Vorbereiten des Einsatzes von IEEE 802.11-Netzwerken in Unternehmen

(Engl. Originaltitel: Making IEEE 802.11 Networks Enterprise-Ready)

Von Tom Fout

Microsoft Corporation

Veröffentlicht: April 2001

Zusammenfassung

Der Wunsch nach unbegrenzter Mobilität und die verbesserten Features, die durch drahtlose Konnektivität bereitgestellt werden, tragen dazu bei, dass IEEE 802.11 als einer für den Einsatz in Untemehmen geeigneten Technologie immer mehr Aufmerksamkeit zuteil wird. Bevor jedoch die drahtlose Kommunikation flächendeckend genutzt werden kann, muss eine weitere Konzentration auf die einfachere Handhabung, die Konfiguration und Verwaltung sowie Fragen der Sicherheit erfolgen. In diesem Dokument werden diese Aspekte der drahtlosen Kommunikation anhand der Erörterung der Anforderungen für RADIUS-Server, drahtlose Zugriffspunkte (Access Points, AP) und drahtlose Netzwerkkarten (Network Interface Cards, NICs) behandelt. Viele diese Technologien betreffen auch verkabelte Netzwerke, und ihre Verwendung kann zu einer Erhöhung der Sicherheit in Netzwerken beitragen, die auf Ethernet oder vergleichbaren Technologien basieren. Abschließend werden in diesem Artikel einige der Verfahren erläutert, durch die Windows 2000 die auf dem Standard 802.11 basierenden drahtlosen Technologien unterstützt und erweitert. Einführung

Dieses Whitepaper stellt technische Detailinformationen zu IEEE 802.11 als einem gemeinsamen Standard für drahtlose lokale Netzwerke (Local Area Networks, LANs) zur Verfügung. Dieses Dokument behandelt schwerpunktmäßig die folgenden Themen: Sicherheitsaspekte, Bereitstellungsaspekte, drahtlose Authentifizierung, Netzwerkkarten, Anforderungen für Zugriffspunkte und RADIUS-Server, Roaming, nicht authentifizierter Zugriff und Ad-hoc- IEEE 802.11.

Der Standard IEEE 802.11

IEEE 802.11 ist ein gemeinsamer Standard für drahtlose LANs. Er verwendet das Protokoll CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance, Vielfachzugriff mit Trägerkennung und Kollisionsvermeidung) auf MAC-Ebene (Media Access Control). Dieser Standard ermöglicht auf der Bitübertragungsschicht (physische Schicht) Übertragungen sowohl mithilfe des DS-Spreizverfahrens (Direct-Sequency) als auch mithilfe des FH-Spreizverfahrens (Frequency-Hopping). Die maximale Datenrate, die von diesem Standard ermöglicht wurde, lag ursprünglich bei 2 Mbit/s. Eine schnellere Version mit einer Definition der physischen Schicht gemäß der IEEE 802.11b-Spezifikation ermöglicht anhand von Übertragungen mittels DS-Spreizverfahren eine Datenrate von bis zu 11 Mbit/s. Das Komitee für IEEE-Standards hat mit der IEEE 802.11a-Spezifikation zudem Kriterien für die physische Schicht definiert. Diese Definition basiert auf einem Mehrträgerverfahren (Orthogonal Frequency Division Multiplexing, OFDM), das Datenübertragungsraten von bis zu 54 Mbit/s ermöglicht.

Sicherheitsaspekte

Während IEEE 802.11 in drahtlosen LAN-Umgebungen bereits eine weite Verbreitung erfahren hat, wurden bezüglich der Sicherheit drahtloser Netzwerke im Allgemeinen eine Reihe von Bedenken laut.

Der Standard IEEE 802.11 für drahtlose LANs definiert Authentifizierungs- und Verschlüsselungsdienste basierend auf dem WEP-Algorithmus (Wired Equivalent Privacy). Der WEP-Algorithmus sieht für die Authentifizierung und Verschlüsselung die Verwendung eines geheimen 40-Bit-Schlüssels vor. Viele IEEE 802.11-Implementierungen ermöglichen darüber hinaus die Verwendung geheimer 104-Bit-Schlüssel. Der Standard definiert jedoch kein Schlüsselverwaltungsprotokoll und geht davon aus, dass die geheimen, gemeinsamen Schlüssel über einen sicheren, von IEEE 802.11 unabhängigen Kanal an die drahtlose IEEE 802.11-Station (STA) übermittelt werden.

Das Fehlen eines WEP-Schlüsselverwaltungsprotokolls stellt eine grundsätzliche Einschränkung für die Gewährleistung der Sicherheit beim Einsatz von IEEE 802.11 dar, insbesondere in drahtlosen Infrastrukturnetzwerken, die eine große Anzahl von Stationen aufweisen. Beispielhaft hierfür sind Unternehmensgelände und öffentliche Orte wie Flughäfen und Einkaufszentren. Das Fehlen von Authentifizierungs- und Verschlüsselungsdiensten wirkt sich auch auf den Betrieb in drahtlosen Ad-hoc-Netzwerken aus, die sich durch die Peer-zu-Peer-Kommunikation zwischen Benutzern auszeichnen, z. B. in einem Tagungsraum.

Dies alles macht deutlich, dass aufgrund der noch größeren Bedeutung von Authentifizierung und Verschlüsselung in drahtlosen Umgebungen Zugriffssteuerungs- und Sicherheitsmechanismen notwendig sind, die das in IEEE 802.11 angegebene Schlüsselverwaltungsprotokoll umfassen.

Bereitstellungsaspekte

Aspekte, die die Bereitstellung von IEEE 802.11 betreffen, lassen sich in drei Hauptgruppen unterteilen: Benutzerverwaltung, Schlüsselverwaltung und Sicherheit.

- Benutzerverwaltung

Die Anbindung an bestehende Tools zur Benutzerverwaltung ist unverzichtbar [RADIUS (Remote Authentication Dial-In User Service) und LDAP-basierte Verzeichnisse (Lightweight Directory Access Protocol)]. Ein Beispiel hierfür wäre die Erstellung einer Gruppe, der der Zugriff über eine drahtlose Verbindung ermöglicht wird. Sobald diese Gruppe einschließlich der entsprechenden Zugriffsberechtigungen eingerichtet wurde, wird jedem Benutzer, der Mitglied der Gruppe ist, der Zugriff über eine drahtlose Verbindung gestattet.

In großen Netzwerkumgebungen kann die Identifizierung anhand des Benutzernamens leichter verwaltet werden als der derzeit verwendete Identifizierungsmechanismus mittels MAC-Adresse. Die Identifizierung des Benutzers anhand seines Namens bietet darüber hinaus die Vorteile der Nutzung auf Benutzerebene, der Kontenverwaltung und der Überwachung.

- Schlüsselverwaltung

Die Verwaltung statischer Schlüssel auf Stationen und Zugriffspunkten (Access Points, APs) gestaltet sich problematisch. Darüber hinaus sind für Lösungen, die die proprietäre Schlüsselverwaltung einsetzen, getrennte Benutzerdatenbanken erforderlich.

- Sicherheit

Für 802.11 gelten die folgenden Sicherheitseinschränkungen:

- Keine Authentifizierung auf Paketebene
- Anfälligkeit für unberechtigte Zugriffe, die den Abbruch einer Funkverbindung herbeiführen können
- Keine Benutzeridentifikation und -authentifizierung
- Keine Unterstützung für zentrale Authentifizierung, Autorisierung und Kontenverwaltung
- