Dr. Suppan International Institute

Der Netzwerk Insider

November 2001

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Port Based Network Access Control 802.1X – Der Wächter am Tor zum Netz

von Markus Schaub

Ein weit verbreiteter Irrglaube in der Netzwerkszene besagt, dass man in einem dedizierten (= zu 100% geswitchten) Netz einem Angreifer wenig Angriffsfläche anbietet, da er keine Pakete zu sehen bekäme, wenn er sich nicht zuvor an der Domäne anmeldet. Richtig ist allerdings, dass man eine ganze Menge zu sehen bekommt, wenn man sich einfach nur an einen Switchport hängt und "nur" mitsniffert. Zwar sieht man keine Passwörter, aber in relativ kurzer Zeit kann man sich anhand der empfangenen Broadcasts ein sehr genaues Bild über die Topologie des Teilnetzes machen, die Server und somit die Angriffspunkte lokalisieren.

Bewacht das Tor zum Netz: 802.1X

Auch gibt es Verfahren manche Switches dazu zu bringen, alle Frames auf allen Ports herauszugeben, womit auch Passwörter wieder mitgesniffert werden können (Stichwort: MAC Adress-Flooding).

Es wäre also wünschenswert, wenn man die Userauthentifizierung vom Server auf den Eintrittspunkt in das LAN vorverlagern könnte: auf den Switchport, so wie man es beim Remote Zugang bereits tut.

Genau das versucht eine neue Erweiterung der IEEE mit Namen "Port based Network Access Control" oder IEEE802.1X.

weiter Seite 7

Zum Geleit

Wireless, Sicherheit und Gigabit: die Trends der nächsten Monate

Natürlich beobachten wir für Sie sehr aufmerksam die Marktentwicklung. Dazu zählen regelmäßige Arbeitstreffen mit den diversen Herstellern sowie die sorgfältige Analyse der Preis- und Produktveränderungen. Die Marktsituation des Jahres 2002 zeigt sich einigermaßen klar.

Im Moment kristallisieren sich mehrere Schwerpunktentwicklungen im Markt immer stärker heraus:.

- Etagen-Switch-Systeme auf Layer-2-Basis werden immer preiswerter, der Trend geht in Richtung 50 DM pro Port bis Ende nächsten Jahres. Reaktion der Hersteller: Aufsplittung in differenzierte Gerätetypen: ein Standard-Low-Cost-Gerät, das alle normalen L2-Verfahren abdeckt und ein höher funktionales, aber teureres Spezialgerät, das beispielsweise optimaler in Policy-Konstrukte integriert werden kann. Gutes Beispiel: Enterasys, ebenso CISCO
- Layer-3-Switch-Systeme fallen im Preis. Alle Hersteller arbeiten an kleineren Entry-Level-Systemen, um den Einstiegspreis deutlich zu senken. Auch diese Entry-Systeme werden OSPF unterstützen. In den nächsten Monaten werden wir hier vielfältige Angebote erwarten können. Layer-3 wird damit für kleinere und mittelständische Unternehmen geöffnet
- Gigabit ist einer der Megatrends des Jahres 2002. Sind bereits heute nahezu alle Backbone-Planungen Gigabit-Planungen, so ist der Einsatz von Gigabit am Endgerät und am Server noch eher selten. Dies wird sich ändern. Der Einsatz von Gigabit an High-end-Servern ist zwangsläufig erforderlich, da diese den Durchsatzbedarf haben. Spätestens mit der Etablierung der neuen 64 Bit Prozessoren von AMD und Intel kommt der Durchbruch in der Fläche. Der Einsatz von Gigabit am Endgerät wird als Standardlösung noch bis 2003 auf sich warten lassen. Die Kosten der Adapterkarten liegen zur Zeit bei mehreren Anbietern um die 300 DM (zzgl. MwSt.) und werden in 2002 voraussichtlich unter 200 DM fallen. Erst ein Absacken auf die 100 DM-Schwelle wird die normative Kraft des Faktischen aktivieren und zu einer starken Mengenausdehnung führen. Größter monetärer Engpass ist der Versorgungsswitch. Hier explodierte in den letzten 4 bis 6 Wochen der Ankündigungsmarkt von nahezu allen Anbietern. Die Portpreise der Etagen-Switch-Systeme für Twisted Pair gehen deutlich im Trend unter die 500 DM, ein weiterer Preisverfall auf das Niveau von 300 DM in 2002 ist nicht auszuschließen. Damit ließe sich gegen Ende 2002 ein Gigabit-Anschluss am Endgerät in der Summe aus Adapter und Portkosten für unter 500 DM realisieren. Für Highend-Workstations sicher eine akzeptable Größenordnung, für den "normalen" PC noch zu teuer.

weiter Seite 2

Wireless, Sicherheit und Gigabit: die Trends der nächsten Monate

Fortsetzung von Seite 1

- Seit dem 11. September wird das Thema Sicherheit wieder häufiger diskutiert. Alle sind sich über die hohen Risiken einig, doch unternommen wird vergleichsweise wenig. Zu viele organisatorische Hürden verhindern eine rasche und vor allem konfliktfreie Umsetzung von Sicherheitskonzepten. Allerdings entwickelt sich das Thema im technischen Bereich gerade in Bezug auf Sicherheit innerhalb unserer Netze in großen Schritten weiter. IEEE 802.1x, Mail- und System-Sicherheit mit Verschlüsselung und Zertifikaten sowie VPN-Technologien sind die Träger einer neuen Welle von Sicherheitsprodukten,

die uns in den nächsten Monaten von mehreren Herstellern ins Haus stehen. Auch Windows XP ist ein Schritt in diese Richtung. Die Möglichkeiten, die sich uns damit auf der technischen Seite bieten, erlauben Sicherheit auf einem hohen Niveau. Aber mit technischen Einzeltechnologien ist es leider nicht getan. Der Anwender benötigt ein Rahmenkonzept, um nicht an einer Stelle sein Unternehmen bombensicher und an der anderen Stelle offen wie ein Scheunentor zu gestalten. Diese Rahmenkonzepte – wie im Grundschutzhandbuch des BSI nachlesbar, siehe www.bsi.de – sind in ihrer Unternehmens-spezifischen Erstellung aufwendig und zeitintensiv. Allein die notwendige Diskussion mit dem Betriebsrat kann locker ein bis zwei Jahre erfordern. Hier kann immer wieder nur betont werden: die heute bestehenden Risiken auch im Bereich der Betriebsspionage sind sehr hoch. Wer heute noch unverschlüsselt im Internet wichtige Daten überträgt, handelt unverantwortlich. Wer heute noch sein Lokales Netzwerk wie eine öffentliche Infrastruktur mit Party-Charakter (kommt nur alle rein) betreibt, missachtet wissentlich die bestehenden Risiken. Von daher bleibt kein anderer Weg als der Einstieg in ein Sicherheits-Gesamtkonzept

- Letzter Megatrend sind Wireles LANs. Hier rollt eine riesige und sehr dynamische Lawine. Im Jahr 2002 wird neben den heute verfügbaren Lösungen noch die 22 Mbit/s-Version verfügbar sein und auch die IEEE 802.11a-Lösung mit 54 Mbit/s wird bis dahin, wenn die Auflagen von ETSI zum Power-Management etc. erfüllt sind, verfügbar sein. Die Preise der angebotenen Produkte gehen dabei weit auseinander. Während immer mehr Einstiegsprodukte mit Antennen im 500 DM-Bereich und PCMCIA-Adapter im Trend auf 200 DM erscheinen, werden auf der anderen Seite für die Highend-Produkte im Antennenbereich immer noch bis zu 4000 DM und für die Adapter bis zu 600 DM verlangt. Sind diese Preisunterschiede zu rechtfertigen? Antworten darauf gibt unser Wireless-Report, den sie käuflich bei der ComConsult Technologie Information erwerben können.

- Voice-over-IP ist im Moment in seiner Grundform auf Eis gelegt. Zu teuer, zu wenig Vorteile gegenüber traditionellen Lösungen. Jedenfalls solange man die Diskussion und den Produktvergleich auf CISCO und Siemens beschränkt, ein typisches Problem des deutschen Marktes. Dies gilt allerdings nicht, wenn mehr als reine Telefonie-Grundfunktionen das Ziel sind und auch Produkte anderer Hersteller in Betracht gezogen werden. Gerade für die Umsetzung von kleineren Call Center und Unified Messaging Lösungen kann Voice-over-IP auch heute schon eine wirtschaftliche und technische Alternative sein. Auf jeden Fall muss betont werden, dass VOIP nicht tot ist sondern sich nur ausruht. Sobald die Internet-Provider mit Netcologne die VOIP-Telefonie in ihrem Einzugsgebiet als kostenlosen Zusatz zum Internet-Anschluss anbieten und sobald brauchbare VOIP-Telefone fester Bestandteil von Microsoft Windows xyz sind, wird sich die Lawine wieder bewegen. Es besteht für mich keinerlei Zweifel, dass VOIP die Zukunft gehört. Auch heute wären viele interessante Lösungen möglich, nur kommen die eben – bisher – nicht zwangsläufig von CISCO und Siemens.

Sie sehen, der Markt bewegt sich trotz aller schlechten Stimmung, die seitens der Medien geradezu professionell produziert wird. Und die Themen des Jahres 2002 sind äußerst spannend. Viele der neuen Technologien sind einerseits sehr leistungsstark und andererseits sehr wirtschaftlich. Natürlich geht mit dieser Entwicklung eine immer stärkere Diversifizierung der Produkte einher. Die Produktauswahl der nächsten Jahre wird aufwendiger werden, da für ein und denselben Anwendungsbereich stark differenzierte Lösungen angeboten werden werden.

Kommen Sie zur Winterschule 2001 im Dezember in Bonn, dort werden wir diese Themen mit Ihnen diskutieren.

Ich würde mich freuen, Sie dort zu sehen

Ihr
Dr. Jürgen Suppan

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

Nachdruck,
auch auszugsweise
nur mit Genehmigung
des Verlages

© Dr. Suppan International Institute b.v.

Top-Veranstaltung

Winterschule der ComConsult Akademie 2001

Die ComConsult Akademie bietet mit der 5-tägigen "Winterschule 2001" vom 3. bis 7. Dezember im Holiday Inn in Bonn eine absolute Top-Veranstaltung mit den zur Zeit heißesten und aktuellsten Netzwerk-Themen und den Spitzenreferenten der Akademie.

In den letzten Wochen und Monaten haben sich Netzwerk-Technologien signifikant weiter entwickelt:

- wir bekommen einen neuen Spanning-Tree-Standard, der in Verbindung mit Link Aggregation und erweiterten VLAN-Standards die Frage aufwirft, ob diese Kombination einem OSPF-Design nicht überlegen ist. Was bedeuten die neuen Redundanz- und Struktur-Verfahren für die Auslegung aktueller Netzwerke? Sind jetzt bessere und gleichzeitig einfachere sowie preiswertere Strukturen möglich? Welchen Stellenwert hat dabei Layer-3-Design? Was bedeutet das für die in Zukunft einzusetzenden Switch-Systeme?

- Ethernet entwickelt sich zur universellen Netzwerk-Technologie. Was bringen die nächsten 18 Monate, welche Möglichkeiten entstehen für Sie mit den neuen Ethernet-Technologien? Wofür und an welcher Stelle wird Ethernet in Zukunft eingesetzt werden können?

- Wireless-LANs haben ihre Kinderstube verlassen, die meisten Produkte einen hohen Reifegrad erreicht. Allerdings zeigen aktuelle Produktuntersuchungen der ComConsult Technologie Information, dass sich die angebotenen Produkte zum Teil deutlich unterscheiden und bei ihrem Einsatz eine ganze Reihe von Faktoren zu berücksichtigen sind. Was leisten Wireless LANs ? Wo sind sie sinnvoll einsetzbar, wo sollten sie nicht eingesetzt werden? Wie wird der Einsatz vorbereitet, welcher Planungsaufwand entsteht? Wie sind Preisdifferenzen von mehreren 100 % zwischen den Produkten zu erklären? Ist das teurere Produkte das bessere?

- Viele neue Ergänzungs-Standards sind kurz vor der Verabschiedung, die gewaltige Auswirkungen auf unsere Netzwerke haben und viele neue Einsatzmöglichkeiten bieten.

802.1x hat das Potential, die gesamte Benutzer-Verwaltung in Netzwerken zu verändern und gleichzeitig die Sicherheit unserer Netzwerke deutlich zu erhöhen.

Stromversorgung über Twisted Pair wird viele neue Nutzungsformen für bestehende Verkabelungen bringen. Gleichzeitig haben sich die aktuellen Arbeiten an den neuen Kabel-Standards stabilisiert. Dabei sind gerade im Glasfaserbereich viele neue Ansätze zu beachten.

Was bringen diese neuen Technologie-Möglichkeiten? In wie weit senken sie die Betriebskosten, erhöhen sie die Sicherheit und die Effizienz der getätigten Investitionen? Wer sollte wann und was nachrüsten?

- Die sichere und redundante Anbindung der Server an unsere Netzwerke wird immer dringlicher. In vielen Netzwerken liegt hier die Hauptschwachstelle des Designs. Wie werden Server redundant und sicher in unsere Netzwerke integriert?

- Homenetworking, einer der wirklich noch weitestgehend unerschlossenen Märkte! Welche Alternativen bestehen für das Netzwerk im privaten Bereich, wofür wird es gebraucht, wie kann es realisiert werden, wie teuer wird es?

Mit unserer Winterschule 2001 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. Alle Referenten kommen aus der Praxis, bewerten die aktuellsten Technologien aus dem Blickwinkel eines erfolgreichen und sicheren Netzwerk-Betriebs.

Diese Veranstaltung setzt Netzwerk-Kenntnisse voraus und ist nicht für Einsteiger geeignet!

Aktuelles Seminar

Winterschule der ComConsult Akademie 2001
Die Inhalte

Montag, 03.12.01
Technologische Entwicklung und die Zukunft von Ethernet
- Rahmenbedingungen: Was müssen Netzwerke zukünftig leisten?
- 10 Gigabit Ethernet
- Ethernet First Mile
- Ethernet als WAN-Standard
- Optische Netzwerke

(Dr. Franz-Joachim Kauffels)

Dienstag. 04.12.01
Redundanz- und Struktur-Technologien: was bringen die neuen Standards, wo stehen die traditionellen Technologien?
- Anforderungen an Redundanz
- Schwachstellen der alten Standards
- Der neue Spanning Tree Standard: Was leistet er, wie komplex ist er?
- Ling Aggregation + neuer Spanning Tree besser als OSPF?
- Der neue VLAN-Standard: Was ändert sich? Sind VLANs jetzt beherrschbar?
- Wo steht OSPF in Kombination mit VRRP/HSRP?
- Wo steht Layer-3-Design?
- Vergleich der neuen Möglichkeiten an einem Beispiel
- Konsequenzen und Empfehlungen

(Markus Schaub, ComConsult Akademie)

Mittwoch, 05.12.01 und Donnerstag, 06.12.01
Neue Normen und Technologien sinnvoll nutzen
- IEEE 802.1x und Radius: die neue Benutzerverwaltung im LAN
- Stromversorgung über Twisted Pair: Wie funktioniert es, was kann man alles damit machen?

(Markus Schaub, ComConsult Akademie)

- Wireless LANs: Wie arbeiten sie, wo können sie eingesetzt werden, wo nicht, wie wird ihr Einsatz geplant?
- Multimedia-Übertragung im Netzwerk: Video-Signale im Netzwerk verbreiten
- Home-Networking: Netzwerktechnologien in den Haushalten

(Dr. Jürgen Suppan, Dr. Suppan International Institute)

- Voice-over-IP letzter Stand: Wie funktioniert es, wofür sollte es eingesetzt werden, wo steht der Markt?

(Dipl.-Ing. Roland Moos, ComConsult Akademie)

- Verkabelungs-Technologie letzter Stand: Was bringt die neue Norm? Wo steht die Twisted Pair Verkabelung? Schirmung: ja oder nein? welcher Stecker? Wo steht die Glasfaser? Welche Faser für die Zukunft? Welcher Stecker? Welche Entfernungen? Messtechnik.

(Dipl.-Ing.Hartmut Kell, ComConsult Beratung und Planung)

Freitag, 07.12.01
Optimale Server-Anbindung ans Netzwerk
- Zielsetzung, Alternative Lösungsmöglichkeiten, Beispiele und Technologie-Vergleiche

(Dr. Behrooz Moayeri, ComConsult Beratung und Planung)

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Winterschule
der ComConsult Akademie 2001

☐ Ich melde mich an zur
Winterschule der ComConsult Akademie 2001
vom 03.12. - 07.12.01 in Bonn
zum Preis von EUR 2.290,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Holiday Inn Bonn

von _____ bis _____
(Übernachtung/Frühstück DM 199,--)

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

Sonderseminar

EMV in Anlagen und Systemen

Am 12. und 13. Dezember 2001 veranstaltet die ComConsult Akademie im Holiday Inn in Bonn das Sonderseminar "EMV in Anlagen und Systeme".

Zum Thema

EMV-Sicherheit hat sich in den letzten Monaten zu einem Schlüsselthema der Netzwerk-Technologien entwickelt. So werden zur Zeit bei den meisten Verkabelungsprojekten massive Fehler gemacht, die sich später in Störungen aller vorhandenen Geräte, in stark erhöhten Bitfehlerraten und in einer Gesundheitsbedrohung beteiligter Personen darstellen können. Wir gehen zum Beispiel für bestehende Verkabelungen davon aus, dass mehr als die Hälfte aller Installationen schwere Fehler im Bereich der Erdung der Kabel und Verteilerschränke aufweist. Gleiches gilt für den Bereich der korrekten Behandlung der Schirme von geschirmten Twisted Pair Kabeln. Auch eine im Sinne des Gesetzgebers erforderliche Abstrahlsicherheit dürfte häufig nicht gegeben sein. Die Konsequenzen können bis zur sofortigen Stillegung des gesamten Netzwerk-Betriebs reichen.

