Dr. Suppan International Institute

Der Netzwerk Insider

Oktober 2003

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Sicherheit in Wireless LANs – neuester Stand

von Dipl.-Math. Cornelius Höchel-Winter

Im Mai hat die Wi-Fi Alliance ihren Sicherheitsstandard WPA veröffentlicht und im August hat die IEEE ihre Sicherheitsergänzung 802.11i zum WLAN-Standard in der Draft-Version 5.0 verabschiedet. Grund genug den aktuellen Stand zu diesem Thema einmal genauer zu betrachten.

Die Buchstabensuppe der WLAN-Standards

Das ursprüngliche Dokument 802.11 von 1999 definiert das grundlegende Konzept für Wireless LANs, einen gemeinsamen MAC-Layer für das Layer-2-Protokoll und drei physikalische Schnittstellen: zwei Funkschnittstellen mit FHSS und DSSS und eine Infrarotschnittstelle, für die es jedoch nie relevante Realisierungen gab. Beide Funkdevices arbeiten im 2,4-GHz-Band mit Übertragungsraten von 1 und 2 Mbit/s.

Noch nicht ganz gar: WLAN-Standard-Buchstabensuppe

Bereits im selben Jahr wurde mit 802.11a eine dritte Funkschnittstelle im 5-GHz-Band mit Übertragungsraten bis 54 Mbit/s definiert. Aufgrund technischer Probleme bei der Realisierung ließen hierauf basierende Produkte jedoch recht lange auf sich warten, erst Ende 2001 wurden erste Access Points und Netzwerkkarten vorgestellt, mittlerweile ist die zweite und dritte Chipgeneration am Start und nahezu jeder WLAN-Anbieter hat auch 11a-Produkte im Angebot.

Wesentlich früher am Markt und damit auch erfolgreicher waren jedoch 11b-Produkte. 802.11b – ebenfalls 1999 verabschiedet – definiert für das bereits vorhandene DSSS-Interface weitere Modulationsverfahren und erweitert damit aufwärtskompatibel die verfügbaren Übertragungsraten auf bis zu 11 Mbit/s.

weiter Seite 15

Zweitthema

TCP/IP unter Windows konfigurieren – Optimieren statt sich ärgern

von Dipl.-Inform. Oliver Flüs

Eigentlich ist ja alles ganz einfach, wenn man einen Rechner dazu bringen will, über TCP/IP-Protokolle Netzwerk-Verbindungen aufzubauen.

Man trägt eine IP-Adresse ein, eine Subnetzmaske, ein default gateway – ach ja, und noch DNS- und WINS-Server, damit auch Namen benutzt werden können.

Das kann schließlich jeder, und schon kann es losgehen. Im Prinzip ja – und doch, es kann ärgerlich ausgehen, wenn man nicht wirklich Bescheid weiß, was man da tut.

weiter Seite 5

Top-Event

Winterschule der ComConsult Akademie 2003

auf Seite 4

Zum Geleit

Wireless LAN: Technologie im Brennpunkt

auf Seite 2

Studie des Monats

Wireless LAN Sicherheit Report: Distribution System als VPN

auf Seite 12

Zum Geleit

Wireless LAN: Technologie im Brennpunkt

Wireless LANs (WLANs) haben sich für viele Unternehmen zu einer Schlüsseltechnologie entwickelt.

Hintergrund sind die immensen Vorteile, die diese Technologie bietet:

- Umsetzung neuer Geschäftsmodelle
- Verbesserung bestehender Betriebsabläufe
- Schaffung mobiler Arbeitsplätze
- Senkung der Client- und Netzwerk-Betriebskosten
- Kontrollierte Einbindung der stark zunehmenden Zahl von Notebooks
- Senkung der Investitionskosten bei Neu-Vernetzungen durch Overlay-Netze

Bedingt durch die Vielfalt der möglichen Vorteile unterscheiden sich die Einsatzszenarien von WLANs erheblich und stellen verschiedene Anforderungen an die Lösung (typische Unterschiede in der Auslegung: Durchsatz pro Client, Sicherheit, Abrechnung, funktechnische Elemente).

Typische Szenarien sind unter anderem:

- Einfache Punktlösung (Konferenzräume o.ä.)
- Partielle Flächendeckung ergänzend zum bestehenden Kabelgebundenen Netzwerk
- Wireless-Overlay-Netzwerke mit Kostenoptimierten Mix von Kabel und Funk zur Senkung von Investitions- und Change-Kosten
- Kompletter Ersatz Kabelgebundener Kommunikation
- Hot Spots mit Abrechnungs- und Geschäftsfunktionalität

Während sich die Zahl erfolgreicher Einsatzszenarien kontinuierlich erweitert ist gleichzeitig die WLAN-Technologie selber im Wandel. Die bisher dominante IEEE 802.11b-Technik, wird angesichts ihrer Einschränkungen immer mehr aus professionellen Projekten verdrängt. Leider ist dabei durchaus unklar, welche der in Frage kommenden Technologien die Nachfolge antreten wird. Dabei stehen nicht nur IEEE 802.11a und 802.11g im Wettbewerb, auch Themen wie VLAN-Integration, QoS, Telephonie over WLAN, Sicherheit, 11h und 11n sowie die immer mehr zunehmenden nicht genormten Varianten einzelner Hersteller prägen die Bandbreite der Diskussion.

Dies hat mehrere Ursachen:

- Zur Zeit kann die Entscheidung zwischen 802.11g und 802.11a nicht wirklich erfolgen. Die durch die RegTP gesetzten Rahmenbedingungen machen einen Einsatz der zur Zeit verfügbaren 802.11a-Technik mehr als fragwürdig. Doch die neue Technik, die dann auch Sendestärken von 200 mW zulassen wird, steht vor der Tür.

- Jede aktuelle Lösung wird massiv durch die dabei zu wählende Sicherheits-Lösung beeinflusst. In den Projekten zeigt sich dabei immer mehr, dass hier komplexe Situationen entstehen können, wenn mehrere Sicherheitslösungen gleichzeitig zum Einsatz kommen. So wird trotz WPA immer ein Teil der vorhandenen Notebooks den Weg über ein VPN nehmen, zum Beispiel dann, wenn das Notebook unabhängig von Wireless auf diesen Weg konfiguriert wurde, um einen mobilen Einsatz außerhalb des Unternehmens zu ermöglichen

- Layer-3-Mobility, also die Fähigkeit der freien Nutzung eines WLAN-Clients (Notebook, PDA, Transportsystem usw) im gesamten Unternehmen über alle Layer-3-Zonen hinweg ist in fast allen Projekten ebenso ein Thema wie komplex in der Umsetzung. Eine Standard-Lösung gibt es bisher nicht, einige Hersteller bieten individuelle Lösungen, nicht alle können aber deren Nutzbarkeit nachweisen

- Für die neuen Technologien kann eine Interoperabilität von Produkten noch nicht im gleichen Umfang wie für 802.11b garantiert werden. Im Gegenteil, eine Reihe von Herstellern scheinen WLAN-Technologien für eine Spielwiese zu halten und bieten hemmungslos Produkte an, die keiner Norm entsprechen und mit Datenraten von 22 und 108 Mbit/s durchaus Fragen zur Interoperabilität offen lassen. Auf jeden Fall muss berücksichtigt werden, dass durch die Notebooks mit integrierten Wireless-Adaptern ein dringender Bedarf nach einer sicheren Interoperabilität entsteht. Auch die von Intel und CISCO ins Leben gerufene Centrino-Zertifizierung kann nur massiv kritisiert werden. Hier unterlaufen Hersteller absichtlich die bewährten Mechanismen der WiFi-Alliance und schaffen damit eine nicht akzeptable Unsicherheit im Markt.

Dabei hat das Einsatzszenario erhebliche Auswirkungen auf die Auswahl der Technik, die zu wählende Architektur und die Betriebssystematik. Aus diesem Grund gibt es zur Zeit erhebliche Diskussionen über folgende Themen:

- Wie sieht der „richtige“ Planungsansatz für ein WLAN aus? Coverage kontra Capacity kontra Security lauten die Schlagworte

- Wie erfolgt die Anbindung an das bestehende Kabelbasierende Netzwerk, benötigen WLANs eine separate Netzwerk-Infrastruktur? Werden Access Points dezentral jeweils an den nächsten verfügbaren Netzwerk-Zugang angebunden oder wird ein kontrollierter zentraler Zugang geschaffen?

- Wie kann Layer-3-Mobility wirklich erreicht werden? Mit welchen Konzepten kann Roaming umgesetzt werden? Welche davon sind wirklich tauglich für einen Alltags-Betrieb?

- Welche Sicherheits-Lösung ist für welchen Einsatzbereich geeignet? Ist die von einigen Herstellern favorisierte Autorisierungs-Infrastruktur zu komplex für einen effizienten Betrieb, reicht ggf. eine einfache WPA-Lösung aus? Wie können gemischte Szenarien realisiert werden?

- Was muss getan werden, damit WLANs in sensiblen Umgebungen wie Kliniken, Personalabteilungen und Vorstandsbereichen eingesetzt werden können?

- Wie kann für große flächendeckende Lösungen das Betriebsproblem für Hunderte von Access Points gelöst werden? Sind Wireless Switches die Technologie der Zukunft für den professionellen Einsatz?

Wireless LAN: Technologie im Brennpunkt

- Wie sieht das optimale Produkt für den jeweiligen Einsatzzweck aus? Unterscheiden sich Produkte überhaupt noch? Worin liegen die Preisunterschiede begründet?
- Welche Funktechnologie wird in einem professionellen Einsatz benötigt? Sind Spezialantennen mit Richt- und Verstärkungswirkung sinnvoll, rechtfertigen sie ihren erheblichen Mehrpreis?
- Wie kann Interoperabilität sicher gestellt werden? Soll man eigene Tests durchführen, wenn ja, wie sehen die aus? Welchem Gremium soll man vertrauen, bleibt WiFi das dominanten Gremium zur Sicherstellung von Interoperabilität oder schaffen es Hersteller wie Intel und CISCO proprietäre Konformität durchzusetzen? Was heisst das ganz praktisch für den täglichen WLAN-Einsatz, wo bei jedem neu gekauften Notebook die Frage der Interoperabilität zur bestehenden Infrastruktur entsteht?

Diese Fragen greift unser Wireless-LAN-Forum 2003 auf, das vom 17. bis 19. November in Königswinter stattfindet. Ich würde mich sehr freuen, Sie hier begrüßen zu können. Heiße und spannende Diskussionen erwarten Sie zusammen mit einem idealen und kompakten Überblick über diese immer noch stark in Bewegung befindliche Technologie.

Bis dahin
Ihr Dr. Jürgen Suppan

Aktueller Kongress

Wireless LAN Forum 2003

Vom 17. bis 19. November veranstaltet die ComConsult Akademie im Maritim Hotel in Königswinter das Wireless LAN Forum 2003.

In einer attraktiven Mischung aus Fachvorträgen, Erfahrungsberichten, Laboranalysen und in Kombination mit einer Ausstellung und in Anwesenheit führender Hersteller bietet es die ideale Umgebung, alle anstehenden Fragen zur Wireless-Technik zu diskutieren und wichtige Hinweise für das eigene Projekt zu sammeln.

1. Tag: Wireless-Technologien in der Analyse: was sie leisten, wo die Grenzen liegen, wie sie sich weiter entwickeln werden
- WLAN: Motivation, Bedarf, Wirtschaftlichkeit, Einsatzszenarien und ihre Bewertung
- Die WLAN-Basis-Technologie in der Analyse wie arbeitet an WLAN, wo sind Schwachstellen, wo liegen die Stärken
- Wie entsteht eine erfolgreiche WLAN-Lösung unter diesen Rahmenbedingungen
- Sicherheit im WLAN: wo sind die Lücken, welche Alternativen bestehen zur Umsetzung von Sicherheit, wo hoch ist der Aufwand

2. Tag: Planung, Betrieb, Trouble Shooting: WLANs in der Realität des Alltags
- Architektur-Varianten im Vergleich
- Planungsmethoden: Capacity kontra Coverage kontra Security: welcher Ansatz ist für wen geeignet
- Störungen und Instabilitäten: Maßnahmen zur Vermeidung, von der theoretischen Flächen-Analyse zur praktischen Umsetzung
- Antennen-Auswahl und Installation: Ergebnisse einer Studie von ComConsult Research
- Abnahme und Trouble-Shooting: alternative Ansätze und Praktikabilität
- Spezialanwendungen und Sonderkonfigurationen: VLAN-Konfiguration, QoS, IP-Telephonie im WLAN
- Wireless Netzwerke im Produktionsumfeld: werden die harten Anforderungen der Industrie erfüllt?

3. Tag: Marktsituation: welche Produkte gibt es, was leisten sie, wer braucht welches Produkt
- Produktvarianten und ihre Leistung, Labor- und Praxisergebnisse
- Wireless Switches kontra Access Point: Produktanforderungen zum Betrieb großer WLAN-Installationen und Projekterfahrungen
- Einsatzerfahrungen mit WLAN-Produkten
- Produktpräsentationen ausgewählter Hersteller

Fax-Antwort an ComConsult 02408/955-399

Kongress-Anmeldung

☐ Ich melde mich an zum
Wireless LAN Forum 2003
vom 17.11. - 19.11.03 in Königswinter
(Preis: € 1.690,-- zzgl. MwSt.)

☐ Buchen Sie für mich ein Hotelzimmer

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

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

Winterschule der ComConsult Akademie

Winterschule 2003: IP-Telefonie-Intensiv-Evaluierung

Vom 1. bis 5. Dezember veranstaltet die ComConsult Akademie im Technologiezentrum der AGIT Aachen ihre diesjährige Winterschule mit dem Schwerpunkt "IP-Telefonie".

IP-Telefonie ergänzt oder verdrängt klassische TK-Lösungen. Auch in den traditionellen TK-Anlagen wird die hybride Integration von IP-Telefonie von den Herstellern immer mehr als Instrument eines kontrollierten Wechsels in Richtung IP positioniert. Einzelne Funktionsnachteile können durch Konfiguration oder Zusatztools ausgeglichen werden. Für den Endanwender stellt sich damit nicht mehr die Frage nach dem ob sondern nach wann und wie viel.

Die Intensiv-Evaluierung von IP-Telefonie ist der Inhalt dieser Winterschule. Wir halten das Thema für so wichtig, dass wir ihm alle 5 Tage der Winterschule widmen. Wir möchten alle Aspekte einer VoIP-Entscheidung beleuchten und Ihnen auf diese Weise wesentlich langwierigere Projektarbeiten ersparen.

Dabei geht es um die Themen:

- Marktsituation, wo stehen Avaya, Cisco, Nortel und Siemens?
- Ergebnisse der aktuellen Studie von ComConsult Research: Cisco contra Siemens – wer hat die bessere TK-Lösung?
- Was bringen die neuen Präsenz-Telefonie-Lösungen am Beispiel Siemens, welche Rolle spielt Microsoft?
- Produktauswahl
- ROI Überlegungen
- Notwendige Netzwerk-Architektur

- IP Basiskonfiguration: DNS/DHCP/NAT geeignet nutzen
- Betrieb und Trouble Shooting
- Handhabung der Sicherheits-Probleme
- Voice over Wireless LAN

Mit unserer Winterschule 2003 wenden wir uns gezielt an die erfahrenen Netzwerker. Wir zeigen auf, wo der Netzwerk-Markt steht und wo er hingeht. Wir diskutieren die aktuellsten technischen Entwicklungen, Sie erfahren, welche Vorteile die neuesten Technologien für Ihr Unternehmen bieten.

5 Tage lang haben Sie die einmalige Möglichkeit, sich von ausgewählten Experten über den neuesten Stand der Technik informieren zu lassen.

Die Moderation der Winterschule hat Petra Borowka von der UBN, sie wird tatkräftig unterstützt von der ComConsult Firmengruppe. Alle Referenten kommen aus der Praxis, bewerten die aktuellsten Technologien aus dem Blickwinkel eines erfolgreichen und sicheren Netzwerk-Betriebs.

Die Winterschule 2003 der ComConsult Akademie bringt Ihnen die 5-Tage-IP-Telefonie-Intensiv-Evaluierung:

- wo steht die IP-Telefonie?
- welche Vorteile entstehen wann und für wen?
- welche Erfahrungen wurden in den bisherigen Projekten gemacht?
- was leistet die aktuelle Standardisierung? Ist das Ende der Hersteller-spezifischen Lösungen nahe?
- was bieten die großen Hersteller? Wie sind die aktuellen Produktlinien zu bewerten? Wer hat die Nase vorne?
- wie entwickeln sich Preise und Leistungen, sind weitere dramatische Preisveränderungen zu erwarten?
- was ist beim Betrieb einer IP-Telefonie-Lösung zu beachten?
- macht ein traditionelles Corporate Netzwerk noch Sinn?

Die Winterschule 2003 beleuchtet alle Vorteile, die eine IP-Telefonie-Lösung bringen kann:

- geringere Investitionskosten
- geringere Betriebskosten inkl. Gebühren und Arbeitsaufwand
- wesentlich vereinfachter Betrieb
- wesentlich flexiblere TK Architektur bei verteilten Lösungen
- geringerer Aufwand zur Umsetzung von ACD und UM in kleinen Umgebungen
- Nutzung neuer Kommunikations-Funktionen

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Winterschule

☐ Ich melde mich an zum
Winterschule der ComConsult Akademie 2003: IP-Telefonie-Intensiv-Evaluierung
vom 01.12. - 05.12.03 in Aachen
(Preis: € 2.290,-- zzgl. MwSt.)

☐ Buchen Sie für mich ein Hotelzimmer

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

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

Zweitthema Oktober 2003

TCP/IP unter Windows konfigurieren – Optimieren statt sich ärgern

Fortsetzung von Seite 1

Dipl.-Inform. Oliver Flüs verfügt über langjährige Kenntnisse im Betrieb von Lokalen Netzen. Im Team der ComConsult Beratung und Planung GmbH bearbeitet er seit Jahren Projekte in den Bereichen informatikorientierte Beratungsleistungen und Organisationsberatung im IT-Bereich. Zu diesen Themengebieten ist er regelmäßig als Referent bei der ComConsult Akademie tätig.

flues@comconsult.com

- Die ursprünglichen Strategien von TCP und IP sind auf Netze zugeschnitten, wie sie in den 80er Jahren realisiert werden konnten

Sicher, 80er Jahre Revival ist in (oder schon wieder out), aber wer würde heute mit einem Auto aus den 80er Jahren fahren und sich dann wundern, dass er nicht besonders schnell vorwärts kommt?

