Übertragung keine schnellere IEEE-802.11n-Station das Medium verwenden kann.

Im Betriebsmodus Green Field wird ein reines 802.11n-Format übertragen, d.h. es ist keine Abwärtskompatibilität gegeben. Dieser Modus ist für Installationen gedacht, die keine Altgeräte mit IEEE 802.11a/g unterstützen müssen.

1.5 Sendeleistung und Regulierung

Die bestehenden Festlegungen für die Frequenzbereiche bei 2,4 GHz und bei 5 GHz gelten weiterhin und werden sinngemäß auf die neue Übertragungstechnik angewandt. Dabei ist der Verstärkungseffekt durch die parallele Übertragung über mehrere Antennen genauso zu beachten wie die mögliche größere Kanalbandbreite von 40 MHz:

- Die Summe über die von den Einzelantennen eines IEEE-802.11n-Systems abgestrahlten Leistungen darf die für ein traditionelles IEEE-802.11a/g-Gerät festgelegten Grenzwerte nicht überschreiten

- Die über einen 40-MHz-Kanal abgestrahlte Leistung darf nicht größer sein, als die Leistung eines entsprechenden Senders in einem 20-MHz-Kanal.

1.6 Folgen für das Design der WLAN-Komponenten

Die Implementierung von IEEE 802.11n erzwingt letztendlich eine komplett neue WLAN-Produktgeneration.

Access Points müssen Gigabit Ethernet unterstützen, damit eine Nettodatenrate jenseits von 100 MBit auf der Luftschnittstelle ohne Verlust in das kabelbasierte LAN abgeführt werden kann. Außerdem benötigen Access Points auch eine höhere Prozessorleistung, um die Luftschnittstelle bedienen zu können. Dabei ist natürlich ein Controller-basiertes Design vorteilhaft, da hier die Access Points von zusätzlichem Ballast befreit sind und sich ihre Funktion auf den reinen Datentransport konzentriert. Weiterhin ist der Aufbau von Access Points mit externen Antennen aufwändig. Man stelle sich nur den Installationsaufwand (und die optische Erscheinung) für einen Access Point mit vier Zügen vor, der mit vier externen Antennen versorgt wird.

Besonders kritisch ist die Stromversorgung der Access Points. Moderne WLAN-Installationen verwenden hier Power over Ethernet nach IEEE 802.3af. Access Points nach IEEE 802.11n werden aber oft einen Strombedarf jenseits von 15 Watt haben,

sofern zwei Radioteile (jeweils ein Radioteil für 2,4 GHz und eines für 5 GHz) parallel betrieben werden sollen. Jetzt könnte man argumentieren, dass IEEE 802.11n bevorzugt bei 5 GHz eingesetzt würde und man daher auf den Parallelbetrieb eines zweiten Radioteils verzichten könnte. Andererseits sind Szenarien attraktiv, in denen ein Access Point bei 2,4 GHz im Legacy Mode arbeitet und im 5-GHz-Bereich im Mixed Mode oder sogar im Green-Field-Modus operiert.

Für die Stromversorgung von Geräten mit einer höheren Leistungsaufnahme ist der Standard IEEE 802.3at „Power over Ethernet Plus“ in Arbeit. Dabei soll ein System spezifiziert werden, dass auf den vorhandenen Verkabelungen mindestens doppelt soviel an Leistung zum Gerät bringt wie heute mit IEEE 802.3af möglich. Eine Verabschiedung ist noch für 2008 geplant, allerdings sind noch einige technische Probleme zu klären. Kritische Bereiche sind dabei die Stromfestigkeit des RJ45-Systems und temperaturabhängige Dämpfungseigenschaften der Datenkabel, was zu Längenrestriktionen führen kann.

Der hohe Strombedarf für Systeme nach IEEE 802.11n hat natürlich auch Auswirkungen auf den Endgerätebereich. IEEE 802.11n wird zunächst eine Domäne für Notebooks, Desktop PCs, Drucker. Für batteriebetriebene Kleingeräte wird es vorerst keine Unterstützung geben. Generell ist damit zu rechnen, dass Einsatz von IEEE 802.11n langfristig einen Mischbetrieb mit IEEE 802.11a/g erfordern wird.

Beim Aufbau eines Overlay-Netzes mit einem Controller-basierten Design muss berücksichtigt werden, dass der gesamte Client-Verkehr zu den WLAN Controllern über einen Tunnel übertragen wird. Die WLAN Controller müssen also die kumulierte Kommunikationslast der Access Points bewältigen können. Bei IEEE 802.11n muss hier eine im Vergleich zu 802.11a/g ca. 10-fache Kommunikationslast verkraftet werden können. Manche Hersteller empfehlen für die Unterstützung von IEEE 802.11n den Client-Verkehr am Access Point in das LAN auszukoppeln und nicht zum WLAN Controller zu tunneln, um den WLAN Controller zu entlasten. Dabei geht allerdings der Overlay-Charakter und damit der entscheidende Vorteil des Controller-basierten Designs verloren. WLAN Controller müssen also einfach leistungsfähiger werden, um IEEE 802.11n sinnvoll unterstützen zu können.

2. Standardisierung oder Pre-N-Zertifizierung

Ursprünglich hatte die Arbeitsgruppe für IEEE 802.11n geplant, bis zum Sommer 2005 einen tragfähigen Kompromiss zu schaffen mit dem Ziel einer baldigen Fertigstellung des Standards. Dieses Ziel wird die IEEE erst mit knapp drei Jahren Verspätung erreichen. Die Verabschiedung von IEEE 802.11n ist jetzt für Ende 2008 geplant. Die aktuelle Vorversion für IEEE 802.11n ist Draft 3.00 vom September 2007.

Auf dem Weg zur Verabschiedung des Standards wurde im Herbst 2007 noch an einer weiteren Front gekämpft. Die australische Forschungseinrichtung CSIRO (Commonwealth Scientific and Industrial Research Organization) besitzt ein US-Patent zum Thema WLAN aus dem Jahr 1996. CSIRO behauptet, dass dieses Patent die eigentlichen technischen Grundlagen für den Leistungsschub in IEEE 802.11n und den aktuell verfügbaren Vorstandardprodukten gelegt habe. Laut einem Gerichtsentscheid in den USA (in einem Rechtsstreit CSIRO gegen den Chip-Hersteller Buffalo Technology) ist das Patent gültig und bietet die Grundlage für die Forderung von Lizenzgebühren. Es gab darauf bereits Andeutungen, dass wegen der unklaren Sachlage die Zustimmung zur Ratifizierung von IEEE 802.11n Ende 2008 durch das IEEE Standards Board verweigert werden könnte. Dies hat natürlich die WLAN-Gemeinde verunsichert, auch wenn es aktuell so aussieht, dass sich die Gemüter wieder beruhigt haben.

Je länger sich die Verabschiedung von IEEE 802.11n hinzieht, desto größer wird die Rolle der Vorstandardprodukte (als Pre-N- oder als Wireless-N-Produkte bezeichnet). Mit den ersten Pre-N-Produkten wurde ausschließlich der Consumer-Bereich abgedeckt und anfänglich lag die Leistung der Systeme teilweise erheblich unter den Erwartungen. Weiterhin bestanden deutliche Probleme in der Interoperabilität. Daher hat die Wi-Fi Alliance im Frühjahr 2007 beschlossen, von der ursprünglich geplanten Vorgehensweise, bei der erst die Verabschiedung von IEEE 802.11n abgewartet und dann ein Zertifizierungsprogramm gestartet werden sollte, abzuweichen. Die Wi-Fi Alliance geht jetzt zweistufig vor und hat zunächst im Juni 2007 ein Zertifizierungsprogramm für Pre-N gestartet, das auf dem Draft 2.00 für IEEE 802.11n basiert. Sobald der Standard verabschiedet ist, wird die Wi-Fi Alliance in die zweite Phase eintreten und Produkte nach dem Standard zertifizieren. Stand Ende Februar 2008 sind bereits 222 Produkte zertifiziert (Abbildung 4).

3. Produktsituation

Inzwischen gibt es eine ganze Palette an Pre-N-Chipsätzen. Zu nennen sind beispielsweise Broadcom Intensi-fi, Marvell TopDog, Atheros XSPAN, Airgo Gen 3 und Intel Next-Gen Wireless-N. Dabei werden IEEE 802.11a/b/g und Pre-N nach Draft 2.0 sowie typischerweise 40 MHz Kanalbandbreite bei 5 GHz unterstützt. Angeboten werden meist zwei MIMO-Züge (Spatial Streams) mit drei Antennen für MRC. Diese Konfiguration wird auch als „2x3 Draft N“ bezeichnet. Damit ist eine maximale Bruttodatenrate von 300 MBit/s möglich (siehe Tabelle 2).

Nachdem Cisco im Herbst 2007 mit dem Aironet 1250 Access Point das erste Pro-

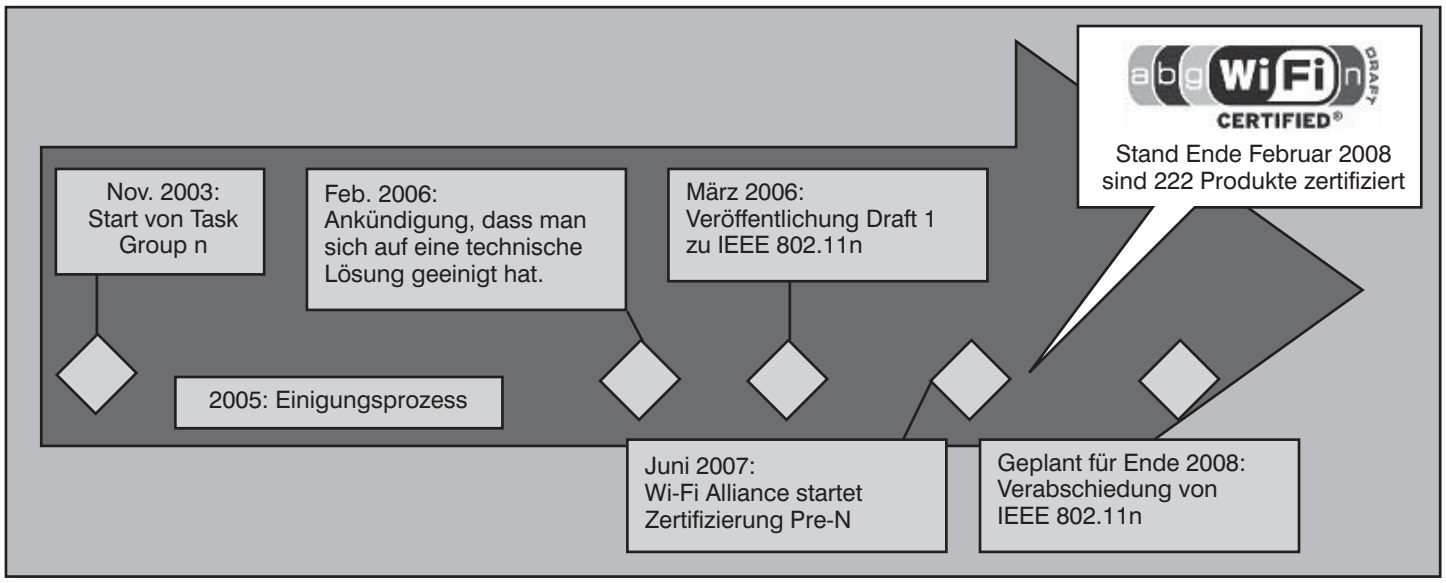


Abbildung 4: Prozess der Standardisierung von IEEE 802.11n

dukt im Enterprise-Bereich auf den Markt gebracht hat, haben andere Hersteller nachgezogen. Beispielsweise hat Siemens für März 2008 die Access Points Hipath Wireless AP3610 und AP3620 angekündigt. Diese Geräte sollen sich insbesondere durch einen vergleichsweise moderaten Stromverbrauch auszeichnen und noch konventionell mit IEEE 802.3af versorgt werden können. Aruba hat die Access Points AP-124 und AP-125 neu im Programm. Der AP-125 bietet eine 3x3 MIMO Konfiguration (d.h. drei MIMO-Züge) und kann damit theoretisch sogar eine Datenrate bis zu 450 MBit/s unterstützen. Weiterhin hat Trapeze für dieses Jahr mit dem MP-432 Access Point auch eine Pre-N-Variante angekündigt.

Es ist also davon auszugehen, dass im Laufe dieses Jahres die meisten Hersteller für den Enterprise-Bereich eine Pre-N-Lösung im Angebot haben werden.

4. Planung und Migration

Ein wesentlicher Aspekt bei der Planung eines WLAN für IEEE 802.11n oder Pre-N ist die Frage der möglichen Reichweiten. Die Hersteller versprechen eine Verdopplung der Reichweite im Vergleich zu einem traditionellen System nach IEEE 802.11a/g. MIMO-Systeme haben, wie bereits erwähnt, ähnlich zu Richtantennen beim Empfang einen Verstärkungseffekt (MRC), der proportional zur Anzahl der Empfangsteile ist. Für Datenraten im Bereich von 100 MBit kann man von einem System nach IEEE 802.11n tatsächlich die Reichweite eines 11ag-Systems (ggf. sogar noch besser) erwarten. Bei einer Datenrate von 300 MBit/s und höher liegt die Reichweite aber typischerweise unter der eines konventionellen Systems nach IEEE 802.11a/g. Die Daumenregel „Je höher die Datenrate, desto niedriger die Reichweite." gilt also trotz MIMO und MRC immer noch.

Dies hat einen positiven Effekt auf die Migration zu IEEE 802.11n bzw. Pre-N, denn beim Umrüsten bestehender Access Points auf neue Access Points ist in den meisten Fällen nicht mit Funklöchern zu rechnen. Eine bestehende Ausleuchtung nach IEEE 802.11a/g kann also quasi für IEEE 802.11n durchaus wieder verwendet werden. Zusätzliche Anschlüsse für Access Points sind wahrscheinlich erst dann erforderlich, wenn eine höhere Leistung von mehr als 100 MBit/s flächendeckend verfügbar sein soll. Da die Access Points einen Mischbetrieb unterstützen, kann eine Migration schrittweise erfolgen, indem beispielsweise zunächst punktuell die Bereiche umgerüstet werden, in denen besonders hohe Anforderungen an die WLAN-Leistung bestehen. Ein Client, der IEEE 802.11n bzw. Pre-N unterstützt, würde in diesen Bereichen dann in den Genuss einer hohen Datenrate kommen und bei Verlassen dieser Bereiche einfach wieder automatisch auf IEEE 802.11a/g zurückfallen.

Bei der optionalen Kanalbandbreite von 40 MHz belegt ein HT-OFDM-System natürlich doppelt soviel Frequenzspektrum, wie ein System nach IEEE 802.11a/g, das ja nur 20 MHz in Anspruch nimmt. Für 2,4 GHz ist das zur Verfügung stehende Spektrum knapp und bei 20 MHz Kanalbandbreite reicht das Spektrum nur für drei überschneidungsfreie Kanäle, d.h. es können in unmittelbarer Nachbarschaft nur drei Systeme störungsfrei parallel betrieben werden. Das reicht kaum für eine flächendeckende WLAN-Installation aus. Eine Kanalbandbreite von 40 MHz macht (außer vielleicht im Consumer-Bereich) also nur bei 5 GHz Sinn. Hier sind immerhin 9 überschneidungsfreie Kanäle für 40-MHz-Systeme möglich, was für flächendeckende WLAN allemal ausreicht. Die Rahmenbedingung ist dabei allerdings, dass im 5-GHz-Bereich mit Dynamic Frequency Selection (DFS) gearbeitet wird, denn sonst darf nicht das gesamte zur Verfügung stehende Spektrum genutzt werden, sondern nur 100 MHz.