GHMT-Fünf-Säulen-Modell

Die neuen Kabelstandards, insbesondere der EN 50174 und die parallel laufende Verschärfung der EMV-Standardisierung innerhalb der EG machen eine Auseinandersetzung mit dem Thema EMV unvermeidbar.

Das Seminar wendet sich an die Betreiber und Errichter sowie Planer und Installateure von Netzwerken und Rechenzentren sowie Gebäuden mit ausgedehnten technischen Ausrüstungen. In diesem Seminar lernen Sie, welche Einflüsse Umgebung, Verkabelung, Energieversorgung und Geräte auf die EMV Ihres Systems haben und zu welchem Zeitpunkt sie beachtet und eingeplant werden müssen.

Das Seminar wird von den Spezialisten der Firma durchgeführt, die in den letzten Monaten mit ihren fundierten Messergebnissen für erhebliche Furore und Unruhe im gesamten Kabelmarkt gesorgt hat. Die Firma GHMT ist zugleich intensiv am Normungsgeschehen beteiligt und informiert direkt von der Quelle über zu erwartende Verschärfungen der Gesetzeslage.

Dieses Seminar vermittelt in zwei Tagen herstellerneutral und kompetent die fachmännische Berücksichtigung des Themas EMV in Neubau- und Umbauprojekten.

Die Teilnehmer werden sensibilisiert für die Einflüsse anderer Gewerke auf ihre Anlagen (z.B. Erdung → IT-Netzwerk) und auf den Menschen und sie erhalten wichtige Hinweise zum Management der EMV in Projekten.

Referent und geschäftsführender Gesellschafter der GHMT: Dipl.-Ing. Dirk Wilhelm

Die Grundlagen der Wirkungsmechanismen werden dabei ebenso erläutert, wie Haftungsrisiken bei Nichtbeachtung der bekannten Bedrohungsgröße.

Durch Einführung eines Fünf-Säulen-Modells wird die Komplexität der Systemwirkung aufgebrochen und Spekulationen über für und wider bestimmter Konzepte (z.B. sternförmige vs. vermaschte Erdung oder ein- bzw. beidseitige Schirmung) werden aufgeklärt. Auch werden die geeigneten Maßnahmen zur Umsetzung in der Praxis aufgezeigt.

Der Referent, Dipl.-Ing. Dirk Wilhelm ist geschäftsführender Gesellschafter der GHMT – Gesellschaft für Hochfrequenz-Messtechnik mbH , die seit ihrer Gründung im Jahre 1992 als neutraler und unabhängiger Dienstleister auf dem Gebiet der Datennetzwerktechnik tätig ist. Als Laboringenieur für HF- und EMV-Messungen ist sein Spezialgebiet die Erstellung von Systemanalysen und Konzepten. Er ist Mitglied der CENELEC TC46X WG 3, der ISO / IEC TC46 WG 5 und im Power Line Telecommunication Forum.

EMV in Anlagen und Systemen

EMV in Anlagen und Systemen

Inhaltlicher Aufbau

Grundlagen der EMV, Störbeeinflussungsmodell, wichtige Begriffe

Anwendbarkeit der EMV-Gesetzgebung, Normung, Haftungsrisiken

Einfluss elektro(-/) magnetischer Felder und Wellen auf den Menschen (EMVU, Elektrosmog)

EMV als Systemeffekt, das GHMT-Fünf-Säulen-Modell
- Modularer und globaler Ansatz professionell anwendbar?

Elektromagnetische Umgebung
- Einteilung in Industrie- und Bürobereich noch zeitgemäß?
- Typische und besondere Störquellen
- Frequenz- und Pegelschema als Werkzeug zur Abschätzung des Risikos
- Intersystem-EMV (Schutzabstände von Mobilfunksystemen)

Aktive Komponenten
- Typische Anforderungen an Störaussendung/Störfestigkeit für CE-Kennzeichnung
- Besondere Anforderungen bei besonderen Umgebungsbedingungen
- Wird der Einfluss der Verkabelung bei Herstellertests ausreichend berücksichtigt?
- Fallbeispiel: Ungeschirmte vs. geschirmte Verkabelung

Energieversorgung, Erdung und Massung
- Problematik bei 4- und 5- Leitersystemen, welches ist die geeignete Lösung?
- Auftrennung in Funktions- und Betriebserde noch zeitgemäß?
- Einseitige oder beidseitige Schirmauflegung?
- Sternförmige oder vermaschte Erdung, welches Konzept für welches System?
- Realisierungsbeispiele Alt- und Neubauprojekte

EMV- gerechter Blitzschutz
- Was sind die Unterschiede zwischen konventionellem und EMV-gerechtem Blitzschutz?
- Charakteristische Kenngrößen des Blitzes
- Ist ein Blitzeinschlag überhaupt wahrscheinlich?
- Von der Risikoanalyse zum effizienten Schutzkonzept
- Wie vermeidet man Schleifenflächen?
- Realisierungsbeispiele Alt- und Neubauprojekte

Kabelinfrastruktur
- EMV-relevante Parameter der Verkabelung
- Grenz- und Messwerte typischer Parameter und Kabelarten
- Trassierung und Ausführung von Tragsystemen

Der Veranstalter behält sich Änderungen im Programm vor.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Sonderseminar
EMV in Anlagen und Systemen

☐ Ich buche das Sonderseminar **EMV in Anlagen und Systemen** vom 12.12.- 13.12.01 in Bonn zum Preis von EUR 1.290,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Holiday Inn, Bonn (Übernachtung/Frühstück DM 199,--)

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name _____ Vorname _____

Firma _____ Abteilung _____

Position _____ Funktion _____

Straße _____ PLZ, Ort _____

Telefon _____ Fax _____

eMail _____ Unterschrift _____

Port Based Network Access Control 802.1X - Der Wächter am Tor zum Netz

Fortsetzung von Seite 1

Aktuell verfügbare Kontrollen

Zugriffkontrolle an sich ist nichts neues, noch nicht einmal am Zugangspunkt zum Netz, am Switchport: die meisten Hersteller bieten eKontrolle auf MAC Adressbasis an, d.h. nur Rechner mit einer dem Switch bekannten MAC Adresse erhalten Zugang zum Netz. Wie ein Switch die Adresse und die Port/Adress-Zuordnung lernt, dafür gibt es viele verschiedene Möglichkeiten, ebenso wie es verschiedene Möglichkeiten gibt, was ein Switch tut, wenn eine ihm unbekannte MAC Adresse auftaucht. Wesentlich ist jedoch, dass all diese Lösungen auf der Hardwareadresse basieren und somit einem bestimmten Gerät und nicht einem User zugeordnet werden.

Auf Routingebene ist es mittels Access-Listen auch schon lange möglich nach Layer 3 Kriterien zu filtern, bedingt auch nach Layer 4, wenn man beispielsweise zusätzlich zur IP Nummer auch auf den TCP Port filterte.

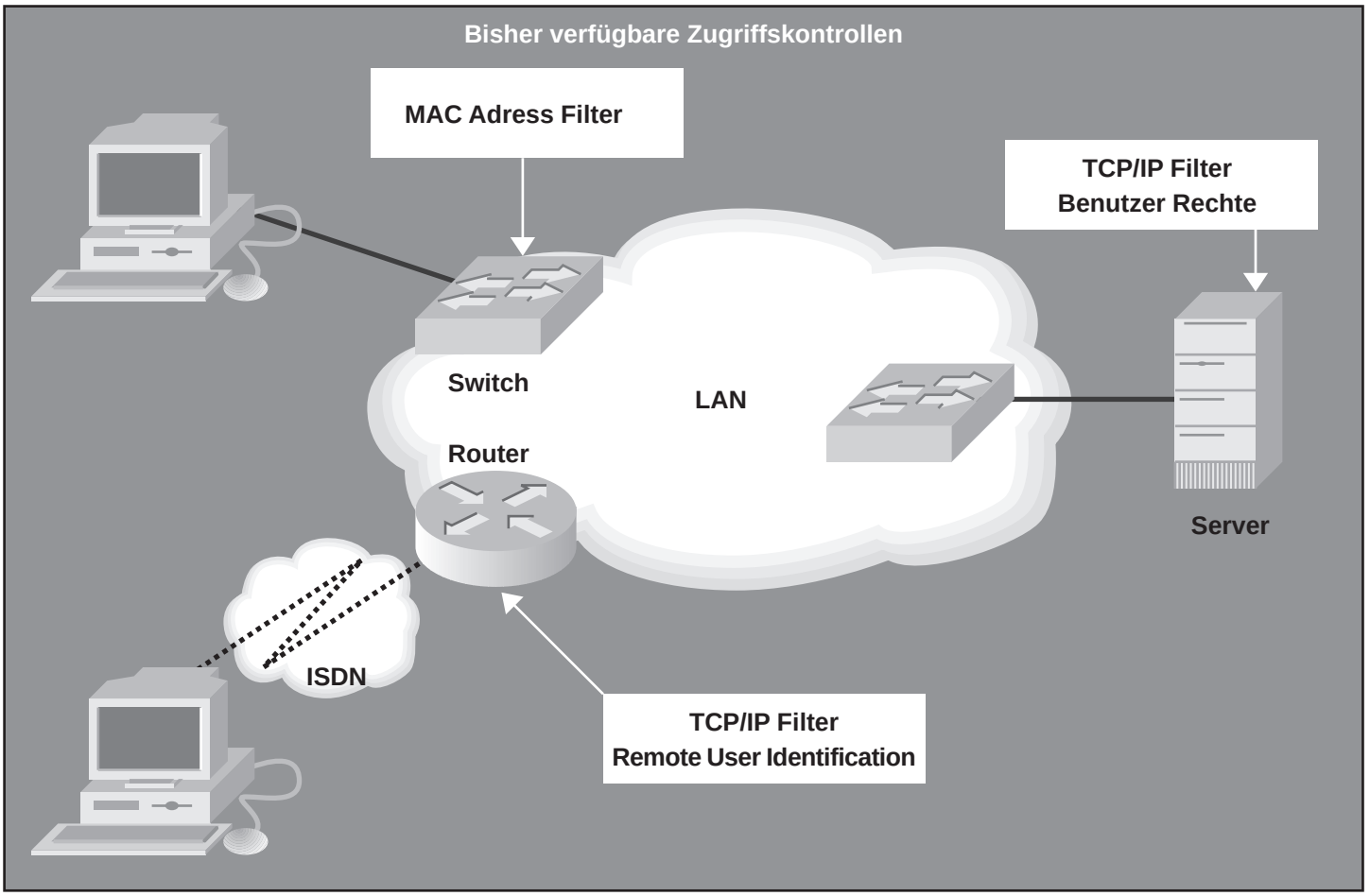
Bedingung für diese Art der Zugriffkontrolle ist jedoch, dass sich beide Systeme entweder in verschiedenen IP Netzen befinden, so dass man auf einem Router oder Layer 3 Switch filtern kann, bzw. dass am Zielgerät solche Filter gesetzt werden können. Windows 2000 wäre ein Bespiel für ein solches Endsystem mit IP Filtern.

Auf User-Ebene Rechte zu verteilen ist ein alter Hut. Nahezu jedes Betriebssystem kennt User und Gruppen, denen bestimmte Rechte eingeräumt oder verwehrt werden können.

Der Autor

Markus Schaub verfügt über langjährige Betriebs- und Praxiserfahrung mit CISCO-Routern und CISCO-Switch-Systemen. Er ist CCNP und ComConsult Certified Network Engineer. Darüber hinaus ist er für den Betrieb des CISCO-Router-Netzes der ComConsult Akademie verantwortlich.

Bild 1 Aktuell verfügbare Kontrollen



Port Based Network Access Control 802.1X - Der Wächter am Tor zum Netz

Es gibt eine Reihe von Schwächen dieser bislang verwirklichten Zugriffskontrollen. Um einige davon zu nennen:

- MAC Adressfilterung am Switch ist fehleranfällig, administrations- und wartungsintensiv. Zudem können mobile User mit Laptops kaum oder nur sehr schwer in eine solche Umgebung integriert werden.

- Sowohl MAC Adressfilter wie auch IP Filter sind meist Geräte und nicht userbezogen. D.h. ein User braucht sich nur an den PC seines Kollegen zu setzen und bekäme schon dessen Zugriffsrechte.

- Ein Angreifer bekommt in aller Regel selbst in einem geswitchten Netz schon eine ganze Menge aufschlussreicher Informationen zu sehen, wenn er nur Broadcast und Multicasts an einem Port mitsniffert, ohne sich irgendwo anzumelden (siehe Bild 2).

- Userbezogene Rechtevergabe durch Betriebssysteme hat den Nachteil, dass ein User bereits Zugriff "bis zum" Server hat, wenn ihm erst ein Weiterkommen verwehrt wird. Häufig ist es sogar so, dass man schon die angebotenen Dienste sehen kann und nur der Zugriff selbst fehlschlägt.

Ein umfassendes Sicherheitskonzept muss also wenigstens auf allen aufgeführten Arten von Schutzmechanismen beruhen, ggf. noch weiteren, je nach eingesetztem Betriebsystem oder Netzwerkumgebung. Die Mechanismen müssen einzeln konfiguriert und aufeinander abgestimmt sein, was einen erheblichen Aufwand an Konfiguration und Dokumentation bedeutet. Wünschenswert wäre also ein Konzept, bei dem die verschiedenen Schutz- und Kontrollmechanismen zusammengeführt werden. Aktuell können wir einen Trend in diese Richtung feststellen und der Standard IEEE802.1X ist ein weiterer Schritt in diese Richtung.

Ein anderer ist die Tendenz zu einem zentralen Authentifizierungsserver, anstatt dass jedes System seine eigene Berechtigungsvergabe hat. Auch wenn zur Zeit viele Authentifizierungsserver zur Auswahl stehen, so scheint sich RADIUS als Schnittstelle zwischen den verschiedenen Systemen durchzusetzen.

Im folgenden werden die beiden Standards RADIUS und 802.1X vorgestellt. Am Ende wird aufgezeigt, wie die beiden Standardprotokolle zusammenarbeiten, und es wird auf einige Besonderheiten des EAPOL Protokolls von 1X eingegangen.

RADIUS

Weder definiert der IEEE Standard 802.1X einen Authentifizierungsserver noch bezieht er sich direkt auf einen speziellen. Jedoch wird die Existenz eines solchen Servers vorausgesetzt. Da einige Teile des Verfahrens erheblich besser zu verstehen sind, wenn man die Funktionsweise eines solchen Authentication Server kennt, wird an dieser Stelle zunächst auf RADIUS (Remote Authentication Dial In User Service) eingegangen.

Auch wenn IEEE in dem Standard so oft wie möglich beschwört, dass RADIUS natürlich nicht der einzige Server ist, der als Authentication Server dienen kann, so ist allein diese permanente Wiederholung, die an den alten Cato erinnert, schon ein deutlicher Hinweis darauf, was aktuell erwartet wird. Für den Fall, dass man diese Signale nicht verstanden hat, gibt es sicherheitshalber noch einen Anhang D, in dem gleich eine Richtlinie für den Einsatz von RADIUS im Zusammenhang mit 802.1X geliefert wird.

Ferner ist bei den Herstellern festzustellen, dass RADIUS sich klar durchsetzt. Selbst Hersteller, die bislang ihr eigenes Produkt bevorzugten, implementieren in aktuellen Software-Releases immer weiterreichendere RADIUS Optionen.

Bild 2 Sniffertrace

No.	Time	Source	Destination	Protocol	Info
66	24.568529	ti1.ti-ac	ntserver1.ti-ac	SMB	SMBtdis Request
67	24.569189	ntserver1.ti-ac	ti1.ti-ac	SMB	SMBtdis Response
68	24.569593	ti1.ti-ac	ntserver1.ti-ac	SMB	SMBtdis Request
69	24.570044	ntserver1.ti-ac	ti1.ti-ac	SMB	SMBtdis Response
70	24.570420	ti1.ti-ac	ntserver1.ti-ac	SMB	SMBlogoffX Request
71	24.570823	ntserver1.ti-ac	ti1.ti-ac	SMB	SMBlogoffX Response
72	24.571527	ti1.ti-ac	ntserver1.ti-ac	SMB	SMBtdis Request
73	24.571947	ntserver1.ti-ac	ti1.ti-ac	SMB	SMBtdis Response
74	24.688671	ti1.ti-ac	ntserver1.ti-ac	TCP	1418 > netbios-ssn [ACK] Seq=487757799 Ack=3049
75	24.973230	00:e0:7b:d3:c6:27	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:e0:7b:d3:c6:27 Cost = 0
76	25.076255	managserv1.ti-ac	ff:ff:ff:ff:ff:ff	ARP	Who has 10.10.10.50 ? Tell 10.10.10.10
77	26.087667	managserv1.ti-ac	ff:ff:ff:ff:ff:ff	ARP	Who has 10.10.10.60 ? Tell 10.10.10.10
78	26.987472	00:e0:7b:d3:c6:27	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:e0:7b:d3:c6:27 Cost = 0
79	27.099150	managserv1.ti-ac	ff:ff:ff:ff:ff:ff	ARP	Who has 10.10.10.70 ? Tell 10.10.10.10
80	27.582348	1013.00a0cc5bc388	1013.ffffffffffff	IPX RIP	Response
81	28.110630	managserv1.ti-ac	ff:ff:ff:ff:ff:ff	ARP	Who has 10.10.10.80 ? Tell 10.10.10.10
82	28.879724	00:04:27:66:6c:21	01:00:0c:cc:cc:cc	CDP	Cisco Discovery Protocol
83	29.002786	00:e0:7b:d3:c6:27	01:80:c2:00:00:00	STP	Conf. Root = 32768/00:e0:7b:d3:c6:27 Cost = 0
84	29.060509	00:e0:7b:d3:c6:27	01:00:81:00:01:00	LLC	U, func = UI; SNAP, OUI 0x000081 (Unknown), PID
85	29.061304	00:e0:7b:d3:c6:27	01:00:81:00:01:01	LLC	U, func = UI; SNAP, OUI 0x000081 (Unknown), PID
86	29.122084	managserv1.ti-ac	ff:ff:ff:ff:ff:ff	ARP	Who has 10.10.10.90 ? Tell 10.10.10.10
87	29.623251	managserv1.ti-ac	10.10.10.255	NTP	NTP
88	29.623365	managserv1.ti-ac	255.255.255.255	NTP	NTP
89	29.837141	ti11.ti-ac	ff:ff:ff:ff:ff:ff	ARP	Who has 10.10.10.30 ? Tell 10.10.10.20
90	29.852193	ti11.ti-ac	ff:ff:ff:ff:ff:ff	ARP	Who has 10.10.10.40 ? Tell 10.10.10.20
91	29.950364	ti11.ti-ac	10.10.10.255	NETLOGON	SAM LOGON request from client

Trace über 5 Sekunden, ohne als User in einem Windows-Netz angemeldet gewesen zu sein

Port Based Network Access Control 802.1X - Der Wächter am Tor zum Netz

Sowohl auf dem diesjährigen Redesign-Forum der ComConsult Akademie wie auch in Arbeitstreffen äußerten Hersteller die Hoffnung, noch in den kommenden Monaten Softwareupdates auf den Markt zu bringen, die eine Netzwerkauthentisierung mittels 802.1X in Kombination mit einem RADIUS Server unterstützen.