- Entsprechend gibt es Neuerungen, die dazu dienen sollen, die Kapazitäten neuer Netzwerk-Techniken auch wirklich auszunutzen.

Die Geschwindigkeitsbegrenzung ist aufgehoben, aber man muss auch wirklich in den höheren Gang schalten, um schneller vorwärts zu kommen. Vollgas fahren geht aber nur, solange man auf der gut ausgebauten Teilstrecke unterwegs ist – kommt eine Verengung, so sollte man vom Gas gehen, um nicht abzufliegen.

Genauso ist es mit den Neuerungen unter TCP/IP: Manche davon führen regelrecht zu Problemen, wenn man sie über „langsame" Verbindungen einsetzt, und wehe, es ist eine Firewall dazwischen – dann führt der ein oder andere „Trick" zur Optimierung dazu, dass gar nichts mehr geht!

So ein Blödsinn, mag manch einer jetzt denken: das LAN ist brandneu, hat Bandbreite „ohne Ende" zu bieten und die Netzwerk-Komponenten langweilen sich (noch). Wo sollen da die Engpassprobleme herkommen?

Aber halt: heutzutage ist längst nicht mehr einfach ein fester PC-Arbeitsplatz in einem LAN zu konfigurieren. Heimarbeitsplätze sind „völlig normale" LAN-Erweiterungen, und eine Vielzahl von Endgeräten sind heute schon „mobil", mit zunehmender Tendenz: in einigen Jahren wird der feste Tisch-PC womöglich die Ausnahme sein. Da sind sie wieder, die Kommunikationswege mit den „knappen Bandbreiten", für die „High Speed-Optimierungen" von TCP/IP zur Überforderung werden können: Modem-basierte Einwahllösungen, WLAN-Verbindungen, die in der Praxis noch auf 2 Mbit/s oder (je nach Empfangssituation) weniger beschränkt sind, u.ä.

Hier ist Vorsicht geboten: zwar können alle typischen LAN-Dienste und –Anwendungen genutzt werden. Wer hier jedoch TCP/IP-Mechanismen ausschaltet, die bewusst „erfunden" wurden, kann erleben, warum diese erfunden wurden: wer zu schnell spricht, überfordert die Verbindung, muss alles zwei- und dreimal wiederholen, bis es endlich angekommen ist – das kann bei beschränkten Ressourcen nicht gerade zu einer kurzen Gesprächsdauer führen.

TCP/IP unter Windows konfigurieren – Optimieren statt sich ärgern

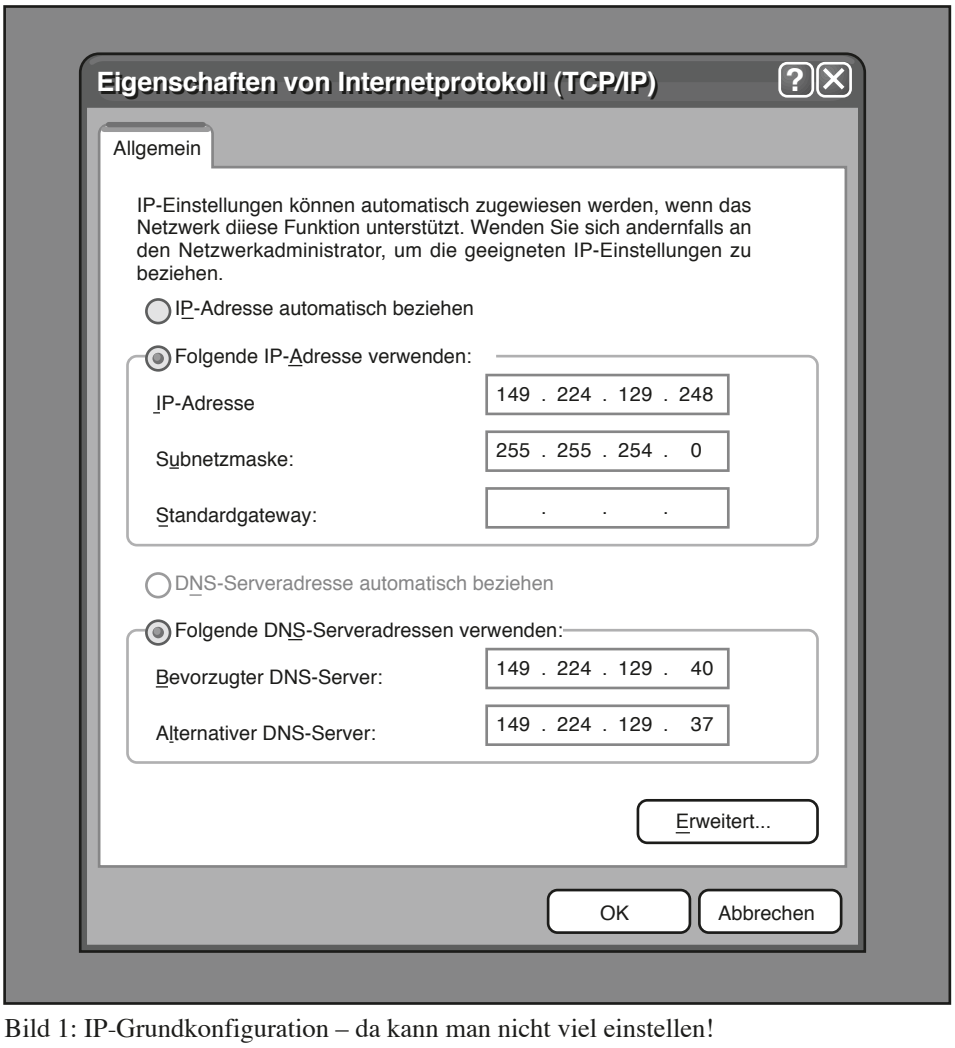


Bild 1: IP-Grundkonfiguration – da kann man nicht viel einstellen!

Im Klartext:

- In schnellen LANs tut man gut daran sicherzustellen, dass alle Optimierungen auch eingeschaltet sind – dies ist bei älteren Windows-Versionen nicht zwingend der Fall. Nur wenn auch alles eingeschaltet ist, was gezielt für „High Speed-Netze“ konzipiert wurde, kann man das moderne Leistungsangebot auch wirklich nutzen.

Andernfalls droht die dümmlichste aller Situationen: mit großem Aufwand wird eine neue Netzwerk-Technik eingeführt – und keiner der Anwender merkt einen echten Unterschied.

- Über remote- oder drahtlose Verbindungen mit beschränkter Performance sollte man bei auftretenden Anzeichen der Überforderung gezielt bestimmte der Neuerungen wieder „herunterregeln“ oder ausschalten – gerade bei Windows-Versionen ab Windows 2000 bedeutet dies, in defaults einzugreifen.

Aber welche Mechanismen sollte man nun gezielt ab- oder einschalten, und vor allem: wie findet man einen guten Kompromiss bei Rechnern, die mal im LAN, mal „remote“ genutzt werden? Und wo nimmt man diese Änderungen vor? Die Einstellmöglichkeiten, die die meisten kennen, beschränken sich auf die „setup-Karte“, die man als „Eigenschaften“ von „TCP/IP“-Protokoll editieren kann (siehe Bild 1).

Außerdem: da war doch eben die Rede von Neuerungen, die an Firewalls „hängen bleiben“ können? Jawohl, so etwas gibt es, wenn auch leicht beherrschbar, wenn man „sich auskennt“.

TCP/IP unter Windows konfigurieren – Optimieren statt sich ärgern

Offenbar ist es doch nicht damit getan, ein paar Grundkonfigurationen vorzunehmen und loszulegen. Ganz im Gegenteil: die wirklich spannenden Prüf- und Einstellmöglichkeiten sind nicht in irgendwelchen hübschen Setup-Karten gegeben, sondern in Form von Registry Keys (siehe Bild 2).

Spätestens jetzt werden viele aufhorchen: einfach in der Registry herumändern, kann sehr gefährlich sein und sogar den Rechner lahm legen. Microsoft selbst erläutert zwar die fraglichen registry keys, warnt aber in jedem solchen TechNet- oder Knowledge Base-Text vor allzu leichtfertigem Umgang mit der Registry.

Microsoft Standard-Warnung vor Registry-Änderungen

„Warnung: Dieser Artikel enthält Informationen zum Bearbeiten der Registrierung. Erstellen Sie eine Sicherungskopie der Dateien System.dat und User.dat (unter Windows Millennium ebenfalls der Datei Classes.dat), bevor Sie die Registrierung bearbeiten. Vergewissern Sie sich, dass Sie die Re-gistrierung wiederherstellen können, falls ein Problem auftritt. Informationen hierzu finden Sie in der integrierten Hilfe der Registrierungseditoren "Regedit.exe" oder "Regedt32.exe". Suchen Sie hier im Index nach "Wiederherstellen der Registrierung" oder nach "Wiederherstellen eines Registrierungsschlüssels". Wenn Sie mit Windows NT oder Windows 2000 arbeiten, sollten Sie zudem Ihre Notfalldiskette (Emergency Recovery Disk - ERD) aktualisieren.“

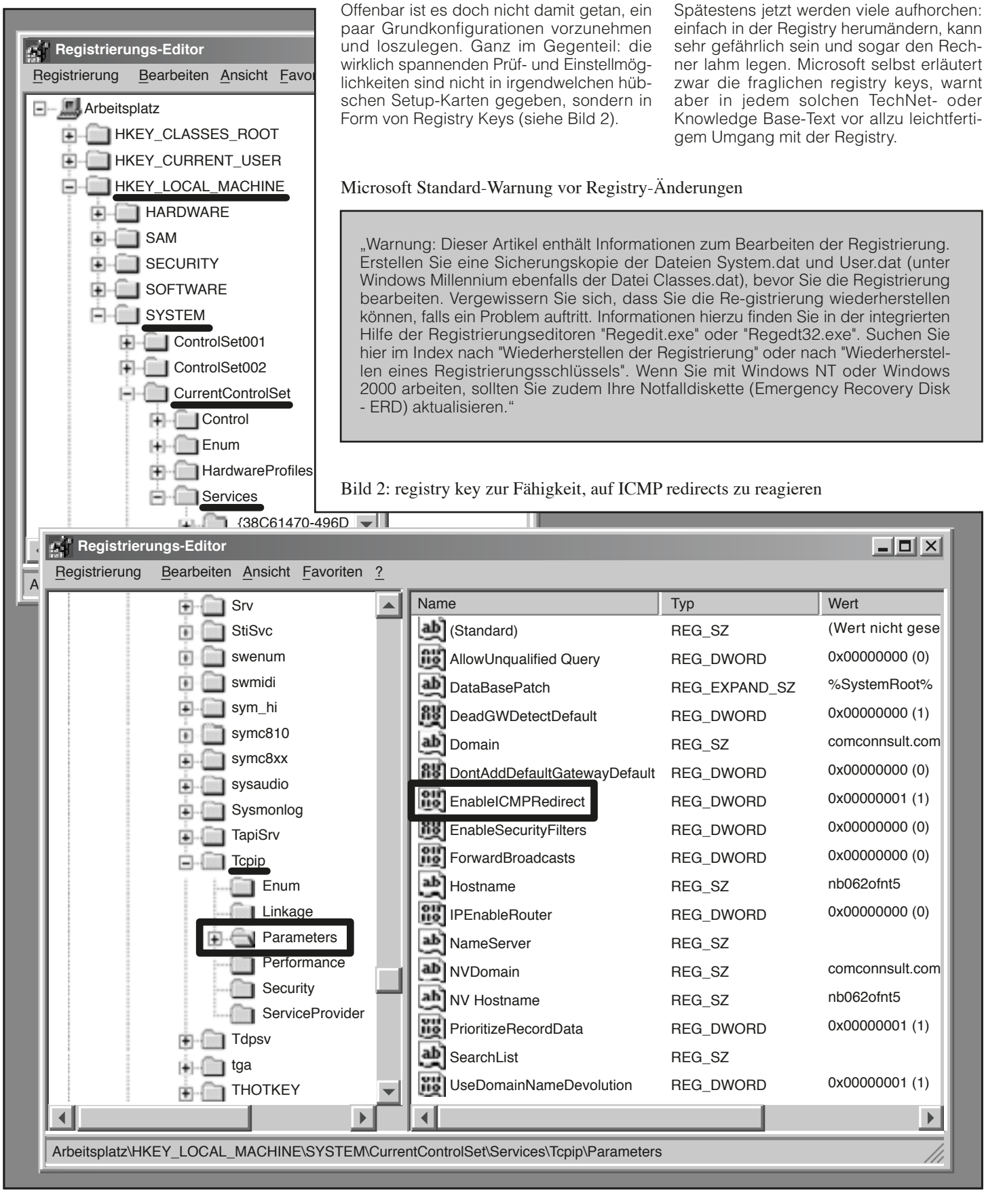


Bild 2: registry key zur Fähigkeit, auf ICMP redirects zu reagieren

TCP/IP unter Windows konfigurieren – Optimieren statt sich ärgern

Dieser nicht gerade einladend klingende Warntext steht z.B. in Knowledge Base Artikel 314053 zum Thema „TCP/IP- und NBT-Konfigurationsparameter für Windows XP“. In englischsprachigen Versionen wird sogar formuliert, das Ändern in der registry erfolge „auf eigene Gefahr“:

> „WARNING: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.” (aus: Microsoft Knowledge Base Artikel 314825).

An Einstellmöglichkeiten mit Einfluss auf die Performance der TCP/IP-Software unter Windows gibt es dabei eine ganze Reihe, wobei man zum Teil zwischen verschiedenen Möglichkeiten abwägen muss.

Beispiel Paketgröße

Wer unnötig kleine Pakete benutzt, belastet die Netzwerk-Komponenten unnötig (eine Transport-Entscheidung je Paket!) und erhöht die Menge der insgesamt zu übertragenden Bytes (mehr Pakete für gleiche Datenmenge bedeutet mehr „Verpackung“ durch Header).

Wer allerdings große Pakete über problematische Übertragungsstrecken schickt, riskiert, häufiger eine größere Datenmenge mehrfach schicken zu müssen (ist ein durch Bitfehler betroffenes Paket groß, so umfasst die „retransmission“ mehr Datenbytes).

Wer mit größeren Paketen startet, als auf dem Transportstück mit kleinster zulässiger Paketgröße („MTU“) funktioniert, erzwingt eine Zerlegung der ursprünglichen Pakete durch einen Router oder Layer 3-Switch („Fragmentierung“) – wieder Mehrarbeit für die Netzwerk-Komponenten, zu Lasten der Übertragungsdauer.

Also: eine der „Tuning“-Aufgaben ist es, für optimale Paketgrößen zu sorgen. Hier gibt es mehrere Einstellmöglichkeiten.

Über den registry key „MTU“ (einstellbar je Netzwerk-Adapter) kann gezielt eine kleinere MTU eingestellt werden, als auf der Netzwerk-Karte des Windows-Rechners, z.B. einer Ethernet-Karte, prinzipiell möglich ist. Damit kann man gezielt die Nachteile einer „Fragmentierung“ vermeiden – wenn man die kleinste MTU entlang des Transportwegs kennt.

Allerdings bremst dies die Performance für Kommunikationswege mit einheitlicher MTU von Sender bis Empfänger, z.B. reine Ethernet-LAN-Strecken. Eleganter wäre eine Methode, mit der für jeden Kommunikationsweg die optimale MTU bestimmt werden könnte. Genau das verbirgt sich hinter der TCP-Neuerung „Path MTU discovery“. Dies ist eigentlich ein alter Hut, spezifiziert in einem RFC 1191 aus 1990, aber erst mit Aufkommen wirklich leistungsfähiger Netze mit typischerweise eher großen MTU-Größen auch durch Lösungen wie Windows-IP-Stacks realisiert.

Path MTU discovery arbeitet mit einem „Trick“: Fragmentierung wird kategorisch vom Sender verboten (dafür gibt es ein Flag im IP-header). Muss nun das ursprüngliche Paket fragmentiert werden, so geht dies nicht – und der zuständige Router sendet dem Erzeuger dieses Pakets eine ICMP-Benachrichtigung. Dieser kann es dann eine Nummer kleiner probieren usw., bis das erste gesendete Paket ohne Router-Protest zum Empfänger gelangt – die optimale MTU für diese Kommunikation ist gefunden. Angenehmerweise ist dieser Lösung bei neueren Windows-Versionen (Windows 2000 und höher) per default eingeschaltet – und genau da liegt in ungünstigen Fällen eine Fußangel: kommt ein „Router-Protest“ nicht zum Sender eines zu großen Pakets durch, so wird dieser weiterhin große Pakete senden und deren Fragmentierung verbieten – es kommt kein Paket zum Empfänger durch, und es kommt keine Verbindung zustande! Genau das passiert aber, wenn zwischen Sender und Empfänger eine Firewall zu durchlaufen ist: diese wird typischerweise ICMP „von außen nach innen“ blockieren, um Ausspähen zu verhindern – und damit prallt die Router-Information über das zu große Paket an der Firewall ab.

Sollte man also Path MTU discovery lieber abschalten, d.h. per default den Microsoft Windows-default überschreiben? Nein, das wäre dumm: es gibt einen proprietären Heilungsmechanismus von Windows. Dieser ist aber aus gutem Grund (auch den sollte man mit Blick auf optimale Performance verstehen!) standardmäßig ausgeschaltet und muss im Fall des Falles gezielt eingeschaltet werden. Außerdem: wer sagt denn, dass alle Rechner über die Firewall kommunizieren und in ein Fragmentierungs-Problem hineinlaufen?

TCP/IP unter Windows konfigurieren – Optimieren statt sich ärgern

Ähnliche Überlegungen und Abwägungen sind anzustellen für eine Vielzahl weiterer Neuerungen gerade im Bereich TCP, dem Haupt-Absicherungsmechanismus für IP-basierte Kommunikation, dem TCP/IP zu einem großen Teil seine Rolle als de facto-Standard in allen modernen Netzen verdankt. Diese werden größtenteils auch unter Windows unterstützt:

Selective Acknowledgement „SACK“

Hier wird versucht, vom Empfänger „gemeldete“ Lücken in der Übertragung durch aufzufüllen, bevor es zu einem Timeout kommt. Hintergrund ist die Tatsache, dass Timeout und Retransmission nach klassischem TCP-Ansatz (slow start recovery / congestion avoidance) zwar für Verlässlichkeit sorgen, aber auch sofort die Senderaktivität brutal beschränken und bei jedem erneuten Timeout die Rückkehr zur alten Sendeleistung stärker erschwert. Die Idee dieses Ansatzes besteht in der Annahme, dass der wahrscheinlichste Grund für einen Timeout ein Engpass sei – eine in modernen Netzen nicht mehr automatisch zutreffende Annahme.