Auch wenn die Enterprise-Hersteller mit ihren Pre-N-Produkten jetzt langsam auf den Markt gehen, wird empfohlen, einen produktiven Einsatz von Pre-N vorsichtig anzugehen und insbesondere die Praxistauglichkeit der Produkte in Labor- und Feldtests zunächst zu erproben. Für Pre-N-Produkte besteht keine Gewährleistung, dass sich das Produkt später durch einen Firmware-Update auf IEEE 802.11n aufrüsten lässt. Sofern sich keine weiteren signifikanten Verzögerungen in der Standardisierung einstellen und man keinen zwingenden aktuellen Bedarf hat, sollten möglichst die Verabschiedung von IEEE 802.11n und die ersten Produkte mit einer 11n-Zertifizierung der Wi-Fi Alliance abgewartet werden.

Mit IEEE 802.11n kommt ohne Zweifel die nächste WLAN-Generation. Welche Rolle Pre-N dabei letztendlich spielen wird, hängt von den weiteren Verzögerungen der Standardisierung und der Produktverfügbarkeit im Enterprise-Bereich ab. Es wäre außerdem nicht das erste Mal, dass die Wi-Fi Alliance mit einem Vorstandard den entscheidenden Erfolg hat. Man erinnere sich nur an Wi-Fi Protected Access (WPA), WPA2 und Wi-Fi Multimedia (WMM).

Report des Monats

Office Communications Server 2007

Im März ist der brandaktuelle Report „Office Communications Server 2007 “ von ComConsult Research erschienen.

Mit der Ankündigung des Office Communications Server 2007 (OCS) hat Microsoft für eine gehörige Unruhe im Markt gesorgt, war doch damit der Einstieg in den bis dato von Microsoft ignorierten Telefoniemarkt verbunden. Microsoft positioniert das Produkt bewusst als Kollaborations-Produkt und setzt es funktional in die direkte Konkurrenz zu Cisco und Siemens/IBM. Damit liegt das Produkt zentral in einem der größten Zukunfts- und Wachstums-Märkte.

In dem Report analysiert ComConsult Research die aktuelle Unified Communications Strategie von Microsoft, in deren Mittelpunkt der Office Communications Server steht.

Im Anschluss haben wir für Sie eine kurze Leseprobe zusammengestellt:

6.2 Integration von Telefoniefunktionen

Bei dieser Integrationsform werden OCS-Clients zur internen und externen Telefonie genutzt. Microsoft unterscheidet hier zwischen der gleichzeitigen Nutzung von OCS und PBX und der alleinigen Nutzung des OCS zur Telefonie.

Wie oben bereits erläutert, ist die Grundlage einer Anlagenkopplung ein OCS Mediation Server, der die „Spezialitäten“ einer OCS-Installation wie Breitband-Codec, verschlüsselte Signalisierung und Medienströme in einfache Standardfunktionen umsetzt, solange die genannten „Spezialitäten“ nicht von der PBX selbst unterstützt werden. Bislang wird eine solche unmittelbare OCS-Unterstützung von keiner am Markt vertretenen PBX geleistet, es gibt aber diverse Ankündigungen, eventuell kann man von Nortel aufgrund deren Microsoft-Kooperation eine solche Unterstützung erwarten.

Voraussetzung für eine gleichzeitige Nutzung von OCS und PBX ist die Unterstützung von so genanntem „Forking“ in der PBX. Darunter versteht man die Fähigkeit der Anlage einen Anruf gleichzeitig auf mehreren Endgeräten eines Teilnehmers signalisieren zu können (siehe Abbildung 51). Dieses Forking geschieht dann auf beiden Seiten sowohl beim OCS als auch bei der PBX für alle die Anrufe, die von der jeweiligen Seite initiiert wurden.

Anrufe aus dem PSTN gelten in diesem Sinne als von der PBX initiiert. Diese Einschränkung ist wichtig, um Endlosschleifen bei der Signalisierung (oder auch nur doppelte Signalisierungen) zu vermeiden.

Hilfreich ist an dieser Stelle auch, dass der Mediation Server „zurückkommende“ Signalisierungen zum selben Ruf erkennt und (in seiner Rolle als B2BUA) unterbindet.

Konkret bedeutet das, dass beispielsweise ein eingehender Ruf aus dem PSTN von der PBX sowohl an die PBX-Telefone, die dem Empfänger zugeordnet sind, signalisiert als auch an den OCS. Dieser wiederum leitet die Signalisierung an alle bei ihm vom Empfänger registrierten Systeme. Entsprechendes gilt für interne Anrufe: der OCS signalisiert Anrufe von OCS-Clients an die PBX und die PBX signalisiert Anrufe, die von PBX-Telefonen geführt werden, an den OCS.

Der Angerufene hat also jeweils die Wahl, ob der den Ruf an seinem OCS-Client oder seinem PBX-Telefon entgegennimmt. Sobald der den Ruf annimmt, wird die Signalisierung an allen anderen Endgeräten beendet – die Telefone hören auf zu klingeln.

Dieses Szenario hat jedoch deutlich Probleme, die man nicht unterschätzen soll-

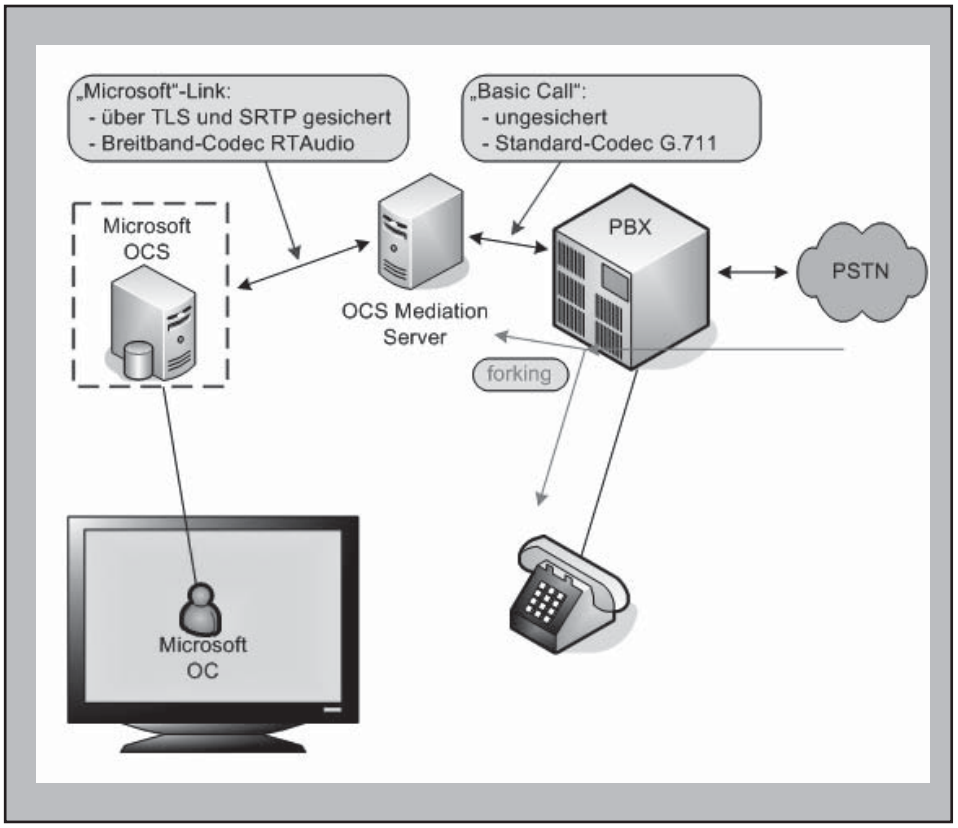


Abbildung 51: Gleichzeitige Nutzung von OCS und PBX

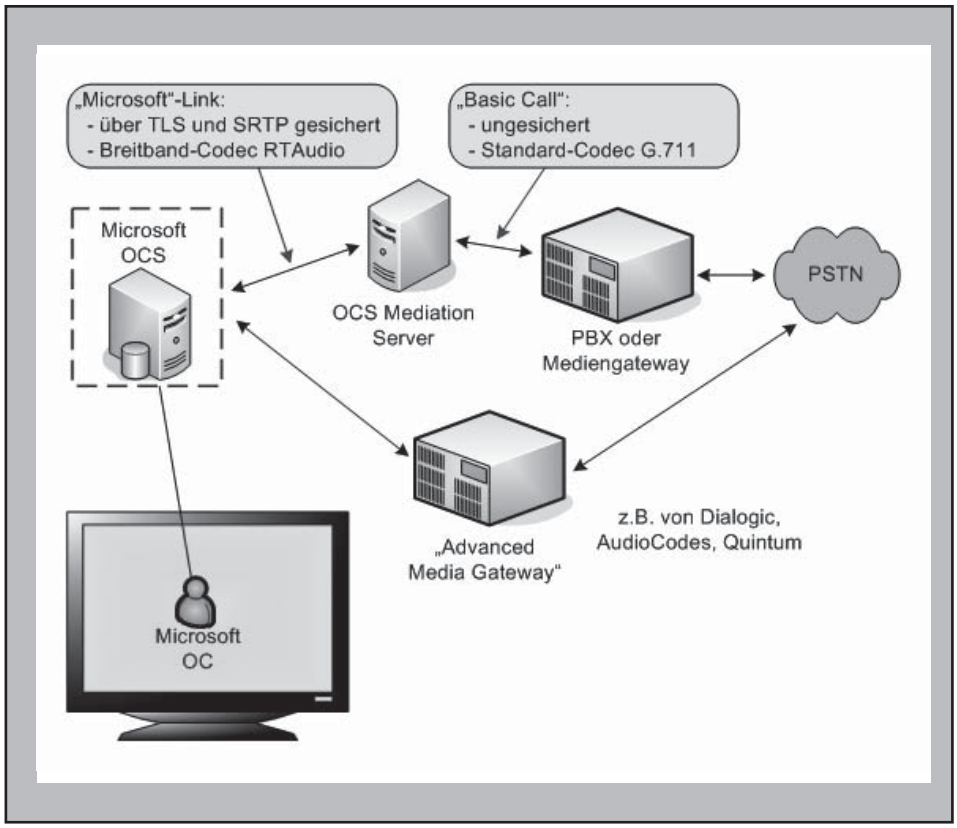


Abbildung 52: Gleichzeitige Nutzung von OCS und PBX

te. Jedes Endgerät verfügt nämlich nur über die Telefoniefunktionen, die vom zugehörenden Server angeboten werden – und diese Telefoniefunktionen werden sich beim OCS und einer PBX-Lösung mehr oder weniger deutlich unterscheiden! Das Gleiche gilt für Telefonkonferenzen: Jede Konferenz wird von derjenigen Seite gesteuert, die die Konferenz initiiert hat, auch wenn Teilnehmer aus beiden Welten an ihr teilnehmen. Das bedeutet, für einen Teilnehmer ist es wahrscheinlich überhaupt nicht nachvollziehbar, an welchem Typ von Konferenz er gerade teilnimmt.

Ebenso können Rufumleitungen und -weiterleitungen Verwirrung stiften, da diese Funktionen auf beiden Seiten problemlos unterschiedlich festgelegt werden können.

Übersichtlicher zumindest für die Endbenutzer wird dieses Szenario, wenn man auf die Gleichzeitigkeit der Nutzung von OCS und PBX verzichtet (siehe Abbildung 52). Dann kann im Prinzip jeder Teilnehmer ein Endgerät für seine bevorzugte Telefonielösung erhalten und auf beiden Systemen wird das Routing so eingestellt, dass die Anrufe beim richtigen System landen.

Letzteres klingt zwar nach beliebig komplexem Chaos für die Administration (und ist es wohl auch, wenn man jeden Mitarbeiter individuell wählen lässt), es handelt sich hierbei jedoch tatsächlich um ein mögliches sanftes Migrationsszenario, um Teilnehmer einzeln, abteilungsweise oder ganze Standorte von der einen Lösung zur anderen zu bringen.

Die Einschränkungen bei diesem Szenario liegen im Wesentlichen in den Einschränkungen des OCS selbst, der in der vorliegenden Version definitiv noch kein vollwertiger Ersatz für eine PBX-Lösung ist:

- Es werden keine analogen Endgeräte (wie z.B. Faxgeräte oder Modems) unterstützt.
- Viele Komfortmerkmale wie Notruf, Call Center, ACD fehlen.
- Es gibt keine Überlebensfähigkeit für remote Standorte. Bricht die Verbindung zum zentralen Front-End-Pool weg, können die OCS-Clients nicht mehr kommunizieren, weder über IM noch über Sprache, weder intern noch über das PSTN (selbst wenn es einen lokalen Übergang ins PSTN gäbe!).
- Es gibt praktisch keine Möglichkeit externe SIP-Provider (via SIP-Trunking) zur Anbindung ans PSTN zu nutzen (es

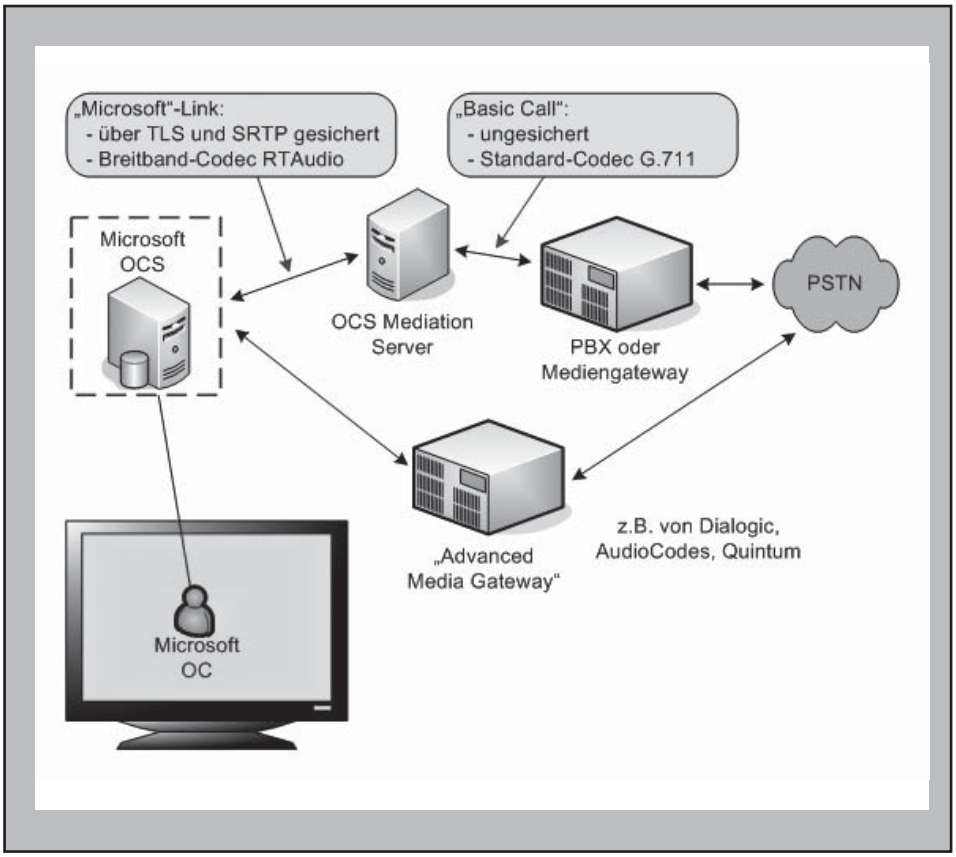


Abbildung 52: Gleichzeitige Nutzung von OCS und PBX

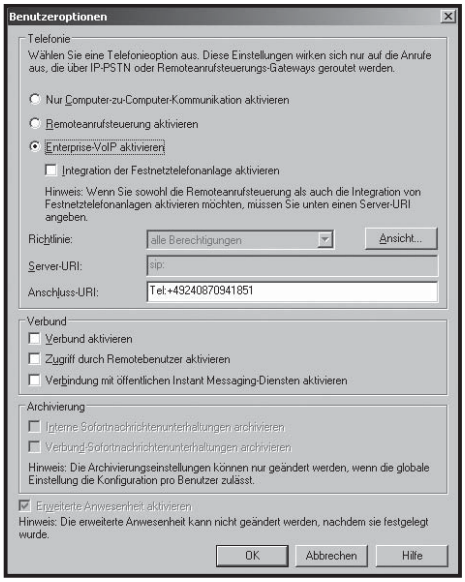


Abbildung 53: Konfigurationsoptionen für OCS-Benutzer

sei denn, der SIP-Provider setzt selbst OCS ein).