Parallel dazu versucht selbst ein Hersteller wie Microsoft seine eigene Remote-User-Authentifizierung über RADIUS zur Verfügung zu stellen. Es gibt einen eigenen RFC, in dem Microsoft RADIUS Erweiterungen vorschlägt, um das hauseigene Einwahlauthentifizierungsprotokoll MS-CHAP durch RADIUS abwickeln zu können. Im Zusammenhang mit 802.1X ist es folglich unerlässlich sich mit RADIUS zu beschäftigen.

RADIUS ist bereits ein "alter" Standard der IETF und streng genommen handelt es sich bei RADIUS nicht um einen Server sondern um ein Protokoll des Application Layers, vergleichbar also mit SNMP. Die Arbeitsgruppe zu RADIUS bei der IETF ist schon seit einigen Monaten geschlossen und die aktuellen Arbeiten werden von der AAA (Authentication, Authorisation und Accounting) Gruppe fortgesetzt. Aktuell kann man RADIUS als erprobten und weitverbreiteten de-facto Standard ansehen, der sich im Rahmen der Implementierung von 1X wohl noch weiter ausbreiten wird.

Das Protokoll zeichnet sich wie im Folgenden auch das Extensible Authentication Protocol (EAP) dadurch aus, dass es nahezu beliebig erweitert werden kann. Und, ebenfalls analog zu EAP, wurde es nicht für 1X entwickelt, sondern wird heute einfach an die Bedürfnisse des IEEE Standards angepasst. Zudem ist es "einfach", also leicht zu implementieren, sowohl auf Komponentenseite wie auch bei der Severprogrammierung. Ursprünglich suchte man nur eine Möglichkeit, einen Remote User bereits bei der Einwahl bei einem Internet Service Provider zu authentifizieren und die dafür notwendigen Daten im Unternehmen zu verwalten anstatt auf dem Einwahlknoten. Aus diesem Grund wurde RADIUS geschaffen: ein Client/Server Protokoll, bei dem auf einem Server userbezogene Daten zur Authentisierung und Einwahlkonfiguration gespeichert werden und ggf. über Proxies an den Einwahlknoten übermittelt werden.

Eine komplette Betrachtung der Möglichkeiten von RADIUS würde den Rahmen eines einzelnen Artikels sicher sprengen, weshalb hier nur der grundsätzliche Kommunikationsablauf für die Authentifizierung beschrieben wird.

Begriffe

Unglücklicherweise werden von RADIUS und 802.1X unterschiedliche Begriffe für die selben Funktionen gewählt. Weil Veröffentlichungen häufig die Begriffe des Protokolls benutzen, auf das sie sich beziehen, werden in diesem Artikel beide Varianten kurz eingeführt und im jeweiligen Umfeld auch benutzt.

Zunächst zu den Rechnersystemen, die für RADIUS von Bedeutung sind:

Peer

Als Peer bezeichnet die IETF das System, das Zugang zu einem Dienst wünscht. Mit anderen Worten, das Einwahlsystem bzw. den User.

Network Access Server (NAS)

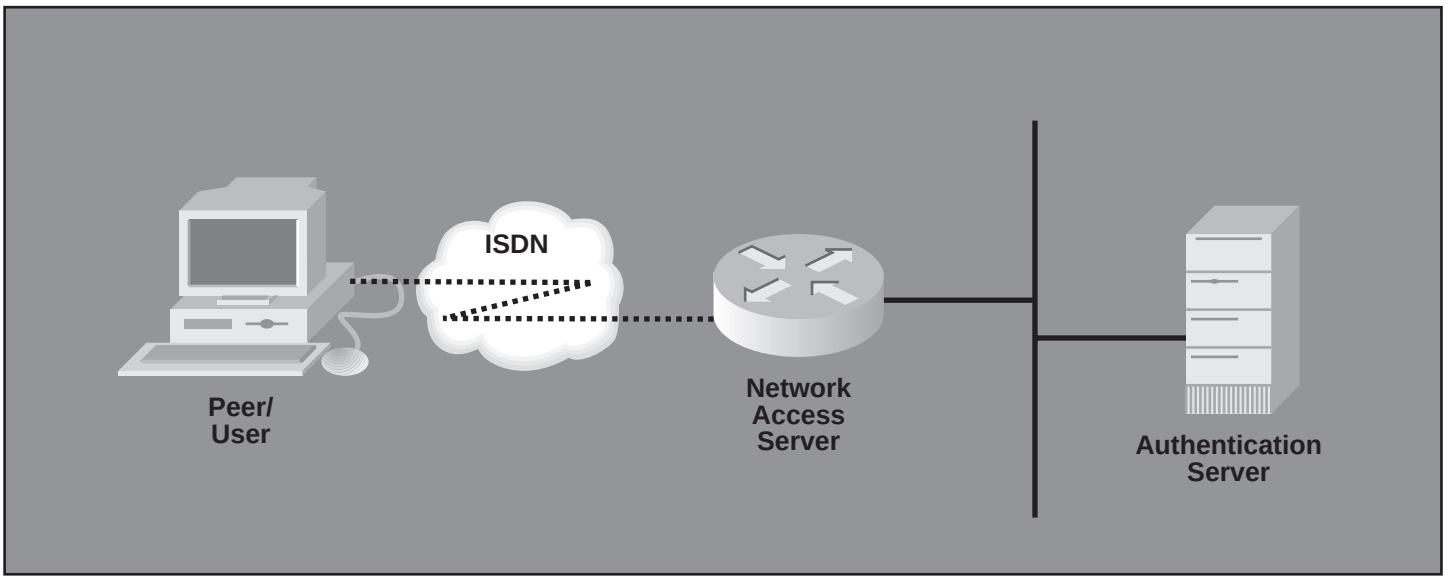
Der NAS ist der Zugangspunkt zu einem Netzwerk. Dies ist häufig ein Router mit einem WAN Interface wie ISDN oder Modem. Grundsätzlich kann es sich aber natürlich auch um einen "klassischen" Server handeln (vgl. Remote Access Server "RAS" bei Microsoft), im Folgenden auch Einwahlknoten genannt.

Authentication Server

Auf dem Authentication Server werden zentral die Authentifizierungsdaten gespeichert. Die vom Peer/User übermittelten Userdaten werden vom Server mit den Daten seiner Datenbank verglichen und anschließend wird der NAS über das Ergebnis informiert. Wird das RADIUS Protokoll benutzt, wird dieser Server auch als RADIUS Server bezeichnet.

Es werden ferner drei Aufgabengebiete unterschieden: Authentication, Authorisation und Accounting. Häufig werden diese drei Funktionen als AAA zusammengefasst. RADIUS stellt als Standard zunächst nur Funktionen und Parameter zur Authentisierung zur Verfügung. Einige wenige wurden auch für die Autorisierung standardisiert, der Accounting-Bereich ist nur "informational". Doch was verbirgt sich nun eigentlich hinter den Begriffen?

Bild 3 Systeme bei Radius



Port Based Network Access Control 802.1X - Der Wächter am Tor zum Netz

Authentication

Zu Deutsch: Authentifizierung. Hiermit ist der Vorgang der Überprüfung eines Remote Users gemeint. Praktisch bedeutet das, dass bestimmte Parameter wie Username und Passwort (ggf. auch weitere wie Telefonnummer, IP Nummer...) überprüft werden. Anschließend wird dem User der Zugang zum Netzwerk, einem Server oder anderen Komponenten wie Routern und Switchen ge- oder verwährt.

Authorisation

Der Zugang zu einem Device ist nur die erste Stufe einer Sicherung eines Netzwerks bzw. einer Komponente. Authorisation bedeutet, dass dem User auch bestimmte Rechte eingeräumt werden. Wenn man einen User beispielsweise einen Telnet-Zugriff auf einen Router gewährt, bedeutet das noch nicht, dass man ihm auch gleich sämtliche Möglichkeiten der Konfiguration geben möchte. Vielleicht handelt es sich um einen Mitarbeiter eines Leitstandes, der nur die Funktionalität der Komponenten überprüfen soll, nicht aber Änderungen der Konfiguration vornehmen darf.

Accounting

Getreu dem Motto "Vertrauen ist gut, Kontrolle ist besser" möchte man auch mitprotokollieren, was ein User macht. Diesen Vorgang nennt man Accounting. Neben einer Kontrollfunktion in Form einer auswertbaren Historie ermöglicht Accounting auch eine Form von Kostenerfassung. Wenn nicht anderweitig verwirklicht, so kann man bei Remote-Usern dabei erfassen, wie lange sie eingewählt waren und welche Dienste sie in Anspruch genommen haben, so dass man entsprechend abrechnen kann.

Im Zusammenhang mit RADIUS werden noch vier weitere Begriffe eingeführt, die der Vollständigkeit halber hier mit aufgenommen werden:

Service

Gemeint sind "handelsübliche" Dienste. Zunächst meinte man damit nur Dienste, die vom Einwahlknoten (NAS = Network Access Server) verwaltet wurden, wie Telnet Zugriffe auf den NAS selbst oder Zugriff auf ein Netz mittels PPP Einwahl. Mit der zur Zeit stattfindenden Erweiterung der Einsatzbereich fällt diese Einschränkung weg. Der Standard selbst hat den Begriff auch nie so eng gefasst.

Session

Eine Session ist die Nutzung eines einzelnen Dienstes durch den User. Eine Session hat einen klar definierten Anfang und ein klar definiertes Ende. Ein User kann verschiedene Sessions gleichzeitig offen haben, beispielsweise kann er gleichzeitig einen FTP Transfer machen und eine Telnetverbindung zum NAS.

Silently discard

Mit "silently discard" wird in diesem Zusammenhang der Vorgang des Verwerfens ohne Benachrichtigung an den Sender bezeichnet. Damit ist anschaulich folgendes gemeint: der NAS sendet eine Meldung an den RADIUS Server, mit der der Server nichts anfangen kann, weil er beispielsweise den NAS gar nicht kennt. Der Server wird diese Meldung ignorieren, d.h. er sendet keine Rückmeldung an den NAS, auch nicht, dass er nichts mit der Meldung hat anfangen können: er "verwirft stillschweigend".

Secret Key

Gemeinsames Passwort zwischen Client und Server, also zwischen Authentication Server und Einwahlknoten. Der Server ermittelt das gemeinsame Passwort aufgrund der IP Nummer des NAS, so dass ein Server, der verschiedene NAS bedient, für jeden ein anderes Passwort haben kann.

Das Passwort stellt sicher, dass der jeweilige Kommunikationspartner auch wirklich derjenige ist, der er zu sein vorgibt. Der Secret Key wird ausschließlich zu Hash-Berechnungen genutzt, so dass er zwar auf beiden Seiten im Klartext vorliegen muss, jedoch niemals im Klartext ausgetauscht wird.

Funktionsweise

Die Abfolge, Anzahl und der Inhalt der Pakete bei RADIUS richtet sich nach der gewählten Authentifizierungsmethode.

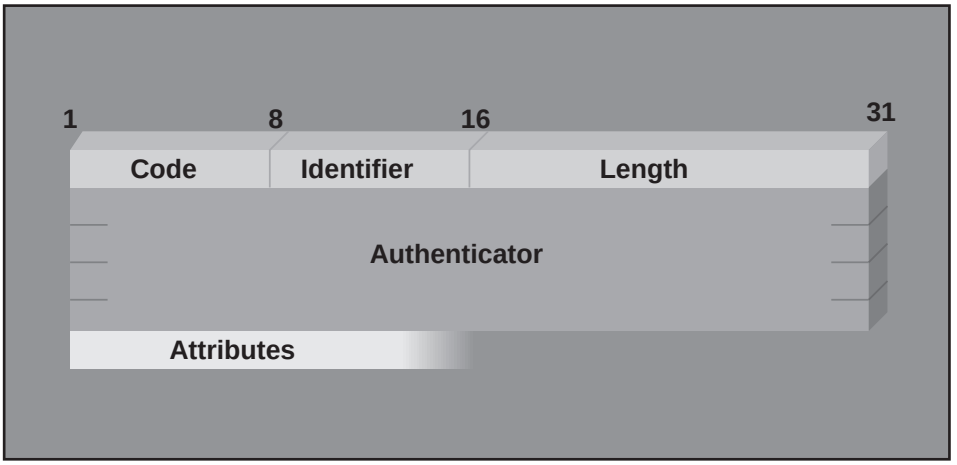
Zwingend notwendig für die Authentifizierung sind von den möglichen Paket-Typen nur drei (siehe Tabelle)

Code	Typ
1	Access-Request
2	Access-Accept
3	Access-Reject

Tabelle

Wesentlich für die Kommunikation ist, dass nicht der Peer, also das System des Endusers, mit dem RADIUS Server kommuniziert, sondern der NAS; der RADIUS Server und das RADIUS Protokoll ist im Regelfall für den Enduser transparent, d.h. er glaubt, er werde vom Einwahlknoten authentifiziert. Wählt sich ein User ein, so übermittelt er mittels eines bestimmten Authentifizierungsprotokolles seine Identifikationsdaten (bspw. PAP, CHAP oder EAP). Dies umfasst zumindest eine User-ID und ein Passwort. Das Passwort muss dabei nicht im Klartext übertragen werden, im Falle von CHAP beispielsweise handelt es sich um einen MD5 Hash, der aus mehreren Parametern berechnet wird, die zuvor zwischen Peer und NAS ausgetauscht werden, und einem beiden Seiten bekannten Passwort.

Bild 4 Radius Paket



Authentifizierungsanfrage/ Access-Request

Sind die Daten zur Identifikation zwischen Peer und NAS ausgetauscht, übermittelt der NAS die Daten als Access-Request an den RADIUS Server. Bei der Kommunikation zwischen Server und Einwahlknoten gibt es eine Reihe von Problemen zu lösen:

1. Es muss sichergestellt werden, dass der RADIUS Server derjenige ist, der er zu sein vorgibt.

2. Jede Authentifikation muss eindeutig sein, ein Playback Angriff muss also ausgeschlossen werden können.

3. Passwörter dürfen nicht im Klartext über das Netz zwischen NAS und Server übertragen werden, auch wenn dies im Einwahlprotokoll der Fall ist (e.g. PAP).

4. Finden auf einem NAS gleichzeitig mehrere Einwahlvorgänge statt, die er von dem selben RADIUS Server authentifizieren lässt, so müssen die Antworten den Anfragen zugeordnet werden können.

Die Lösung des ersten Punktes liegt im "Secret Key". Wie bereits beschrieben, handelt es sich bei dem Secret Key um ein Passwort, das sowohl dem RADIUS Server wie auch dem NAS bekannt ist. Hinzu kommt im Access-Request noch eine Zufallszahl, die der Server, analog zu CHAP, für seine Hash-Bildungen später benötigt. Diese Zufallszahl, genannt "Authenticator", ist 16 Byte (128 bit) lang und wird im Access-Request vom NAS an den Server übertragen. Um sicherzustellen, dass kein Playback Angriff stattfinden kann (Punkt 2) muss diese Zufallszahl eineindeutig sein, solange der Secret Key nicht geändert wird.

Ist das vom Peer (User) übermittelte Passwort bereits ein Hash, so wird es vom Client (NAS) für die RADIUS Übertragung nicht weiter verschlüsselt.

Handelt es sich zwischen Peer und NAS allerdings um eine Klartext-Authentifizierung (e.g. PAP), so verschlüsselt der NAS das Passwort für die Übertragung dergestalt, dass nur der RADIUS Server das Passwort entschlüsseln kann (siehe unten):

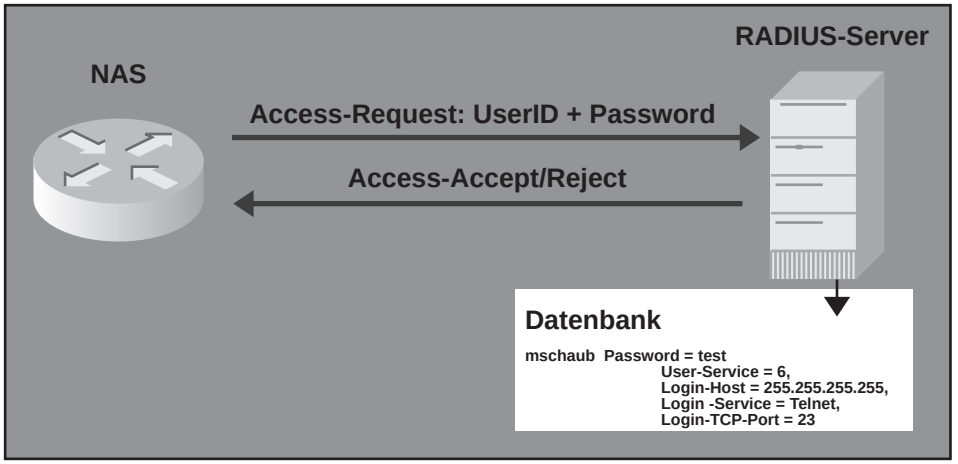


Bild 5 Einfache Radius-Kommunikation

Damit der Server mit dem Passwort etwas anfangen kann, muss zusätzlich natürlich noch eine Userkennung übermittelt werden. Dies geschieht unverschlüsselt.