Kann die Abkehr von der alten Grundannahme durch SACK denn aber Nachteile haben? Ja: Retransmissions „vor der Zeit“ bedeuten zusätzliche Sendeaktivität; trifft die Engpass-Annahme zu, so wird die Situation hierdurch sogar noch verschlimmert!

Large Windows

Mit RFC 1323 ist es möglich, das TCP sliding window auf einen Wert deutlich größer als den Windows default von 64 KB zu setzen, nämlich auf bis zu 1 GB. Bleibt man bei 64 KB, so kommt das in aktuellen Ethernet-Netzen einer Autobahn-Fahrt mit angezogener Handbremse gleich. Stellt man aber ohne langes Federlesen die Obergrenze auf das Maximum von 1 GB, so riskiert man etwa, eine Modem- oder bandbreitenschwache WLAN-Verbindung in einen Engpass zu treiben.

Dabei gibt es bei der Einstellung des entsprechenden registry key in der Praxis auch noch eine Stolperfalle: nachdem es diverse Schwierigkeiten gegeben hat, wenn diese Einstellung je Netzwerk-Zugang eines Rechners einzeln (und womöglich unterschiedlich) eingestellt wird, empfiehlt Microsoft zur Zeit eine einheitliche Einstellung als „globalen Parameter“, der für alle Netzwerk-Schnittstellen gilt.

Ähnlich wird man vor echte Entscheidungsfragen gestellt mit der Möglichkeit, die Anzahl der Wiederholungen bei Timeouts zu Beginn einer TCP-Verbindung bzw. bei Versand eines Datenpakets im Laufe einer solchen Verbindung festzulegen.

Auch das Thema redundanter Netzwerk-Strukturen stellt vor neue Herausforderungen. Was ist besser: Nutzung und Verwaltung der Konfiguration mehrerer default gateway-Alternativen für einen Windows-Rechner, die dieser nach Aktivierung von „dead gateway detection“ bei TCP-timeouts der Reihe nach durchprobiert, oder das Arbeiten mit Router-Redundanz-Protokollen wie VRRP auf den Routern bzw. Layer 3-Switches?

Viel Feind – viel Ehr’, aber nur dann, wenn man in den Kampf auch vorbereitet hineingeht: Man muss mehr „drauf haben“, als nur die registry keys zu kennen. Wer gezieltes Tuning betreiben will, muss die grundlegenden Mechanismen verstehen, d.h. denken wie ein Netzwerk-Fachmann – für viele Windows-Administratoren eine neue Herausforderung. Wer damit nicht zurecht kommt, sollte im Zweifel lieber die defaults stehen lassen, und hoffen, dass es keine Probleme (wie etwa mit Path MTU detection möglich) gibt.

Oft müssen dabei gerade für mobile Rechner Kompromisse gefunden werden: sich ängstlich auf die alten Werte zu stützen aus der Zeit, „als die Netze laufen lernten“, schützt zwar vor Problemen über remote-Verbindungen, nimmt aber den neuen LANs deutlich an Wert. Wer andererseits einseitig alles so einstellt/ eingestellt lässt, dass im LAN „Vollgas“ gegeben werden kann, wird häufig mit RAS- oder VPN-Zugriffen Probleme bekommen.

Überhaupt liegen hier die größten Herausforderungen der aktuellen Praxis im Umgang mit IP-Konfigurationen unter Windows:

Wie schafft man eine Windows-Konfiguration, die den beiden Umgebungen „daheim und unterwegs“ (LAN bzw. Homeoffice oder Dial in aus dem Hotel), gerecht wird?

Wie kontrolliert man den Gesamtzustand, wenn es Probleme gibt?

TCP/IP unter Windows konfigurieren – Optimieren statt sich ärgern

Alternative Konfiguration für Büro-LAN und anderswo

Neueste Windows-Versionen wie Windows XP haben die Bedeutung der wechselnden Umgebung erkannt. So bietet Windows XP neben der Standard-Konfiguration über DHCP, die heute weit verbreitete Konfigurationsform im LAN, die Möglichkeit der Festlegung einer alternativen IP-Grundkonfiguration mit festen Einstellungen für IP-Adresse, Subnetzmaske, default gateway usw. (Bild 3)

Aber auch für die etwas älteren Windows-Versionen kann man hier etwas vorbereiten, das einigermaßen komfortabel vom Anwender benutzt werden kann und ein vergleichbares Ergebnis bringt. Man muss sich dabei nur an etwas erinnern, was für manchen direkt mit der Maus groß Gewordenen ins Museum gehört: Skripte / Batch-Dateien. Mit Rückgriff eines DOS-Kommandos, das umfassenden Zugriff auf die IP-Konfiguration eines Windows-Rechners ermöglicht, lassen sich Batch-Dateien schreiben, mit deren Aufruf die IP-Konfiguration durch den Anwender auf die jeweilige Umgebung umgestellt werden kann, ohne dass er selber viel davon verstehen muss (Bild 4).

Wenn man jetzt noch eine geschickte Reihenfolge an den Tag legt (optimal: als letztes vor dem Herunterfahren die Batch-Datei für den nächsten Standort aufrufen), kann man unter Windows 2000 mit der jeweils passenden Konfiguration loslegen. Schlimmstenfalls muss man wie bei Änderung über die Eigenschaften-Karte von TCP/IP neu booten, wenn man per entsprechender Batch-Datei auf DHCP-basierte Konfiguration umgestellt hat.

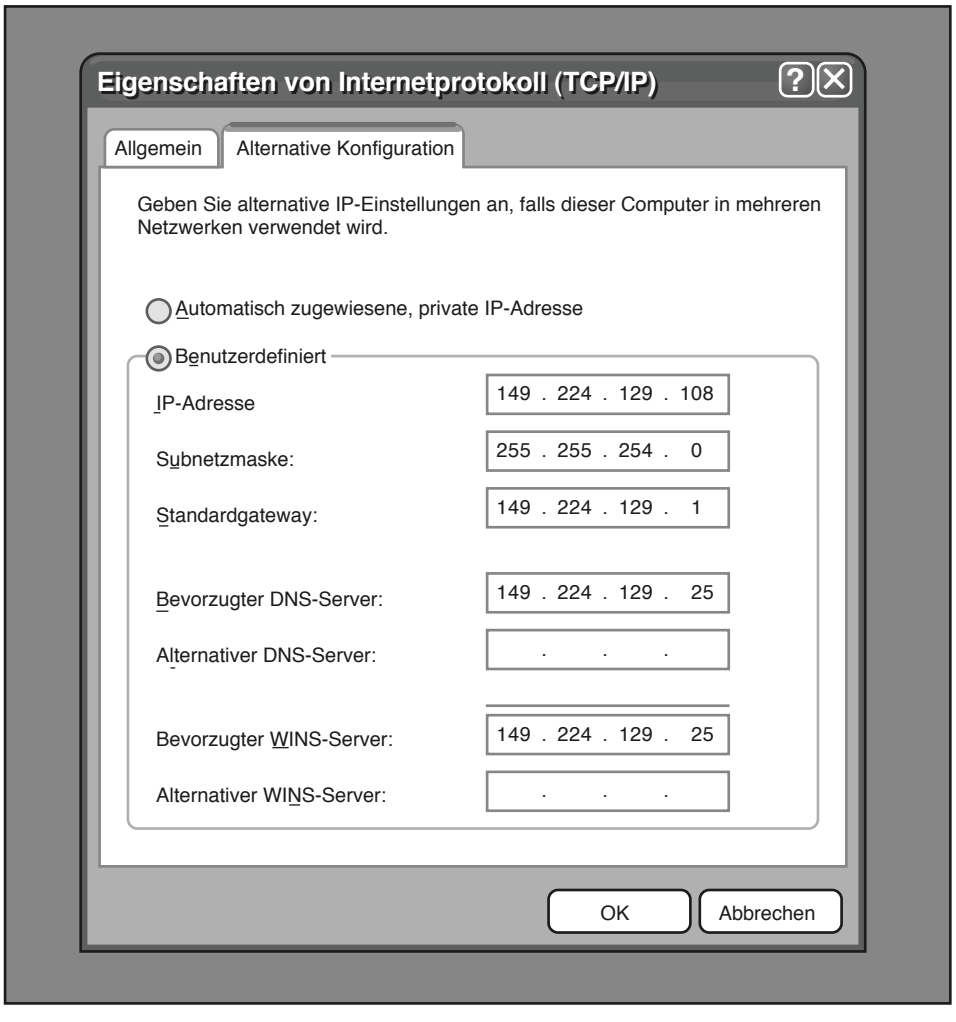
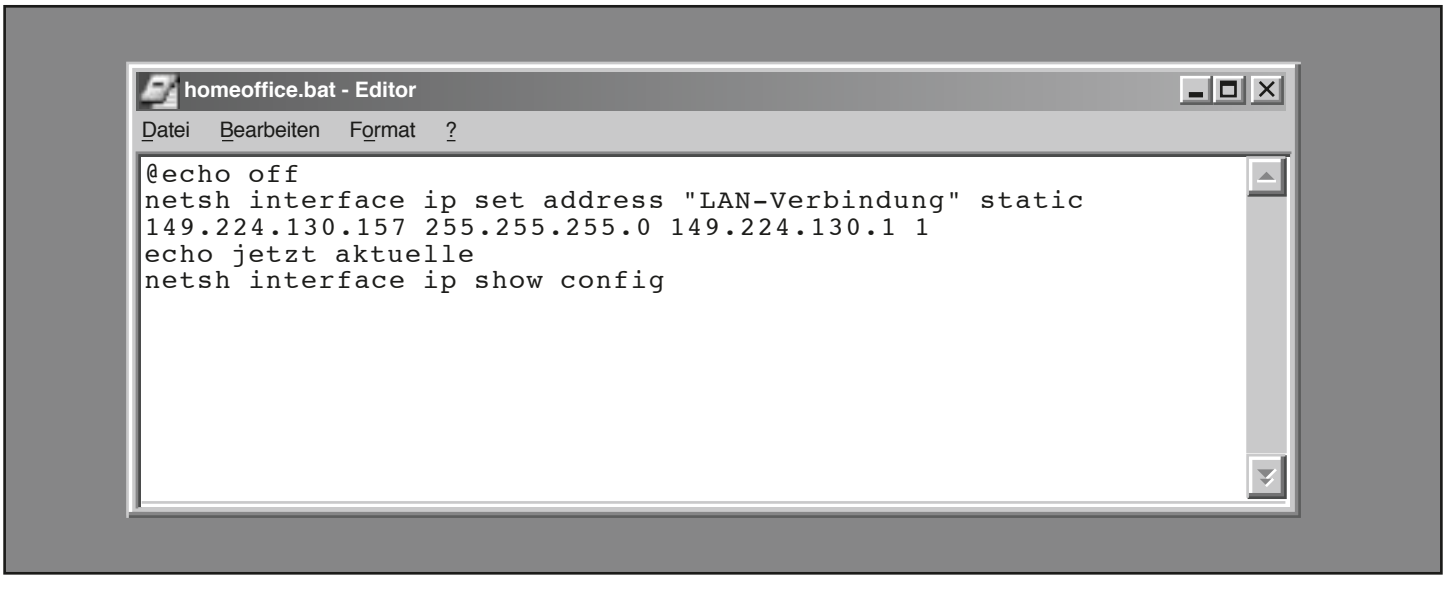


Bild 3: alternative IP-Konfiguration unter Windows XP

Bild 4: Beispiel für eine Batch-Datei zur Änderung der IP-Konfiguration



Fehlersuche mit DOS-Kommandos

Das hier benutzte DOS-Kommando ist eines von vielen, die zu Diagnose-Zwecken unter Windows zur Verfügung stehen.

Ping und Tracert sowie nslookup kennen wahrscheinlich viele, aber man kann jahrelang mit Windows zu tun gehabt haben, ohne jemals auf netsh gestoßen zu sein. Die ARP-Tabelle auslesen mit ARP und insbesondere versuchsweise auf deren Inhalt Einfluss nehmen, um einen Verdacht zur Fehlerursache zu erhärten, gehört ebenso zum notwendigen Repertoire der Fehlersuche auf Windows-Rechnern mit IP-Kommunikation wie der Umgang mit der routing table über „netstat“ bzw. „route“.

Auch die Mechanismen im Zusammenhang mit Ressourcen im Windows-Netzwerk können gezielt getestet werden, etwa mit dem „net“-Kommando. Dieses bringt erfahrungsgemäß vertrauenswürdigere Ergebnisse als der Windows-Explorer (Abfrage von Ressourcen über „Netzwerk-Umgebung“ usw.).

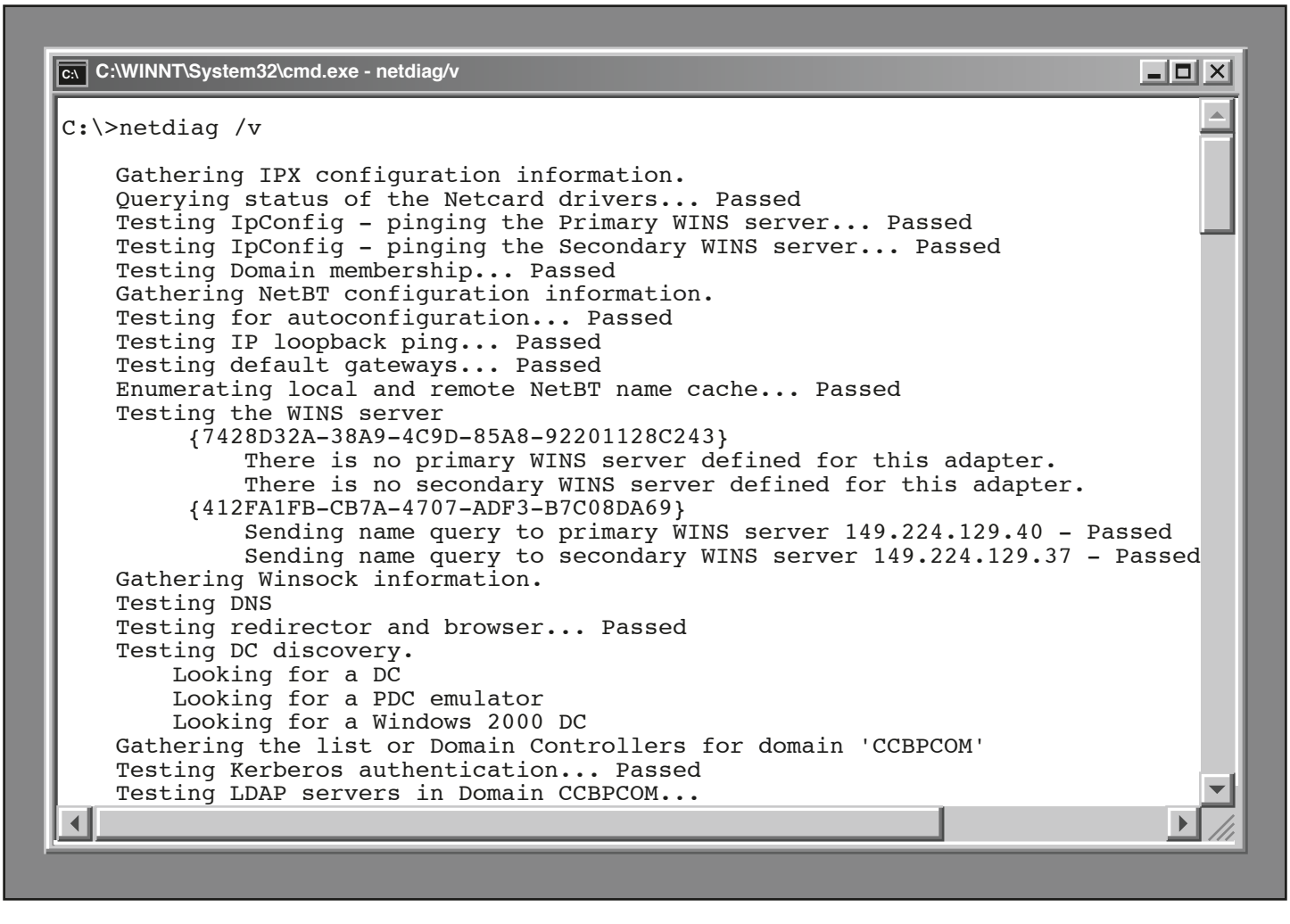
„Profis“ benutzen weitere Prüfmöglichkeiten, die im Windows Administrator Pack enthalten sind. Insbesondere ist hier ein Kommando enthalten, mit dessen Hilfe man automatisch und systematisch alles testen lassen kann, was an Diensten in einem Windows-Netzwerk wichtig ist (Bild 5).

Mit den bislang genannten Aspekten zu TCP/IP unter Windows ist das Thema aber noch nicht abgeschlossen: wichtige Windows-Dienste basieren auf IP und sind kaum hiervon zu trennen. Das Verständnis, wann welcher Namensdienst zuständig ist (WINS oder DNS) und welche Konfigurationsmöglichkeiten hier bestehen, erfordert auch „wohlsortierte“ Kenntnisse. Mit dem active directory muss DNS zur dynamischen Variante DDNS erweitert werden – was kann hier „schief gehen“?

Zuletzt, aber in der Praxis äußerst wichtig, ist da noch das Thema IP-Security.

Man sieht: je länger man sich mit dem Thema „IP unter Windows konfigurieren“ beschäftigt, umso mehr stellt man fest, dass hier eine Vielzahl von Einstell- und Prüfmöglichkeiten besteht. Wenn man viel einstellen kann, kann man aber auch viel Schaden anrichten – oder viele Chancen auslassen, gezielt Probleme zu vermeiden oder „Tuning“ vorzunehmen. Daher widmet sich ein neues Seminar der ComConsult-Akademie diesem Themenkreis. Die Referenten sind Windows- und Fehlersucheerfahren, aber vor allem auch Experten für TCP/IP-Protokolle. Zu jedem in der langjährigen Praxis als wichtig erfahrenen TCP/IP-Themen werden die notwendigen Netzwerker-Grundlagen erklärt, die entsprechenden Windows-Einstellmöglichkeiten vorgestellt, die möglichen Einstellungen diskutiert, und Möglichkeiten zur Überprüfung im Fehlerfall aufgezeigt.