Präsenzinformationen werden im Übrigen bei diesen Szenarien nicht ausgetauscht, hierfür muss man zusätzlich beispielsweise das Szenario gemäß Abbildung 50 umsetzen.

Beide Szenarien, insbesondere das erstere, können ebenfalls auf der Basis von Einzelfall-Entscheidungen pro Benutzer realisiert werden. Das heißt insbesondere, dass diese Telefonieszenarien auch gemischt mit den oben vorgestellten CTI-Szenarien betrieben werden können – nur nicht gleichzeitig bei ein und demselben Benutzer. Pro Benutzer muss natürlich entschieden werden, ob er über seinen Office Communicator direkt telefoniert oder sein PBX-Telefon via CTI steuert (siehe Abbildung 53).

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

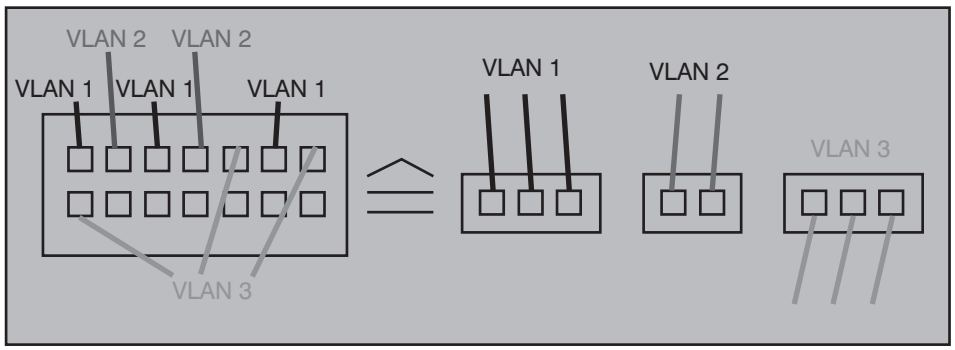


Abbildung 1: Abbildung mehrerer VLANs auf eine Layer-2-Struktur

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

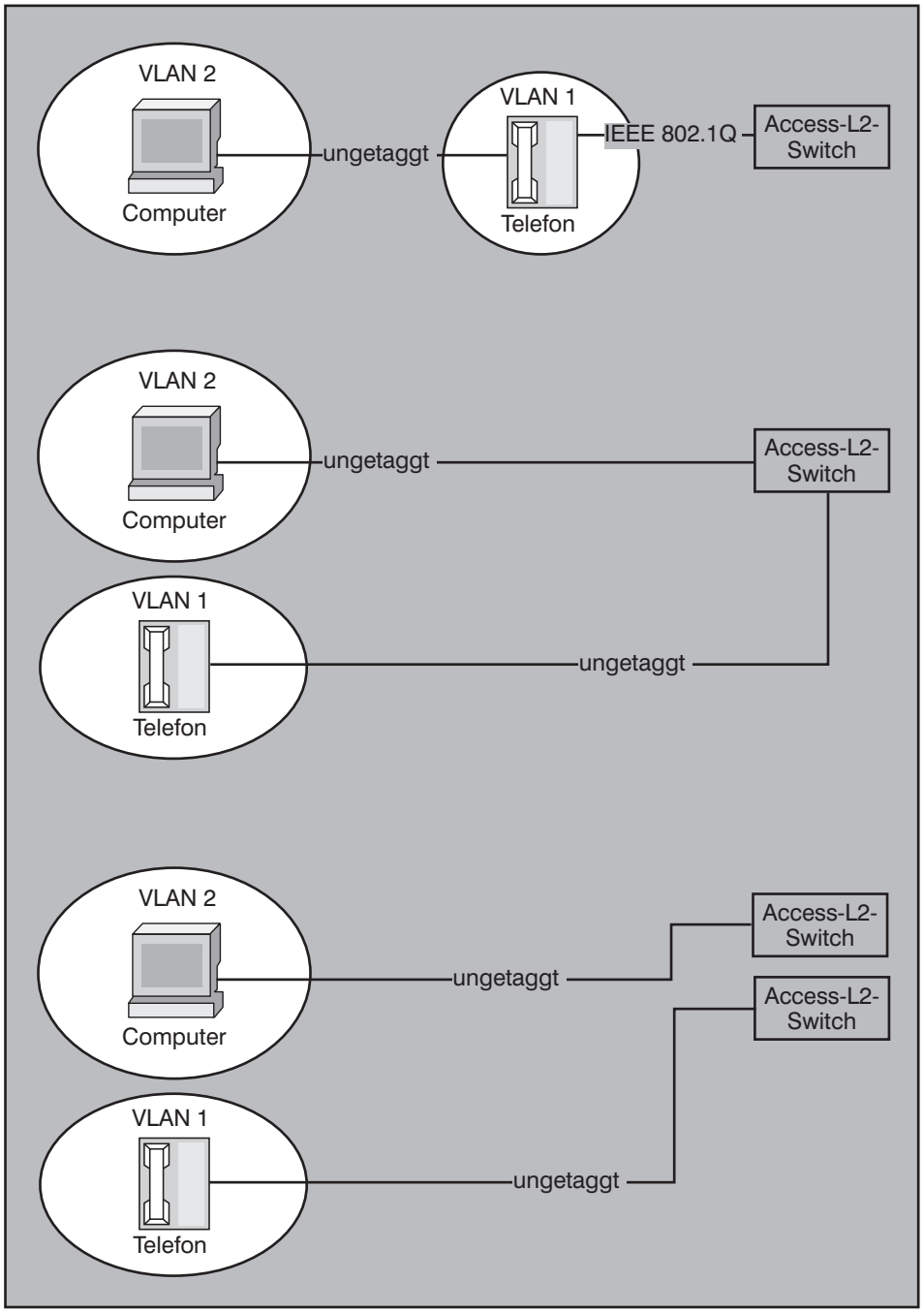


Abbildung 2: VLANs am Arbeitsplatz

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

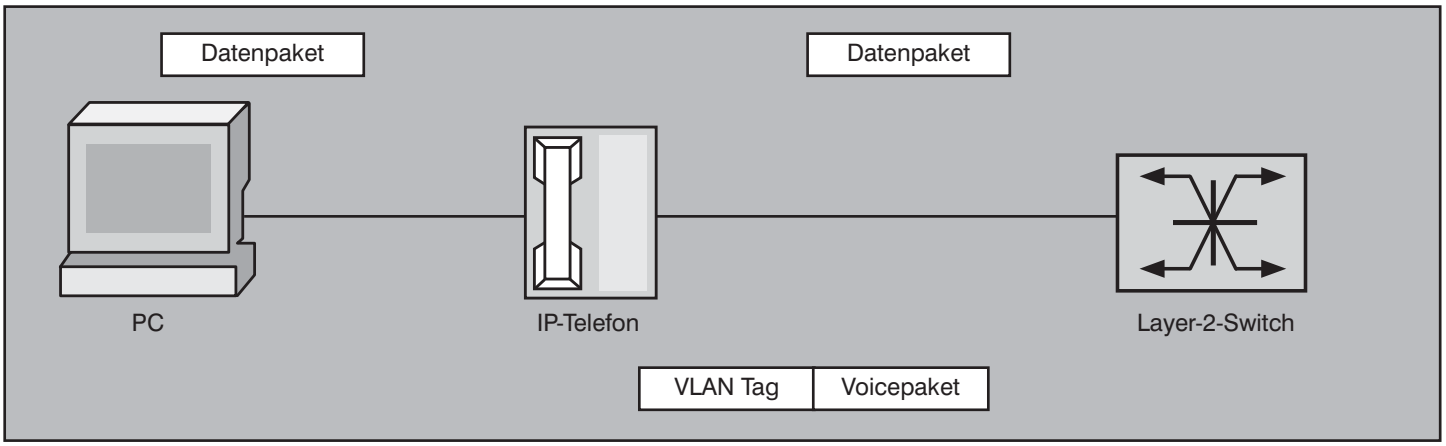


Abbildung 3: Tagging durch das Telefon

Voice VLAN ID ändert, eine Änderung am Telefon erforderlich ist. Im laufenden Betrieb kann dies mit zwei wesentlichen Nachteilen verbunden sein: mit erhöhtem Betriebsaufwand und mit längeren Wartezeiten von Benutzern, bevor sie nach Umzügen arbeitsfähig sind.

- Ein anderes Verfahren, dass von einigen Herstellern von IP-Telefonen angewandt wird, besteht darin, dass das Telefon zunächst im gleichen VLAN wie der PC bootet und ungetaggt kommuniziert. Das Telefon erhält temporär eine IP-Adresse aus dem Adressbereich für PCs. Gleichzeitig bekommt das Telefon auch eine VLAN ID für Voice zugewiesen. Dann schaltet das Telefon auf das Voice VLAN um und beantragt in diesem VLAN mit der richtigen VLAN ID eine neue IP-Adresse.

- Das dritte Verfahren besteht darin, dass das IP-Telefon und der Access Switch miteinander über ein Protokoll der Schicht 2 kommunizieren, das vor der IP-Konfiguration des Telefons diesem die Möglichkeit gibt, die passende Voice VLAN ID vom Access Switch in Erfahrung zu bringen. Ein solches Protokoll gab es zunächst nur als das proprietäres Cisco Discovery Protocol (CDP). Diejenigen Unternehmen, die sich für die Konfiguration der Voice VLAN ID mittels CDP entschieden haben, haben zugleich eine Konstellation geschaffen, in der sowohl der Access Switch als auch das Telefon von Cisco stammen müssen. Man kann dann ohne Umstellung des Netzes keine anderen Telefone einsetzen und umgekehrt, was eine wesentliche Abhängigkeit von einem Hersteller bedeutet. Seit 2005 gibt es aber auch den Standard IEEE 802.1AB mit dem Titel „Station and Media Access Control Connectivity Discovery“, in dem das Link Layer Discovery Protocol (LLDP) spezifiziert ist. Dieses Protokoll soll ein standardisiertes Pendant zu CDP darstellen. In jüngster Zeit sind Switches und IP-Telefone auf den Markt gekommen, die angeblich LLDP unterstützen. Der Autor hat bisher jedoch keine funktionierende Abstimmung der Voice VLAN ID zwischen einem Telefon und einem Switch auf der Basis von LLDP gesehen. Hinzu kommt, dass CDP (und künftig auch LLDP) aus dem Blickwinkel der Informationssicherheit kritisch gesehen wird. Nicht ohne Grund ist ein Bestandteil vieler Sicherheitsaudits in Cisco-Umgebungen die Empfehlung, CDP abzuschalten. Darüber kann nämlich ein Angreifer wertvolle Informationen über das Netz in Erfahrung bringen. CDP und LLDP sind durch keinerlei Sicherheitsmechanismus geschützt.

Die anderen beiden in der Abbildung 2 dargestellten Varianten sind etwas einfacher als die oberste Variante. Die zweite Variante sieht die Verwendung unterschiedlicher Ports und die dritte sogar die Verwendung unterschiedlicher Switches für PC und Telefon vor. Die Notwendigkeit von VLAN Tagging bis zum Arbeitsplatz entfällt somit. Verschiedene VLANs nutzen verschiedene Kabel und Dosen am Arbeitsplatz.

Allen drei Varianten ist jedoch gemeinsam, dass die VLAN-Trennung auf das Wohlverhalten aller beteiligten Personen angewiesen ist. In keiner Variante kann technisch verhindert werden, dass ein Telefon an das PC-VLAN angeschlossen wird oder umgekehrt. Dazu bedarf es mehr, nämlich der fälschungssicheren Authentifizierung

von Endgeräten und der Zuweisung dieser zum richtigen VLAN.

Authentifizierung und VLAN-Zuweisung

Erst dann, wenn technisch verhindert werden kann, dass ein Endgerät an das falsche VLAN angeschlossen wird, gilt die VLAN-Trennung als wirklicher Sicherheitsmechanismus. Deshalb ist die VLAN-Trennung am Arbeitsplatz unweigerlich mit der Authentifizierung von Endgeräten verbunden.

Seit 2004 gibt es nämlich den Standard IEEE 802.1X mit dem Titel Port-Based Network Access Control. Ohne Port-basierende Authentifizierung erlauben Netze gemäß den Standards der Standardfamilie IEEE 802 (LAN) auch nicht autorisierten Geräten bzw. Benutzern den Zugriff auf die LAN-Infrastruktur. Die Authentifizierung eines Benutzers erfolgt üblicherweise über ein Network Operating System (NOS) auf der Ebene höherer OSI-Schichten (5-7). Die Infrastruktur-Komponenten eines LANs (OSI-Layer 2) sind an diesem Anmeldeprozess in der Regel nicht beteiligt. Die Identifizierung des Benutzers ist eine NOS- oder Sicherheitsfunktion und nicht Bestandteil der Aufgaben des Netzes selbst.

Aus diesen Gründen wurde die Idee von IEEE 802.1X geboren, nämlich die Idee der Port-basierten Netzzugangskontrolle. Unter Ausnutzung der physikalischen Besonderheiten des Netzzugriffs in einem LAN werden gemäß IEEE 802.1X Authentifizierungsvorrichtungen an den LAN-Ports bereitgestellt. Unter Ports werden dabei Ports von MAC Bridges gemäß IEEE 802.1D (d.h. Layer-2-Switches), von Routern und Access-Points in einem Wireless LAN nach IEEE 802.11 verstanden. Ziel ist die Bereitstellung einer zusätzlichen Systemfunktion auf OSI-Layer 2, um den unautorisierten Zugang zum System oder zu einem Dienst des Systems zu unterbinden. Dabei werden die beim Remote Access Service (RAS) auf genutzten Authentifizierungsmechanismen auf das LAN übertragen.

Gemäß IEEE 802.1X können einem Port zwei unterschiedliche Rollen zugeordnet werden:

- Authenticator: Dieser Port verlangt eine Authentifizierung, bevor er den Zugang zu einem Dienst erlaubt, der über diesen Port erreicht werden kann.
- Supplicant: Dieser Port möchte den Zugang zu einem Dienst erlangen, der vom System des Authenticators angeboten wird.

Um einen vollständigen Authentifizierungsablauf zu ermöglichen, wird schließlich noch ein Authentication Server benötigt. Der Authentication Server bietet für den Authenticator die notwendige Authentifizierungsfunktion an, um die Login-Daten des Supplicants zu überprüfen. Der Server überprüft, ob der Supplicant autorisiert ist, Zugang zu dem über den Authenticator angebotenen Dienst zu erlangen.