Bliebe noch Punkt 4, die Zuordnung: hierfür gibt es ein im RADIUS Protokoll ein Byte großes Identifikationsfeld, in dem eine Zahl steht, die bei der Antwort durch den Server wiederholt wird.

Neben der User-ID und dem Passwort können weitere Informationen zwischen NAS und Server zwecks Überprüfung ausgetauscht werden. Beispiele wären der Einwahl Port oder der angeforderte Dienst, wie z.B. PPP Einwahlzugriff auf das Netz oder Telnet-Zugriff auf den NAS selbst.

Authentifizierung

Der RADIUS Server sucht die Daten des Users aus seiner Datenbank heraus und vergleicht diese mit den übermittelten. Stellt der Server bei einer einzigen Bedingung fest, dass dies nicht zulässig ist, so wird ein Access-Reject an den NAS zurück übermittelt. Dabei ist es unerheblich, ob alle anderen Bedingungen erfüllt sind. Optional kann eine Mitteilung über den Grund der Ablehnung in dem Access-Reject stehen.

Stimmen alle Bedingungen mit den hinterlegten Daten überein, so übermittelt der Server ein Access-Accept an den NAS, der wiederum dem Peer gegenüber ein Accept übermittelt. Auch in diesem RADIUS Paket können weitere Parameter übermittelt werden, wie eine Klartext-Nachricht oder ein Idle-Timeout.

Da der IETF Standard nur das RADIUS Protokoll beschreibt, bleibt es den Herstellern überlassen, wie die Daten hinterlegt werden. Hier gibt es dementsprechend auch die größten Unterschiede zwischen den aktuellen RADIUS Servern, da die Funktionalität selbst durch das Protokoll definiert wird. Als Beispiel sei der Microsoft Windows 2000 Server erwähnt, bei dem der IAS (Internet Access Server) als Dienst gestartet werden kann und RADIUS Funktionalität zur Verfügung stellt. Die RADIUS Daten werden in – für Windows 2000 Administratoren – gewohnter Weise im ActiveDirectory hinterlegt. Andere im Unix Umfeld verfügbare RADIUS Server, zumeist Abkömmlinge des ursprünglichen Livingston Servers, setzen auf eine vom Betriebsystem unabhängige Datenbank, die zumeist in textbasierten Konfigurationsdateien gepflegt wird.

Authentifizierungsantwort/ Access-Reject bzw. Access-Accept

Ist die Entscheidung durch den Server gefällt, so benachrichtigt er den NAS, indem er entweder ein Reject- (Ablehnung) oder ein Accept- (Annahme) Paket zurücksendet. In der Antwort muss der RADIUS Server zunächst beweisen, dass er derjenige ist, der er zu sein vorgibt (s.o. Punkt 1). Hierzu schreibt er in das Reject/Accept Paket im Feld Authenticator einen Hash, in den sowohl die in der Anfrage (Request) übermittelte Zufallszahl wie auch das gemeinsame Passwort (Secret Key) einfließen. Konkret wird ein 128 bit Authenticatorwert gemäß folgender Formel gebildet:

Übertragungswert = MD5(SecretKey + Authenticator) XOR UserPassword

ResponseAuthenticator = MD5 (PaketTypID + PaketID + Länge + RequestAuthenticator + Daten + SecretKey)

Da dem Empfänger die selben Daten vorliegen, kann er den Hash erneut bilden. Stimmt sein Ergebnis mit dem übermittelten Wert überein, so muss auch der Secret Key des Senders mit seinem übereinstimmen.

In der Antwort des Servers können weitere Attribute (Daten) an den NAS übermittelt werden; beispielsweise:

- der Grund für eine Ablehnung
- im Falle eines Accept-Message der Idle-Timeout
- eine Filter-ID für die gebilligte Einwahl.

Wenn man RADIUS neben der reinen Authentifizierung auch zur Authorisation benutzen will, so ist hier die Möglichkeit dazu gegeben, da man entsprechende Parameter an den Einwahlknoten übermitteln kann, bzw. von vornherein nur bestimmte Verbindungstypen mit zulässt.

Sonderfall: Challenge

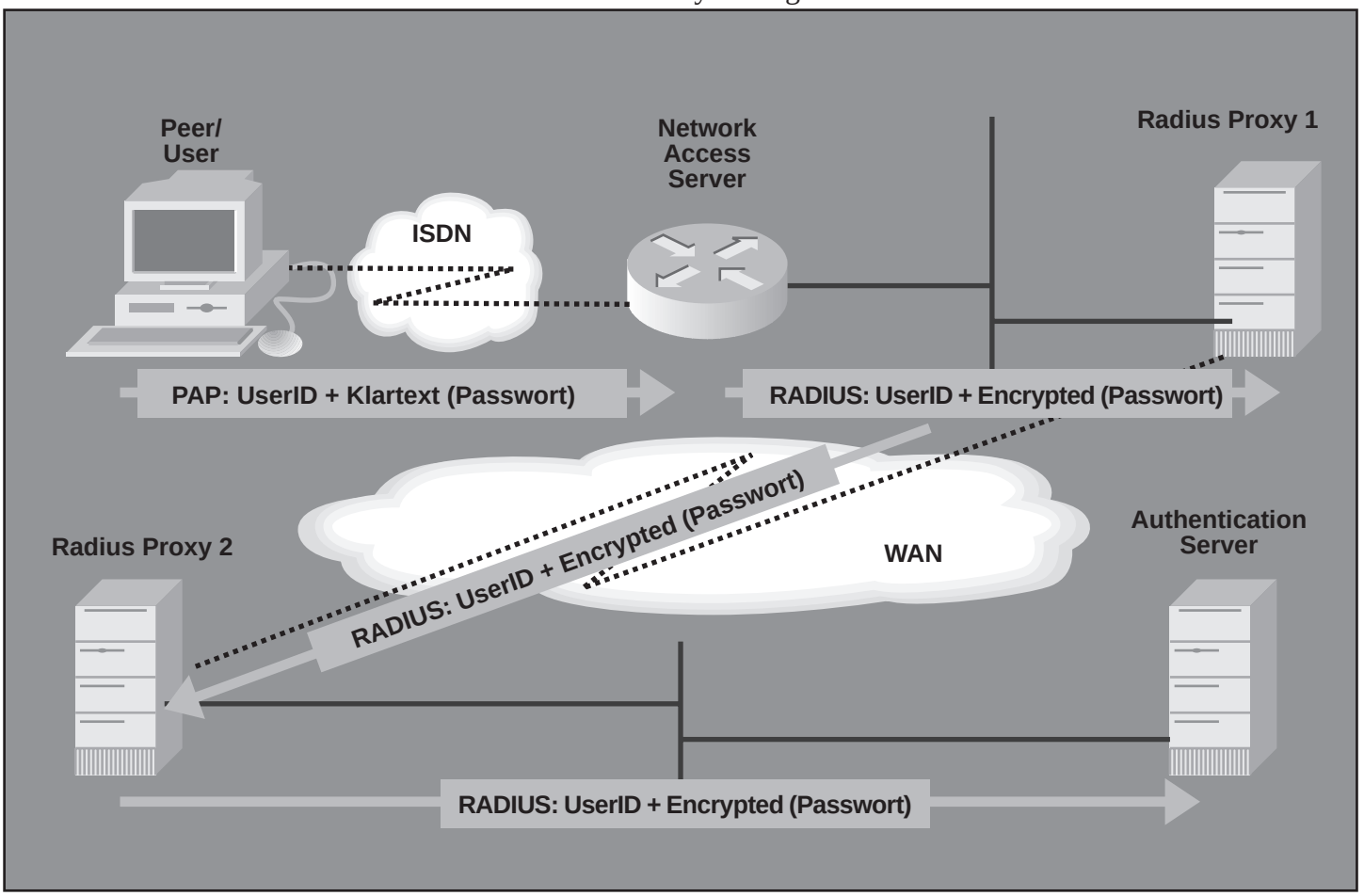
Das Access-Challenge wird nur benötigt, wenn eine Authentifizierungsmethode gewählt wird, die ein Challenge vom Authentifizierungsserver erwartet. Interessant ist dabei, dass das nicht bedeutet, dass jedes Verfahren, das mit einem Challenge arbeitet, zwangsläufig ein Challenge-Paket vom Server erwartet; Beispiel CHAP: bei der Authentifizierung mittels CHAP erwartet der Peer eine Zufallszahl vom Einwahlserver, diese wird auch vom NAS generiert und der vom Peer übermittelte Hash wird als Hash-Passwort inklusive der zuvor generierten Zufallszahl unverändert vom NAS an den RADIUS Server weitergeleitet.

Es gibt allerdings Authentifizierungsverfahren, bei denen es nötig ist, dass der Server das Challenge an den Peer übermittelt. Als Beispiel dafür kann das One-Time-Password Verfahren (Einmalpasswort) angeführt werden, wo nur dem User und dem Server die Passworttabelle vorliegt. Also muss auch der Server dem User mitteilen, welches Passwort er zu sehen wünscht.

In diesem Spezialfall wird von dem NAS zunächst ein Access-Request an den RADIUS Server geschickt, in dem das Passwort entweder leer ist oder einen vordefinierten, belanglosen Wert enthält, wie beispielsweise "passwort". Der Server generiert darauf hin ein Access-Challenge Paket, in dem ein zu dem geforderten Protokoll und dem sich einwählenden User ein passendes Challenge Attribut steht, das wiederum vom NAS an den User weitergeleitet wird.

Dieser Sonderfall ist nun für das von 1X genutzte EAP (Extensible Authentication Protocol) von Bedeutung, wie im weiteren Verlauf des Artikel deutlich werden wird.

Bild 6 Radius Proxy Anfrage



Besonderheiten von RADIUS

Es gibt noch einige Besonderheiten des RADIUS Protokolls, auf die hier kurz eingegangen werden soll.

Alternative Server

Einem NAS kann mehr als ein RADIUS Server angegeben werden. In welcher Weise er sich für welchen Server wann entscheidet, bleibt den Herstellern überlassen.

Retransmission

Bekommt ein NAS auf ein Paket nicht binnen eines kurzen Zeitraums im Sekundenbereich eine Antwort auf seine Anfrage, so sendet er das selbe Paket erneut. Ob er sich dabei an einen alternativen Server wendet oder den selben nochmals benutzt, bleibt ebenfalls den Herstellern überlassen. Sendet er zweimal das selbe Paket an den selben Server, so erkennt dieser das daran, dass beide Pakete die selbe Nummer im Identification Feld stehen haben.

Transportprotokoll UDP

Bei RADIUS hat man sich für UDP entschieden. Das klingt zunächst nach einem Widerspruch, ein Sicherheitsprotokoll über ein ungesichertes Protokoll zu übertragen. Aber schaut man genauer hin, findet man überzeugende Argumente der Entwickler:

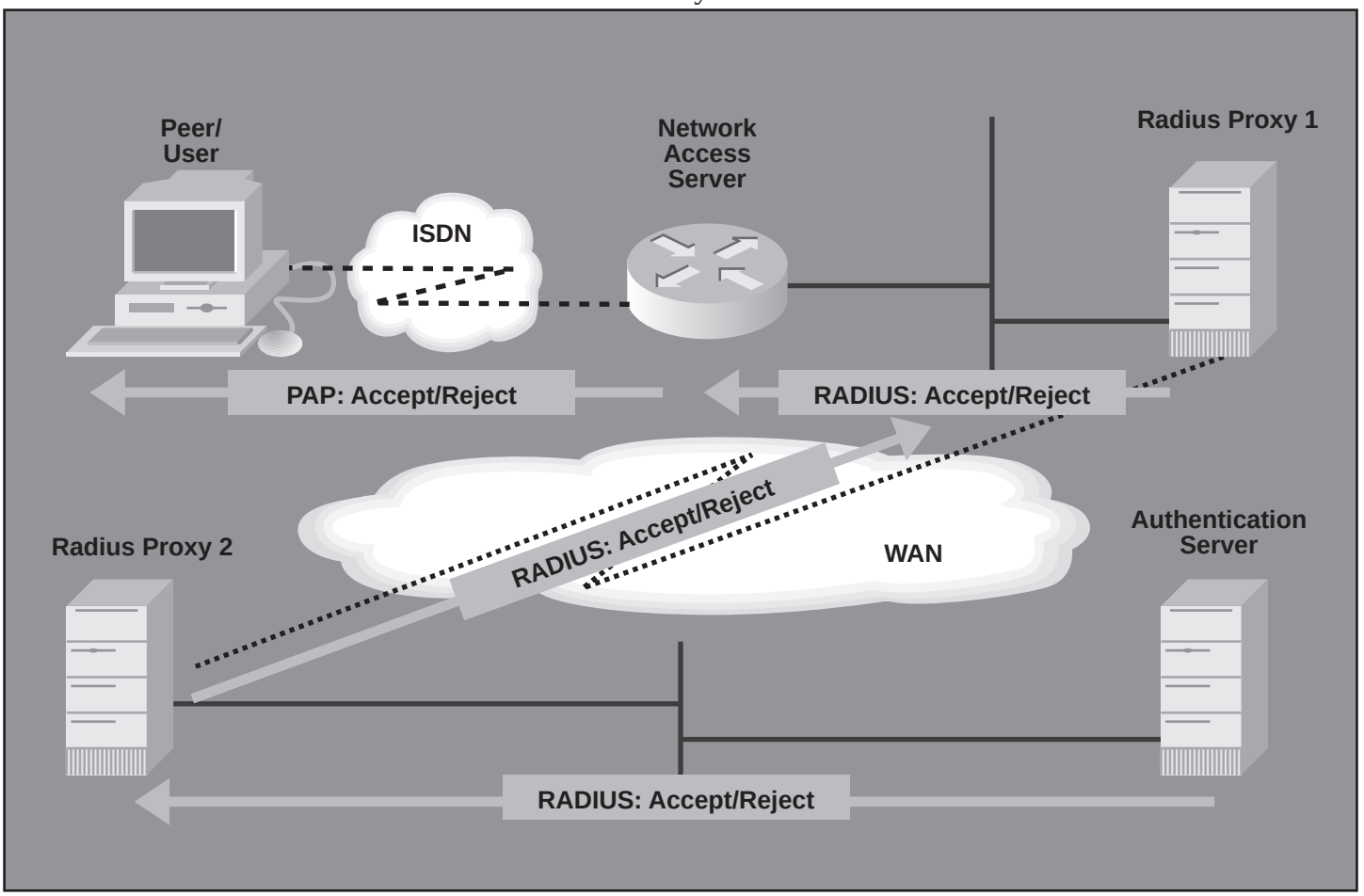
1. Kann ein RADIUS Server nicht erreicht werden, so kann RADIUS einen weiteren Server anfragen. Daraus folgt aber, dass RADIUS selbst eine Kopie des ersten Paketes behalten muss, somit benötigt die Applikation bereits einen eigenen Retransmission Timer, woraus folgt: der von TCP ist nicht vonnöten.

2. Das geforderte Zeitverhalten von RADIUS unterscheidet sich grundlegend von dem von TCP. Von der Einwahl her ist man gewohnt, einige Sekunden zu warten. Geht also ein RADIUS Paket verloren, so ist die "aggressive" Retransmission-Politk von TCP überzogen. Auf der anderen Seite akzeptiert ein User aber kein minutenlanges Warten während des Verbindungsaufbaus. Ist eine TCP Verbindung zwischen NAS und RADIUS Server zustande gekommen aber der Server überlastet, so befindet sich der Timeout bei TCP jedoch schnell im Minutenbereich. Ein schneller Wechsel auf einen alternativen Server wäre also wünschenswert.

3. RADIUS hat ein verbindungsloses Verhalten. Es werden nur wenige Pakete pro Einwahl zwischen NAS und Server gewechselt. Der Overhead für den Aufbau einer TCP Verbindung wäre somit vergleichsweise hoch. Hinzu kommt, dass jeweils nur ein einzelnes Paket vom NAS geschickt wird und er darauf eine Antwort erwartet. Das entspricht eher dem Verhalten von UDP als von TCP. Wofür ein Acknowledge, wenn ohnehin jedes Paket beantwortet wird?

4. UDP ist auf Serverseite einfacher zu implementieren. Nun, als Netzwerker glauben wir das einfach mal.

Bild 7 Radius Proxy Antwort



Port Based Network Access Control 802.1X - Der Wächter am Tor zum Netz

Proxy

Ursprünglich war die Proxy-Funktionalität von RADIUS dafür gedacht, dass Mitarbeiter sich bei einem Provider einwählen und über diesen ein VPN zu ihrer Firma aufbauen, anstatt sich direkt in der Firma einzuwählen. Vielerorts ist eine Interneteinwahl billiger als ein direktes Telefongespräch (außer lange Zeit in Deutschland, wo Telefon- und Onlinekosten anfielen). Was man nun wollte, war, dass die Einwahldaten selbst nicht vom Provider gepflegt werden, sondern von dem Betrieb des Mitarbeiters.

Hinzu kommt ein providerinternes Problem. Man wünscht sich bei RADIUS eine Vereinfachung, vorzugsweise möchte man die Userdaten an einer zentralen Stelle bzw. an zwei Stellen für den Backup pflegen und nicht an allen Standorten, wo Einwahlen stattfinden. Ein Beispiel zur Veranschaulichung: die meisten Aachener werden sich zumeist wohl auch in Aachen einwählen. Es ist also sinnvoll, sie auf dem Aachener RADIUS Server zu hinterlegen. Macht ein Aachener jetzt allerdings Urlaub in Hamburg, möchte er sich dort natürlich auch über seinen Provider lokal in der Hansestadt einwählen können. Der Hamburger Server kennt den Aachener jedoch nicht, kann jedoch erkennen, dass es sich um einen Aachener handelt und leitet die Anfrage weiter an den Aachener RADIUS Server.

In Bezug auf 1X kommt dieser Funktionalität natürlich weitere Bedeutung zu, wenn man Mitarbeiter hat, die sich in verschiedenen Standorten einloggen können.

Diese Proxy-Funktionalität ist natürlich nicht ganz trivial - Stichwort: Secret Key.

Erweiterbarkeit

RADIUS ist von vorne herein darauf ausgelegt worden, dass es nahezu beliebig erweiterbar ist. So wird von dem Standard ein "vendor specific attribute" vorgesehen, dessen Wert identisch mit der Vendor Nummer von SNMP ist. Analog zu SNMP kann ein Hersteller an dieses Attribut beliebige weitere selbst definierte Attribute anhängen. Viele Hersteller machen davon zumindest in kleinem Rahmen Gebrauch.

Zugriffskontrolle eines Systems durch 1X

Port basierte Zugriffskontrolle (Port Based Network Access Control) bedeutet nun im Sinne von 802.1X, dass ein System bereits an seiner Netzwerkschnittstelle sicherstellen kann, dass nur autorisierte Systeme Zugriff auf die eigenen, angebotenen Dienste erhalten. Der Begriff "Dienste" wird bei dieser Definition zunächst noch sehr allgemein gehalten und nicht auf Netzwerkfunktionen beschränkt, sondern er kann ebenso typische Serverfunktionen wie File- oder Maildienste umfassen. Schwachpunkt dieser sehr allgemeinen Definition ist, wie später noch ausführlicher erläutert wird, dass die Zugriffskontrolle nur auf einer Punkt-zu-Punkt Verbindung standardisiert ist und ein einmal freigeschalteter Port nur die direkte Gegenstelle authentifiziert, nicht den Kommunikationspartner in Bezug auf einen Dienst. Als Folge davon wäre ein einmal freigeschalteter Mailserver für alle Clients offen. Außerdem werden nur Layer 2 Informationen ausgewertet, also beispielsweise der Ethernet-Typ. Folglich können Applikationen nicht voneinander unterschieden werden.

Begriffe

Der IEEE Standard unterscheidet zwischen Systemen und Ports. Mit 'System' ist ein Gerät gemeint, das Zugang zu einem Netzwerk hat, mit 'Port' der Zugangspunkt zum LAN. Damit muss also jedes System zumindest über einen Port verfügen, wie es bei einer normalen Workstation der Fall ist. Es ist allerdings ebenso möglich, dass ein System mehrere Ports besitzt; Beispiele wären sowohl Netzwerk-Hardware wie Switche und Router, aber auch Server mit mehreren Netzwerkkarten.

Bei der Zugriffskontrolle werden insgesamt drei funktionale Rollen unterschieden. Leider unterscheiden sich die Begriffe von denen der IETF, obwohl im Prinzip die selben Rollen beschrieben werden.

Supplicant

(RADIUS: "Peer")

Als Supplicant wird das System bezeichnet, das Zugriff auf eine Ressource wünscht. Statt des Begriffes "Supplicant", der im IEEE Standard verwendet wird, benutzen die Autoren anderer Veröffentlichungen häufig die Bezeichnung "Peer".

Authenticator

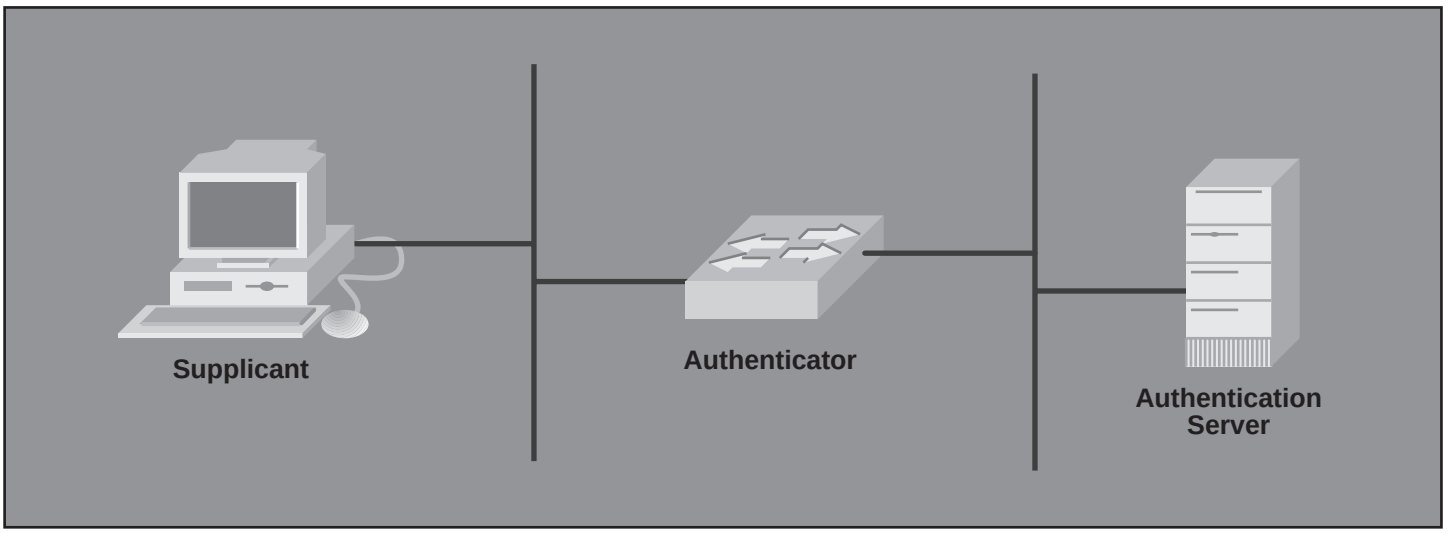
(RADIUS: "NAS")

Der Authenticator ist das System, das eine Ressource anbietet.

Authentication Server

(analog zu RADIUS)

Bild 8 Systeme bei IEEE 802.1X



Als nächstes wird eine Port Access Entity (PAE) als die Einheit definiert, die für die Abwicklung aller mit der Autorisierung in Zusammenhang stehender Prozesse zuständig ist. Was wie ein sehr abstraktes Modell wirkt, ist in Wirklichkeit der Dreh- und Angelpunkt der gesamten Authentifizierung, da alle Definitionen in Bezug auf diese PAE getroffen werden und nicht für den physikalischen Port, der selbst nur Bestandteil der PAE ist.

Es muss zwischen zwei PAEs mit den oben beschriebenen funktionalen Rollen unterschieden werden: der Supplicant PAE und der Authenticator PAE. Für den Authentication Server wird keine solche Einheit definiert, genau genommen legt sich IEEE ja gar nicht auf einen bestimmten Server fest.

Die Aufgaben der PAEs lassen sich wiederum in zwei Bereiche aufteilen: die zur Authentifikation notwendige Kommunikation und die Steuerung des Ports, sprich der Freigabe bzw. des Blockierens des Zugriffs.

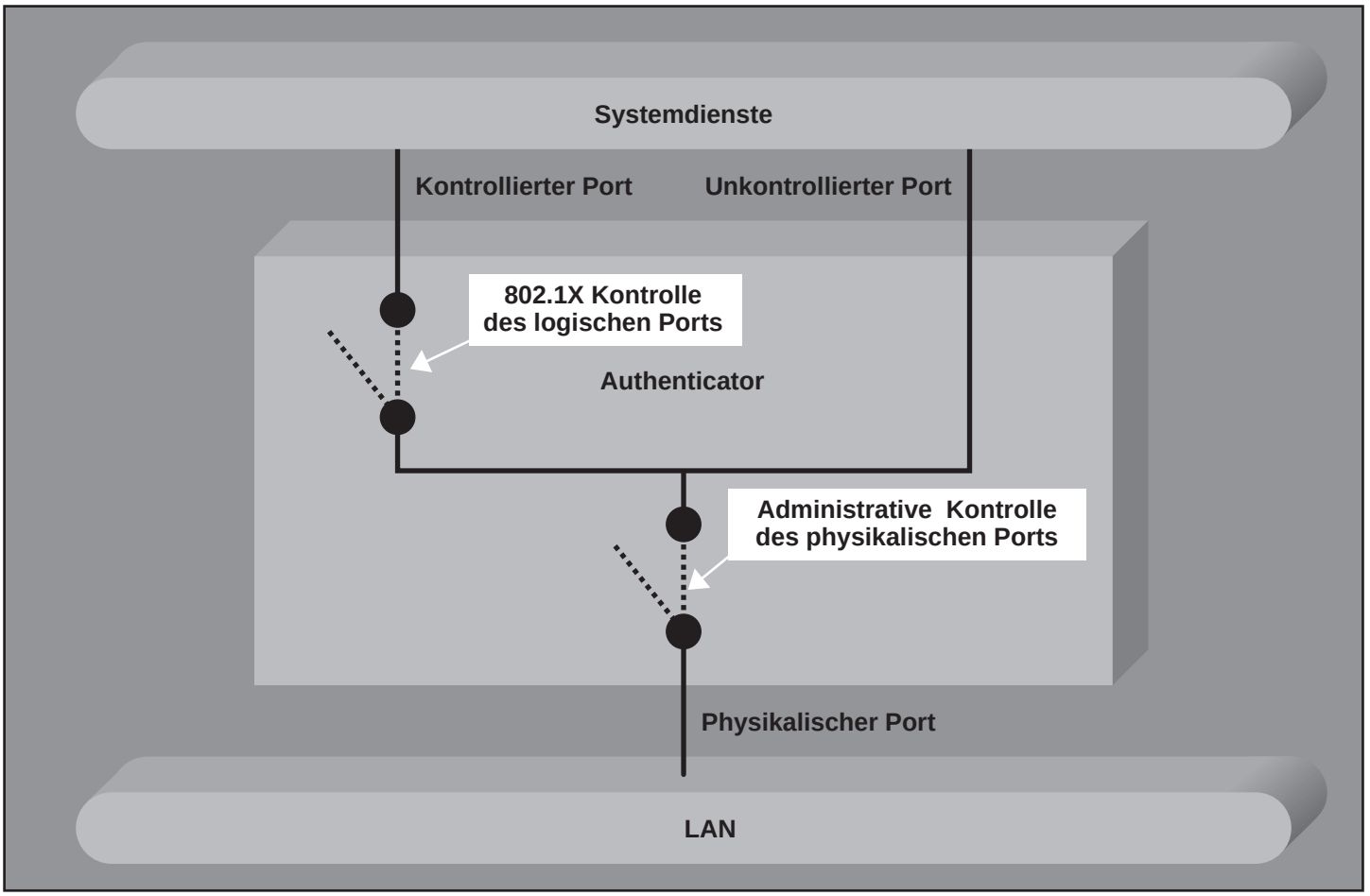
Portkontrolle

Es leuchtet ein, dass ein Port in Bezug auf einen "Port Access" Algorithmus nicht auf physikalischer Ebene gesperrt werden darf, da auch für die Authentifizierung zwischen Supplicant und Authenticator PAE ein Austausch von Paketen notwendig ist. Die bisherige Portlogik wird also durch 802.1X erweitert, wie in Bild 9 dargestellt. Zwischen dem physikalischen Zugriff auf das LAN (Point of Attachment) und den vom System angebotenen Diensten werden zwei neue logische Ports eingeführt: der kontrollierte und der unkontrollierte Port.

Beide stellen parallel eine Verbindung zwischen dem physikalischen Port und dem eigentlichen System her. Somit sind sie zunächst zum einen gleichberechtigt und zum anderen unabhängig voneinander. Weiterhin ist sofort ersichtlich, dass eine administrative Deaktivierung des Ports jegliche Authentifizierung übersteuert, da sie den Port komplett ausschaltet.

Pakete, die auf dem Interface empfangen werden, werden sowohl an den kontrollierten wie an den unkontrollierten Port weitergeleitet. Ist der kontrollierte Port blockiert, also die Verbindung zu den Systemdiensten unterbrochen, werden sie von ihm nicht weiter verarbeitet, ist er freigegeben, werden alle Pakete an das System zur Weiterverarbeitung durchgelassen. Für den unkontrollierten Port hingegen gilt, dass er nur bestimmte Pakete an das System weiterleitet. Um welche Art von Paketen es sich dabei handelt, wird offen gelassen. Da die Verarbeitung aber durch einen Layer 2 Mechanismus geschehen muss, sind die Selektionsmöglichkeiten damit sehr eingeschränkt. In der Praxis wird es wohl darauf hinauslaufen, dass ausschließlich der Authentifikationsprozess selbst über den unkontrollierten Port abgewickelt werden wird und jegliche anderen Pakete über den kontrollierten (Bilder 10 und 11). Die Identifikation der zur Authentifikation genutzten Pakete erfolgt über den LLC Sublayer des Layer 2, woraus folgt, dass für diesen Prozess nur Pakete mit 802.2 Header in Frage kommen, also 802.3, 802.5 und 802.11.

Bild 9 Zusammenhang zwischen kontrolliertem, unkontrolliertem und physikalischem Port



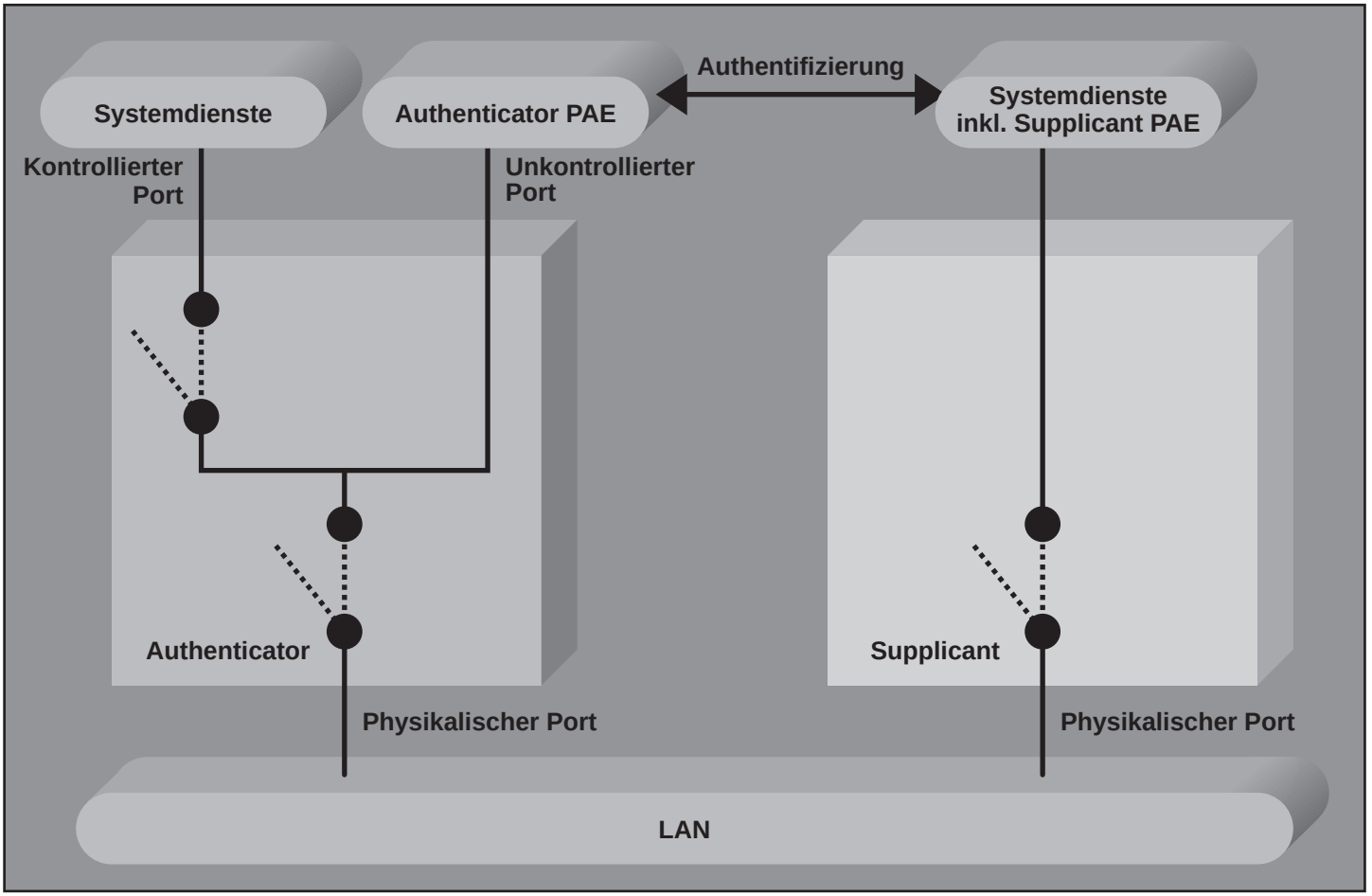


Bild 10 Kommunikation der PAEs

War eine Authentifikation erfolgreich, so ist es ebenfalls Aufgabe der Authenticator PAE den kontrollierten Port frei zuschalten und somit dem Supplicant Zugriff auf die Systemdienste zu gewähren.

Natürlich kann ein System beide Rollen einnehmen, also sowohl Authenticator wie auch Supplicant sein. In diesem Fall würde eine gegenseitige Authentifizierung stattfinden.

Es gibt noch eine weitere Besonderheit: man kann unterscheiden, ob sich die Authentifizierung nur auf eingehende oder gleichermaßen auf ein- und ausgehende Datenströme beziehen soll. Will man einem Angreifer möglichst wenig Angriffsfläche lassen, ist es selbstverständlich beide Richtungen zu kontrollieren!

Link Aggregation

Es ist zu beachten, dass die bis hier beschriebene Erweiterung des Standards sich auf einen physikalischen, nicht auf einen logischen Port bezieht. Wer also Link Aggregation betreibt und nicht nur Enduser sondern auch Switche untereinander oder Server mit mehreren Netzwerkkarten authentifizieren will, muss die Einstellungen für alle physikalischen Interfaces eines Links vornehmen, nicht für die Gruppe.

Kommunikation der Systeme

Bisher wurde beschrieben, wie ein einzelnes System den Zugriff auf seine Dienste verhindert bzw. gewährt. Betrachten wir nun, wie die Kommunikation zur Authentifizierung überhaupt abläuft.

Dazu müssen wir zwei getrennte Kommunikationsabläufe betrachten:

1. zwischen Supplicant und Authenticator mittels EAPOL

2. zwischen Authenticator und Authentication Server; bspw. mittels RADIUS

EAPOL

IEEE macht es sich einfach: für die Kommunikation zwischen Supplicant und Authenticaton Server, also zwischen Endsystem und Switch, wird kein neues Protokoll erfunden, sondern man bedient sich eines bereits vorhandenen (proposed) Standards der IETF und erweitert es um die eigenen Bedürfnisse. Gemeint ist das "PPP Extensible Authentication Protocol" (EAP), RFC 2284. EAP ist eine Erweiterung von PPP, genau genommen handelt es sich um einen weiteren Authentifizierungsmechanismus neben den beiden wesentlich bekannteren Mechanismen PAP und CHAP.

Hauptvorteil von EAP ist, dass es nicht auf einen einzelnen Authentifizierungsalgorithmus festgelegt ist. Bereits der ursprüngliche Standard Track sieht verschiedene Möglichkeiten vor:

- MD5 Challenge
- One-time-Password
- Generic Token Card

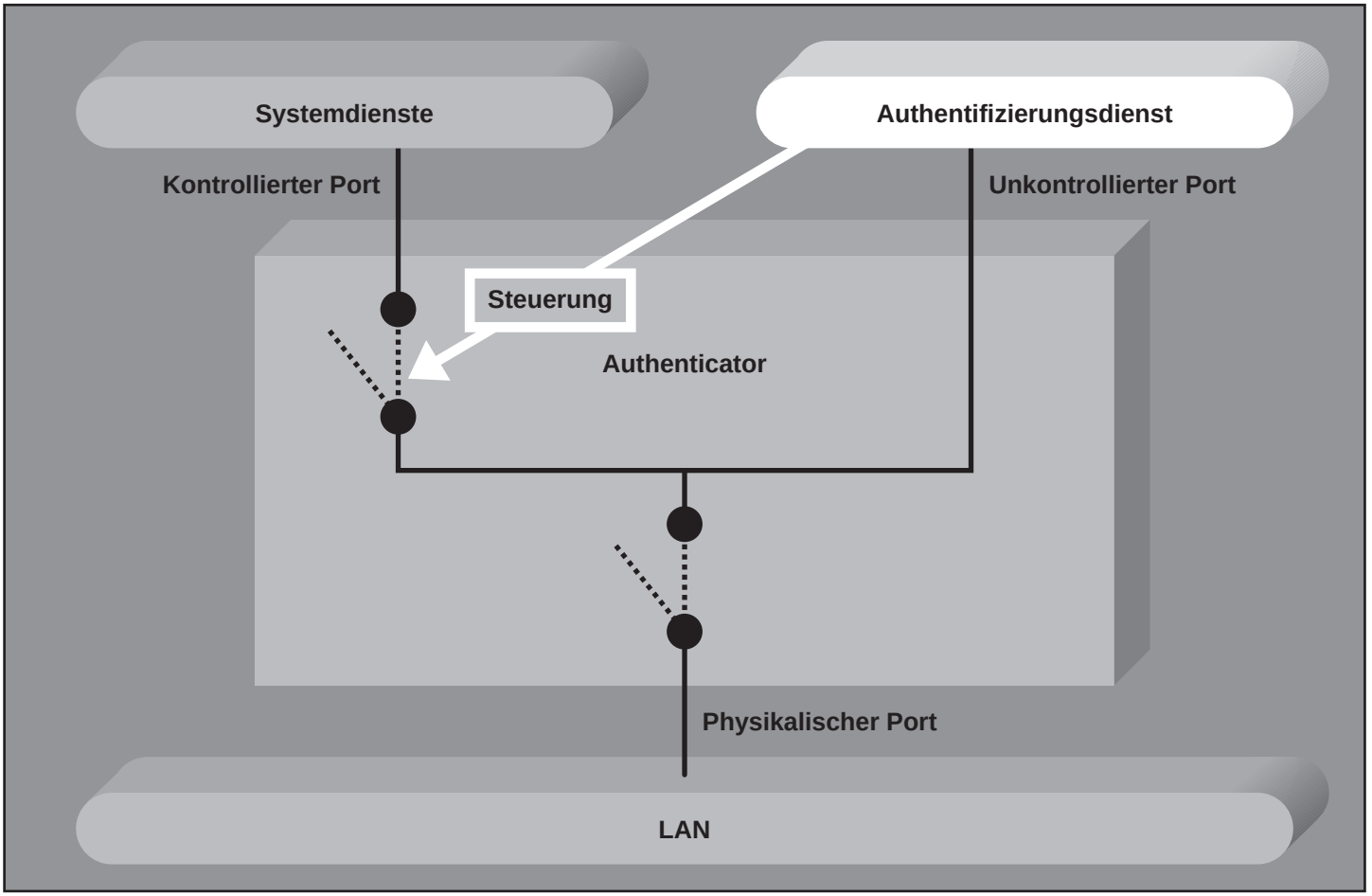


Bild 11 Steuerung des kontrollierten Ports

Um die Art des Algorithmus anzuzeigen gibt es im EAP Frame ein 8 bit Feld mit einer Kennziffer. Die Kennziffern 1-3 sind für protokolleigene Informationen vorgesehen und die Null ist nicht vergeben, so dass von den 256 Möglichkeiten 252 für die Angabe einer Authentifizierung verbleiben. Kurz: das Protokoll ist vorläufig offen für zukünftige Verfahren.

Ein weiterer Vorteil von EAP ist, dass der Zugangspunkt zu einem Netz, im Falle von 802.1X der Authenticator also, die Authentifizierung nicht selbst übernehmen muss, sondern die Informationen, die via EAP übermittelt werden, an einen zentralen Server (Authentication Server) übermitteln und von diesem bestätigen lassen kann. Führt man beispielsweise ein neues Verfahren ein, so ist es nicht notwendig sämtliche Zugangspunkte mit neuen Softwareupdates zu versehen, sondern eine Anpassung des Servers und des Supplicant reicht, um das neue Verfahren einsetzen zu können. Eine Anpassung sämtlicher Authenticator – wie Switche – wäre nicht von Nöten.

Dank dieser beiden Vorteile ist EAP ein Protokoll, welches für die Kommunikation zwischen Supplicant und Authenticator hervorragend geeignet ist: es ist offen genug für neue Verfahren und es verlangt keine hohe Funktionalität vom Authenticator. Allerdings hat EAP auch einen Nachteil: es wurde für Punkt-zu-Punkt-Verbindungen geschaffen, nicht für LANs.

Aus diesem Grund ist es notwendig einige Anpassungen vorzunehmen. Das Resultat nennt man EAP over LAN, kurz EAPOL.

EAP ist kein Layer 2 Protokoll sondern in Bezug auf Netzwerke handelt es sich bereits um Nutzdaten, die von einer Applikation weiter verarbeitet werden müssen. EAPOL beschreibt, wie diese EAP Frames bei verschiedenen LAN Protokollen enkapsuliert werden sollen. Bislang gibt es EAPOL für Ethernet nach 802.3 und Token-Ring/FDDI. In den Paketen sind also keinerlei Layer 3 Informationen enthalten und somit sind sie auch nicht routbar. Da sie ausschließlich zwischen Supplicant und Authenticator ausgetauscht werden, ist Routing nicht notwendig, weil die Authentifizierung vor Eintritt in das Netzwerk stattfinden soll.

Zusätzlich zur reinen Enkapsulation von EAP Daten, dem "EAP Frame" in EAPOL, werden noch vier weitere Pakettypen definiert:

1. EAPOL Start

2. EAPOL Logoff

3. EAPOL Key

4. EAPOL Encapsulated-ASF-Alert

Die Bedeutung der ersten beiden Typen wird deutlich, wenn der Ablauf und der Betrieb eines Netzes im Folgenden beschrieben wird.

Auf die beiden letzten Typen wird danach kurz eingegangen.

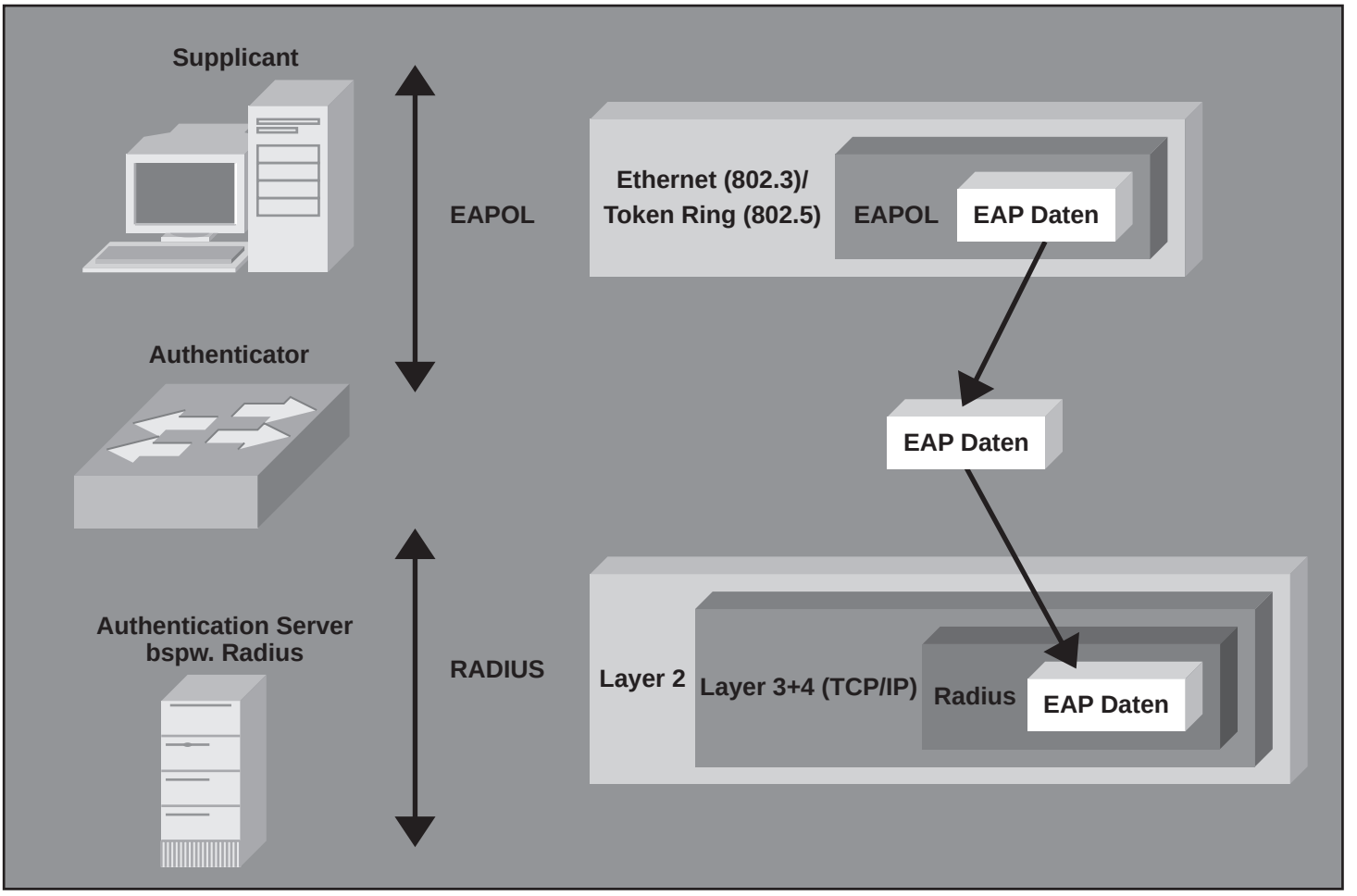


Bild 12 Encapsulation

Ablauf der Authentifizierung

Allgemeine Kommunikationsmerkmale

Grundsätzlich gilt, dass der Authenticator Informationen des Supplicant an den Authentication Server nur durchreicht ohne sie zu verändern. Dabei muss er die Informationen natürlich "umpacken", da EAPOL nur für die Kommunikation zwischen dem Supplicant und dem Authenticator definiert ist. Zudem ist die Enkapsulation zwischen Authenticator und Authentication Server vom jeweiligen Server abhängig und IEEE legt sich nicht auf einen bestimmten Servertyp fest, auch wenn aktuell erwartet wird, dass es sich um einen RADIUS Server handeln wird. Mit anderen Worten, die Daten aus EAP Frames werden unverändert in RADIUS eingepackt. Die Authentifizierung selbst findet also zwischen Supplicant und Authentication Server statt, der Authenticator fungiert nur als Vermittler. Seine Aufgabe ist es, den Authentifizierungsprozess zu starten und den Portstatus des kontrollierten Ports zu steuern.

Für EAPOL gilt weiterhin, dass jeder Request des Authenticator durch ein Response des Authentication Servers beantwortet werden muss. Das ist notwendig, um sicherzustellen, dass alle notwendigen Informationen ausgetauscht werden, da das EAPOL für ungesicherte Layer 2 Verbindungen definiert und keine Retransmission durch ein höheres Protokoll wie bspw. TCP vorgesehen ist.

Initialisierung

Auch wenn IEEE kein CHAP kennt, wie es vom PPP genutzt wird, so entdeckt man doch Parallelen bei der hier beschriebenen Port Access Authentifizierung. Das ist auch nicht verwunderlich, ist EAP doch von Hause aus eine Alternative zu CHAP oder PAP des PPP Protokolls. Viele Schritte beim Kommunikationsablauf sind optional, in diesem Artikel werden die wesentlichen beschrieben. Augenmerk dabei ist der typische Ablauf, wie er bei den künftigen Implementierungen zu erwarten ist. Im Einzelnen lässt es der Standard offen, ob die in Bild 13 durch Pfeile dargestellten notwendigen Informationen durch ein einzelnes Paket oder durch eine Abfolge von mehreren Requests und Responses ausgetauscht werden. In Bezug auf EAP spielt das auch keine Rolle, entscheidend wird die zur Authentifizierung ausgewählte Methode sein.

Ein Beispiel zur Veranschaulichung:

Wählt man eine Methode, bei der der Supplicant gleichzeitig Username und Passwort übermitteln kann, also ein Verfahren ähnlich dem PAP, so würde ein einzelner Response auf den Identity-Request ausreichen. Wird hingegen ein MD5 Challange genutzt - analog zu CHAP - so muss der Authentication Server zunächst ein Challenge an den Supplicant übermitteln, das dieser für die Errechnung des MD5 Hashes benötigt.

Optional kann der Prozess mit einer Aufforderung des Supplicant an den Authenticator beginnen. Dazu schickt der Supplicant eine EAPOL Start Message an den Authenticator. Informationen zur Authentifizierung sind in diesem Frame keine enthalten, da es sich lediglich um die Aufforderung handelt mit der Authentifizierung zu beginnen. Dieser Schritt ist deswegen nicht zwingend erforderlich, da auch der Authenticator mit dem EAP Request/Identity die Authentifizierung direkt eröffnen kann, wenn er eine Änderung des Link Status des entsprechenden Ports bemerkt. Es gibt jedoch zwei Gründe, warum auch ein Supplicant in der Lage sein muss, die Authentifizierung anzufordern:

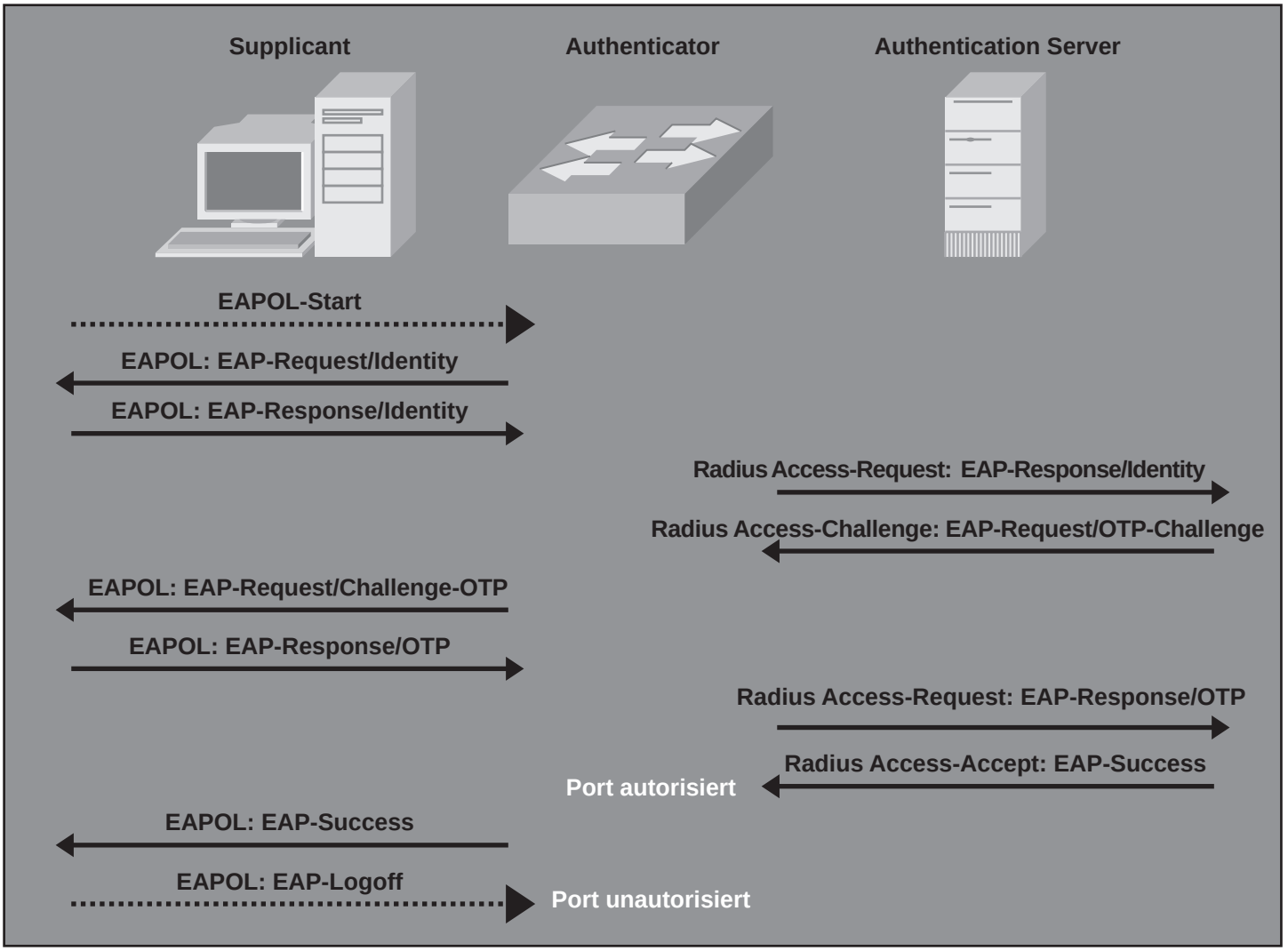
1. Bootet ein Supplicant, so wird je nach Softwareimplementation der Link Status der NIC deutlich eher geändert als das entsprechende System die zur EAP Verarbeitung notwendigen Routinen geladen hat. In diesem Fall "verpasst" der Supplicant also u.U. die EAP Request/Identity Nachrichten des Authenticators und im schlimmsten Fall würde somit keine Authentifizierung stattfinden können.

2. Der häufigste Fall der Nutzung der Port Access Authentifizierung wird der sein, dass ein Endsystemuser sich an seinem Switch anmeldet. Verlässt ein Benutzer nun seinen Arbeitsplatz und loggt sich aus, so wird - bei sauberer Softwareimplementation des Betriebsystems - der Switch darüber mittels EAP Logoff Message informiert und der Port wechselt vom autorisierten in den unautorisierten Zustand. Meldet sich dieser oder ein anderer User wieder an, so ist es wünschenswert, dass er das kann, ohne das System zu rebooten oder kurzzeitig den Netzwerkstecker zu ziehen, nur um den Link Status der Netzwerkkarte zu ändern. Auch in diesem Fall würde also der Supplicant einen EAP Start Frame an den Authenticator schicken, um den Authentifizierungsprozess zu initialisieren.

Die Authentifizierung selbst beginnt mit einem "EAP Request" des Authenticator, anschaulich mit der Aufforderung des Switches an den Client seine Identität mitzuteilen. Dieser Request kann wiederholt werden, sollte er nicht beantwortet werden.

Auch wenn dieses Vorgehen logisch erscheint, so ist auch dieser Schritt nicht zwingend erforderlich. Es ist denkbar, dass der Authenticator weiß, welcher Benutzer sich auf welchem Port verbinden wird. Dies wäre beispielsweise möglich, indem Hersteller einen entsprechenden Parameter bei der Portkonfiguration ihrer Switche vorsehen, der vom Administrator gesetzt werden kann.

Bild 13 Ablauf der Authentifizierung



Port Based Network Access Control 802.1X - Der Wächter am Tor zum Netz

Authentifizierung

Der Supplicant beantwortet den Identity-Request mit einem Identity-Response. Dieser Response ist, wie schon weiter oben beschrieben, von der Art der Authentifizierung abhängig. In Bild 13 ist der Vorgang für ein One-Time-Password (OTP) dargestellt, allerdings kann er auf viele andere Mechanismen wie bspw. MD5 Challenge übertragen werden.

Die Daten des EAPOL Paketes werden vom Authenticator (hier dem Switch) extrahiert und an einen Authentifizierungs-Server weitergeleitet. Dazu werden die Informationen neu enkapsuliert, beispielsweise in RADIUS.

Der Authentifizierungsserver wiederum antwortet dem Supplicant. Im abgebildeten Beispiel indem er ein Challenge an den Authenticator zurückschickt, der die Daten erneut enkapsuliert, diesmal in EAPOL, um sie an den Supplicant weiterzureichen.

Dieser sucht im Beispiel (siehe Bild 13) das entsprechende Passwort heraus, führt den OTP Algorithmus aus und sendet dem Switch ein EAPOL Packet mit dem errechneten Hash. Wieder packt der Switch die EAP Daten in ein RADIUS Paket und übermittelt sie dem Server.

Im Prinzip kann das noch sehr oft so hin und her gehen, je nach EAP Authentifizierungsmethode, bis der Server über Accept bzw. Reject entschieden hat.

Ist die Authentifizierung abgeschlossen, sendet der Server dem Authenticator eine Accept, wenn erfolgreich, bzw. Reject, wenn nicht erfolgreich. Der Authenticator öffnet im Falle des Accept den kontrollierten Port und informiert den Supplicant mit einem EAP Success.

Neben dem Accept/Reject können weitere Informationen vom Server an den Authenticator übermittelt werden, wie zum Beispiel ein "Session-Timeout", der angibt, nach welcher Zeit eine erneute Authentifizierung notwenig ist.

Eine andere Möglichkeit wäre eine Begründung für einen Reject, die an den Supplicant weitergegeben wird.

Welche Informationen das im einzelnen sind wird primär von der Software des Authentication Servers und des Authenticators abhängen.

Ist der Port freigeschaltet stehen dem Supplicant nun alle Dienste offen.

Reauthentifizierung

Der beschriebene Authentifizierungsvorgang kann auf Verlangen des Authenticators jederzeit wiederholt werden. Während der Reauthentifzierung bleibt der kontrollierte Port geöffnet, erst ein Fehlschlagen der Authentifizierung veranlasst den Authenticator den Port in den unautorisierten Zustand zu versetzen.

Der Standard sieht vor, dass der dazugehörige Timer einen Default-Wert 3600 Sekunden haben soll, der Mechanismus selbst solle jedoch per Voreinstellung nicht eingeschaltet sein. Die Implementierung der Reauthentifizierung wird von IEEE zwar empfohlen, jedoch wäre ein Gerät auch ohne eine entsprechende Routine standardkonform.

Logoff

Sendet der Supplicant mittels EAPOL eine Logoff Nachricht an den Authenticator, setzt dieser den Port sofort in den unautorisierten Modus. Eine Rückmeldung an den Supplicant erfolgt nicht.

Dieser explizite Logoff durch das Endsystem macht Sinn, wenn sich ein User abmeldet, sei es beim Herunterfahren des Rechners oder sei es, weil er sich nur als Benutzer abmeldet, wenn er seinen Arbeitsplatz verlässt und jemand anderes die Station übernimmt. Auf diese Weise wird sichergestellt, dass jeder User sich zunächst am Netz anmelden muss und nicht den Rechner eines anderen "hijacken" kann.

Es kann jedoch auch eine weitere Reihe von Gründen geben, warum ein Port vom autorisierten in den unautorisierten Modus wechseln kann:

- eine Reauthentifizierung schlägt fehl
- der Reauthentifzierungs-Timer läuft ab, ohne dass eine Reauthentifizierung stattgefunden hat
- der physikalischer Link zwischen Supplicant und Authenticator bricht lange genug ab
- MAC Sublayer arbeitet nicht (mehr), sei es durch administrativen Eingriff oder Hardwarefehler
- administrative Änderung auf dem Authenticator.

Weitere EAPOL Frames

Der "EAPOL Key"

EAPOL Key Frames können genutzt werden, um Informationen zu Schlüsseln auszutauschen, wenn der EAP Datenstrom verschlüsselt werden soll. Aktuell ist das nur für das von RSA Data Security Inc. entwickelte Verfahren RC4 vorgesehen. Es ist anzunehmen, dass der Blick bei der Standardisierung von 802.1X dabei in Richtung 802.11 ging, da der WEP Verschlüsselung von WirelessLAN der RC4 Algorithmus zugrunde liegt.

Grundsätzlich kann 1X jedoch jederzeit erweitert werden, so dass auch andere Key-Informationen ausgetauscht werden können.

Der "EAPOL Encapsulated-ASF-Alert"

In Ausnahmefällen können Endgeräte Systemmeldungen an eine Managementstation senden, um "besondere Vorkommnisse" zu melden. Beispiele wären Überhitzung, Probleme mit der Spannungsversorgung oder Ausfall von Hardwarekomponenten. Zumeist werden diese Meldungen als SNMP Traps verschickt. Befindet sich eine Station nun an einem Port, der (noch) nicht von dem Switch freigeschaltet wurde, so würde eine solche Alarmmeldung nicht weitergeleitet. Um diese Situation zu verhindern, gibt es bei EAPOL die Möglichkeit des "EAPOL Encapsulated-ASF-Alert". Dieser Mechanismus ist nicht auf ein bestimmtes höheres Protokoll wie SNMP festgelegt, sondern der Authenticator generiert aus den EAPOL Daten eine entsprechende Meldung.

Aus Sicht der Endstation kann es zwei Situationen geben, wenn eine Alarmmeldung generiert wird:

1. Die Station ist authentifiziert und hat somit freien Zugang zum Netz.

2. Die Station ist nicht authentifiziert und die Meldung würde verworfen.

Der Standard sieht zwei Möglichkeiten vor, um sicherzustellen, dass Warnmeldungen auf alle Fälle ankommen. Die erste ist denkbar trivial: die sendende Station generiert immer zwei Meldungen, einen "normalen" Trap und einen in EAP enkapsulierten. Variante zwei ist: der Supplicant nutzt sein Wissen über seinen Authentifizierungsstatus und sendet entweder eine normale Meldung oder aber, wenn der aktuelle Status "unauthentifiziert" ist, einen EAP Alert.

Port Based Network Access Control 802.1X - Der Wächter am Tor zum Netz

Vorteil der zweiten Taktik ist es, dass jede Meldung nur einmal verschickt wird, Nachteil hingegen wäre, dass Meldungen nicht ankommen, wenn der Supplicant vom Authenticator "ausgetimed" wurde oder einen Log-Out übersehen hätte. Bei Variante eins (zwei Pakete) wäre es genau umgekehrt.

Analog zum Supplicant hat auch der Authenticator zwei Möglichkeiten einen empfangenen EAPOL Encapsulated-ASF-Alert zu behandeln. Entweder leitet er ihn grundsätzlich weiter oder aber er nutzt sein eigenes Wissen um den Authentifizierungszustand des Ports, auf dem der Alert empfangen wird.

In beiden Fällen soll der Switch jedoch zunächst die Gültigkeit der im EAPOL Frame enthaltenen Meldung prüfen, wobei IEEE offen lässt, wie ein gültiger Inhalt aussieht und auf die Gremien verweist, die sich mit der Entwicklung von Managementprotokollen beschäftigen. Ist die Meldung gültig und soll sie weitergeleitet werden, so muss vom Authenticator ein neuer Frame generiert werden, wie er von dem Supplicant generiert worden wäre, gäbe es keine Authentifizierung. Mit anderen Worten, aus Sicht der Managementstation ist der Authenticator bezüglich von Traps transparent, eine aktive Überwachung kann natürlich nicht stattfinden.

Ein weiterer Fall ist in Bezug auf den Authenticator noch zu beachten: handelt es sich um ein System, das bridged, also eine Bridge oder einen Switch, und ist der entsprechende Port authentifiziert, so würde ein EAP Alert auf beiden logischen Ports empfangen und von beiden verarbeitet werden, dem kontrollierten und dem unkontrollierten. In diesem Falle wird von der Switching-Logik erwartet, einen EAP Frame zu erkennen und ihn nicht auf irgendeinem anderen Port zu senden, sondern ihn auf alle Fälle systemintern zu verarbeiten.

Offene Frage zu 1X

So schön sich das ganze Verfahren auch lesen mag, so gibt es doch noch ein schwerwiegendes Problem zu klären.

Migrationsproblem

Port Access Control muss durch das Betriebssystem unterstützt werden. Grund dafür ist, dass die Authentifizierung stattfindet, bevor eine Verbindung zum Netzwerk hergestellt werden kann. D.h. weder steht dem Supplicant ein Domänenkontroller zur Verfügung noch ein DHCP Server. Das Betriebsystem muss also darauf ausgelegt sein, noch vor der Aktivierung der Netzwerkdienste eine Authentifizierung durchzuführen. Aktuell ist das ausschließlich bei Windows XP der Fall.

Zu betrachten sind zwei Fälle:

1. Der Client spricht 1X, der Switch nicht. Hier passiert nichts besonderes. Der Client muss nur bereit sein, "einfach weiterzumachen wie früher", wenn seine EAPOL Start Frames nicht beantwortet werden. Da der Switch vollen Zugang zum Netz gewährt, funktioniert alles.

2. Der Switch verlangt 1X, was der Client nicht unterstützt. Resultat: nichts geht mehr.

Ist Fall 1 noch einfach zu lösen, so ist Fall 2 unlösbar.

Zusammenfassung

Betrachtet man die Möglichkeiten von RADIUS als universalen Authentifizierungsserver und 1X als zusätzliche Sicherheitsbarriere von LANs, so kann man nur hoffen, dass die Hersteller sich auf diese Möglichkeiten einlassen.

Ein erheblich geringerer administrativer Aufwand, da userbezogene Rechte zentral auf einem Server verwaltet werden können, ist ein entscheidender Vorteil.

Ob sich diese Technologie durchsetzt oder nicht, wird von den Herstellern abhängen. Diesmal allerdings nicht allein von denen der Hardware. Alle führenden Netzwerkhersteller haben bereits entweder Produkte auf dem Markt oder angekündigt diese sehr bald zur Verfügung zu stellen (häufig durch ein "einfaches" Softwareupdate). Entscheidender werden aber die Softwarehersteller sein. Ein Kernpunkt wird die Integration in die Betriebsysteme werden: 1X muss vom Betriebsystem unterstützt werden, Updates für alle gängigen Betriebsysteme sollten möglichst zügig erfolgen. Ebenso wird über Erfolg und Misserfolg des Verfahrens entscheiden, ob der User sich einmal mehr Authentifizieren muss, also am Server und neuerdings zusätzlich am Netz, oder ob das Betriebsystem die Daten zwischenspeichert und die spätere Server-/Domänenanmeldung automatisch durchführt. Viele User werden einen weiteren Anmeldevorgang als störend empfinden und ihn nur schwer oder gar nicht akzeptieren. Wünschenswert wäre, wenn sich weitere Softwarehersteller ebenfalls auf RADIUS einlassen würden. Beispiel: Datenbankserver. Radius ist offen genug, um auch Zugriffsrechte für Datenbankserver zu verwalten.

Im günstigen Fall müsste sich ein User nur noch einmal anmelden, statt wie heute so oft, einmal an der Domäne und beliebig oft bei verschiedenen Applikationen. Hätte man eine zentrale Verwaltung und ein Betriebsystem, das die Anmeldeinformationen zwischenspeichert, so wären Mehrfachanmeldungen Vergangenheit. Ich befürchte jedoch, dass die Befindlichkeiten vieler Softwarehersteller das eine schöne Utopie bleiben lassen werden.

Abk.	
AAA	Authentication, Authorisation und Accounting
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
FTP	File Transfer Protocol
IAS	Internet Access Server
NAS	Network Access Server
RAS	Remote Access Server
OTP	One-Time-Password
RADIUS	Remote Authentication Dial In User Service
UDP	User Datagram Protocol

Anzeige

Ausbildung zum ComConsult Certified Network Engineer

Termine 01/02

Lokale Netze für Einsteiger

Einzelpreis: EUR 1.990,-- zzgl. MwSt.

- 21.01. - 25.01.02 in Aachen
- 18.02. - 22.02.02 in Aachen
- 18.03. - 22.03.02 in Aachen
- 15.04. - 19.04.02 in Aachen
- 17.06. - 21.06.02 in Aachen

Internetworking

Einzelpreis: EUR 1.990,-- zzgl. MwSt.

- 03.12. - 07.12.01 in Aachen
- 28.01. - 01.02.02 in Aachen
- 04.03. - 08.03.02 in Aachen
- 22.04. - 26.04.02 in Aachen
- 17.06. - 21.06.02 in Aachen

Neue Ethernet Technologien

Einzelpreis: EUR 1.990,-- zzgl. MwSt.

- 10.12. - 14.12.01 in Aachen
- 28.01. - 01.02.02 in Aachen
- 08.04. - 12.04.02 in Aachen
- 10.06. - 14.06.02 in Aachen

TCP/IP und SNMP

Einzelpreis: EUR 1.990,-- zzgl. MwSt.

- 03.12. - 07.12.01 in Berlin
- 21.01. - 25.01.02 in Düsseldorf
- 04.03. - 08.03.02 in Berlin
- 22.04. - 26.04.02 in Berlin
- 24.06. - 28.06.02 in Berlin

Nutzen Sie unsere Paketpreise!

3er Paket: Buchen Sie drei beliebige Seminare unserer Ausbildung zum ComConsult Certified Network Engineer und Sie zahlen statt EUR 5.970,-- nur den Paketpreis von EUR 5.190,-- zzgl. MwSt.

Komplett-Paket: Für die komplette Ausbildung mit allen vier Seminaren zum ComConsult Certified Network Engineer zahlen Sie statt EUR 7.960,-- nur den Paketpreis von EUR 6.690,-- zzgl. MwSt.

ComConsult Akademie

ComConsult Certified Network Engineer

"Die Ausbildung wird in jedem Fall aktuellen Trends der Netzwerk-Technologie gerecht."

Michael Ederer (36) ist Systemtechniker beim bvv-Versicherungsverein, eine Pensionskasse der großen deutschen Bank- und Kreditinstitute.

Der Netzwerk Insider sprach mit ihm unmittelbar nach seiner bestandenen Prüfung zum ComConsult Certified Network Engineer.

Insider: Was machen Sie in Ihrem Beruf?

Michael Ederer: Ich arbeite dort im Client-Server-Umfeld. Ich betreue bei uns den Bereich Intranet-Technologie und Datenbank-Technik. Netzwerkerfahrung habe ich bisher ausschließlich im IBM-Umfeld, das heißt Token Ring und Grundlagen TCP/IP. Wir haben noch eine eigene Netzwerk-Abteilung, die aus zwei Kollegen besteht. Wir sind insgesamt sieben Techniker, die sich um die Bereiche Client-Server-Computing, Mainframe, PC-Management und Datenbank-Technik kümmern.

Insider: Wie lange machen Sie das schon?

Ich bin jetzt seit 9 Jahren bei der bvv beschäftigt. Ich komme aus der Mainframe-Welt, seit vier Jahren bin ich im Umfeld Datenbank-Technik, und das ganze ging dann auch in Richtung Internet-Kalenderdienste, Internet-Webserver.

Insider: Wie kamen Sie dazu die Ausbildung zum ComConsult Certified Network Engineer zu machen?

Michael Ederer: Ich habe in den letzten zwei Jahren sehr viel Arbeitsgruppen- und Projektmitarbeit geleistet. Ich wollte ganz einfach mal wieder technologisches Basiswissen aufbauen. Im Zeitalter von E-Networking und E-Commerce erschien mir das technische Know How im Netzwerk-Bereich sehr wichtig.

Insider: Wie lange brauchten Sie bis zur Prüfung?

Ich habe Anfang des Jahres begonnen alle vier Kompakt-Seminare zu besuchen, bin das also relativ komprimiert angegangen, habe aber natürlich auch zu Hause einiges zusätzlich nachgearbeitet.

Michael Ederer, ComConsult Certified Network Engineer, (unten) im Kreise der Mitabsolventen (2.v.l.)

Insider: Wie ist Ihr Eindruck von den Kursen auch für Ihre tägliche praktische Arbeit?

Michael Ederer: Die Ausbildung wird in jedem Fall aktuellen Trends der Netzwerk-Technologie gerecht. Das bewerte ich als sehr positiv. Sie deckt die gesamte Bandbreite der verschiedensten Netzwerk-Ebenen ab. Es wird ein breites Basiswissen aufgebaut und nicht eine Detail-Spezialisierung. Die Vorträge waren sehr lebendig und praxisnah.

Insider: Wie ist für Sie die Prüfung gelaufen?

Michael Ederer: Sehr erfolgreich. Sie trägt dem Zweck Rechnung, das erlernte Basiswissen erfolgreich einzusetzen.

Insider: Vielen Dank, und viel Erfolg für Ihre weitere berufliche Zukunft.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Betrieb von TCP/IP-Netzen, 19. - 21.11.01 im Queens Hotel München

Das Seminar vermittelt praxisnah die für den erfolgreichen Betrieb von IP-Netzen notwendigen Basis-Kenntnisse der TCP/IP-Technologie und geht insbesondere wird auf die für den professionellen Betrieb unverzichtbaren Hilfsmittel ein.

Prozess-Optimierung, 26. - 27.11.01 im Holiday Inn Bonn

In diesem Seminar lernen Führungskräfte und Spezialisten die methodischen Grundlagen der Wege zur Optimierung von Geschäftsprozessen um Verbesserungen in unternehmensinternen Strukturen und Abläufen zu realisieren.
Referent: Dr. Ralf Hillemacher Preis: EUR 1.290,-- zzgl. MwSt.

Migration von Windows 2000 Active Directory, 26. - 27.11.01 im Holiday Inn Bonn

Das Seminar vermittelt die grundsätzlichen Migrationsansätze und welche Tools in welcher Form dabei eingesetzt werden können.
Referenten: Markus Holländer, Dipl.-Ing. Michael van Laak Preis: EUR 1.290,-- zzgl. MwSt.

Optische Netze Forum 2001, 26. - 28.11.01 im Maritim Königswinter

Das Forum behandelt die inhaltlichen Schwerpunkte: Technologie Optischer Netze,High End Glasfaser-Übertragungssysteme, Metro- und WAN-Entwicklungen in Deutschland, Speichernetze und 10 Gigabit Ethernet.
Moderation: Dr. Franz-Joachim Kauffels Preis: EUR 1.590,-- zzgl. MwSt.

IP-VPNs erfolgreich einsetzen, 26. - 28.11.01 im Holiday Inn Bonn

Das Seminar beschäftigt sich mit dem Home-Office-/Teleworker-Zugang, dem Unternehmens-WAN-Backbone, dem Filialnetzwerk und der Standort-Kopplung, denn VPNs stellen die wichtigste Weiterentwicklung im Bereich der Weitverkehrskommunikation dar.
Referenten: Dipl.-Inform. Andreas Meder, Dr. Behrooz Moayeri, ComConsult Beratung und Planung Preis: EUR 1.590,--zzgl. MwSt.

DNS-/IP-Design für Windows 2000 Active Directory, 03. - 05.12.01 im Holiday Inn Bonn

Dieses Seminar behandelt in konzentrierter Form die Implementierungsgrundlagen aus dem IP-Bereich für Windows 2000 bzw. für das Active Directory. Dabei spielt DNS die Hauptrolle, wobei auch insbesondere die dynamische Verbindung zum DHCP betrachtet wird.
Referenten: Markus Holländer, Lars Kuhl, Michael van Laak, Frank Neunzig Preis: EUR 1.990,-- zzgl. MwSt.

Sicherer Internet-Zugang ... 03. - 05.12.01 im Holiday Inn Bonn

Das Seminar erläutert die technischen und begleitenden organisatorischen Maßnahmen, mit denen ein sicherer Internet-Zugang für E-Mail, Web und E-Business erreicht werden kann.
Referenten: Dr. Behrooz Moayeri, Dipl.-Inform. Andreas Meder Preis: EUR 1.590,-- zzgl. MwSt.

Winterschule der ComConsult Akademie 2001, 03. - 07.12.01 im Holiday Inn Bonn

Die Winterschule 2001 wendet sich gezielt an die erfahrenen Netzwerker und zeigt auf, wo der Netzwerk-Markt steht und wo er hingeht. Ausgewählte Experten diskutieren die aktuellsten technischen Entwicklungen, erläutern die Hintergründe und bewerten Vor- und Nachteile. Preis: EUR 2.290,-- zzgl. MwSt.

Internetworking, 03. - 07.12.01 im Holiday Inn Bonn

Das Seminar vermittelt die technischen und methodischen Kenntnisse zur erfolgreichen Strukturierung von Netzwerken mit Switching und Routing wobei Grundlagen-Kenntnisse Lokaler Netzwerk-Technologien erforderlich sind.
Referentin: Dipl.-Inform. Petra Borowka Preis: EUR 1.990,-- zzgl. MwSt.

TCP/IP und SNMP, 03. - 07.12.01 im Excelsior Hotel Berlin

Das Intensiv-Seminar vermittelt einen praxis-orientierten Einblick in den Aufbau und den Betrieb von heterogenen Netzen, die den Kommunikationsstandard TCP/IP und den Netzmanagement-Standard SNMP benutzen.
Referenten: Dipl.-Phys. Frank Breitschaft, Dipl.-Inform. Detlef Weidenhammer (GAI NetConsult) Preis: EUR 1.990,-- zzgl. MwSt.

xDSL: Technik und Nutzen..., 06. - 07.12.01 im Holiday Inn Bonn

Das Seminar beschreibt die Konzepte und Möglichkeiten der xDSL-Technologiefamilie, die praktisch alle Kommunikationserfordernisse heutiger Anwendungen unter vergleichsweise minimalen Investitions- und Betriebsaufwänden abdecken kann.
Referent: Dipl.-Ing. Ralf Boden, Professional Multimedia Network Systems GmbH Preis: EUR 1.290,-- zzgl. MwSt.

Anmeldeformular auf Seite 25

ComConsult Veranstaltungskalender

Die letzten Veranstaltungen 2001

Betrieb von Windows 2000 Active Directory, 06. - 07.12.01 im Holiday Inn Bonn

Das Seminar stellt an praktischen Beispielen eine Reihe von aktuellen Verwaltungswerkzeugen für den alltäglichen Betrieb vor.
Referent: Dipl.-Ing. Lars Kuhl — Preis: EUR 1.290,-- zzgl. MwSt.

Verkabelungssysteme für Lokale Netze, 10. - 11.12.01 im Holiday Inn Bonn

Das Seminar basiert auf der Erfahrung einer Vielzahl aktueller Verkabelungsprojekte und deren Betrieb. Es führt methodisch vom aktuellen Stand der Technik bis zu den Leistungsmerkmalen zukünftiger Lösungen.
Referent: Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung — Preis: EUR 1.290,-- zzgl. MwSt.

Voice over IP, 10. - 12.12 im Holiday Inn Bonn

Das Seminar informiert Sie über die Integration der Sprache in Datennetze. Sie erfahren, wie Sie diese Technik in WAN und LAN gewinnbringend einsetzen können, welche technischen Voraussetzungen erforderlich sind und wie Quality-of-Service gestaltet wird.
Referent: Dipl.-Inform. Petra Borowka, Dr.-Ing. Behrooz Moayeri — Preis: EUR 1.590,-- zzgl. MwSt.

Projekt-Management, 10. - 12.12.01 im Holiday Inn Bonn

In diesem Seminar lernen Projektleiter ein Projekt effektiv zu organisieren und überzeugend zu führen. Es basiert auf einem kreativen Mix aus Lehrvorträgen, Erfahrungsaustausch und praktischen Übungen.
Referent: Dr. Ralf Hillemacher — Preis: EUR 1.590,-- zzgl. MwSt.

Moderne Datenkommunikation, 10. - 14.12.01 im Holiday Inn Bonn

Das Intensiv-Seminar vermittelt Techniken, Verfahren und Systeme der Datenkommunikation für Ein- und Umsteiger. Der Schwerpunkt liegt auf dem erfolgreichen Einsatz der Internet/Intranet-Technologien.
Referent: Dr. Franz-Joachim Kauffels — Preis: EUR 1.990,-- zzgl. MwSt.

Neue Ethernet-Technologien, 10. - 14.12.01 in der AGIT Aachen

Das Intensiv-Seminar beschäftigt sich mit dem Ausbau bzw. Umbau dieser Netze in Richtung Fast Ethernet und Frame Switching für alle Betreiber traditioneller Ethernet-Netzwerke. Referenten: Dipl.-Inform Oliver Flüs, Dipl.-Inform. Andreas Meder, Dipl.-Ing. Hartmut Kell, Dipl.-Ing. Harald Krause, Dr. Joachim Wetzlar, ComConsult Beratung und Planung — Preis: EUR 1.990,-- zzgl. MwSt.

EMV in Anlagen und Systemen, 12. - 13.12.01 im Holiday Inn Berlin

Das Seminar stellt das GHMT-Fünf-Säulen-Modell zur Planung der elektromagnetischen Verträglichkeit in Neubau- und- Umbauprojekten vor und zeigt geeignete Maßnahmen zur Umsetzung in der Praxis auf.
Referent: Dipl.-Ing. Dirk Wilhelm (GHMT) — Preis: EUR 1.290,-- zzgl. MwSt.

ComConsult Akademie – Telefax: 02408/955-399

Anmeldung

Titel des Seminars	Name	Vorname
Termin	Firma, Abteilung	Position, Funktion
☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel	Straße	PLZ, Ort
Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**	Telefon	Fax
	eMail	Unterschrift

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebrauchte Netzwerk-Komponenten

Die Spielregeln

Gebrauchte Netzwerk-Komponenten, die im Rahmen eines Redesigns ausgemustert werden, könnten einige Betriebe sehr gut gebrauchen. Hier wollen wir helfen. Wir bauen für unsere Kunden eine Handelsplattform für gebrauchte Netzwerk-Komponenten auf. Die Spielregeln: Sie melden uns, welche Produkte/Komponenten Sie anbieten/suchen mit Ihrer Preisvorstellung.

Ihr Angebot wird in anonymer Form auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de und im Netzwerk Insider veröffentlicht.

Interessenten melden sich per Mail, mit dem Fax-Formular (unten) oder über den Web-Server bei uns. Wir stellen den Kontakt zwischen Anbieter und Nachfrager her.

Wir erhalten vom Verkäufer für diese Leistung 10% Provision auf den erzielten Kaufpreis. Davon stellen wir die Hälfte ausgewählten Schulen als Spende zum Aufbau ihres Internet-Zugangs oder ihres internen Netzwerks zur Verfügung. Der Kaufvertrag entsteht direkt zwischen Käufer und Verkäufer. Wir selber haften in keiner Form für die Qualität oder Nutzbarkeit der Komponenten.

Aktuelle Gebote und Gesuche

finden Sie auf der nächsten Seite

Weitere Gebote und Gesuche

finden Sie auf dem Web-Server der ComConsult Akademie unter

www.comconsult-akademie.de

ComConsult Akademie – Telefax: 02408/955-399

☐ **Ich suche**
☐ **Ich biete**

Produkt/Komponente/Release/Software

_____

_____

_____

_____

Preisvorstellung_____

_____

Ansprechpartner

_____

Firma

_____

Ort

_____

Straße

_____

Telefon, Fax

_____

eMail

☐ **Antwort auf Gesuch**
☐ **Antwort auf Gebot**

Produkt/Komponente/Release/Software

_____

_____

_____

_____

Preisvorstellung_____

_____

Ansprechpartner

_____

Firma

_____

Ort

_____

Straße

_____

Telefon, Fax

_____

eMail

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebote

Adapter

Madge, Token Ring BM2, MKII, MKIII alles PCI, über 100 Stck., DM 50,- /Stk.
B10802

Olicom TR PCI Adapter OC-3137, 10 Stück, DM 40,-- pro Stck. VB
B10808

Concentrator

SysKonnect SK-FDDI Concentrator, 12 Port (4x Fiber MIC + 8 x RJ45), 2 Stck., DM 3.500,--/Stck. VB,
B11006

Printserver

Hewlett Packard, Jet Direct J2594A, TR-Printserver,12 Stck., 250,-- DM/Stck. (4 Stck. ohne Netzteil)
B11003

Nortel Networks Printserver, 1 Stck. DM 250,--
B10702

Hewlett Packard, Jet Direct J2550-60013, Printserver original verpackt, 2 Stck., VS
B10903

Intel Netport Express Pro, Printserver mit 2 par. und 1 ser. Port, 1 Stck., VS
B10902

Ringleitungsverteiler

Madge, Smart CAU/LAM STP, 10 Stck., VS
B10801

Olicom OC-3612, Anzahl 17, DM 150,-- /Stck. VB, TR LAN (RJ45)
B11007

Olicom OC-3610, Anzahl 6, DM 400,-- VB, TR CAU (RI + RO = IBM-Stecker)
B11008

Switch/Brücke

IBM, 8229-01 TR/TR, 23 Stck., VB DM 500,--. Alle Brücken sind in sehr gutem Zustand, ggf. kann eine Umrüstung als Token Ring/Ethernet Brücke durchgeführt werden. Preis auf Anfrage.
B10805

Cisco Catalyst 1800, 2 Stck., je 6.000,-- DM, TR/FDDI-Switch jeweils mit 2 Netzteilen, 12 Ports TR (RJ45), 1 Port FDDI (MIC)
B11002

Sternkoppler

ASGEZ-ZE, ASGE 4, ENT 10522R mit Interfacekarten, 2 Stck., DM 4.030,--
B11001

Hirschmann Sternkoppler (HUB) mit beliebigen Modulen, LWL und Kupfer, große Mengen, VS
B11010

Sonstiges

Digital, verschiedene 900er und 90er Komponenten, z. B. VN Switches, FDDI, Glasfaser, DEC Server, Repeater in Kupfer und LWL
B10904

Allied Telesis CenteCom MX10s, Ethernettransceiver AUI-UTP, 4 Stck.,
B10901

HP FDDI-LAN-Probe J3322A, 1 Stck., DM 4.500,-- VB
B11004

HP TR-LAN-Probe 4985B, 1 Stck., DM 1.250,-- VB
B11005

Gesuche

Adapter

Lexmark MarkNet Prinserver, Anzahl min. 1, mindestens 2 x par. Anschlüsse, VS
S10806

Olicom TR Adapter 16/4 (TR3140), ca. 5 Stck., VS
S10905

CPV V.32BIS Modem, 1 Stck., VS
S11009

Ringleitungsverteiler

Madge, Smart Lan Plus, Anzahl 1 bis 2, VS
S10704

Router

Cisco kleiner Router zu Übungszwecken, Typ spielt keine Rolle, 1 Stck., bis 200,-- DM
S10809

Switch/Brücke

IBM 32-PT 10/100 TX Switching Modul RJ 45 2 k CAM 8274-0562, 1 Stck., VS
S10807

Xylan/Alcatel/IBM, Omni Switch Serie (Switche und Module) mehrere Stck., VS
S10701

Sonstige

3Com Beschreibungen/Handbuch zur Nutzung des Routing L3 auf 3Com Switches 3Com 4007 (Command Reference Guide vorhanden), VS
S10803