Bild 5: Netdiag-Kommando.



Studie des Monats

WLAN Sicherheit: Distribution System als VPN

Aus dem ComConsult Research Wireless LAN Sicherheit Report*

Die größtmögliche Sicherheit bei der Übermittlung von Daten bieten VPN-Lösungen, wurden sie doch entwickelt, um vertrauliche Daten über öffentliche Netzwerke wie beispielsweise das Internet zu transportieren.

VPN-Lösungen bauen meist einen verschlüsselten IP-Tunnel auf Netzwerk-Ebene auf, in dem den eigentlichen IP- und TCP-Verkehr transportiert. Damit realisieren sie einen durchgehenden, verschlüsselten Datenstrom vom Endgerät bis zum so genannten Tunnelendpunkt oder auch VPN-Gateway, welches in der Regel bereits innerhalb des LANs positioniert ist. Damit sind schon vom Ansatz her höhere Protokollebenen in die Verschlüsselung einbezogen als bei einer MAC-Layer-basierten Verschlüsselungstechnik. Kenntnisse über die eingesetzten Verfahren und Algorithmen brauchen nur die Clients und der Tunnelendpunkt zu haben. Für alle anderen Geräte dazwischen ist der transportierte IP-Verkehr transparent, dies gilt insbesondere für die Access Points.

Ein in der Regel verschmerzbarer Nachteil solcher Lösungen ist, dass typische IPSec-basierte Lösungen nur IP-Verkehr transportieren können. Stärker ins Gewicht fällt aber die offensichtliche Anforderung, dass der Wireless Client die VPN-Lösung unterstützen muss. Letzteres wird bei PC-basierten Clients zwar kein großes Problem darstellen, aber PDAs oder auch Wireless Druckeradapter bieten im Allgemeinen keine VPN-Unterstützung und fallen damit aus diesem Lösungsszenario heraus. So genannte Pflichttunnel, also Tunnel die von einem Netzwerkgerät wie beispielsweise einem Access Point aus aufgebaut werden, sind keine Alternative, da eine solche Lösung gerade den kritischen Teil der Übertragung, nämlich die Funkstrecke außer Acht lässt.

Setzt man eine VPN-basierte Lösung ein, so kann man getrost auf jede Verschlüsselung und Authentisierung im Funk-LAN verzichten und gewinnt so im Durchsatzengpass WLAN auch noch einen deutlichen Performancevorteil. Bedingung hierfür ist jedoch, dass die Clients keine Verbindungen außerhalb des Tunnels entgegennehmen und dass am Übergang zum zentralen LAN ausschließlich autorisierte VPN-Tunnel durchgelassen werden. Das einzige Gerät, das die Umsetzung dieser Forderung sicher gewährleisten kann, ist offensichtlich der Tunnelendpunkt selbst. Nur hier sind alle Endgeräte authentisiert und hier kann, da hier die Tunnel beendet werden, der ankommende IP-Verkehr als gültiger Tunnel verifiziert werden.

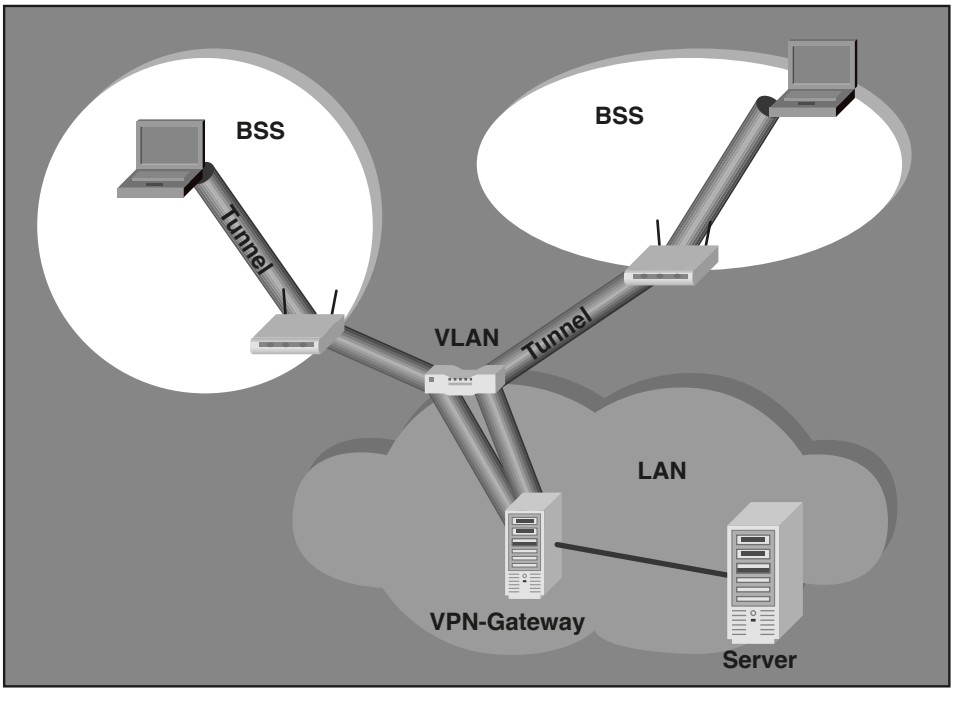
Das heißt, der VPN-Server muss als Gateway zwischen Distribution System und LAN fungieren und er muss über eine minimale Firewallfunktionalität verfügen, um VPN-fremden Verkehr zu filtern.

Zur Dimensionierung des VPN-Servers ist zu beachten, dass bereits eine Hand voll Access Points mehr Last produzieren kann als so manche Standleitung ins Internet. Die Authentisierung der Clients erfolgt meist über Zertifikate, so dass dann zusätzlich auch noch eine Public-Key-Infrastruktur aufgebaut werden muss. Als Authentisierungsverfahren können neben proprietären Verfahren mittlerweile 802.1x-basierende Verfahren über zentrale Authentisierungsserver eingesetzt werden.

Bei windowsbasierten Netzen bietet sich als elegante und sichere Lösung der Einsatz von VPN-Servern an, die den in Windows 2000 und Windows XP integrierten IPSec-Client unterstützen. Damit braucht dann keine zusätzliche Software auf den Clients installiert und gepflegt werden.

Ein Nachteil von VPN-Lösungen soll aber noch erwähnt werden. Wenn alle Funkclients nämlich Tunnel zum zentralen VPN-Gateway aufbauen, können die Funkclients nicht mehr auf direktem Weg miteinander kommunizieren. Anwendungen, die von der üblichen Client-Server-Architektur abweichen und stattdessen eine Peer-to-Peer-Struktur verwenden, wie beispielsweise Voice-over-IP werden daher mit Performanceeinbußen zu rechnen haben. Gerade bei Voice-over-IP kann die damit einhergehende zusätzliche Verzögerung ein KO-Argument für den Einsatz von VPN sein.

VPN-Tunnel durch das Funknetz bis ins LAN



* Wireless LAN Sicherheit, ComConsult Research Technologie Report,
zu beziehen über den Verlag ComConsult Technologie Information (weitere Informationen unter **www.comconsult-research.com**)

Aktueller Report

Studie des Monats: Wireless LAN Sicherheit Report

Sicherheit bleibt ein Schlüsselthema bei der Einrichtung und beim Betrieb von Wireless LANs:

- Zu einfach ist das Abhören einer unprofessionell gesicherten Installation.
- Eine WEP-Verschlüsselung ist auch mit 128-Bit-Schlüsseln unzureichend.
- Die Hersteller gleichen die Unzulänglichkeiten des Standards durch proprietäre Erweiterungen aus.
- Die Wi-Fi Alliance zertifiziert seit Mai 2003 eine Übergangslösung unter der Bezeichnung WPA.
- Der Sicherheitsstandard IEEE 802.11i steht vor der Verabschiedung, die ersten Chips, die die geforderte AES-Verschlüsselung unterstützen, sind verfügbar.
- Neben dem allgemeinen Bestreben nach Sicherheit gibt es Anwendungsbereiche, in denen weitergehende Sicherheitsmaßnahmen zwingend erforderlich sind: Notebooks von Führungskräften, Konferenz- oder Besprechungsbereiche, sensible Anwendungsbereiche in der Medizintechnik oder der Personalverwaltung.

Eine Sicherheitsanalyse von Funknetzen unterliegt speziellen Aspekten, wobei neben funktechnischen und netzwerktechnischen Besonderheiten eben auch betriebliche Gesichtspunkte eine große Rolle spielen. Der Report lenkt Ihren Blick auf die grundsätzliche Problematik und stellt verschiedene Lösungsmöglichkeiten vor.

In dem Sicherheitsreport erfahren Sie:
- welche prinzipiellen Sicherheits-Anforderungen an Datenübertragungen in Funknetzen zu stellen sind,
- in wie weit und wie die aktuellen Standards diese Anforderungen umsetzen,

- warum der klassische Sicherheitsstandard für WLANs gescheitert ist,
- wie bekannte Angriffsszenarien und Hackertools gegen WLANs arbeiten und wie das jeweilige Gefährdungspotenzial realistisch einzuschätzen ist,
- welche ergänzenden Sicherheitsfeatures aktuelle Produkte bieten,
- welche Verschlüsselungsverfahren zur Verfügung stehen,
- wie Integrität und Authentizität der Daten garantiert werden.

Dabei werden alle Fragen beantwortet, die Sie schon immer einmal stellen wollten:
- Was bedeutet eigentlich Session-Hijacking?
- Mit welchem Aufwand können verschlüsselte WLANs abgehört werden?
- Soll WEP-Verschlüsselung eigentlich eingesetzt werden oder besser nicht?
- Was ist von dem Sicherheitsmerkmal „Closed System“ zu halten?

Zukünftige Sicherheitsstandards für WLANs werden auf den IEEE-Standard 802.1X zur „Netzwerkanmeldung“ aufsetzen. Der Report stellt auch diesen Standard vor und zeigt Ihnen, welche Anpassungen auf das Design von Wireless LANs und des umgebenden Netzwerks sich daraus ergeben.

Ein letzter Teil stellt „strukturierte Funknetze“ vor und untersucht:
- In wie weit taugen Sicherheitskonzepte wie VPN oder Firewalls, um Wireless LANs abzusichern?
- Welche Rolle spielen spezielle Clients und warum muss zwischen Wireless Druckern, Notebooks und PDAs unterschieden werden?
- Welche grundlegenden Design-Entscheidungen müssen Sie bereits heute berücksichtigen, um auf die neuen WLAN-Generationen umsteigen zu können?
- Wie können Umstiegsszenarien aussehen und wann soll man umsteigen?
- Worauf sollten Sie bei kurzfristigen Investitionsentscheidungen achten?
- Wie werden sich Funknetze in der Zukunft weiterentwickeln?

Funknetze – und das machen die beschriebenen Lösungen deutlich – lassen sich im Gegensatz zur häufig kolportierten Meinung sicher betreiben. Jedoch handelt es sich hierbei nicht um ein einfach zu installierendes Plug'n-Play-Produkt, Funknetze benötigen eine spezielle Infrastruktur und müssen zudem in einen unternehmensweiten Sicherheitsstandard integriert werden. Der Report hilft Ihnen bei der Bewertung aktueller und zukünftiger Technologien und gibt Ihnen Argumentations- und Entscheidungshilfen genauso wie detaillierte technische Informationen.

Fax-Antwort an ComConsult 02408/955-399

Bestellung Wireless LAN Sicherheit

☐ Ich bestelle den Research Report
Wireless LAN Sicherheit
(Preis € 298,-- zzgl. MwSt.)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

Bestellen Sie auf unsere Web-Seite
www.comconsult-research.com

Neues Seminar

DNS / DHCP / NAT: IP-Infrastrukturdienste optimal einsetzen und Zusatzpotenziale nutzen

Vom 10. bis 12. November veranstaltet die ComConsult Akademie im Park Plaza Köln zum ersten Mal ihr neues Seminar "DNS / DHCP / NAT: IP-Infrastrukturdienste optimal einsetzen und Zusatzpotenziale nutzen".

Dieses Seminar vermittelt, wie DNS, DHCP und NAT arbeiten und wie eine professionelle Umsetzung aussieht.

Zum Thema

TCP/IP und unsere gesamte Client-Server-Welt basieren auf den IP-Infrastrukturdiensten. Deren professionelle und kompetente Umsetzung ist Voraussetzung für einen stabilen und performanten Betrieb unserer gesamten IT. Umso erstaunlicher ist es, dass viele mit diesen Verfahren gegebene Möglichkeiten in der Praxis ungenutzt bleiben und häufig nur ein Funktionskern zum Einsatz kommt. Speziell im Bereich NAT werden zudem häufig die im Zusammenspiel mit einigen Applikationen gegebenen Einschränkungen häufig übersehen.

Dabei wird im Detail auf die Varianten der Verfahren eingegangen und das damit verbundene Potenzial aufgezeigt.

An Fallbeispielen und typischen Einsatzszenarien werden die Teilnehmer auf die praktische Umsetzung vorbereitet. Typische Konfigurations- und Umsetzungsfehler werden erklärt.

Abhängigkeiten mit anderen Technologien werden mit den sich daraus ergebenden Einschränkungen aufgezeigt. Dabei wird sowohl auf die typischen Produkte von CISCO und Microsoft als auch auf Open Source Lösungen eingegangen. Möglichkeiten und Einschränkungen dieser Produkte werden erklärt.

In diesem Seminar lernen Sie

- wie IP-Infrastrukturdienste funktionieren und wie man sie nutzbringend anwendet
- welche wichtigen Zusatzpotenziale die Verfahren bieten
- welche typischen Fehler gemacht werden und wie es besser geht
- wie typische Produkte einzuschätzen sind
- wie DNS arbeitet, was wichtige Zusätze wie DynDNS leisten, wie eine DNS-Server-Lösung aufgebaut wird
- wie DHCP arbeitet, welchen Stellenwert die verschiedenen Parameter haben, wie eine redundante Lösung entsteht, wo Schwachstellen liegen, was ein Relay Agent leistet, wie DNS und DHCP zusammen hängen
- wie NAT arbeitet, warum NAT ein sehr kritischer Dienst ist, welche Störungen und Probleme immer wieder auftauchen, was die Varianten statisch, dynamisch, Portbezogen bedeuten, was ein NAT-Router ist, wie NAT und DNS zusammen spielen, wo Grenzen und Nachteile liegen
- was sich bei DHCP, DNS und NAT mit IPnG (V6) ändert

Der Referent Markus Schaub ist seit vielen Jahren für die ComConsult Technologie Information GmbH tätig. Seine Aufgabenbreiche umfassen die Evaluierung, Konfiguration und Inbetriebnahme neuster Hard- und Software aus dem Netzwerkumfeld. Darüber hinaus ist er für den Betrieb des Cisco-Router-Netzes der ComConsult Akademie verantwortlich.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung DNS / DHCP / NAT

☐ Ich melde mich an zum
DNS / DHCP / NAT: IP-Infrastrukturdienste optimal einsetzen und Zusatzpotenziale nutzen
vom 10.11. - 12.11.03 in Köln
(Preis € 1.590,-- zzgl. MwSt.)

☐ Buchen Sie für mich ein Hotelzimmer

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

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

Schwerpunktthema Oktober 2003

Sicherheit in Wireless LANs

Fortsetzung von Seite 1

Dipl. Math. Cornelius Höchel-Winter ist Leiter des Testlabors der ComConsult Technologie Information GmbH. In dem Labor werden regelmäßig Messungen und Evaluierungstests neuster Hard- und Softwareprodukte durchgeführt und ausgewertet. Er besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von Windows- und Unixnetzen; so hat er als verantwortlicher Projektmanager die Rechenzentren und Netzwerke auf dem Gelände der EXPO2000 in Hannover aufgebaut und während der Weltausstellung betrieben.

hoechel@comconsult-research.com

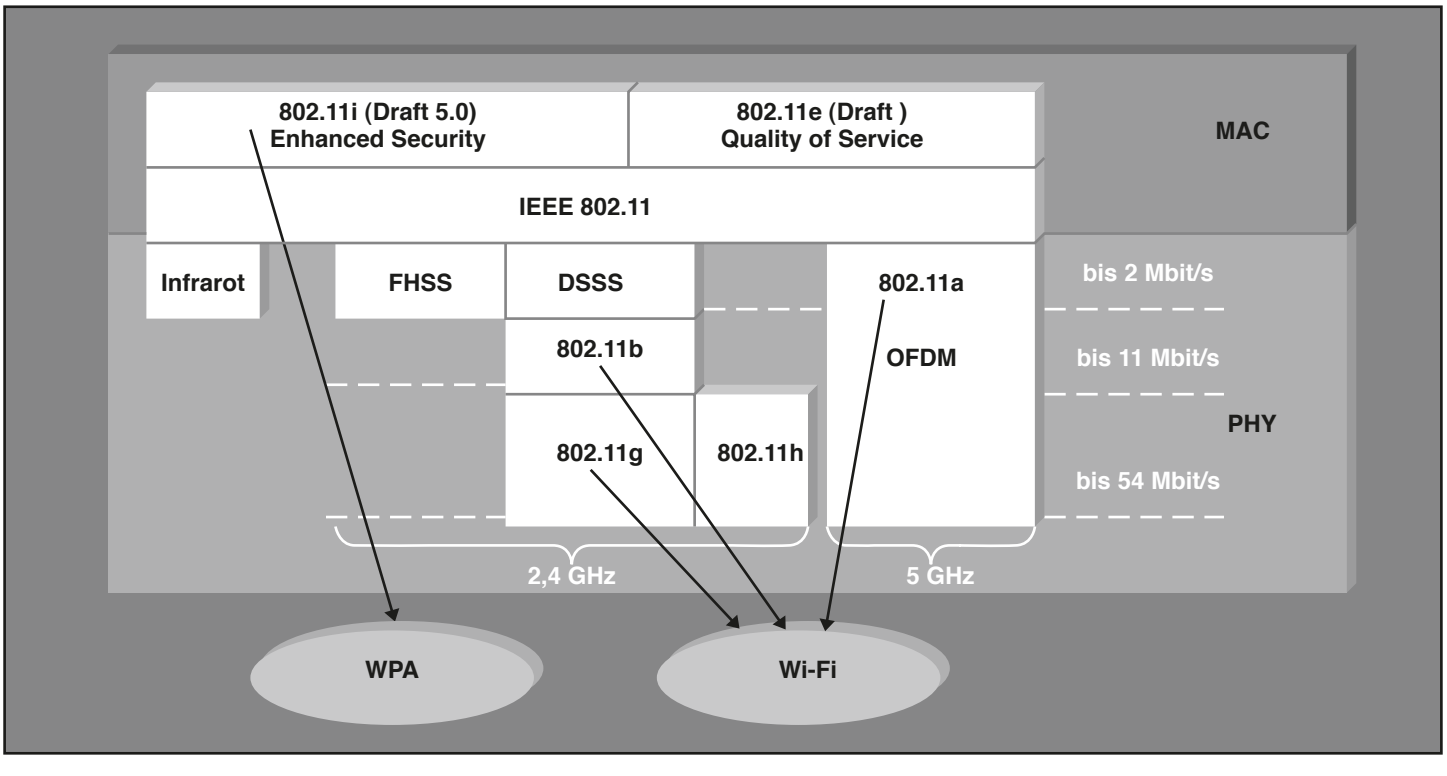
Mit dem großen Markterfolg der 11b-Produkte traten schnell die ersten Lücken in der Protokolldefinition zu Tage und bei der IEEE gründeten sich weitere Arbeitsgruppen mit dem Ziel jeweils spezielle Aspekte bei der WLAN-Übertragung zu verbessern. Im Wesentlichen ist keine dieser Arbeitsgruppen bis heute fertig.