Damit eine Geräteauthentifizierung gemäß IEEE 802.1X funktioniert, müssen daher folgende Bedingungen erfüllt sein:

- Das Gerät, das authentifiziert und somit Zugang zum Netz erhalten soll (Supplicant), muss eine Authentifizierung

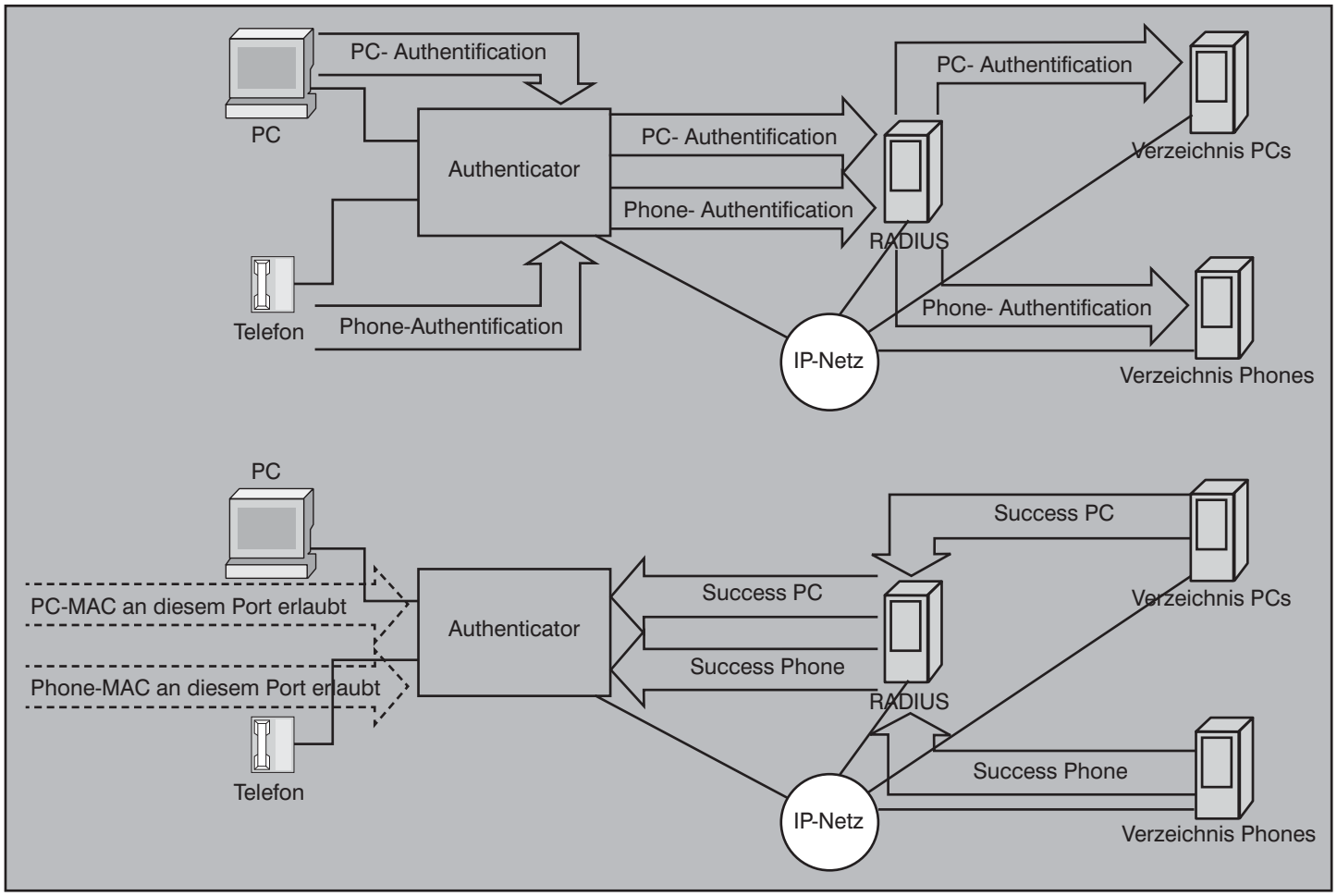


Abbildung 4: Authentifizierung von zwei Endgeräten an zwei verschiedenen Ports

gemäß dem im Standard IEEE 802.1X vorgesehenen Extensible Authentication Protocol Over LAN (EAPOL) unterstützen.

- Die Netzkomponente, die den Zugang des Endgerätes zum Netz sichern und prüfen soll, ob dazu die Bedingung der Authentifizierung erfüllt ist, muss die im Standard vorgesehene Rolle des Authenticators übernehmen.

- Im Hintergrund muss der Authenticator mit dem Authentifizierungsserver kommunizieren und die Daten, die der Supplicant zwecks Authentifizierung übergeben hat, an den Server weiterleiten, damit dieser die Berechtigung des Endgerätes für die Erlangung des Netzzugangs prüfen kann.

- Da es mehrere Methoden der Authentifizierung gibt, müssen der Supplicant und der Authentifizierungsserver mindestens eine gemeinsame Methode unterstützen, zum Beispiel die Verwendung von Zertifikaten gemäß dem Standard Transport Layer Security (TLS). In diesem Fall würde die Authentifizierungsmethode EAP-TLS heißen.

Eine Erweiterung der Vorgänge gemäß IEEE 802.1X besteht darin, abhängig vom Ergebnis der Authentifizierung eine Zuordnung des Endgerätes zu einem VLAN zu veranlassen. Dies erfolgt in der Regel durch eine Anweisung des Authentifizierungsservers an den Authenticator, zum Beispiel den LAN-Switch, das authentifizierte Endgerät einem bestimmten VLAN zuzuweisen. Somit ist auf den ersten Blick nicht nur für eine Authentifizierung der an das Netz angeschlossenen Endgeräte gesorgt, sondern darüber hinaus auch für ihre Zuordnung zum richtigen VLAN zu somit zur richtigen Vertrauensdomäne.

Die Abbildung 4 zeigt den Fall, dass zwei Endgeräte unterschiedlichen Typs an zwei verschiedene Ports eines LAN-Switches angeschlossen sind. Der PC und das IP-Telefon stellen jeweils einen Authentifizierungsrequest, der über den LAN-Switch (den Authenticator) an den Authentifizierungsserver, in der Regel einen Remote Access Dial-In User Service (RADIUS) weitergeleitet wird. Dieser kann die Requests je nach Endgerätetyp an verschiedene nachgelagerte Authentifizierungsdienste übergeben, zum Beispiel Verzeichnisserver für PCs und Telefone. Diese überprüfen den Authentifizierungsrequest und beantworten ihn positiv, wenn die Bedingungen für die Authentifizierung erfüllt sind (zum Beispiel wenn ein Challenge-Response-Verfahren erfolgreich abgeschlossen wird). Danach lässt der LAN-Switch das authentifizierte Endgerät ins Netz und schaltet in der Regel die MAC-Adresse des Endgerätes an dem verwendeten Port frei.

Nicht nur die Authentifizierung eines Endgerätes, sondern auch dessen Zuordnung zu einem VLAN kann abhängig vom Ergebnis der Authentifizierung erfolgen. Wie in der Abbildung 5 dargestellt kann der Authentifizierungsserver zwischen verschiedenen Gruppen von Supplicants unterscheiden und bei Erkennung einer bestimmten Gruppe den Authenticator anweisen, das Endgerät einem bestimmten VLAN zuzuordnen. In der Abbildung 5 wird der PC dem VLAN 1 und das IP-Te-

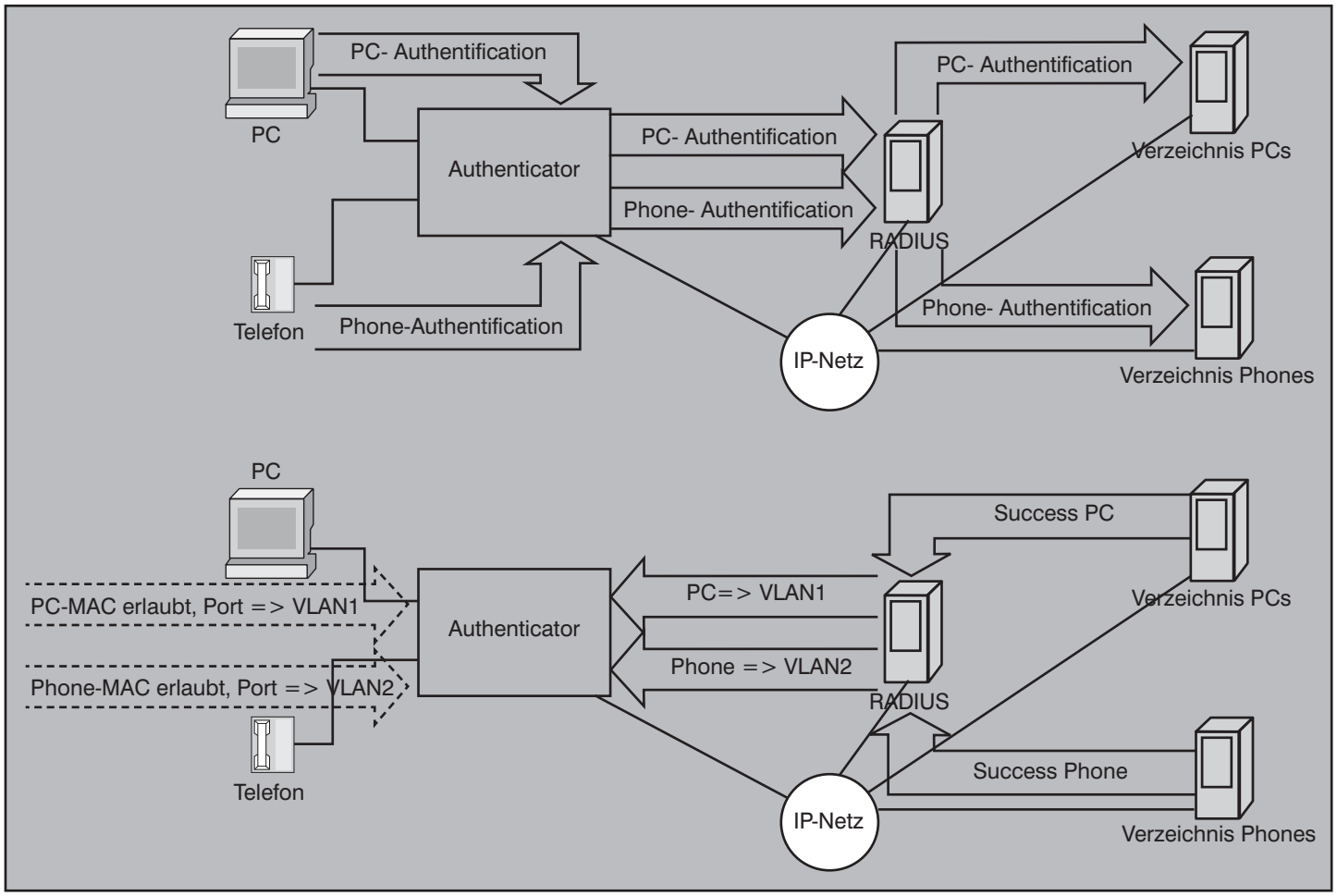


Abbildung 5: Dynamische VLAN-Zuweisung

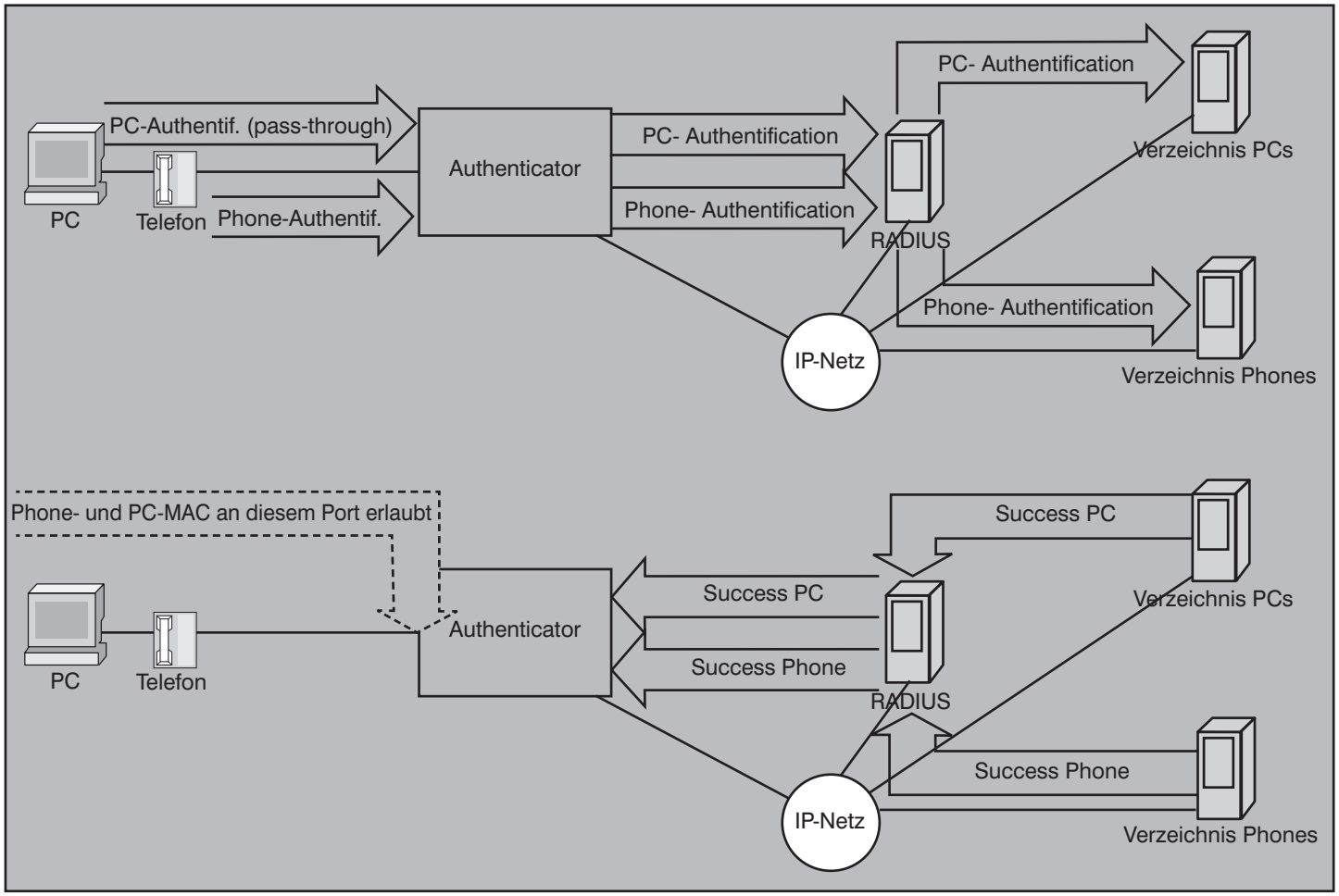


Abbildung 6: Authentifizierung von zwei Endgeräten an einem Port

lefon dem VLAN 2 zugeordnet. Technisch erfolgt dies so, dass der LAN-Switch die beiden eigenen Ports, an die der PC bzw. das Telefon angeschlossen sind, mit dem VLAN 1 bzw. VLAN 2 verbindet.

Der Fall, dass zwei Endgeräte an ein und den selben Port des LAN-Switches angeschlossen werden, ist in der Abbildung 6 dargestellt. Ein gängiges Beispiel dafür ist die Kaskadierung eines PCs und eines Telefons, indem der PC mit dem so genannten PC-Port des Telefons verbunden wird. In vielen IP-Telefonen ist ein Mini-Switch integriert, der dazu verwendet wird, den selben Port am Switch und das selbe Kabel zwischen dem Arbeitsplatz und dem Verteilerraum zwei Endgeräten zur Verfügung zu stellen und Kosten für Switch Ports und Kabel einzusparen.

Wie aus der Abbildung 6 hervorgeht, erhält der LAN-Switch (Authenticator) am selben Port die Authentifizierungsrequests von zwei Endgeräten (PC und Telefon) und muss diese weiter leiten. Der LAN-Switch muss in der Lage sein, den Authentifizierungsstatus von mehr als einem Endgerät pro Port zu überwachen und mehr als eine authentifizierte MAC-Adresse pro Port zuzulassen.

Damit der Authentifizierungsrequest des PCs den Authenticator erreicht, muss das IP-Telefon, das zwischen PC und LAN-Switch geschaltet ist, die Kommunikation zwischen PC und Authenticator unverändert weiter leiten, d.h. im so genannten Pass-Through-Modus arbeiten.

Dabei ist die Überwachung des Authentifizierungsstatus jedes Endgerätes von Bedeutung. Es muss verhindert werden, dass ein „Trittbrettfahrer“ eine bereits erfolgte Authentifizierung zum Eindringen in das Netz missbraucht. Abbildung 7 zeigt eine gängige Variante der Überwachung des Authentifizierungsstatus an einem Switch-Port. Die meisten Switches, die IEEE 802.1X unterstützen, überwachen den Status des physikalischen Links an einem Port. Der Wechsel dieses Status von aktiv (up) zu inaktiv (down) wird vom Switch (Authenticator) als ein Ereignis gewertet, welches den Status des bisher an den Port angeschlossenen Endgeräts von „authentifiziert“ in „nicht authentifiziert“ ändert. Das muss sein, weil sonst ein beliebiges Ersetzen authentifizierter Endgeräte durch andere Endgeräte möglich wäre. Überwacht der Switch den Status des Links, führt jede auch nur kurzzeitige Unterbrechung der Kabelverbindung zwischen Switch und Endgerät dazu, dass die Authentifizierung wiederholt werden muss.