Daneben entstanden das Problem der Kompatibilität verschiedener Produkte und die in unserer realen Netzwerkwelt natürliche Anforderung, WLANs an das alles dominierende Ethernet anzuschließen.

Gerade die letztere Anforderung wird von der IEEE größtenteils ignoriert. WLANs nach 802.11 sind zwar wie Ethernet nach 802.3 Layer-2-Protokolle in der IEEE-802-Familie und ordnen sich damit dem gemeinsamen, übergeordneten LLC-Layer nach 802.1 (Brückenstandard) unter. Da Ethernet jedoch keine Fragmentierung vorsieht, können wie schon beim Token Ring (802.5) zu lange WLAN-Frames nicht in ein Ethernet-LAN weitergeleitet werden.

Beiden Problemen hat sich die WECA gewidmet. WECA steht für Wireless Ethernet Compatibility Alliance, es handelt hierbei sich um eine herstellerübergreifende Organisation, die zunächst als Marketingmaßnahme für 11b-Produkte gegründet wurde. Die WECA entwickelte das Wi-Fi-Gütesiegel (Wireless Fidelity), welches eine grundlegende Kompatibilität von 802.11b zwischen verschiedenen Herstellern garantiert und außerdem das WLAN-Protokoll „Ethernet-kompatibel“ zurechtstutzt. Nach der erfolgreichen Markteinführung von 11a-Produkten hat die WECA ihr Betätigungsfeld erweitert und seit Oktober 2002 werden auch diese Produkte Wi-Fi-zertifiziert, seit Juli 2003 auch 11g-Produkte.

Bild 1: Die IEEE-802.11-Standards und abgeleitete Zertifizierungen



Sicherheit in Wireless LANs

Die zerbrochene Sicherheit

Bei allen Lücken und wünschenswerten Erweiterungen im WLAN-Protokoll zeigte sich bald, dass insbesondere die Sicherheitstechnik ein einziges Desaster war und speziell hier unverzüglich Abhilfe geschaffen werden musste. Die bereits etablierte Arbeitsgruppe 11e wurde daher aufgeteilt und alle sicherheitstechnischen Aspekte in der Arbeitsgruppe 802.11i zusammengefasst. Trotz der verheerenden Presse und des Vorpreschens einzelner Hersteller, die ihre Kunden nicht länger im Regen stehen lassen wollten, sind die Ergebnisse der 11i-Gruppe nach wie vor nicht verabschiedet.

Auch in dieser Situation übernahm die WECA, mittlerweile unter der Bezeichnung Wi-Fi Alliance, das Zepter des Handelns und verabschiedete den Sicherheitsstandard WPA (Wireless Protected Access, siehe [1]). WPA beruht auf dem damals verfügbaren Draft 3.0 von 802.11i und zertifiziert einen erweiterten Sicherheitsmodus, den die IEEE als Übergangslösung für bestehendes 802.11-Equipment definiert hat. Die IEEE selbst strebt dagegen im 11i-Standard eine umfassende Reform der Verschlüsselungs- und Authentisierungsverfahren von WLANs an, wofür letztendlich allerdings neue Hardware notwendig sein wird.

An dieser Stelle sei auch gleich mit einem verbreiteten Irrtum aufgeräumt: Der neue Sicherheitsstandard 802.11i ist nicht allein eine Erweiterung von 802.11b, sondern betrifft alle physikalischen Interfaces, neben 11b also auch 11a und 11g/h.

Warum ist gerade bei Funk-LANs Sicherheit so wichtig? Aus zwei Gründen:

Erstens lässt sich das Übertragungsmedium Funk nicht ohne weiteres räumlich eingrenzen. Funkübertragungen enden nicht an Grundstücksgrenzen oder Bürotüren und sind somit prinzipiell immer abhörbar.

Zweitens handelt es sich bei diesem Übertragungsmedium um ein Shared Medium, das heißt, ein Übertragungskanal wird nicht exklusiv zugeteilt, sondern stets unter allen Teilnehmern aufgeteilt. Insbesondere gibt es prinzipiell keine Möglichkeit zu verhindern, dass andere den gleichen Übertragungskanal benutzen und es gibt prinzipiell keine Möglichkeit festzustellen, wer alles zuhört.

Damit ergeben sich zwei grundsätzliche Anforderungen für Datenübertragungen über Funk:

1. Geheimhaltung

Da ein Abhören der Übertragung nicht ausgeschlossen werden kann, müssen alle Daten verschlüsselt übertragen werden.

2. Authentisierung

Da fremde Teilnehmer (Empfänger oder Sender) im Netz nicht ausgeschlossen werden können, müssen sich alle Teilnehmer anmelden und ausweisen.

Last but not least bleibt festzustellen, dass bestimmte Denial-of-Service-Angriffe in Funknetzen nicht verhindert werden können.

Beide Anforderungen waren der IEEE im Wesentlichen von Anfang an bewusst und sie hat durchaus versucht sie im ursprünglichen Standard 802.11 zu erfüllen. Trotzdem hat dieser erste Entwurf nicht funktioniert.

Die Gründe hierfür sind mannigfaltig, einige sollen hier noch einmal kurz angerissen werden (für eine umfassende Analyse der Sicherheitsfeatures von Wireless LANs siehe [6]). Der wichtigste Aspekt ist, dass im 802.11 und damit auch bei allen marktrelevanten Produkten nach wie vor unverschlüsselter Datenverkehr der Defaultmodus ist, in dem alle Stationen betrieben werden. Verschlüsselung und hierbei insbesondere die zu verwendenden Schlüssel müssen erst umständlich konfiguriert werden. Daher ist es verständlich, dass die Mehrzahl der Wireless LANs unverschlüsselt betrieben wird. Da zusätzlich die Authentisierung der Clients eng mit der verschlüsselten Datenübertragung verknüpft wurde, waren Tür und Tor für Manipulationen und unberechtigte Netzbenutzer geöffnet.

Der zweite wichtige Aspekt ist ein fehlendes Schlüsselmanagement. Zwar wirft der Standard die Frage nach einem solchen Management auf, beantwortet sie aber nicht und gibt somit diese Aufgabe an die Hersteller weiter. Außer wenigen proprietären Lösungen (z.B. Ciscos LEAP) haben die meisten Hersteller dieses Problem ignoriert und den Benutzern bzw. Netzwerkadministratoren nur eine manuelle Schlüsselverteilung ermöglicht. Alle WEP-Schlüssel mussten also manuell an allen teilnehmenden Kommunikationspartnern in bunt wechselnden Konfigurationsmenüs eingetippt werden.

Da es schon in mittleren Organisationen völlig unrealistisch ist, anzunehmen, man könnte alle mobilen Geräte zu einem bestimmten Zeitpunkt im Zugriff haben, um beispielsweise die WEP-Schlüssel auszutauschen, werden diese Schlüssel in der Regel unverändert immer weiter genutzt.

Das Weiterverwenden von gebrauchten Schlüsseln, genauer das mehrfache Kodieren von Daten mit dem gleichen Schlüssel kompromittiert jedoch auf die Dauer jedes noch so gute Kryptografie-Verfahren.

Zu diesen prinzipiellen Erwägungen kommen noch weitere gravierende technische Mängel des WEP-Protokolls, die schließlich in einem Papier von Fluhrer, Mantin und Shamir ([7]) gipfelten, in dem beschrieben wurde wie aus bestimmten verschlüsselten Daten der geheime WEP-Schlüssel zurückgerechnet werden kann. Entsprechende Tools, die diese Anleitung umsetzten, ließen nicht lange auf sich warten und stehen im Internet zur Verfügung(siehe [16]).

Ein solcher Angriff ist allerdings nicht ganz so trivial wie es sich anhört. Zunächst muss der Angreifer überhaupt 802.11-Datenframes fehlerfrei in beträchtlichem Umfang empfangen können. Mit handelsüblichen PC-Karten keine leichte Aufgabe, insbesondere nicht wenn der Funkverkehr innerhalb eines Gebäudes von außen abgehört werden soll und massive Wände zu überbrücken sind. Allerdings können mit einigem Bastler-Knowhow deutlich leistungsfähigere Empfängerantennen gebaut werden. Details und Grundlagen zu Antennen können Sie in [9] nachlesen.

Darüber hinaus muss der Angreifer den MAC-Layer seiner Wireless Karte dahingehend verändern, dass die Karte Frames an fremde MAC-Adressen entgegennimmt – die Standardtreiber aller Netzwerkkarten verwerfen diese Frames nämlich schon während des Empfangs. Für diesen so genannten „Promiscuous-Mode“ stehen im Internet zwar mittlerweile Treiber zumindest für die Karten der großen Hersteller zur Verfügung, jedoch wird in der Regel nur LINUX als Betriebssystem unterstützt und viele dieser Treiber funktionieren nur mit einem bestimmten Firmware-Level.

Ergänzende Anforderungen an eine Sicherheitslösung

Welche ergänzenden Forderungen an eine „echte“ Sicherheitslösung sind also zu stellen?

A) Es muss ein kryptografisch sicheres Verschlüsselungsverfahren gewählt werden.

Aber was heißt „kryptografisch sicher“? Die Qualität eines kryptografischen Systems wird im Allgemeinen daran bemessen, wie gut die Schutzwirkung dieses Systems gegenüber Angriffen ist. Hierzu sind zwei Kriterien zu berücksichtigen: die Stärke des Algorithmus und die Größe des Schlüsselraums

Nur die Kombination aus gutem Algorithmus und langem Schlüssel weist die geeignete Qualität auf. Gute Algorithmen mit zu kleinem Schlüsselraum sind ebenso unsicher wie große Schlüsselräume auf der Basis kryptografisch schwacher Algorithmen.

Nun darf man im Zusammenhang mit Wireless LANs trotz allem einige Randbedingungen nicht außer Acht lassen. Dazu gehört zunächst, dass die erforderlichen Ver- und Entschlüsselungsleistungen von einfachen Prozessoren, wie sie beispielsweise in PDAs eingesetzt werden, oder hardware-basiert von Chips auf Netzwerkkarten erbracht werden müssen – und das in der Größenordnung der Übertragungsgeschwindigkeit von zukünftig 100 Mbit/s und mehr. Damit wird die Auswahl auf symmetrische Verschlüsselungsverfahren eingeschränkt. Und obwohl das RC4-Verfahren 1999 durchaus noch als sicheres Verfahren galt, hat man sich im neuen 802.11i-Standard für den DES-Nachfolger AES (Advanced Encryption Standard, siehe [10]) entschieden.

Damit sind wir bei einem Dilemma, in das sich die IEEE hineinmanövriert hat. Der AES ist ein Blockverschlüsselungsverfahren, also ein Verfahren, welches gänzlich anders arbeitet als der Stromverschlüsseler RC4. Daher braucht man für AES und mithin für die neuen 802.11i-Verfahren neue Hardware, die alten Produkte können nicht mit AES verschlüsseln. Will man bestehende Produkte via Firmware-Upgrade „aufrüsten“, muss man notgedrungen beim RC4 und damit im Kern bei WEP bleiben. Einzig aus diesem Grund sieht der 11i-Entwurf einen zweiten Sicherheitsmodus vor, der zwar nicht die volle Sicherheitsstufe erreicht, aber als Firmware-Upgrade in die meisten Produkte integrierbar sein soll. Damit soll eine Übergangszeit, in der noch alte, im Wesentlichen 11b-Hardware eingesetzt wird, überbrückt werden.

Diesen Übergangsmodus mit der Bezeichnung TKIP hat die Wi-Fi Alliance aus dem Draft 3.0 des 802.11i herausgelöst und als eigenen Standard unter der Bezeichnung WPA veröffentlicht.

Eine weitere Einschränkung ergibt sich daraus, dass es bei dem 802.11-Protokoll vorkommen kann, dass Frames abgesendet werden, die niemals beim Empfänger ankommen. Es kann also keinen paketübergreifenden, zusammenhängend verschlüsselten Datenstrom geben. Stattdessen muss der Verschlüsselungsstrom mit jedem Paket neu beginnen.

Mit anderen Worten: Jedes Paket muss mit einem eigenen, paketspezifischen Schlüssel verschlüsselt werden und der Empfänger muss in der Lage sein, aus dem Paketinhalt auf den verwendeten Schlüssel zu schließen. Das beim WEP-Verfahren eingeführte Prinzip einen Initialisierungsvektor im Klartext zu übermitteln, wird im Prinzip also beibehalten.

B) Die (verschlüsselten) Daten dürfen nicht verändert werden können.

Der MAC-Layer des 802.11 schützt den gesamten Frame durch eine angehängte Checksumme (CRC) gegen statistische Veränderungen (Bitfehler) wie sie bei jeder physikalischen Übertragung vorkommen. Diese Checksumme schützt jedoch nicht vor absichtlichen Verfälschungen! Aus diesem Grund sehen die beiden neuen Modi des 802.11i eine zusätzliche Hashsumme vor, die mit den Daten übertragen wird.

C) Die (unverschlüsselten) Headerdaten dürfen nicht verändert werden können.

Hierzu zählen insbesondere die MAC-Adressen der Sender und Empfänger. Kann beispielsweise die Empfängeradresse manipuliert werden, können die Frames umgeleitet und dort entschlüsselt werden. In der Praxis bedeutet diese Anforderung, dass auch die MAC-Header durch den eben angesprochenen Hash geschützt werden müssen. Hierbei ist zu beachten, dass im 802.11-Header mehr als zwei MAC-Adressen vorkommen können.

D) Aufgezeichnete Pakete dürfen nicht erneut abgespielt werden.

Einen Replayschutz implementiert man am einfachsten über einen Zähler: Der Empfänger akzeptiert ausschließlich Pakete, deren Zähler höher ist als das zuvor empfangene Paket. Natürlich muss dann die Integrität des Zählers gewährleistet werden, das Feld muss also ebenfalls über die Hashsumme geschützt werden. Die beiden neuen Verfahren im 802.11i interpretieren den Initialisierungsvektor des Verschlüsselungsverfahrens als Zähler und installieren damit einen Replayschutz, bei WEP ist das nicht so.

Für Access Points bedeutet dies höhere Anforderungen an die Hardware: empfängt nämlich eine Station Pakete von mehreren Sendern, dann muss für jeden dieser Sender eine eigene lokale Variable geführt werden.

E) Die Stationen müssen sich gegenseitig authentisieren.

Authentisierung war eine der anfangs formulierten Grundanforderungen. Das heißt, jeder Kommunikationspartner muss sich vor Beginn der Übertragung ausweisen. Dies wird wie im täglichen Leben dadurch erreicht, dass man nachweist im Besitz einer einmaligen Information bzw. Dokuments zu sein. In der Datenverarbeitung wird diese Information in der Regel Passwort oder Schlüssel genannt.

In Wireless LANs ist es darüber hinaus wichtig, dass eine gegenseitige Authentisierung von Client und Access Point gewährleistet wird, und nicht nur einseitig der Client authentisiert wird. Denn anders als in kabelgebundenen Netzen kann sich ein Client in Funknetzen nicht sicher sein, dass das Netzzugangsgerät auch das ist, das er angewählt hat. Wird die Authentizität des Access Points nicht überprüft, können sich „Men in the Middle“ einschleichen.

F) Der behaupteten Herkunft der Daten muss vertraut werden können.

Der Empfänger muss sich sicher sein, dass das Paket tatsächlich vom mutmaßlichen Sender kommt. Das heißt, jeder Kommunikationspartner muss sich nicht nur zu Beginn der Übertragung ausweisen, sondern jedes einzelne Datenpaket muss ebenfalls auf seine Authentizität überprüft werden. Daten können aber nur dann authentisiert werden, wenn sichergestellt ist, dass der Inhalt nicht verändert wurde. Dies geschieht in der Regel indem man eine geeignete Hashsumme hinzufügt. Wird zur Hash-Berechnung ein einmaliger Schlüssel einsetzt, anhand dessen der Sender zu erkennen ist, dann können damit auch die Daten authentisiert werden.

Wegen der Beschränkung auf symmetrische Schlüssel hat dies jedoch eine Einschränkung der oben formulierten Anforderung zur Folge:

Es können nur Unicasts sicher authentisiert werden, falls paarweise eindeutige Schlüssel verwendet werden. Falls auch Multicasts und Broadcasts verschlüsselt übertragen werden, müssen hierfür getrennte Gruppenschlüssel verwendet werden. Doch selbst dann können sich Teilnehmer, mit denen der Gruppenschlüssel ausgetauscht wurde, fälschlicherweise als Absender von Multicasts/Broadcasts maskieren.

Darüber hinaus werden in WLANs so genannte Management- und Controlframes stets unverschlüsselt übertragen, können also auch unentdeckt gefälscht werden.

G) Es dürfen keine Frames von Fremden eingeschleust werden.

In der Praxis bedeutet das, dass alle Frames verschlüsselt übertragen werden müssen, dass die Verfahrensschlüssel über einen vertrauenswürdigen Mechanismus verteilt und danach geheim bleiben und dass sich alle Teilnehmer zunächst authentisieren müssen.

Wie oben erwähnt gilt das für Management- und Controlframes nicht.

H) Es muss ein geeignetes Schlüsselmanagement implementiert werden.

Ein solches Verfahren muss gewährleisten, dass verbindungsspezifische oder besser noch sessionspezifische Schlüssel ausgetauscht werden können ohne den Schlüssel selbst zugefährden. In jedem kryptografischen System ist, unabhängig von seiner Stärke, der Schlüssel primäres Angriffsziel. Denn die Kenntnis des Schlüssels gibt dem Angreifer die Möglichkeit, über den vorliegenden verschlüsselten Text hinaus, beliebige weitere Daten zu entschlüsseln – zumindest solange wie der Schlüssel nicht verändert wird. Ist der Schlüssel hinreichend geschützt, so lässt sich ein starkes Kryptosystem nur durch Absuchen des gesamten Schlüsselraums brechen. Dies jedoch ist bei hinreichender Schlüssellänge nicht in sinnvoll überschaubarer Zeit möglich.

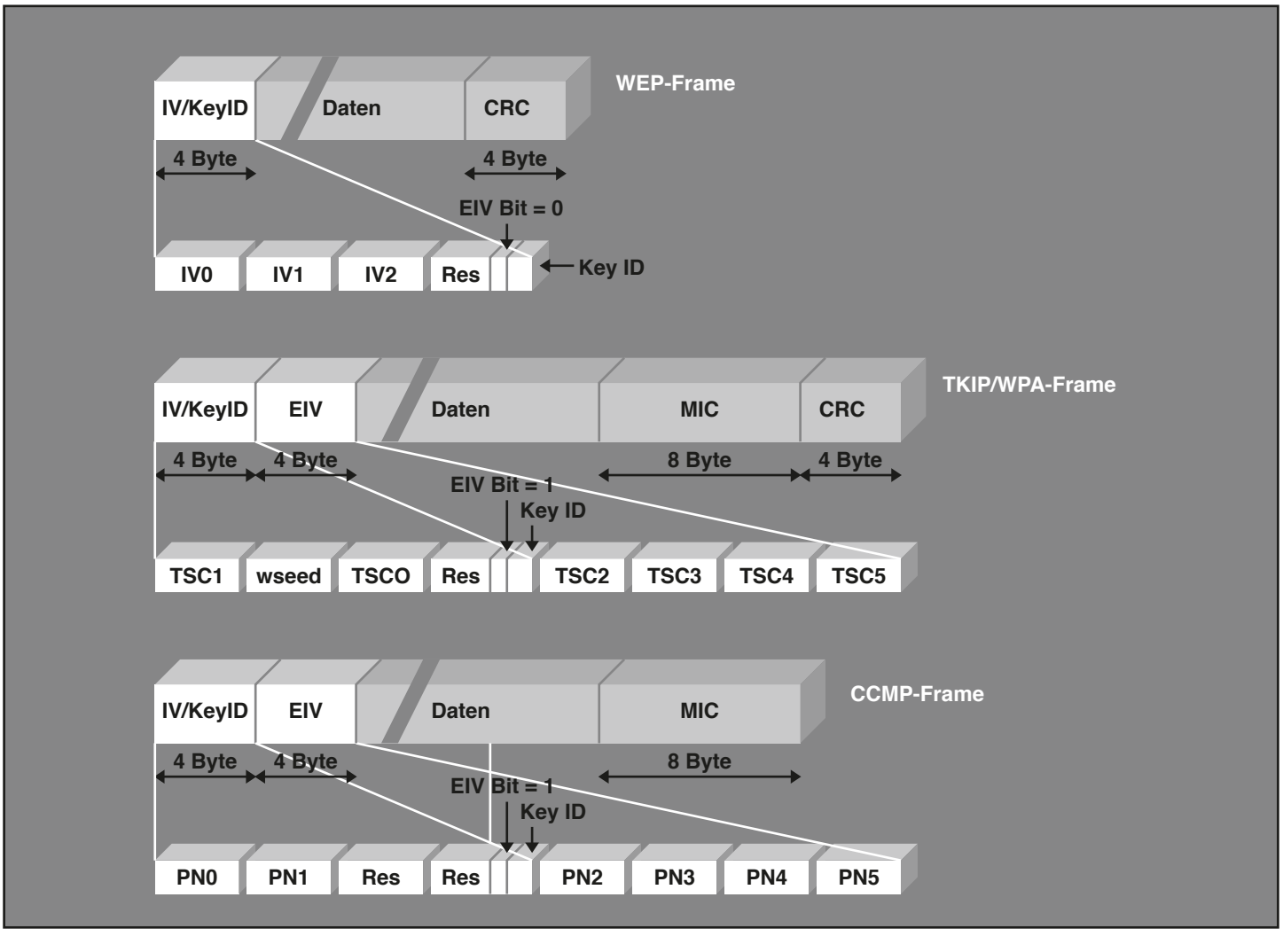
Die Kryptografie-Verfahren der 802.11-Standards

Wie bereits erwähnt, werden WLAN-Produkte in Zukunft mehrere verschiedene Kryptografie-Verfahren einsetzen. So definiert schon der 802.11i allein drei Verschlüsselungsalgorithmen, hinzu kommt noch WPA von der Wi-Fi Alliance.

Im Folgenden sollen die wesentlichen Unterschiede dieser Verfahren diskutiert werden. Der wichtigen Frage, ob und wie sich die Produkte auf ein gemeinsames Verfahren einigen und was eine solche Einigung für die Sicherheitspolitik eines Unternehmens bedeutet, werden sich die abschließenden Abschnitte widmen.

Alle Sicherungsverfahren sind auf die gleiche Weise in den MAC-Frame eingebaut, nämlich als zusätzlicher Sicherheitslayer mit eigenem Header, einem zusätzlichen Trailer und dem jetzt verschlüsselten Datenteil. Durch die zusätzlichen Header und Trailer wird die MPDU, also die vom MAC-Layer transportierten Bruttodaten, größer. Was natürlich negative Auswirkungen auf die Performance hat, insbesondere bei eingeschalteter Fragmentierung.

Bild 2: Die Frameformate der Sicherheitslayer



WEP – Der gescheiterte Sicherheitsstandard

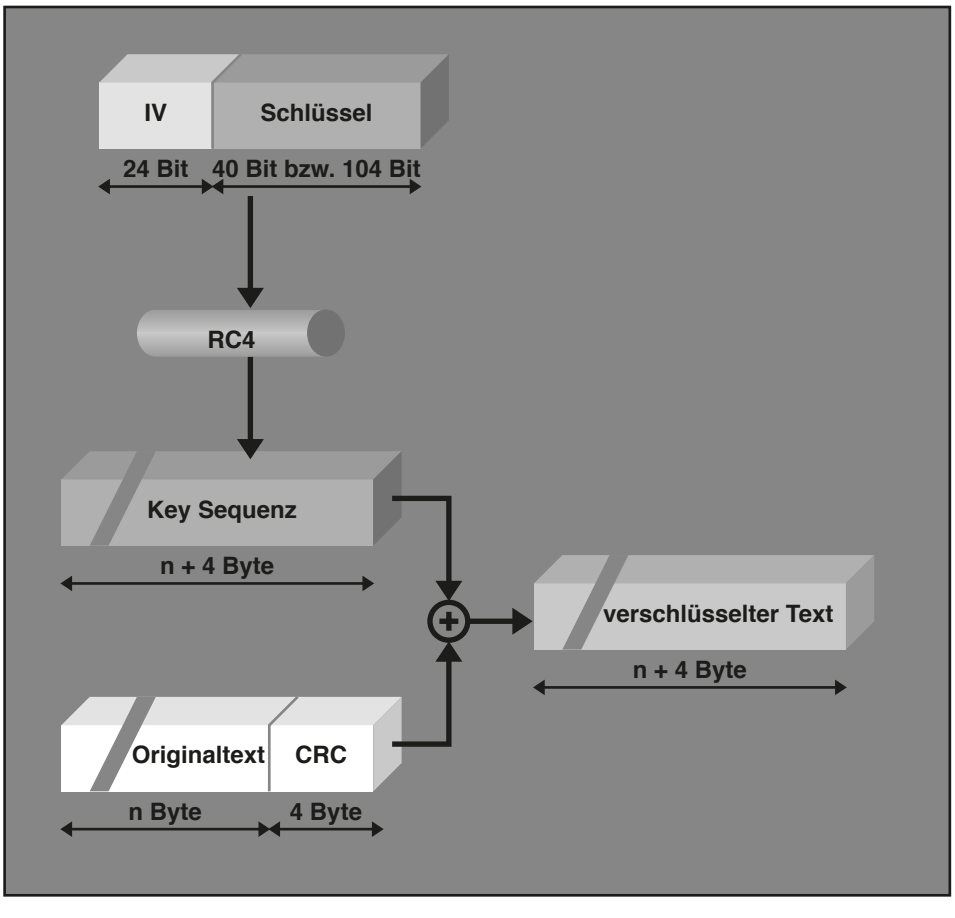
Die Grundanforderung „Geheimhaltung“ wird im Standard mit dem Schlagwort „privacy“ belegt. Wireless Equivalent Privacy (WEP) ist ein einfaches Verschlüsselungsverfahren, welches einen vergleichbaren Schutz bieten sollte, wie physikalische Barrieren das Kabel als Übertragungsmedium schützen (das kann allerdings je nach Umgebung alles oder nichts bedeuten).

Das Verfahren basiert auf dem symmetrischen Algorithmus RC4 von RSA. Ursprünglich waren nur 40 Bit lange Schlüssel standardisiert, diese Beschränkung war in den 1999 noch bestehenden Ausfuhrbeschränkungen der USA für Verschlüsselungsprodukte begründet. Mittlerweile bieten jedoch praktisch alle Hersteller Erweiterungen mit so genannten 128-Bit-Schlüsseln an – tatsächlich werden auf Grund des Verfahrens nur 104 Bit lange Schlüssel verwendet – und auch im 802.11i-Dokument sind beide Varianten unter den Bezeichnungen WEP-40 und WEP-104 vorgesehen.

Beide Verfahren verwenden einen 24 Bit langen Initialisierungsvektor (IV), der vor den geheimen WEP-Schlüssel gehängt wird. Zusammen ergibt sich daraus ein 64 Bit beziehungsweise 128 Bit langer Schlüssel, der als Eingangsparameter für das RC4-Verfahren verwendet wird. RC4 generiert aus diesem Schlüssel eine pseudozufällige Sequenz, die genau so lang ist wie der zu verschlüsselnde Text. Beide Bytefolgen, die erzeugte Key-Sequenz und der Originaltext, werden bitweise über XOR kombiniert und das Ergebnis als verschlüsselter Text übertragen.

Um die Gegenseite in die Lage zu versetzen, denselben RC4-Schlüssel zu erzeugen, wird der IV als der variable Anteil am gesamten Verfahren im Klartext gemeinsam mit den verschlüsselten Daten übertragen. Der Empfänger kann dann auf Grund der Kenntnis des geheimen WEP-Schlüssels mit Hilfe des RC4-Algorithmus dieselbe Key-Sequenz erzeugen. Diese Sequenz wird nun wiederum mittels XOR mit dem empfangenen, verschlüsselten Text verknüpft und man erhält den unverschlüsselten Originaltext.

Bild 3: WEP Verschlüsselungsverfahren



Der Standard spezifiziert den Algorithmus zur Auswahl des IVs nicht, fordert jedoch, dass für jedes übertragene Paket ein neuer IV zu wählen ist. Eine Möglichkeit dies zu tun ist natürlich simples Zählen, was den Vorteil gehabt hätte, eine Replaykontrolle implementieren zu können. Das ist aber im 802.11 nicht vorgesehen, alle standardgemäßen Implementationen müssen sogar den Extremfall akzeptieren, dass ein Sender immer mit dem gleichen IV verschlüsselt. Daher ist auch die aus kryptografischer Sicht wesentlichste Forderung nicht umgesetzt, nämlich dass der WEP-Schlüssel ausgetauscht werden muss, sobald der IV seinen gesamten Werteraum durchlaufen hat.

CCMP

Zu dem schon bekannten WEP wird als deutlich stärkeres und zuverlässiges Verfahren CCMP definiert und als einziges Verfahren für alle zukünftigen Produkte verbindlich vorgeschrieben. CCMP (Counter-Mode/CBC-MAC Protocol) basiert auf einer 128-Bit-Variante des Kryptografie-Standards AES. Der AES (Advanced Encryption Standard) ist der offizielle Nachfolger des DES (Data Encryption Standard) beziehungsweise dessen Erweiterung 3DES und in [10] definiert. AES ist ein Blockverschlüsselungsalgorithmus und wird im konkreten Fall mit einer Schlüssellänge von 128 Bit und einer Blocklänge von 128 Bit eingesetzt. Solche Algorithmen verschlüsseln jeweils einen Klartextblock in einen Chiffreblock, im Gegensatz zu so genannten Stromverschlüsselungsalgorithmen wie der RC4, die jeweils ein Bit nach dem andern verschlüsseln.

Blockverschlüsselungsverfahren haben die Eigenschaft in verschiedenen Betriebsmodi eingesetzt zu werden. Das im 802.11i-Standard definierte CCMP-Verfahren benutzt den CCM-Modus des AES. Der CCM-Modus ist seinerseits im RFC 3610 ([11]) definiert. Dieser Modus ist eine Kombination aus dem CTR-Modus (Counter Mode) zur Verschlüsselung und CBC-MAC (Cipher Block Chaining Message Authentication Code siehe [12]) zur Berechnung einer MIC (Message Integrity Code). Damit verschlüsselt dieser Modus nicht nur die Daten, sondern schützt sie auch gleichzeitig vor Manipulationen und gewährleistet die Authentizität der Daten. Beide Verfahren nutzen zur Berechnung der jeweiligen Startwerte eine 48 Bit große Paketnummer PN, die sowohl die Wiederverwendung von Schlüsseln verhindert als auch zur Replaykontrolle eingesetzt wird.

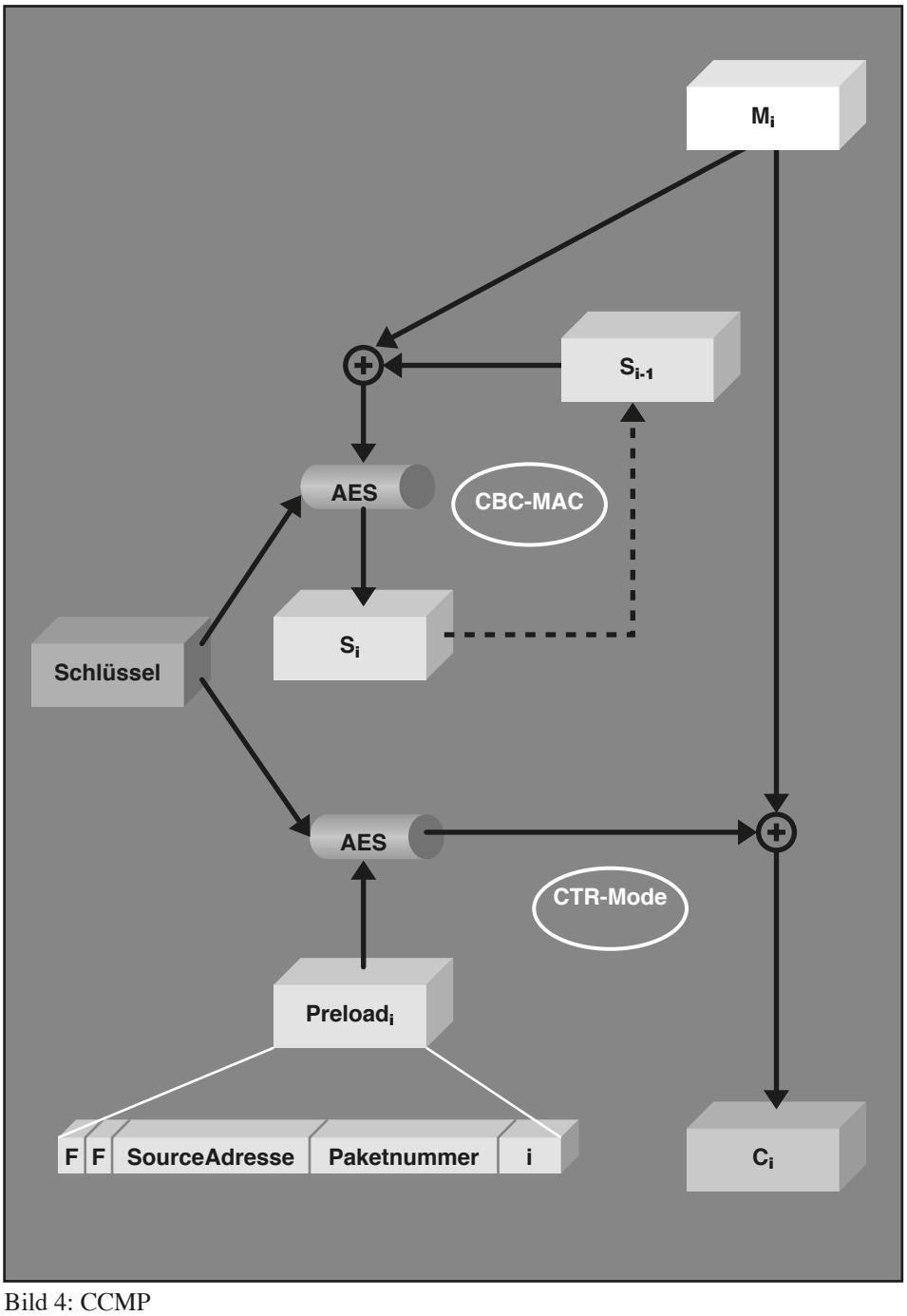


Bild 4: CCMP

Diese Verfahren sind schon längere Zeit bekannt und untersucht. Beide Verfahren, CTR und CBC-MAC, haben gute kryptografische Eigenschaften und können sehr effektiv implementiert werden, beispielsweise werden Verschlüsselung und Hashbildung nebeneinander in einem Durchgang berechnet.