Der Authenticator kann nur den Status jener physikalischen Verbindungen überwachen, die an seinen eigenen Ports terminiert werden. Dabei entsteht eine Sicherheitslücke, die in der Abbildung 8 dargestellt ist. Zwei Endgeräte sind an ein und dem selben Port eines Switches authentifiziert, sodass die zu den beiden Endgeräten gehörenden MAC-Adressen an diesem Port zugelassen sind. Der Authenticator überwacht den Status der physikalischen Verbindung zum IP-Telefon. Aber nicht das Telefon, sondern der PC, der an den PC-Port des Telefons angeschlossen ist, wird durch ein anderes Endgerät ersetzt. Von diesem Wechsel der physikalischen Verbindung zwischen

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

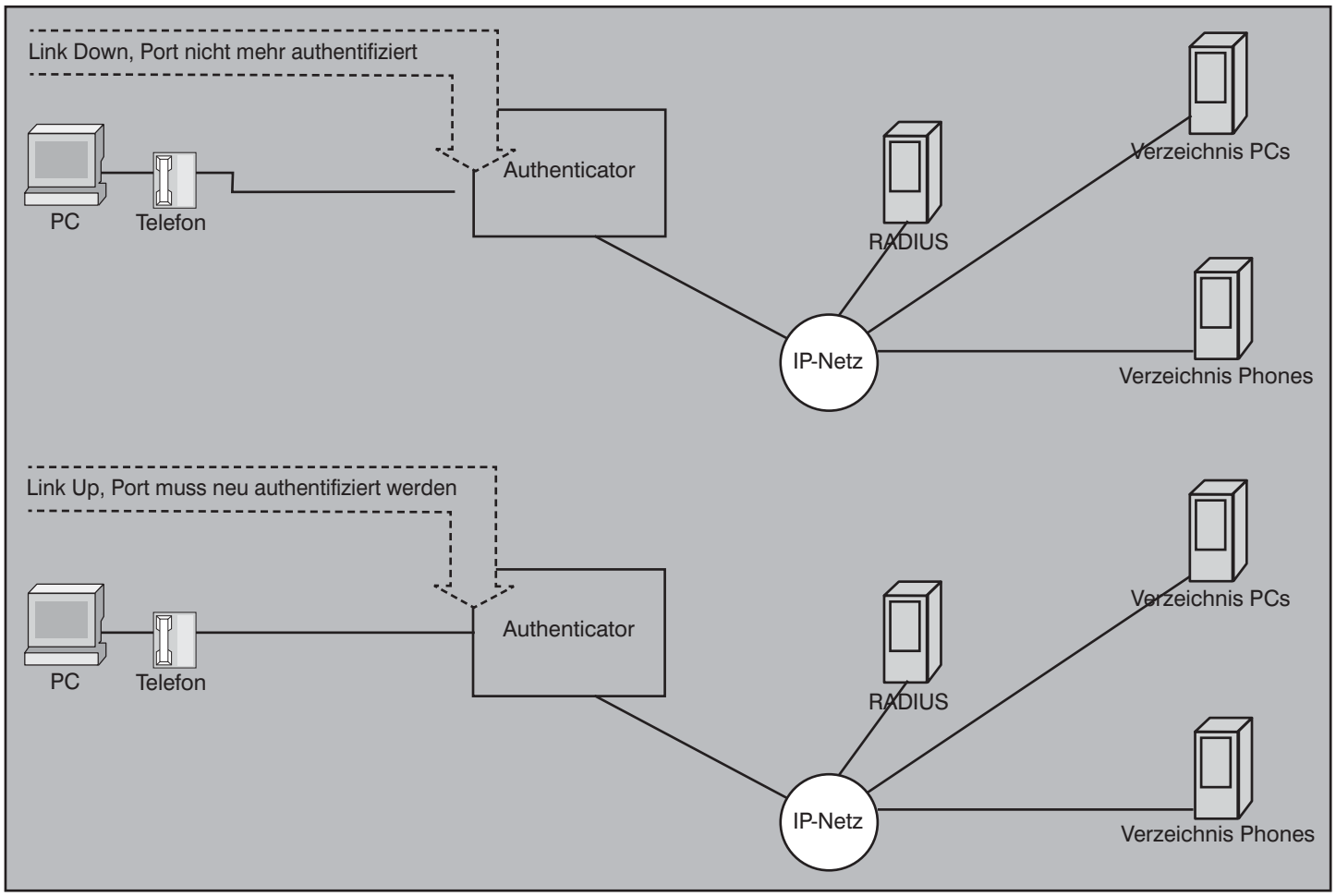


Abbildung 7: Überwachung des Link-Status

Telefon und PC in den inaktiven Status erfährt der Authenticator nichts, weil er nur die direkt an den eigenen Ports endenden Verbindungen überwachen kann. So kann ein Endgerät lediglich durch Einstellung der MAC-Adresse des authentifizierten PCs den Zugang zum Netz erlangen, ohne die Bedingungen der Authentifizierung (Zertifikat etc.) erfüllen zu müssen.

Um die in der Abbildung 8 dargestellte Sicherheitslücke zu schließen, haben einige Hersteller von IP-Telefonen die so genannte Proxy-Logoff-Funktion in ihren IP-Telefonen implementiert. Wie in der Abbildung 9 dargestellt besteht diese Funktion darin, dass statt des LAN-Switches das IP-Telefon den Zustand des Links zwischen dem IP-Telefon und dem PC überwacht. Wechselt dieser Zustand von aktiv zu inaktiv, meldet das Telefon stellvertretend für den PC diesen beim Authenticator ab (daher die Bezeichung Proxy Logoff). Beim erneuten Versuch des Zugriffs auf das Netz fordert der Authenticator von dem Endgerät, das an den PC-Port des Telefons angeschlossen ist, eine neue Authentifizierung. Ein Endgerät, das die Bedingun-

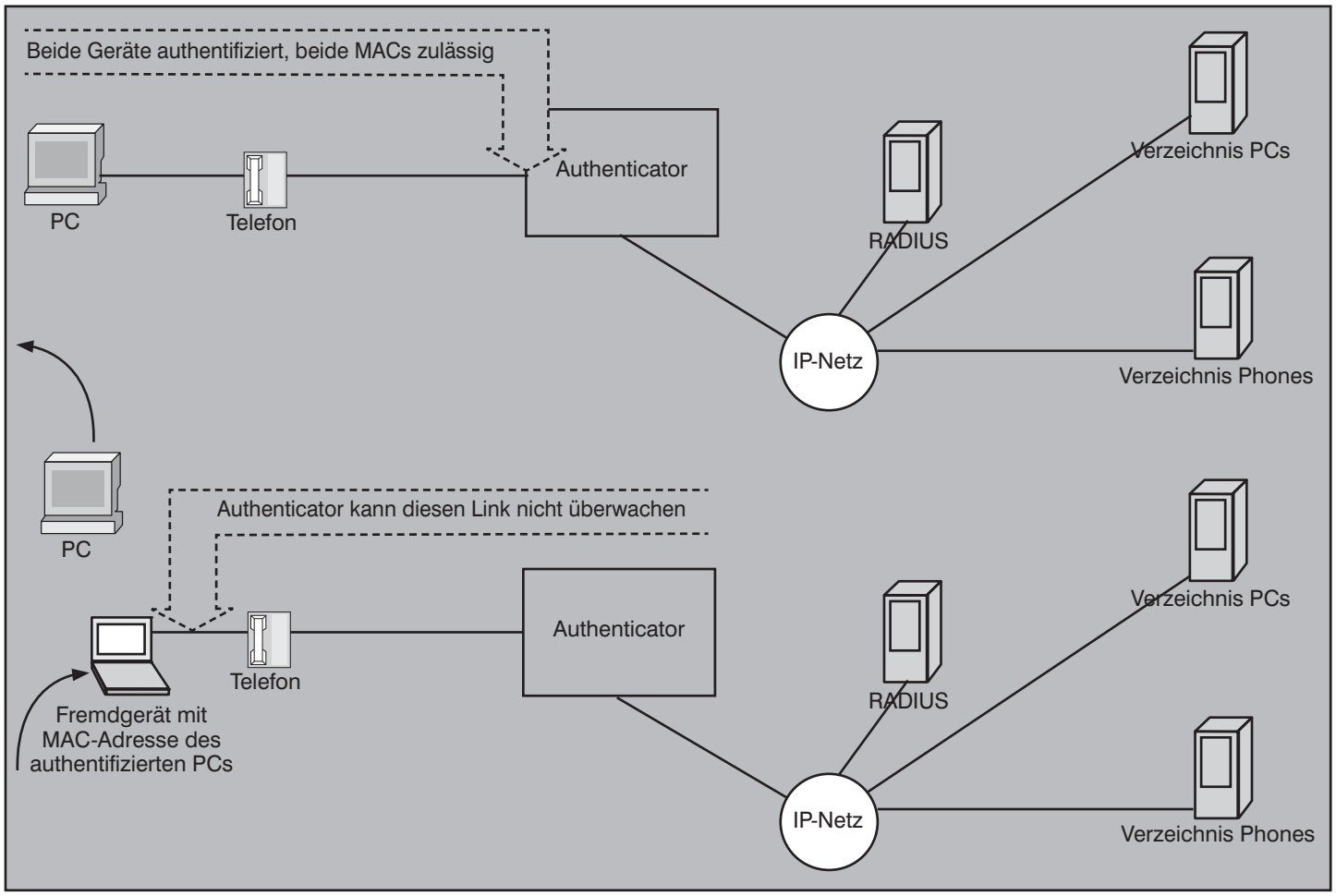


Abbildung 8: Authenticator kann Link zwischen Telefon und PC nicht überwachen

gen der Authentifizierung nicht erfüllt, wird nicht in das Netz gelassen.

Unabhängig davon, ob das IP-Telefon im Pass-Through- oder Proxy-Logoff-Modus arbeitet, ist bei Anschluss eines PCs an den PC-Port des Telefons die dynamische Zuordnung der beiden Endgeräte zu verschiedenen VLANs komplexer als bei Verwendung von zwei verschiedenen Ports des LAN-Switches durch die beiden Endgeräte. Wie aus der Abbildung 10 hervorgeht, bedarf es dazu nicht nur einer Anweisung an den LAN-Switch, die Pakete von Telefon und PC verschiedenen VLANs zuzuordnen, sondern auch einer dynamischen VLAN-Zuordnung auf dem Telefon selbst. Ist diese dynamische VLAN-Zuordnung mit einem Protokoll wie Cisco Discovery Protocol (CDP) bzw. Link Layer Discovery Protocol (LLDP) sichergestellt, kann sie nicht vom Ergebnis einer Authentifizierung gemäß IEEE 802.1X abhängig gemacht werden, denn CDP bzw. LLDP sind in der Regel unabhängig von einem Authentifizierunsgprozess. Bei diesen Protokollen handelt es sich um Kommunikationsbeziehungen, die auf eine

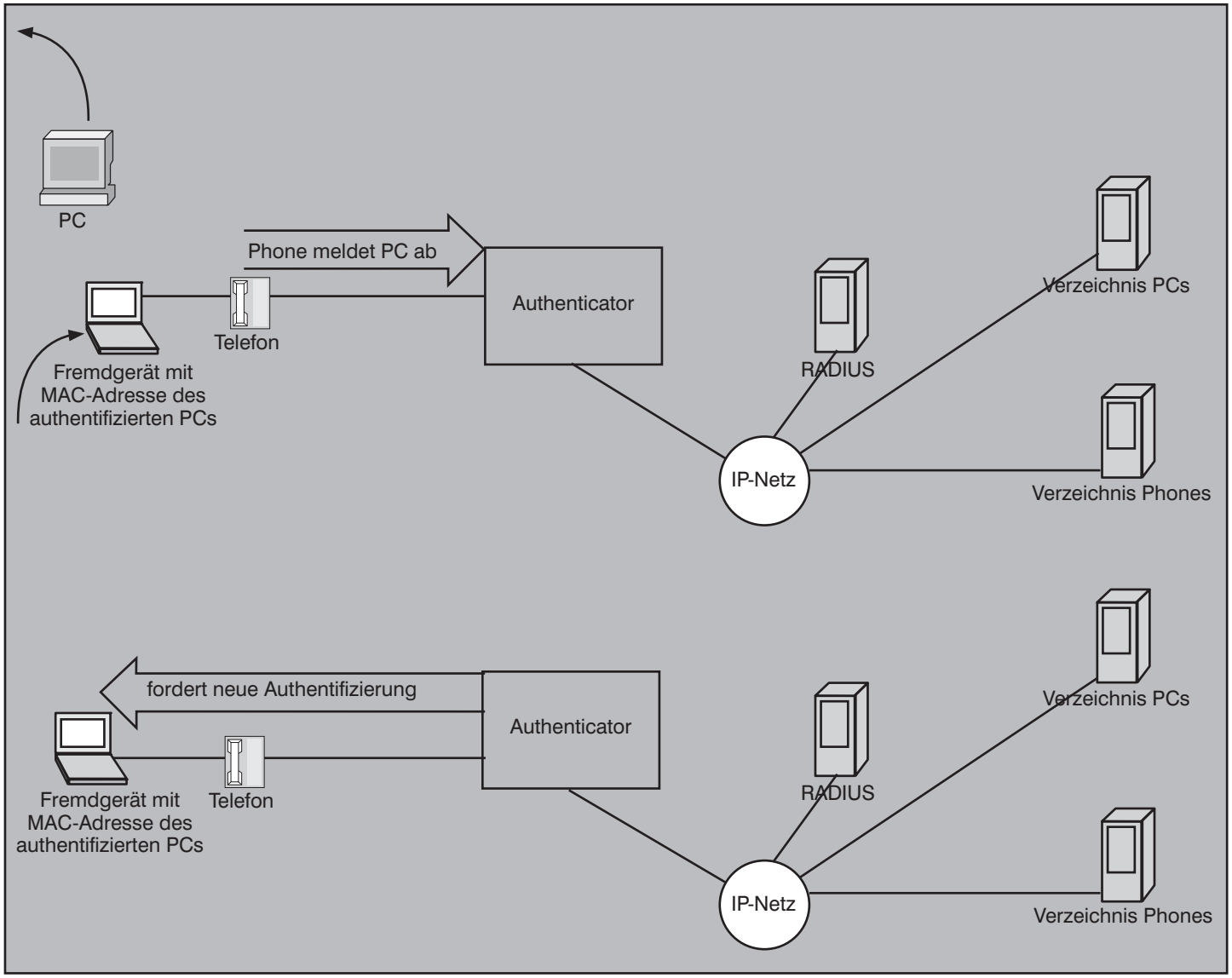


Abbildung 9: Proxy Logoff

physikalische Verbindung begrenzt sind. Außerdem unterstützen viele LAN-Switches die dynamische VLAN-Zuweisung nur bei Ports, die nicht als so genannte Trunk Ports konfiguriert sind, sondern Pakete ohne VLAN-Zuordnung übertragen.

Aber selbst wenn die dargestellten Probleme auf Umwegen wie zum Beispiel mehrstufige DHCP-Kommunikation gelöst werden, bleiben, wie der nächste Abschnitt zeigen wird, wesentliche Sicherheitslücken.

Grenzen der reinen Geräteauthentifizierung

Der Standard IEEE 802.1X beschreibt eine reine Geräteauthentifizierung, ohne dass nach der Authentifizierung des Gerätes dessen Pakete ebenfalls authentifiziert werden. Hier kommt es zu einem Problem, das bei jedem Szenario der reinen Geräteauthentifizierung am Anfang einer Verbindung entsteht, nämlich zu dem Problem, dass eine einmal erfolgreiche Authentifizierung von einem „Trittbrettfahrer“ missbraucht werden kann.