Die Rolle des IV, nämlich paketspezifische Schlüssel zu generieren, wird bei diesem Verfahren von der 48 Bit großen Paketnummer PN übernommen. Um diesen längeren Wert in einem erweiterten Header zu übertragen, wird vor das Datenfeld ein vier Byte langer extended IV (EIV) eingefügt. Die Präsenz dieses zusätzlichen Feldes wird durch ein bislang ungenutztes Bit (EIV-Bit) im vierten Byte des vorangehenden IV/KeyID-Feldes angezeigt.

TKIP und WPA

Wireless Protected Access (WPA) ist die von der Wi-Fi Alliance aus dem IEEE-Standard vorzeitig herausgelöste Übergangslösung für bestehende Hardware. WPA ist bis auf einige Änderungen in der Verhandlungsphase identisch mit TKIP, sämtliche von der Wi-Fi Alliance vorgeschriebenen Anpassungen an TKIP sind mittlerweile von der IEEE übernommen worden und finden sich im aktuellen Draft wieder.

Da TKIP anerkanntermaßen jedoch nur eine Übergangslösung darstellt, hat die Wi-Fi Alliance bereits den Nachfolger WPA2 angekündigt. WPA2 wird voraussichtlich den 11i-Standard vollständig umsetzen und damit auch das CCMP-Verfahren zertifizieren.

TKIP steht für Temporal Key Integrity Protocol und erweitert lediglich WEP als Übergangslösung für bestehende Hardware. Bei der Definition von TKIP galt als wichtigste Voraussetzung: Bestehende Wireless-Geräte sollen softwaremäßig aufrüstbar sein, das heißt das neue Verfahren soll als Firmware-Upgrade in (die meisten) bestehende Hardwareprodukte implementierbar sein. In der Konsequenz bedeutet das allerdings auch umgekehrt, dass das Verschlüsselungsverfahren RC4 weiterhin verwendet werden muss.

Tatsächlich verwendet TKIP das „historische“ WEP zur Verschlüsselung der Daten weiter, es ist lediglich ein Hashalgorithmus zur Sicherung der Daten und ein Verfahren zur Generierung dynamischer, sitzungsspezifischer WEP-Schlüssel und zur Replaykontrolle vorgeschaltet.

TKIP besteht aus zwei Teilen. Im ersten Teil wird mit Hilfe eines Algorithmus mit dem Pseudonym „Michael“ und eines 64 Bit langen MIC-Schlüssels eine ebenfalls 64 Bit lange Checksumme (MIC – Message Integrity Code) über den Datenteil und die Quell- und Sourceadressen berechnet. Diese MIC wird an die noch unverschlüsselten Daten angehängt und zur Authentizitätsprüfung übertragen. Diese MIC-Berechnung ignoriert explizit den MAC-Header um eine Implementierung im Software-Treiber der Netzwerkkarte zu erlauben. Dies hat aber zur Folge, dass eine eventuell notwendige Fragmentierung erst danach stattfindet.

Mit eingeschalteter Fragmentierung werden bei TKIP mehr Frames fragmentiert übertragen als bei einer unverschlüsselten Übertragung. Bei den anderen Verfahren ist das nicht so!

Im zweiten Teil wird zunächst in einem zweistufigen Verfahren aus einem 128 Bit langen Schlüssel (Temporal Key) ein paketspezifischer WEP-Schlüssel mit dazugehörendem IV berechnet und damit schließlich die altbekannte WEP-Verschlüsselung durchgeführt.

Bild 5 verdeutlicht das Verfahren. Entscheidend ist ein 48 Bit großer Paketzähler (TSC – TKIP Sequence Counter), der als Ausgangswert zur Berechnung des WEP-Schlüssels dient und daher niemals mit dem gleichen Temporal Key zusammen wieder verwendet werden darf. Dieser Zähler ersetzt also wie beim CCMP den IV des WEP-Verfahrens und sorgt einerseits – wie der IV – dafür, dass pro Paket unterschiedliche Schlüssel produziert werden, wird aber andererseits, da er als Zähler konzipiert ist, zur Replaykontrolle eingesetzt.

Wie bei den anderen Verfahren muss auch hier der variable Anteil des Verfahrens, also der 48 Bit lange TSC an den Empfänger übermittelt werden. Daher muss wie beim CCMP auch hier der Header des Verfahrens um den vier Byte EIV (Extended IV) erweitert werden. In diesem Feld werden die oberen 32 Bit des TSC transportiert. Die restlichen 16 Bit werden im 24-Bit-breiten IV-Feld befördert, wobei das Verfahren zur Schlüsselgenerierung so arbeitet, dass die ersten 24 Bit des RC4-Schlüssels mit diesen 24 Bit übereinstimmen. Es werden also weiterhin „WEP-kompatibel“ im IV-Feld des Header die ersten 24 Bit des RC4-Schlüssels transportiert.

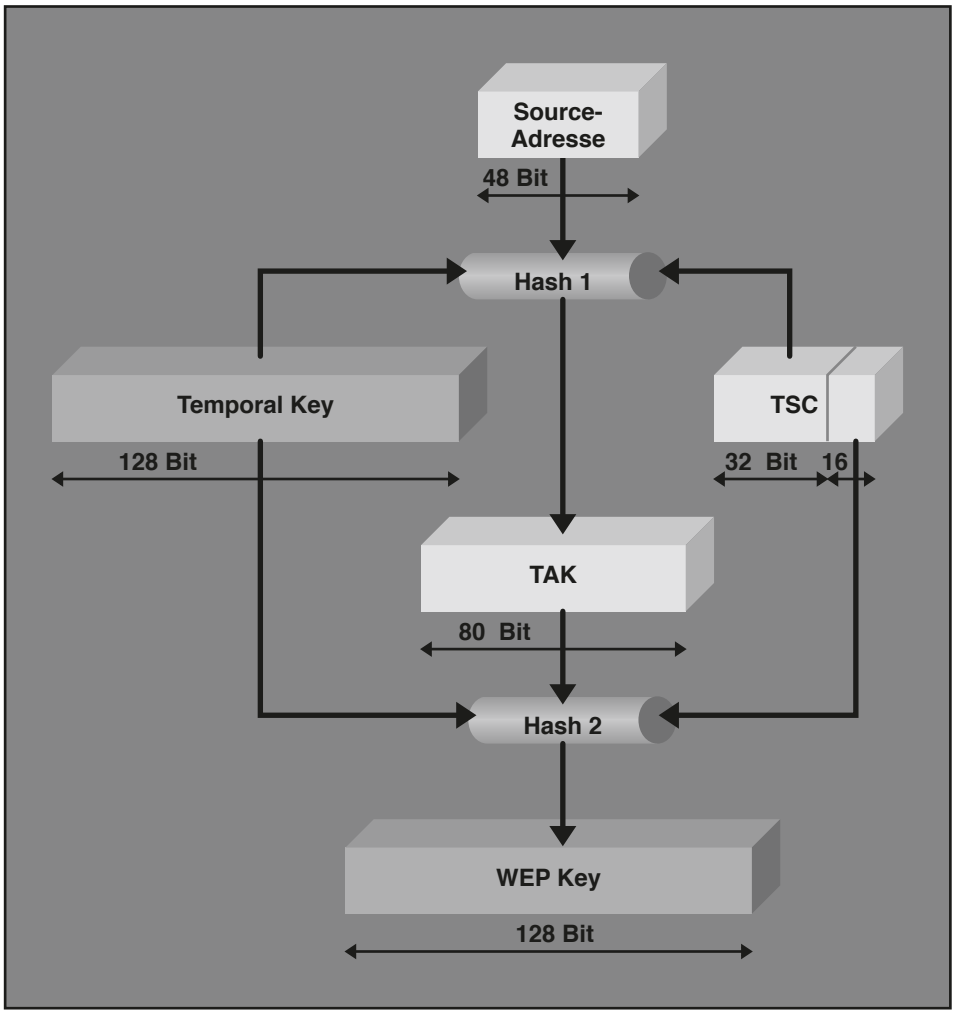


Bild 5: TKIP zur Generierung eines sessionspezifischen WEP-Schlüssels

Authentisierung

Der ursprüngliche 802.11-Standard sieht zwei Authentisierungsverfahren vor, „Open System“ und „Shared Key“.

Der Open-System-Modus ist kein wirkliches Authentisierungsverfahren und steht im Wortsinne für ein „offenes System“, denn in diesem Modus sollen alle Authentisierungsanfragen positiv beantwortet werden. Das Verfahren besteht aus zwei Managementframes vom Typ Authentication, Frame 1 wird vom anfragenden Client geschickt, die Antwort in Frame 2 enthält im Wesentlichen nur ein Status-Feld, welches die Authentisierung bestätigt. Das heißt eine Authentisierung im eigentlichen Sinne findet nicht statt, sondern nur eine administrative Anmeldung des Clients beim gewünschten Netzwerk.

Dagegen setzt der Shared-Key-Modus die Kenntnis eines gemeinsamen, geheimen Schlüssels voraus. Dieser Modus wird nur in Verbindung mit WEP durchgeführt und als geheimer Schlüssel wird der WEP-Schlüssel der Verbindung gewählt. Leider hat dieser Modus so schwerwiegende konstruktive Mängel, dass von seinem Einsatz dringend abgeraten werden muss (siehe [6]).

Einige Hersteller haben einen dritten Modus unter Bezeichnungen wie „Closed System“ oder ähnlichen etabliert. Hierbei übermittelt der Access Point in seinen Beacons keinen SSID mehr, der Netzwerkname soll damit geheim bleiben und vor den Clients versteckt werden. Jedoch wird der SSID trotzdem weiterhin von anderen Managementframes übertragen und bleibt mithörenden Lauschern also auch in diesem Modus nicht sehr lange verborgen. Im 11i-Standard wird dieser Modus daher auch als unnötig und überflüssig abgelehnt.

802.11i lässt also nur noch Open System als Proforma-Authentisierung zu und setzt stattdessen auf den Authentisierungsstandard 802.1X entweder über Pre-shared Keys oder über eine EAP-basierende Authentisierung bei einem übergeordneten Authentisierungsserver.

Der IEEE-Standard 802.1X wurde im Jahr 2001 unter dem Titel „Standard for Port based Network Access Control“ ([13]) mit dem Ziel veröffentlicht, ein höheres Sicherheitsniveau für Netzwerke zu erreichen. Wie die Nummer des Standards bereits andeutet, ist er nicht an eine spezielle Netzwerktechnologie gebunden, sondern definiert eine allgemeine Grundlagentechnologie, wie Benutzer beim Zugriff auf ein beliebiges 802-kompatibles Netzwerk authentisiert werden können. Der Standard kann damit in Ethernet- oder Token-Ring-Netzen genauso angewendet werden wie in Wireless LANs.

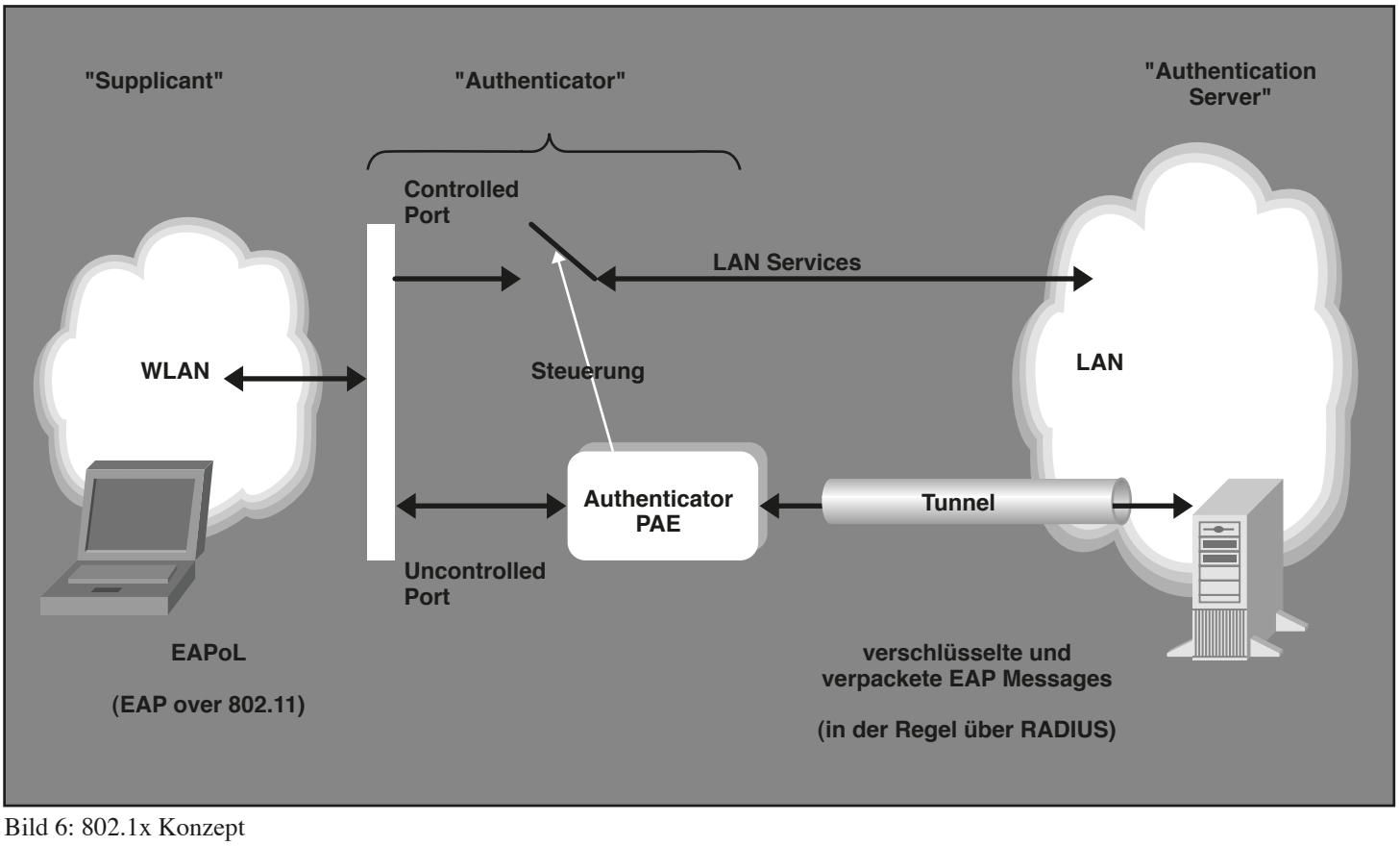


Bild 6: 802.1x Konzept

802.1x betrachtet den gesamten Authentisierungsprozess in zwei Teilen. Zum einen findet eine Kommunikation zwischen Client und Access Point statt – hierfür definiert der Standard ein Protokoll mit der Bezeichnung EAPoL (EAP over LAN) – und zum anderen wird eine bestehende, sichere, d.h. verschlüsselte Kommunikationsbeziehung zwischen dem Access Point und einem Authentisierungsserver im Hintergrund vorausgesetzt. Die Art dieser Kommunikation mit dem Authentisierungsserver lässt der Standard explizit offen, in Frage kommen Tunnelprotokolle wie TLS oder IPSec. WPA legt sich hier auf RADIUS fest, ein Protokoll auf das auch im Standard mehrfach hingewiesen wird. Da auch auf Seiten der Hersteller sowohl von Netzzugangsgeräten wie Access Points, Switches oder Routern als auch von Betriebssystemen (Windows 2000, Linux, etc.) RADIUS vermehrt unterstützt wird, kann man davon ausgehen, dass es sich in diesem Bereich allgemein durchsetzen wird. Eine detaillierte Betrachtung von 802.1X und RADIUS finden Sie in [14].

Der 802.1X-Standard sieht vor, dass das Netzzugangsgerät, im Falle von WLANs also der Access Point, keine Pakete von oder zu einem nicht authentisierten Client weiterleitet, außer solchen die unmittelbar zum Authentisierungsprozess gehören. Die Idee des Verfahrens ist nun, dass der Access Point sich nicht weiter mit der eigentlichen Authentisierung beschäftigt, sondern die Authentisierungsdaten in einem Transportprotokoll mehr oder weniger unverändert über die gesicherte Verbindung an den Authentisierungsserver weiterreicht und auch umgekehrt den Client im Wesentlichen von den Antworten des Servers unterrichtet. Der Vorteil dieses „Durchreichens“ ist die hohe Flexibilität und Durchgängigkeit, die hierdurch erreicht wird. Die Access Points beschäftigen sich nicht mit der Authentisierung der Benutzer, stattdessen wird eine zentrale Benutzerverwaltung geschaffen, bei der man problemlos neue Authentisierungsverfahren einführen kann.

Die Access Points regeln lediglich den Verbindungszustand der Clients. Im anfänglichen, nicht authentisierten Zustand hat der Client keinerlei Zugang zu Netzwerkdiensten, weder zu Anmeldediensten von Netzwerk- oder Fileservern noch zu Basisdiensten wie DHCP oder DNS. Erst wenn der Authentisierungsserver die Anmeldung des Clients positiv bestätigt hat, darf der Access Point dem Client Zugang zum restlichen Netz geben, und zwar sowohl zum restlichen Funk-LAN als auch zum zentralen, kabelgebundenen LAN.

Für den Transport der Authentisierungsdaten verwendet das Verfahren ein bereits älteres Protokoll namens EAP (Extensible Authentication Protocol) der IETF (siehe [15]). EAP bietet dabei lediglich den Rahmen, um die eigentlichen Authentisierungsdaten für eine Vielzahl verschiedener Methoden zu transportieren. Da EAP ursprünglich für Punkt-zu-Punkt-Verbindungen entwickelt wurde, hat es keinen Layer-2-Header und kann daher im LAN nicht ohne weiteres transportiert werden. Dieses Manko gleichen die beiden Transportprotokolle EAPoL und RADIUS aus. EAPoL transportiert die EAP-Daten über ein Layer-2-Protokoll wie 802.11 und RADIUS transportiert sie auf Layer-3 über TCP/IP.

Wie oben erwähnt ist es in Wireless LANs wichtig, dass hierbei ein Authentisierungsverfahren gewählt wird, welches die gegenseitige Authentisierung beider Partner gestattet. Es muss sich also auch der Access Point oder stellvertretend für ihn der Authentisierungsserver beim Client ausweisen. Mögliche Authentisierungsverfahren sind beispielsweise EAP-TLS oder PEAP, aber nicht EAP-MD5.