Die Abbildung 11 zeigt dieses prinzipielle Problem bei IEEE 802.1X. Ist das Endgerät mit der MAC-Adresse A an einem Switch authentifiziert, kann diese Authentifizierung von jedem Endgerät missbraucht werden, dass die MAC-Adresse A verwendet. Der Angreifer kann nämlich zwischen dem Supplicant und dem Authenticator einen Hub einsetzen. Der Authenticator kann nach dieser Aktion zwar die erneute Authentifizierung des Gerätes mit der MAC-Adresse A erzwingen, aber nicht mehr kontrollieren, ob außer dem authentifizierten Endgerät nicht auch noch ein anderes Endgerät die MAC-Adresse A verwendet. Das kann durchaus der Fall sein, nämlich wenn an den zwischen Supplicant und Authenticator eingesetzten Hub ein weiteres Gerät angeschlossen wird, an dem die MAC-Adresse A eingestellt ist. Auch wenn die Authentifizierung periodisch wiederholt wird, hat sie nur das Ergebnis, eine bestimmte MAC-Adresse an einem Port des Switches freizugeben. Da die Pakete des authentifizierten Endgerätes nicht einzeln authentifiziert werden, kann der Authenticator nicht zwischen den Paketen des authentifizierten Endgerätes und den anderen Paketen unterscheiden, die als Source-Adresse die MAC-Adresse A tragen.

Da der Hub alle empfangenen Pakete auf alle Ports flutet, findet an keiner Stelle eine Prüfung statt, ob das an den Hub ange-

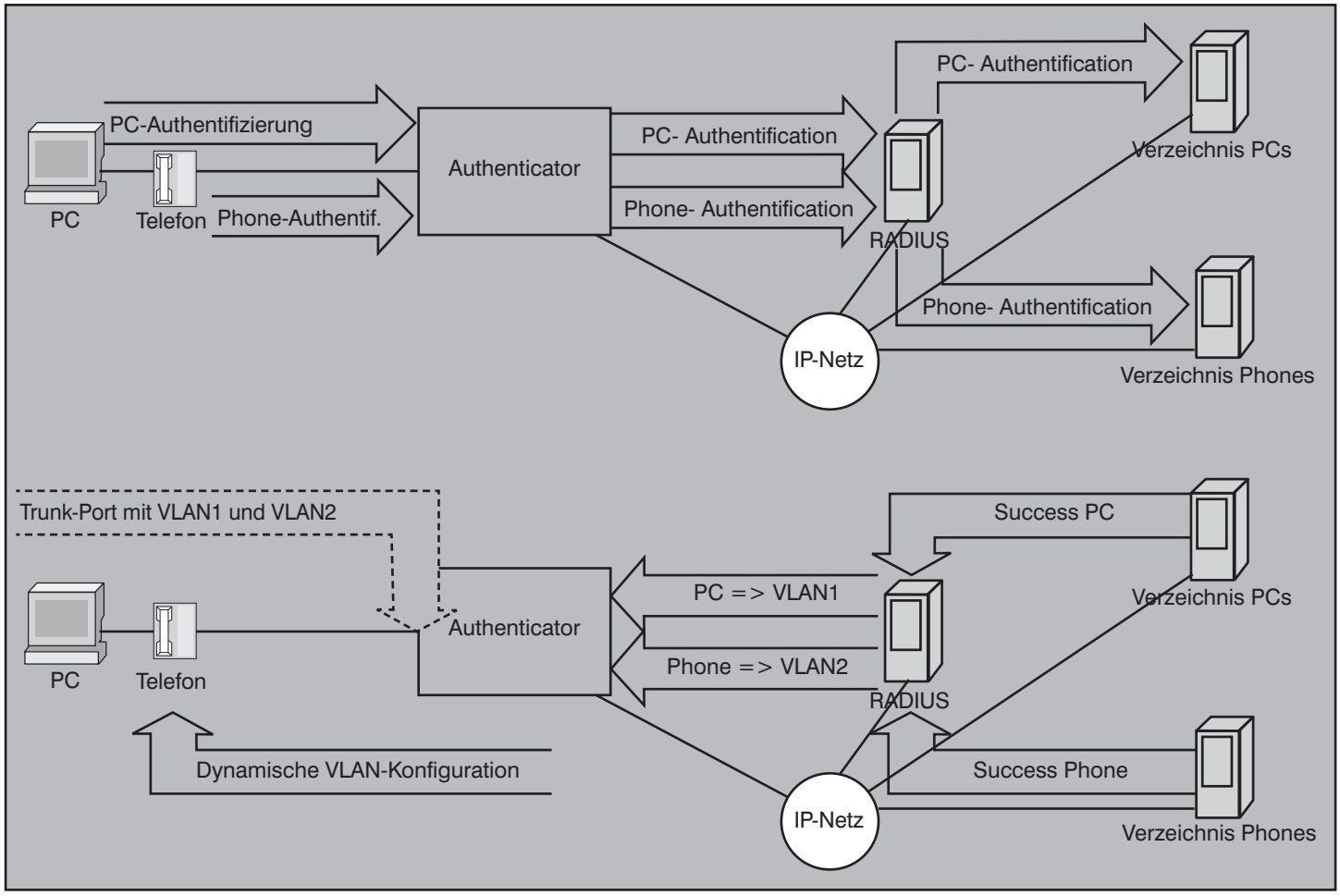


Abbildung 10: Dynamische VLAN-Zuordung bei Kaskadierung von PC und Telefon

schlossene Endgerät die MAC-Adresse A fälscht. Lediglich der authentifizierte PC mit der selben MAC-Adresse könnte erkennen, dass ein anderes Endgerät diese Adresse auch verwendet. Selbst wenn man auf allen Endgeräten einen Mechanismus implementieren würde, der bei einem solchen Ereignis Alarm schlägt (was bei den gängigen Endgerätetypen nicht möglich ist), kann der Angreifer leicht solche Alarmmeldungen am Hub blockieren. Er könnte darüber hinaus dafür sorgen, dass die Pakete des zusätzlich hinzugefügten Endgerätes nicht an das Endgerät weiter geleitet wird, das die MAC-Adresse A legitim besitzt. Dazu könnte zum Beispiel statt eines Hubs ein Switch eingesetzt werden, der mittels eines Filters alle Pakete mit der Source-Adresse A an dem zum authentifizierten PC gerichteten Port blockiert.

Das Problem ist grundsätzlich auf die folgenlose Anfangsauthentifizierung zurückzuführen. Zwar wird das Endgerät am Anfang authentifiziert, aber die darauf folgende Kommunikation wird nicht mehr überprüft. Dies öffnet Trittbrettfahrern Tür und Tor.

Aus diesem Grund wurde die Authentifizierung gemäß IEEE 802.1X bei Wireless LAN anders angewandt und mit weiteren Verfahren kombiniert. Bei WLAN war der Leidensdruck groß, nachdem offensichtlich geworden war, dass der im Standard IEEE 802.11 vorgesehene Mechanismus WEP (Wired Equivalent Privacy) große Sicherheitslücken hat. Das Medium WLAN bietet anders als kabelgebundene Netze auch Angreifern außerhalb der Gebäude des Netzbetreibers die Möglichkeit, auf das Netz zuzugreifen. Deshalb musste WEP durch ein sicheres Verfahren ersetzt werden. Bei diesem zweiten Versuch hat man es dann gründlich gemacht. Die Anfangsauthentifizierung gemäß IEEE 802.1X wurde eingesetzt, aber gleichzeitig dazu genutzt, um ein Schlüsselmanagement direkt mit der Authentifizierung einzuleiten. Mit dem Schlüsselaustausch wurde auch der Aufbau einer sicheren Kommunikationsbeziehung zwischen zwei WLAN-Partnern ermöglicht. Sämtliche Pakete, die in einem sicheren WLAN zum Beispiel gemäß dem Standard IEEE 802.11i ausgetauscht werden, werden von den Kommunikationspartnern authentifiziert und verschlüsselt. Ein Angreifer kann zwar das Shared Medium WLAN nutzen und Pakete an beliebige Kommunikationspartner senden, aber diese sind in der Lage zu erkennen, ob diese Pakete wirklich von dem authentifizierten Partner stammen. Darüber hinaus werden die Pakete verschlüsselt. Das Schlüsselmaterial dazu ist ja vorhanden.

Dass eine solche sichere Kommunikation mit Authentifizierung und Verschlüsselung aller Pakete möglich ist und keine unlösbaren Probleme und keine zu hohe Belastung für die Hardware der angeschlossenen Endgeräte schafft, hat die Praxis der sicheren WLANs in den letzten Jahren bewiesen. WLANs sind somit hinsichtlich Sicherheit weiter als die kabelgebundenen LANs, was plausibel ist, weil bei WLANs der größere Leidensdruck die Implementierung einer lückenlosen Sicherheit erforderlich gemacht hat. In sicheren WLANs wird keine Scheinsicherheit durch Hinzufügen eines leicht zu verfälschenden VLAN Tags genutzt, sondern eine Verschlüsselung, die erst auf zwei als vertrauenswürdig eingestuften Geräten aufgehoben wird: WLAN Access Point einerseits und WLAN-

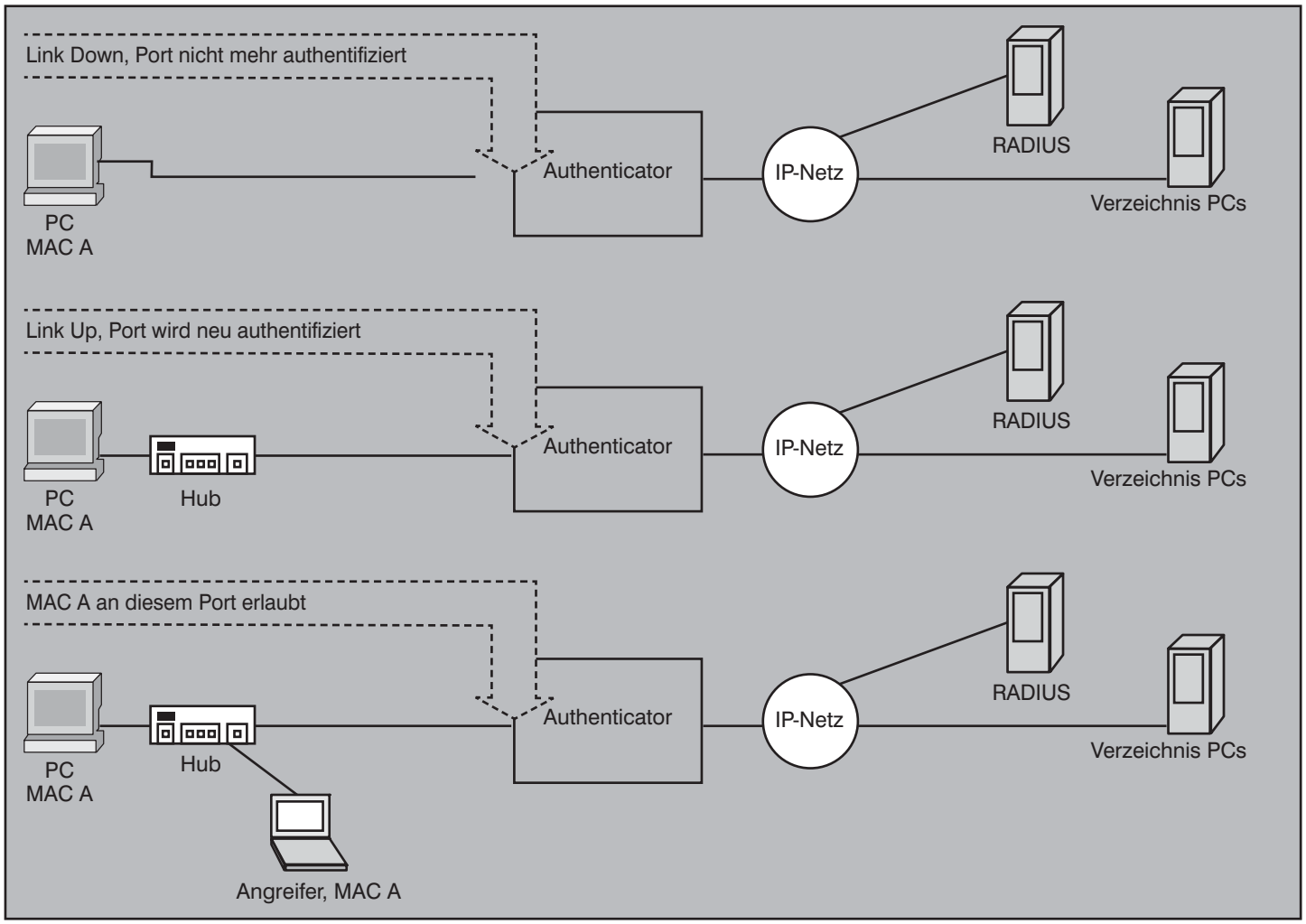


Abbildung 11: Sicherheitslücke bei IEEE 802.1X

Endgerät andererseits. Der WLAN Access Point wird von einem Netzbetreiber administriert. Ist die physikalische Sicherheit des AP gewährleistet (was nicht immer leicht zu bewerkstelligen ist), und ist der Netzbetreiber als vertrauenswürdig eingestuft, kann der Nutzer jedes Endgerätes in einem sicheren WLAN davon ausgehen, dass die Kommunikation im WLAN von Dritten weder abgehört noch manipuliert oder gefälscht werden kann. Mittel dazu ist die Verschlüsselung. Ohne Verschlüsselung ist die anfängliche Authentifizierung wertlos.

MACsec gemäß IEEE 802.1AE

Die Grenzen der reinen Geräteauthentifizierung sind natürlich auch den Gremien klar, die für die Standardisierung von LAN-Sicherheit zuständig sind. Deshalb gibt es seit August 2006 den Standard IEEE 802.1AE mit dem Titel Media Access Control (MAC) Security. Bei diesem Standard geht es darum, in einem Medium, das Zugriffsmechanismen gemäß den Standards der IEEE-Standardfamilie 802 verwendet und auf der Ebene der Schicht 2 Media Access Control (MAC) einsetzt, vor allem in einem Ethernet, auf der Ebene der Schicht 2 (MAC) vor Angriffen zu schützen. Der Standard IEEE 802.1AE beschreibt Mechanismen, die unter dem Oberbegriff MAC Security (MACsec) die Vertraulichkeit der ausgetauschten MAC-Rahmen sicherstellen sowie dafür sorgen, dass die Integrität dieser Rahmen gewahrt bleibt und dass überprüfbar ist, ob ein Paket wirklich von dem Kommunikationspartner stammt, dessen Identität im Frame Header als Source-Adresse angegeben ist.

MACsec gemäß IEEE 802.1AE ist ausdrücklich nicht für ein WLAN gedacht, denn für Wireless LANs hat der Standard IEEE 802.11i von 2004 bereits die Grundlagen zum Erreichen der selben Ziele geschaffen, die mit dem Standard IEEE 802.1AE für kabelgebundene LANs angestrebt werden.

Das Prinzip von MACsec ist in der Abbildung 12 dargestellt. Der Authentifizierung folgt der Aufbau von Sicherheitsassoziationen auf der MAC-Ebene. Diese Sicherheitsassoziationen erlauben, alle ausgetauschten Pakete entweder nur zu authentifizieren oder auch noch zu verschlüsseln. Somit hätte ein Angreifer mit physikalischem Zugang zum Medium keine Chance, eigene Pakete für solche auszugeben, die von einem der authentifizierten Geräte stammen. Der Angreifer kann ebenso wenig die zwischen den Endgeräten ausgetauschten Pakete manipulieren. Und wenn die Pakete verschlüsselt sind, kann der Angreifer sie ebenso wenig abhören.

Der Standard MACsec befasst sich ausdrücklich nicht mit der Authentifizierung und Autorisierung von Endgeräten, sondern damit, wie bereits authentifizierte und autorisierte Endgeräte sicherstellen, dass die Vertraulichkeit, die Integrität und die Echtheit der ausgetauschten Pakete erreicht werden. Insofern ist MACsec ohne Kombination mit anderen Verfahren

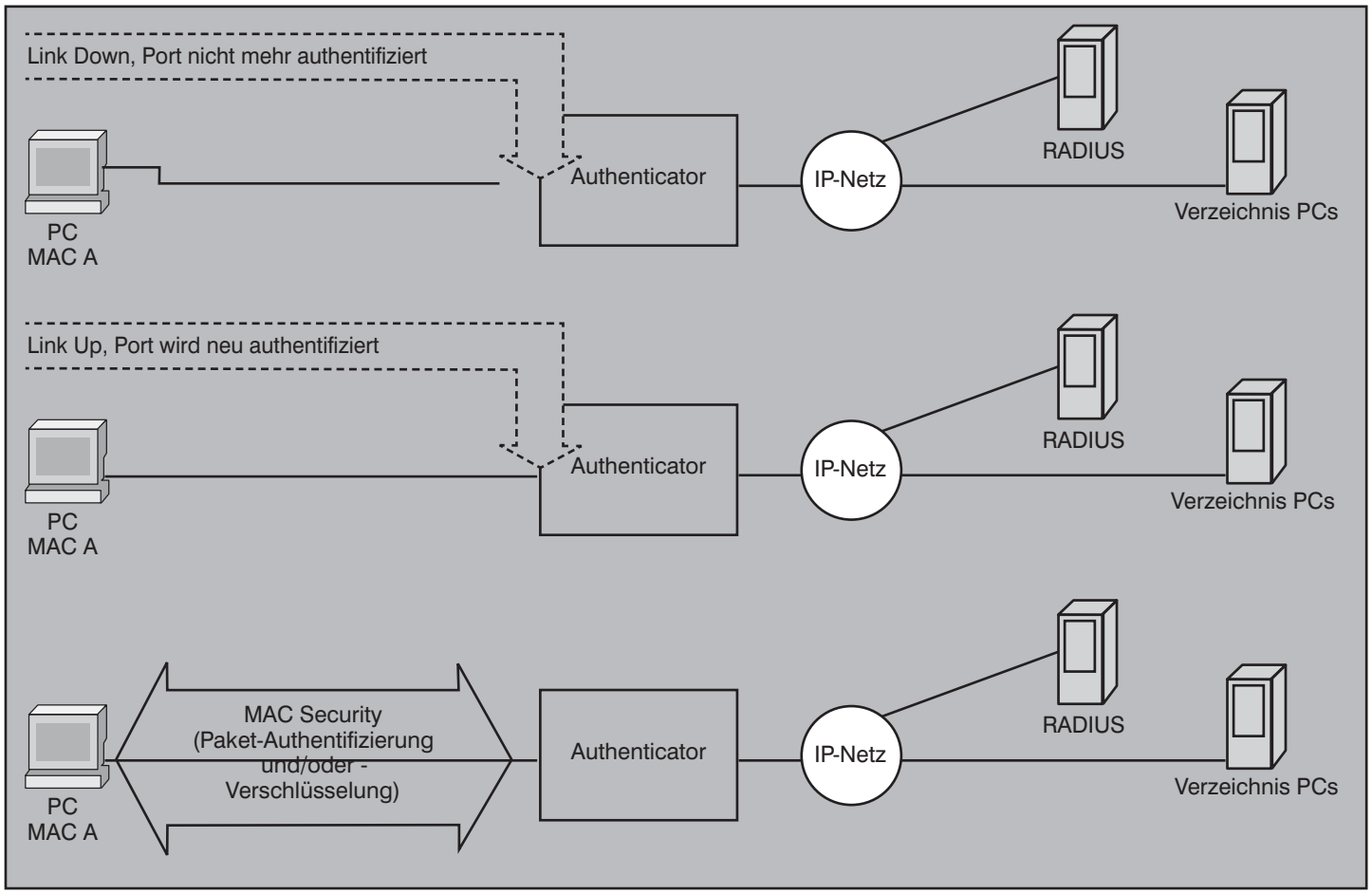


Abbildung 12: MAC Security (MACsec) gemäß dem Standard IEEE 802.1AE

zur Authentifizierung meistens nicht sinnvoll. Das ist auch der Grund, dass bereits auf Seite 6 des Standardtextes von IEEE 802.1AE auf IEEE 802.1X hingewiesen wird und auch darauf, dass einer künftigen Ergänzung des Authentifizierungsstandards IEEE 802.1X, nämlich IEEE 802.1af, die Aufgabe vorenthalten bleibt, die beiden Standards für Authentifizierung (IEEE 802.1X) und MAC-Sicherheit (IEEE 802.1AE) miteinander zu kombinieren. Ergebnis wird dann ein sicheres LAN sein, in dem sich die angeschlossenen Geräte gegenseitig authentifizieren und darauf aufbauend auch die Vertraulichkeit, Integrität und Echtheit aller ausgetauschten Pakete sicherstellen können.

Aber auch ohne Authentifizierung gemäß IEEE 802.1X wären sinnvolle Einsätze der Mechanismen von MACsec denkbar, nämlich dann, wenn die Geräte auch ohne IEEE 802.1X sicher authentifiziert werden. Ein Beispiel dafür wären die Netzkomponenten selbst. Ein Netzbetreiber kann durch andere Mechanismen wie zum Beispiel sichere physikalische Aufstellung der Netzkomponenten dafür sorgen, dass diese Netzkomponenten nur dem Zugriff authentifizierter Personen ausgesetzt sind. Um die ausgetauschten Pakete vor Abhörszenarien sowie Manipulation und Fälschung auf dem Übertragungsweg zu schützen, kann MACsec eingesetzt werden. Dies ist vor allem dann sinnvoll, wenn zwar die Netzkomponenten und ihre physikalische Lokation, nicht aber das Medium dazwischen (das Kabel) als sicher eingestuft wird. Dann hilft MACsec, aus diesem nur teilweise sicheren Szenario ein sicheres zu machen. Ein typisches Einsatzszenario wäre die Verbindung von zwei Komponenten über eine physikalische Verbindung, die über öffentliches Gelände verläuft, zum Beispiel die Verbindung von zwei Ethernet-Switches über Dark Fiber.

Einige Hersteller haben die Unterstützung von MACsec von ihren Produkten schon angekündigt. Der erste Schritt wird sein, dass MACsec auf den Verbindungen zwischen den Netzkomponenten eingesetzt wird.

Ob das Verfahren MACsec auch bis zu den Endgeräten eingesetzt werden kann, hängt von den Herstellern von Chipsätzen und Treibern für die LAN Interfaces ab, die in den Endgeräten eingesetzt werden. Ein vollständiges MACsec-Szenario im Access-Bereich ist erst dann möglich, wenn der Standard IEEE 802.1af vorliegt, wenn also MACsec mit der Authentifizierung gemäß IEEE 802.1X kombiniert werden kann. Vermutlich wird die Unterstützung von MACsec durch die Endgeräte erst nach der Verabschiedung von IEEE 802.1af kommen.

Verschlüsselung: segmentweise oder Ende zu Ende?

Es wird noch Jahre dauern, bis MACsec nicht nur in Form eines durchgängig standardisierten Ansatzes, sondern auch in der Gestalt von Geräten verfügbar sein wird, die keine Interoperabilitätsprobleme aufweisen. Wenn man bedenkt, dass fast vier Jahre nach der Verabschiedung des Standards IEEE 802.1X immer noch viele Endgeräte diesen Standard nicht unterstützen und selbst bei Endgeräten, die angeblich 1X-konform sind, die Interoperabilität mit Switches und Authentifizierungsservern keineswegs sichergestellt ist, und dass viele Probleme wie zum Beispiel die Behandlung von Kaskaden von Endgeräten existieren, fällt es schwer zu glauben,

dass wir in diesem Jahrzehnt funktionierende MACsec-Umgebungen sehen werden. Davor werden noch einige Jahre vergehen.

Aber selbst wenn man optimistisch ist und glaubt, dass die Kombination von MACsec und Authentifizierung in wenigen Jahren in den Endgeräten implementiert sein wird, bleibt die Frage, was damit erreicht wird.

Mit der Kombination von Port-basierender Authentifizierung gemäß IEEE 802.1X und MACsec wird erreicht, dass eine bestimmte Kommunikationsbeziehung innerhalb eines Layer-2-Netzes gegen Abhören, Manipulation und Fälschung gesichert wird. Kommunikationsbeziehungen gehen aber fast immer über mehrere Layer-2-Netze. In jedem dieser Segmente müsste die Kombination aus MACsec und Authentifizierung implementiert werden. Außerdem muss den Betreibern aller dieser Layer-2-Netze Vertrauen entgegengebracht werden, denn diese Betreiber haben Zugriff auf Daten, die nicht gemäß MACsec verschlüsselt sind.

Dagegen ist heute schon bei vielen Kommunikationsbeziehungen eine Ende-zu-Ende-Verschlüsselung machbar. Diese Verschlüsselung erfolgt entweder auf der Ebene der Schicht 3 von IP-Endgerät zum IP-Endgerät mittels IP Security (IPsec), auf der Ebene der Schicht 4 durch Nutzung von Transport Layer Security (TLS) oder auf der Ebene der Schichten 5 bis 7 mithilfe von Verfahren wie E-Mail-Verschlüsselung, z.B. durch S/MIME, bzw. Secure Real-time Transport Protocol (SRTP) wie im Falle von Echtzeit-Audio bzw. Echtzeit-Video. Es ist fraglich, ob angesichts der zunehmenden Verfügbarkeit und Verbreitung der Ende-zu-Ende-Verschlüsselung die mühsam zusammengestellte Kombination von Verfahren, die für die Sicherheit auf der Ebene der Schicht 2 erforderlich ist, irgendeinen Vorteil bringen wird, wenn sie irgendwann einmal tatsächlich verfügbar und anwendbar ist.

Die Ende-zu-Ende-Verschlüsselung ist nämlich die vollständigste Art, eine Kommunikationsbeziehung zu schützen, die physikalische Medien mit anderen Kommunikationsbeziehungen teilen muss. Keine logische Netztrennung, keine segmentweise Verschlüsselung erreicht das Niveau an Sicherheit, das mit der Ende-zu-Ende-Verschlüsselung realisierbar ist. Nur mit der Ende-zu-Ende-Verschlüsselung wird eine universelle Kommunikationssicherheit möglich, die von den variierenden Kommunikationswegen und den Betreibern der verschiedenen Pfade des Kommunikationspfades unabhängig ist.

Dennoch die VLAN-Trennung am Arbeitsplatz?

In diesem Beitrag wurde begründet, warum die Zuordnung von Endgeräten zu verschiedenen VLANs die Authentifizierung von Endgeräten erfordert, die wiederum Sicherheitslücken aufweist, wenn sie eine reine Geräteauthentifizierung bleibt und nicht eine Authentifizierung jedes einzelnen Paketes zur Folge hat. Da für eine solche Authentifizierung die selben Mechanismen erforderlich sind für eine Verschlüsselung, wäre der Schritt zur Implementierung von MAC Security (MACsec) nicht weit. Im Moment fehlen dafür sowohl in der Standardisierung als auch bei den Produkten einige wesentliche Bausteine. Dagegen ist bei vielen Applikationen, u.a. bei Voice over IP, E-Mail und Web eine Ende-zu-Ende-Verschlüsselung verfügbar, die im Vergleich zu MACsec die ohnehin bessere Lösung darstellt.

Und dennoch wird VLAN-Trennung am Arbeitsplatz angewandt. Neben den angeblichen Sicherheitsvorteilen wird auch geltend gemacht, dass eine solche VLAN-Trennung Vorteile für die Ausfallsicherheit der Applikationen habe. Um welche Vorteile geht es? Wann könnte sich eine VLAN-Trennung positiv auf die Verfügbarkeit von Applikationen auswirken?

Um diese Frage zu beantworten, muss man alle Szenarien betrachten, in denen die Verfügbarkeit eines VLANs trotz der gemeinsamen Nutzung eines physikalischen Netzes durch Fehler und Probleme in einem anderen VLAN nicht beeinträchtigt wird. Vorstellbar sind folgende Fälle:

- In einem VLAN kommt es zu einem Broadcast-Sturm. Die Broadcasts in einem VLAN breiten sich jedoch in den meisten Fällen nicht auf andere VLANs aus. Deshalb gilt die Eindämmung der Auswirkung von Broadcast-Stürmen als wesentliches Argument für die VLAN-Trennung. Grundsätzlich ist gegen die Verkleinerung von Broadcast-Domänen nichts einzuwenden, nur warum muss die Einteilung in verschiedene Broadcast-Domänen unbedingt anhand einer Kategorisierung von Endgeräten erfolgen?

- Eine häufige Ursache von Problemen ist die fehlerhafte Vergabe von IP-Adressen. Entweder durch eine falsche manuelle Konfiguration oder durch die Aktivierung eines DHCP-Servers, der falsche IP-Konfigurationen verteilt, kommt es hin und wieder dazu, dass Endgeräte in einer Broadcast-Domäne (Wirkungsfeld eines unerwünschten DHCP-Servers) von der Kommunikation mit anderen Subnetzen abgeschnitten werden. Es ist verständlich, dass man IP-Telefone vor solchen Szenarien schützen will. Aber verdienen die anderen Clients keinen solchen Schutz? Ist es tolerierbar, wenn in einer Broadcast-Domäne Dutzende PCs nicht auf ERP-Anwendungen oder andere geschäftskritische Applikationen zugreifen können, weil sie von einem „wilden“ DHCP-Server eine falsche IP-Konfiguration erhalten haben?

- Die gezielte Manipulation der per Address Resolution Protocol ermittelten Zuordnung von IP- zu MAC-Adressen – als ARP Poisoning bekannt – ist immer nur in einer Broadcast-Domäne möglich. Je kleiner die Broadcast-Domäne, umso weniger die Kommunikationsbeziehungen, die mittels ARP Poisoning von einer Station aus abgehört werden können. Trennt man die VLANs für Voice und Data, können PCs keinen ARP-Posioning-Angriff mehr gegen IP-Telefone durchführen. Aber ist es tolerierbar, wenn mit solchen Angriffen Datenapplikationen ausspioniert werden? Sind Inhalte von übertragenen Dateien weniger kritisch und schützenswert als Telefongespräche?

- Probleme werden manchmal auch durch die Flutung von Paketen verursacht. Die Auswirkungen solcher Probleme bleiben in der Regel jedoch nicht auf eine Broadcast-Domäne beschränkt. Muss ein Layer-2-Switch in einem VLAN die Pakete fluten, weil zum Beispiel ein fehlerhafter Netzadapter zu viele MAC-Adressen als Source-Adressen von Paketen verwendet und so die MAC-Adresstabellen von Switches zum Überlauf bringt oder weil eine asymmetrische Verkehrsführung Pakete verursacht, dessen Ziel dem Layer-2-Switch unbekannt ist, steigt die Belastung des Switches insgesamt. Das wirkt sich auf die gesamte Switch-Leistung aus und nicht bloß in einem VLAN.

- Auch undefinierte Netzzustände und Spanning-Tree-Probleme wirken sich manchmal auf alle VLANs aus, sodass die VLAN-Trennung nicht immer die Eindämmung solcher Probleme bewirkt.

- Die VLAN-Trennung erleichtert die Zuordnung von separaten Adressbereichen zu verschiedenen Gerätetypen. Beim Betrieb des Netzes ist es hilfreich, Subnetze und somit IP-Adressen eindeutig einem der beiden Bereiche Daten oder Sprache zuordnen zu können.

Das gilt zum Beispiel für die Priorisierung von Voice in Weitverkehrsnetzen oder für die Implementierung von Access Control Lists (ACL), die dafür sorgen, dass bestimmte Kommunikationsbeziehungen zwischen dem Daten- und dem Voice-Bereich unterbunden oder nur namentlich eingestellte Kommunikationsbeziehungen zwischen den beiden Bereichen erlaubt werden. Aber auch ohne VLAN-Trennung lassen sich separate Adressbereiche für verschiedene Gerätetypen vergeben. Einige DHCP-Server unterstützen zum Beispiel die Vergabe von Adressen aus bestimmten Pools an Geräte, deren MAC-Adressen mit einer vorgegebenen Folge von Bytes (einer Herstellerkennung, Vendor ID) beginnen.