Unmittelbare Konsequenz hieraus ist, dass der Zugang zum Authentisierungsserver möglichst sicher gestaltet werden muss. Insbesondere muss der Authentisierungsserver alle Access Points sicher authentisieren und dann zu jedem einen abhörsicheren Tunnel aufbauen. Falls nicht-autorisierte Access Points Authentisierungen über den Server durchführen können, ist die Sicherheit des gesamten Netzes in Frage gestellt.

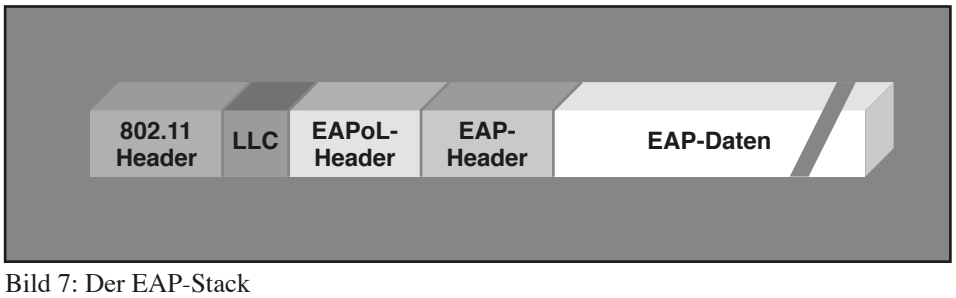


Bild 7: Der EAP-Stack

Nach Abschluss der EAP-Authentisierung haben Client und Authentisierungsserver einen gemeinsamen Sicherheitskontext aufgebaut, d.h. beide Seiten haben auf der Grundlage des verwendeten Algorithmus und der Authentisierungsdaten (wie Benutzername, Passwort, Zertifikat u.v.a.m) einen gemeinsamen geheimen Schlüssel erzeugt, ohne dass dieser jemals über das Netz ausgetauscht wurde. Der WLAN-Standard fordert für diesen so genannten EAP Master Key eine Mindestlänge von 256 Bit. Dieser Master Key wird schließlich vom Authentisierungsserver über die gesicherte Verbindung dem Access Point mitgeteilt. Damit verfügen der Wireless Client und der Access Point über ein gemeinsames, verbindungsspezifisches, je nach Verfahren sogar benutzerspezifisches Geheimnis.

Falls keine solche EAP-basierte Authentisierung über einen Authentisierungsserver konfiguriert wurde, kann die Rolle dieses EAP Master Keys auch von Pre-shared Keys übergenommen werden. Zu beachten ist hierbei, dass Pre-shared Keys in der Regel nicht verbindungsspezifisch sein werden!

EAP Master Key oder Pre-shared Key werden jetzt auf beiden Seiten als so genannter PMK (Pairwise Master Key) installiert. In dem anschließenden Schritt authentisieren sich dann Client und Access Point gegenseitig. Hierzu bestätigen sich beide über den so genannten 4-Way-Handshake, dass sie mit dem gleichen PMK arbeiten und tauschen dabei weiteres Schlüsselmaterial aus. Hieraus wird in Verbindung mit dem PMK und den MAC-Adressen beider Stationen ein temporärer, 512 Bit langer Schlüssel (Pairwise Transient Key – PTK) erzeugt, welcher letztendlich das gesamte benötigte Schlüsselmaterial für die eingesetzten Verschlüsselungsverfahren für Unicasts umfasst, also die EAPoL-Schlüssel und die Schlüssel für WEP, TKIP oder CCMP. Abschließend teilt der Access Point im Group-Key-Handshake dem Client das Schlüsselmaterial für Multicasts und Broadcasts mit.

Erst jetzt, nachdem die gegenseitige Authentisierung erfolgreich abgeschlossen wurde und alle Verfahrensschlüssel auf beiden Seiten installiert sind, schaltet der Access Point den (virtuellen) Datenport des Clients für beliebige Datenpakete frei und der Client kann mit der Kommunikation zum LAN beginnen.

Schlüsselverwaltung

Alle oben beschriebenen Verschlüsselungsverfahren beruhen also auf symmetrischen Algorithmen, das heißt Sender und Empfänger benötigen den gleichen Schlüssel zum Verschlüsseln wie zum Entschlüsseln. Dabei wird jeweils ein geheimer Startwert mit einem variablen Teil, der meist als Zähler ausgelegt ist, kombiniert, um einen paketspezifischen Schlüssel zu erhalten, der von den Verfahren letztlich benutzt wird. Tabelle 1 fasst die Schlüsseleigenschaften der Verfahren noch einmal zusammen.

Bei allen Verfahren wird der jeweils variable, paketspezifische Anteil im Klartext im Header des Pakets übermittelt. Um also identische Verfahrensschlüssel auf beiden Seiten generieren zu können, müssen irgendwann auch die geheimen Schlüssel zwischen Sender und Empfänger ausgetauscht worden sein.

Darüber hinaus war es eine der oben gestellten Anforderungen, dass niemals eine einmal verwendete Kombination ein zweites Mal wieder verwendet werden darf. Nach spätestens 2^{24} WEP-Paketen bzw. 2^{48} Paketen bei den beiden anderen Verfahren muss also ein neuer geheimer Schlüssel gewählt und ausgetauscht werden.

802.11 sieht für WEP zwei verschiedene Schlüsselarten vor, so genannte Default Schlüssel und Key-Mapping Schlüssel. Und ignoriert die Notwendigkeit Schlüssel auszutauschen völlig!

Als Default Schlüssel wird ein Satz von vier Schlüsseln definiert und mit einem Index von 0 bis 3 versehen. Zum Senden wird im Konfigurationsmenü für jede Station einer dieser vier Schlüssel festgelegt. Der Sender übermittelt im Header den Key-Index, der Empfänger weiß damit, welcher der vier Schlüssel verwendet wurde.

Tabelle 1: Schlüsselgenerierung der 802.11-Verfahren

	geheimer Schlüssel	variabler Anteil	weitere Daten	Methode zur Generierung des Verfahrensschlüssel
WEP-40	40 Bit WEP	24 Bit IV	keine	aneinander hängen
WEP-104	104 Bit WEP	24 Bit IV	keine	aneinander hängen
TKIP	64 Bit für MIC 128 Bit TK	48 Bit TSC	Source-Adresse	Hash
CCMP	128 Bit TK	48 Bit PN	Source-Adresse	AES

Die zweite Methode verwendet eine Schlüsseltabelle. In dieser Tabelle ist zu jedem Kommunikationspartner dessen MAC-Adresse und ein hierzu spezifischer Schlüssel eingetragen. Falls ein solcher Eintrag existiert, wird die gesamte Kommunikation, also Senden und Empfangen, zu bzw. von dieser MAC-Adresse mit diesem Schlüssel verschlüsselt. Diese verbindungsspezifische Variante von WEP-Schlüsseln wird allerdings von den wenigsten Produkten realisiert.

802.11i fordert nun unabhängig vom verwendeten Verschlüsselungsverfahren, dass die Stationen dazu in der Lage sind, pro direktem Kommunikationspartner einen eigenen Schlüssel bzw. Schlüsselsatz zu verwalten. In einem „normalen" ESS, also im Infrastruktur-Modus mit Access Points, betrifft dies natürlich in erster Linie die Access Points; die Clients haben – vom Roaming-Vorgang mal abgesehen – ja nur einen direkten Gesprächspartner. Leider wird diese Anforderung von vielen etablierten Geräten jedoch nicht erfüllt, sie unterstützen lediglich die vier Default WEP-Schlüssel. Dies kann zu Problemen mit den Key-Indizes führen, wenn solche Geräte TKIP/WPA und klassisches WEP gleichzeitig unterstützen.

Als Schlüsselaustauschverfahren sieht der neue 11i-Standard den oben eingeführten 4-Way-Handshake über das im IEEE-Standard 802.1x bzw. dessen Nachfolger 802.1aa definierte Protokoll vor. Im Anschluss an die Authentisierung über den 4-Way-Handshake haben nämlich beide Stationen einen sessionspezifischen PTK etabliert, dem alle Schlüssel für die einzelnen Verfahren entnommen werden. Diesen 4-Way-Handshake können beide Stationen nach beliebigen Kriterien, zum Beispiel zeitgesteuert neu initiieren und damit neue Verfahrensschlüssel vereinbaren.

Drei-Klassen-Gesellschaft

Mit den oben beschriebenen Verfahren zur Verschlüsselung, Authentisierung und zum Schlüsselaustausch sind also wenigstens drei verschiedene Sicherheitsarchitekturen am Markt, nämlich:

1. „klassische" Produkte, die ausschließlich WEP unterstützen
2. WPA-Produkte, hier ist TKIP als Standardverfahren vorgeschrieben
3. zukünftige Hardware, die CCMP voraussetzt.

Innerhalb dieser groben Klassifizierung gibt es natürlich noch weitere Unterschiede, so muss man zwischen WEP mit 40-Bit-Schlüsseln und WEP mit 104-Bit-Schlüsseln unterscheiden, bei TKIP und WEP wird es Produkte geben, die Key-mapping Schlüssel verwalten können, und solche, die es nicht können, und es sind weitere, herstellerspezifische Verfahren in einigen Produkten implementiert.

Damit ist es notwendig geworden, dass sich jeder Client mit dem Access Point darüber einigt, welches Verfahren gemeinsam eingesetzt wird. Da darüber hinaus ein Access Point unterschiedlich intelligente Clients gleichzeitig verwalten kann, muss ein weiteres Verfahren als kleinster gemeinsamer Nenner zur Übertragung von Multicasts und Broadcasts festgelegt werden. Diese Vereinbarungen werden unmittelbar, nachdem ein Client einen Access Point gefunden hat, getroffen. Hierzu gibt es ein neues Informationselement, welches in allen Beacons und den Association-Frames übertragen wird. In diesem Informationselement teilt eine WLAN-Station mit, welche Verschlüsselungs- und Authentisierungsverfahren sie unterstützt. Neben den standardisierten Verfahren können hier beliebige weitere, auch proprietäre Verfahren angekündigt werden.

Ein Client kann also anhand der regelmäßig ausgesandten Beacons erkennen, welche Verfahren der Access Point unterstützt und damit welche Sicherheitsstufe dieser Access Point erreicht. Somit kann sich der Client neben der ebenfalls übermittelten technischen Merkmale und der SSID auch anhand dieser Sicherheitsinformationen entscheiden, ob er mit dem Access Point Kontakt aufnehmen will oder nicht. Entscheidet er sich für die Kontaktaufnahme, muss er jetzt seinerseits dem Access Point mitteilen, welche Verfahren er selbst unterstützt, und auch der Access Point kann entscheiden, ob er die Anfrage annimmt oder zurückweist.

Hierbei ist es nicht allein wichtig, ein von beiden Seiten gemeinsam (technisch) unterstütztes Verfahren zu finden, sondern auch ein Verfahren auszuwählen, welches der Sicherheitspolitik beider Seiten genügt!

So kann es beispielsweise sinnvoll sein, dass ein Client die Verbindungsaufnahme zu einem Access Point ablehnt, weil dieser außer den starken Verschlüsselungsmethoden eben auch noch WEP unterstützt. Ein solcher Access Point kann leicht kompromittiert werden und dies könnte die Sicherheitspolicy des Clients verletzen.

An dieser Stelle haben wir jedoch die rein technischen Merkmale des Protokolls verlassen und sind bei der Frage angekommen, was die Konfigurationstools der einzelnen Produkte leisten werden. Gerade für die Übergangszeit, in der klassische WEP-Produkte mit neuer AES-Hardware gleichzeitig unterstützt werden, ist die Konfiguration einer detailreichen Sicherheitspolicy unumgänglich.

Fazit und Empfehlungen

Mit WPA ist die zweite Generation Sicherheitstechnik in WLANs am Start. Die Liste zertifizierter Produkte umfasst zurzeit 18 Hersteller, Tendenz wachsend. Damit hat WEP endgültig ausgedient; um jetzt noch Produkte zu kaufen, die kein WPA unterstützen, braucht man schon sehr spezielle Argumente. Aber WPA ist nicht der Weisheit letzter Schluss. Insbesondere bei nachgerüsteten Access Points wird man genau hinterfragen müssen, welche Produktmerkmale tatsächlich unterstützt werden. Die gleichzeitige Einbindung von WPA- und WEP-Clients auf solchen Geräten könnte zu Problemen führen.

WPA schließt sicherlich die größten und meisten Sicherheitslücken von WEP, aber WPA bleibt eine aufgepfropfte Notlösung, der Hashalgorithmus „Michael“ ist weitgehend unbekannt und wenig untersucht. Konsequenterweise wird man beim Erwerb neuer Produkte darauf achten, dass das AES-basierte CCMP (eventuell bald unter der Bezeichnung WPA-2?) unterstützt oder zumindest vorbereitet ist. Der Umstieg auf CCMP wird nicht in Software machbar sein, dafür braucht man andere Chips, die es jedoch bereits gibt.

WPA und die Nachfolgeprodukte brauchen eine 802.1x-fähige Infrastruktur. Damit ergibt sich die große Gelegenheit, eine zentrale, plattformübergreifende Benutzerverwaltung zu schaffen, die nicht nur für Wireless LANs sondern auch in vielen anderen Bereichen riesige Vorteile mit sich bringt, gerade in Zeiten der Konsolidierung.

Wenn mit 802.11i tatsächlich das Ende der Sicherheitsdiskussion kommt, werden wieder andere Produktmerkmale im Vordergrund stehen. Als Beispiele seien hier genannt: zentrales Management, Wireless Switche und natürlich die Konkurrenz zwischen 11g und 11a.

Als enttäuschend ist zu vermerken, dass weiterhin alle Management- und Controlframes unverschlüsselt übertragen und somit auch unentdeckt gefälscht werden können. Ebenso bleibt nach wie vor der unverschlüsselte Übertragungsmodus der Defaultmodus, das heißt fabrikneue Geräte werden zunächst unverschlüsselt kommunizieren. Damit liegt es in der Hand und in der Verantwortung des Netzbetreibers, seine WLANs geeignet zu sichern. Die Mittel hierzu stehen ihm mit dem neuen Standard 802.11i zur Verfügung, Migrationspfade gibt es sehr viele, aber:

> Solange noch WEP-Clients unterstützt werden, ist man sicherheitstechnisch nicht einen einzigen Schritt vorangekommen.

Literatur

[1] Wi-Fi Protected Access (WPA), Version 2.0, Wi-Fi Alliance, April 2003

[2] IEEE Std. P802.11i/D5.0: Medium Access Control (MAC) Security Enhancements, August 2003

[3] IEEE Std. 802.11, ISO/IEC 8802-11: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, August 1999

[4] IEEE Std. 802.11a-1999: High-Speed Physical Layer in the 5 GHz Band, September 1999

[5] IEEE Std. 802.11b-1999: Higher-Speed Physical Layer Extension in the 2,4 GHz Band, September 1999

[6] Cornelius Höchel-Winter: Sicherheit in Wireless LANs, Technologie Report der ComConsult Technologie Information GmbH, Oktober 2002

[7] Scott Fluhrer, Itsik Mantin, Adi Shamir: Weaknesses in the Key Scheduling Algorithm of RC4

[8] A. Roos: A Class of Weak Keys in the RC4 Stream Ciper

[9] Simon Hoff, Gaby van Laak, Joachim Wetzlar, Cornelius Höchel-Winter: Wireless LAN Antennenguide, Technologie Report der ComConsult Technologie Information GmbH, Juli 2003

[10] FIPS PUB 197: Advanced Encryption Standard (AES), NIST, November 2001

[11] IETF RFC3610: Counter with CBC-MAC (CCM), September 2003

[12] FIPS PUB 113: Computer Data Authentication, NIST, Mai 1985

[13] IEEE Std. 802.1X: Standard for Port based Network Access Control, Januar 2001

[14] Markus Schaub: Port Based Network Access Control: 802.1x - Der Wächter am Tor zum Netz, Der Netzwerk Insider, Dr. Suppan International Institute, November 2001

[15] IETF RFC 2284: PPP Extensible Authentication Protocol (EAP), März 1998

[16] http://sourceforge.net/projects/wepcrack/

CCNE

ComConsult Certified Network Engineer

Lokale Netze
- **10.11. - 14.11.03 Aachen**
- **02.02. - 06.02.04**

TCP/IP und SNMP
- **08.12. - 12.12.03 Berlin**
- **02.02. - 06.02.04 Bonn**

Internetworking
- **08.12. - 12.12.03 Aachen**
- **02.02. - 06.02.04 Aachen**

Ethernet Technologien – neuester Stand
- **08.12. - 12.12.03 Aachen**
- **08.03. - 12.03.04 Aachen**

Paketpreis für alle vier Seminare: € 6.690,-- zzgl. MwSt.
(Einzelpreise: € 1.990,--/€ 2.290,--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
- **17.11. - 21.11.03 Aachen**
- **02.02. - 06.02.04 Aachen**

Trouble Shooting in geswitchten Ethernet-Umgebungen
- **10.11. - 14.11.03 Aachen**
- **01.03. - 05.03.04 Aachen**

Trouble Shooting für TCP/IP-und Windows-Umgebungen
- **03.11. - 07.11.03 Aachen**
- **19.01. - 23.01.04 Aachen**

Paketpreis für alle 3 Seminare mit Sniffer-Lizenz:
€ 7.500,-- zzgl. MwSt. (Seminar-Einzelpreise: je € 2.490,--)

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

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I:
Von den Einzelbausteinen zur integrierten Lösung
- **24.11. - 28.11.03 Berlin**
- **01.03. - 05.03.04 Köln**

Sicherheitslösungen II:
IP-VPNs, der Kern einer Sicherheits-Infrastruktur
- **08.12. - 10.12.03 Bonn**
- **22.03. - 24.03.04 Bonn**

Sicherheitslösungen III:
Planung und praktische Konfiguration
- **01.12. - 05.12.03 Aachen**
- **19.04. - 23.04.04 Aachen**

Paketpreis: € 4.990,-- zzgl. MwSt.
(Einzelpreise: € 1.690,-- / € 2.290,--)

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

Impressum

Verlag:
Dr. Suppan International Institute b.v.
Ahornenlaan 12
4493 DG Kamperland, Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan

Gestaltung:
Zweipfennig

Erscheinungsweise:
Monatlich, 12 Ausgaben im Jahr

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

Für unverlangt eingesandte Manuskripte
wird keine Haftung übernommen