Insgesamt können also die technischen Argumente für eine VLAN-Trennung am Arbeitsplatz entkräftet werden.

Insbesondere Anbieter von IP-Telefonielösungen empfehlen dennoch ihren Kunden standardmäßig die Zuordnung von IP-Telefonen und PCs zu unterschiedlichen VLANs. Um Empfehlungen von Herstellern zu befolgen und diesen keinen Vorwand zu liefern, die technische Unterstützung insbesondere bei Problemen einzuschränken, lassen sich viele Unternehmen auf diese Art VLAN-Trennung am Arbeitsplatz ein. Der Beobachtung des Autors zufolge ist längst keine technisch nachvollziehbare Begründung mehr für diesen Schritt vorhanden, sondern lediglich der Hinweis auf die eine oder andere von wem auch immer dokumentierte „Best Practice“. Die Empfehlung der VLAN-Trennung zwischen Voice und Data wurde von White Paper zu White Paper, von Studie zu Studie übernommen und entwickelte eine Eigendynamik. Auf technische Diskussionen lässt man sich häufig nicht mehr ein. Dass die Argumente für eine VLAN-Trennung einer technischen Prüfung nicht standhalten, interessiert wenig.

Es wird übersehen, dass Voice nicht mehr und nicht weniger ist als eine Applikation im IP-Netz. Diese Applikation hinsichtlich der damit verbundenen Verkehrsströme anders zu behandeln als andere, ebenfalls geschäftskritische und in einigen Fällen sogar noch wichtigere Anwendungen ist langfristig nicht haltbar. Jedes Unternehmen nutzt eine Vielzahl von Applikationen, jede Applikation hat ihre Daseinsberechtigung, sonst würde sie ja nicht genutzt werden. Wo käme man denn hin, wenn man für jede Applikation ein separates logisches Netz fordern würde?

Dass die immer noch in vielen Fällen praktizierte VLAN-Trennung am Arbeitsplatz nicht mehr technisch begründet ist, sieht man am besten daran, dass in den allermeisten Fällen im Layer-2-Bereich zwar eine logische Netztrennung zwischen Voice und Data realisiert wird, gleichzeitig jedoch diese Trennung an der ersten Layer-3-Instanz aufhört. Mühsam getrennte VLANs für Sprache und Daten werden in über 90 % der Fälle auf der Ebene von Schicht 3 miteinander verbunden, ohne dass irgendein Sicherheitsmechanismus die Kommunikation zwischen diesen VLANs einschränken würde.

Dabei wäre nur jene VLAN-Trennung konsequent, die sich auf der Ebene der Schicht 3 fortsetzen würde. Die getrennten logischen Netze müssen logischerweise auch auf der Ebene der Schicht 3 getrennt gehalten werden. Die Verfahren dazu sind Multi-Protocol Label Switching (MPS) oder Virtual Routing and Forwarding (VRF). Jedes Voice-VLAN muss demnach mit einer logischen Routing-Instanz verbunden werden, die einem MPLS-VPN oder einer VRF-Instanz für Voice zugeordnet ist, während die Daten-VLANs an das entsprechende MPLS-VPN bzw. VRF-Instanz für Daten angeschlossen werden.

Dass dadurch die Komplexität der Netzstruktur steigt, steht außer Frage. Aber die Komplexität steigt schon mit der Einführung von getrennten VLANs am Arbeitsplatz. Die Trennung auf Layer 3 ist nur die logische Konsequenz der Netztrennung auf Layer 2.

Problematischer als die erhöhte Komplexität dürfte die immer noch fehlende Unterstützung von MPLS bzw. VRF durch die meisten Hersteller von LAN-Switches sein. Zwar ist MPLS- und VRF-Unterstützung bei WAN-Routern mittlerweile Standard, aber das lässt sich für LAN-Switches nicht sagen. Die meisten Layer-3-Switches unterstützen keine logische Trennung von Routing-Instanzen auf der Basis der selben Hardware. Nicht zuletzt deshalb belässt man es in den allermeisten Fällen bei getrennten VLANs für Voice und Daten, die an Layer-3-Switches verbunden werden.

In letzter Zeit ist in die Diskussion über VLAN-Trennung am Arbeitsplatz Bewegung gekommen, besonders seitdem neue Anbieter den Markt der Sprachkommunikation adressieren. Man nehme zum Beispiel Microsoft mit ihrem Office Communications Server (OCS). Der OCS ist die IP-basierende Kommunikationslösung von Microsoft, die bei den Clients keinen Unterschied mehr macht zwischen PC-basierenden und anderen Endgeräten. Der zu bevorzugende Client ist sogar der PC mit dem Microsoft Office Communicator. Die ersten funktionierenden OCS-Umgebungen sehen den Einsatz von PC-basierenden Clients vor. Dass Microsoft mit dieser Lösung Marktanteile bei der Sprachkommunikation gewinnen will, steht außer Frage. Dass solche Lösungen keinen Raum mehr für die Zuordnung der Applikation Voice zu einem eigenen VLAN mehr lassen, kann ebenso wenig bezweifelt werden. Die Microsoft-Strategie gibt dem Einsatz von Softphones neuen Auftrieb, nachdem jahrelang weder die traditionellen Hersteller von TK-Lösungen noch die neuen Anbieter wie Cisco ein wirkliches Interesse an der Vermarktung von Softphones gezeigt haben. Dieses Desinteresse ist an der mangelhaften Qualität vieler Softphone-Implementierungen erkennbar. Teilweise sind die Funktionsdefizite von Softphones durch keinerlei technischen Zwang zu erklären. Warum unterstützen zum Beispiel viele Softphones keine Verschlüsselung, wenn es einen verhältnismäßig kleinen Aufwand bedeuten würde, die Softphones mit Funktionen in diesem Bereich zu erweitern? Es liegt der Verdacht nahe, dass viele Hersteller kein Interesse an der breiten Vermarktung von Softphones haben, weil sich mit Hardphones einfacher Geld verdienen lässt.

Jetzt ändert sich jedoch die Situation. Einerseits kommen Benutzer in das Berufsleben, die seit ihren sehr jungen Jahren den PC für sämtliche Kommunikationszwecke, auch für die Sprachübertragung, genutzt haben. Von diesem Anwenderkreis kommen weniger Bedenken gegen ein Telefon, das täglich erst einmal minutenlang booten muss. Andererseits betritt mit Microsoft ein Anbieter den Markt, für den das eigene Softphone der eigentliche strategische Client ist. Ein Softphone ist eine Applikationen neben anderen auf dem PC. Das Softphone ist der Tod der VLAN-Trennung am Arbeitsplatz.

Fazit

Dass der Versuch zum Erreichen der Kommunikationssicherheit mit VLAN-Trennung am Arbeitsplatz ein Irrweg ist, wurde in diesem Beitrag damit begründet, dass diese Praxis einerseits die Netzbetreiber vor kaum lösbare Probleme stellt und andererseits angesichts der fehlenden Bausteine, die insgesamt für die Sicherheit auf der Ebene der Schicht 2 sorgen würden, praktisch keine Sicherheit bringt. Angesichts der verfügbaren Lösungen für Ende-zu-Ende-Verschlüsselung ist nämlich dieser Ansatz der zu bevorzugende Weg der Kommunikationssicherheit.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Trouble Shooting für Netzwerk-Anwendungen, 01.04. - 04.04.08 in Aachen

Sicherheitskonzepte müssen mehr sein als Papier. Ihre erfolgreiche Umsetzung erfordert: eine umsichtige Planung und Beschaffung der Sicherheitsinfrastruktur, eine effektive Integration in Prozesse und Organisation, konzeptkonforme Einbindung externer Leistungen (Lieferung, Implementierung, Wartung und Betriebsleistungen). Bei der notwendigen Erfolgskontrolle helfen Standards wie BS7799, ISO 27001 und die IT-Grundschutz-Standards und -Kataloge des BSI. Eine entsprechende Zertifizierung des erreichten Sicherheitsniveaus ist möglich, aber auch eine Verwendung solcher Standards als internes Hilfsmittel. Preis: € 2.190,- zzgl. MwSt.

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs, 07.04. - 11.04.08 in Aachen

Dieses einmalige Seminar vermittelt intensiv innerhalb von 5 Tagen den praktischen Umgang mit Firewalls, VPNs, Windows-Sicherheit und WLAN-Sicherheit. Im Rahmen von praktischen Live-Übungen werden typische Konfigurationen analysiert und vermittelt. Als Übungsbasis stehen typische Produkte des Marktes zur Verfügung, die vermittelten Konfigurationen sind aber nicht produktspezifisch sondern auf jedes ähnliche Produkt direkt übertragbar. Die Teilnehmer werden so in die Lage versetzt, dieses Wissen direkt nach dem Seminar aktiv in der Praxis einzusetzen. Preis: € 2.290,- zzgl. MwSt.

Office Communications Server 2007, 08.04. - 09.04.08 in Köln 21.04.-22.04.08 in Frankfurt

In diesem Seminar werden sowohl die technischen als auch die strategischen Aspekte des Office Communications Servers analysiert. Unsere herstellerunabhängigen und neutralen Experten haben sich sehr ausführlich mit den technischen Details befasst und verfügen über langjährige Erfahrung bei der Implementierung von Microsoft-Lösungen, bei der Konzeption von TK-Lösungen sowie bei der Bewertung von Kommunikationstechnologien. Preis: € 1.390,- zzgl. MwSt.

Elektrische Störungen in Datennetzen und Computerinstallationen erfolgreich erkennen und beseitigen, 10.04. - 11.04.08 in Bonn

Sie erfahren in diesem 2-tägigen Seminar, welche typischen Ursachen den in den letzten Jahren festgestellten Störungen und Schäden in Netzwerken und DV-Installationen zu Grunde liegen, wie gefährlich diese Störungen sind und wie sie messtechnisch erkannt und beseitigt werden können. Preis: € 1.390,- zzgl. MwSt.

Netzwerk-Redesign Forum 2008, 10.04. - 11.04.08 in Bonn

Das Netzwerk-Redesign Forum, unser Top-Kongress des Jahres 2008, analysiert die aktuellsten Entwicklungen der Netzwerk-Technologien und bewertet Markttrends und Produktentwicklungen. Netzwerke werden immer stärker integraler Teil von Applikations-Architekturen. Zum Teil sind sie auf Infrastruktur-Aufgaben reduzierbar, aber immer mehr werden sie selber Teil der Lösung.

Preis: € 2.190,- zzgl. MwSt.

SIP- und Unified Communication Forum 2008, 21.04. - 22.04.08 in Frankfurt a.M.

Wenige Standards in der Geschichte der TK, der Netzwerke und der IT werden unsere Branche so verändern wie das Session Initiation Protocol SIP. Der Wechsel von Cisco und Siemens zu SIP mit dem CallManager 6 und der HiPath 8000 unterstreichen das genauso wie der Einstieg von Microsoft zusammen mit Nortel in diesen Markt. SIP ist ohne Frage ein Megathema. Nach wie vor wird dabei insbesondere der Leistungsumfang von SIP weit unterschätzt. Auch so verbreitete Implementierungen wie Asterisk oder SER werden in ihrer Nutzbarkeit häufig falsch eingeschätzt. Das SIP-Forum 2008 analysiert für Sie wo SIP steht, was es leistet und wie Sie am besten von der bestehenden Marktsituation profitieren. Preis: € 1.590,- zzgl. MwSt.

EMV-gerechte Planung der Elektroinstallation für Rechnerräume und Rechenzentren, 24.04. - 25.04.08 in Bonn

Dieses Seminar zeigt, wie eine EMV-gerechte, hochverfügbare und störungsarme Elektroinstallation mit gleichzeitig hoher Betriebssicherheit geschaffen werden kann. Es vermittelt mit engem Bezug zur Praxis wie ausgehend von Analyse und Messtechnik bestehende Mängel beseitigt werden und ein wartungsoptimierter Betrieb aufgebaut wird. Preis: € 1.390,- zzgl. MwSt.

SIP (Session Initiation Protocol)- Basis-Technologie der IP-Telefonie, 05.05. - 07.05.08 in Bonn

Dieses 3-tägige Seminar vermittelt Planern und Betreibern Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des neuen Standards SIP. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert. Preis: € 1.690,- zzgl. MwSt.

Sicherheitsmechanismen für Voice over IP, 05.05. - 06.05.08 in Bonn

Angesichts der Offenheit und geringeren Verfügbarkeit von Datennetzen ist das Thema Sicherheit das zentrale Projektthema bei der Umsetzung von Voice over IP. VoIP benötigt Sicherheitsmechanismen, die mindestens ein den konventionellen Telekommunikationsnetzen entsprechendes Niveau an Vertraulichkeit, Verlässlichkeit, Verfügbarkeit und Integrität sicherstellen. Darüber hinaus bietet die Umstellung die Chance, die Sicherheit der Sprachkommunikation über das bisherige Niveau hinaus zu verbessern.

Preis: € 1.390,- zzgl. MwSt.

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
09.06. - 13.06.08 in Aachen
15.09. - 19.09.08 in Aachen
24.11. - 28.11.08 in Aachen

TCP/IP und SNMP
26.05. - 30.05.08 in Aachen
20.10. - 24.10.08 in Berlin

Internetworking
10.03. - 14.03.08 in Aachen
23.06. - 27.06.08 in Bonn
13.10. - 17.10.08 in Aachen

Paketpreis für alle drei Seminare € 6.183,-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

ComConsult Certified Trouble Shooter

Trouble Shooting 1
17.06. - 20.06.08 in Aachen
09.09. - 12.09.08 in Aachen

Trouble Shooting 2
01.04. - 04.04.08 in Aachen
24.06. - 27.06.08 in Aachen
14.10. - 17.10.08 in Aachen

Paketpreis für beide Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 3.940.-- zzgl. MwSt. (Einzelpreise: je € 2.190.--)

ComConsult Certified Security Expert

Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit
05.05. - 09.05.08 in Bonn
22.09. - 26.09.08 in Bonn

Sicherheit 2: Erarbeitung und Umsetzung von Sicherheitskonzepten
10.03. - 14.03.08 in Frankfurt
23.06. - 27.06.08 in Bonn
03.11. - 07.11.08 in Bonn

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs
07.04. - 11.04.08 in Aachen
25.08. - 29.08.08 in Aachen
01.12. - 05.12.08 in Aachen

Paketpreis für alle drei Seminare und die beiden Reports „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ und „Sicherheit in Wireless LANs“. € 6.183.-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

ComConsult Certified Voice Engineer

Basis-Seminar: Session Initiation Protocol-Basis-Technologie der IP-Telefonie
05.05. - 07.05.08 in Bonn
15.09. - 17.09.08 in Frankfurt
17.11. - 19.11.08 in Frankfurt

Basis-Seminar: Sicherheitsmechanismen für Voice over IP
05.05. - 06.05.08 in Bonn
03.11. - 04.11.08 in Bonn

Alternative 1: IP-Telefonie evaluieren, planen, betreiben
04.06. - 06.06.08 in Königswinter
01.09. - 03.09.08 in Stuttgart
27.10. - 29.10.08 in Bonn

Alternative 2: IP-Telefonie: Vorbereitung, Migration, Management
10.03. - 12.03.08 in Frankfurt
02.06. - 04.06.08 in Stuttgart
13.10. - 15.10.08 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
10.06. - 11.06.08 in Bonn
08.09. - 09.09.08 in Bonn
17.11. - 18.11.08 in Frankfurt

Basis-Paket Alternative 1: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 1“ Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Basis-Paket Alternative 2: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 2“ Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 990,-- zzgl. MwSt. statt € 1.390,-- zzgl. MwSt.

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd. - RD1 - Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 3234415
German Hotline of ComConsult-Research:
02408-955300

E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie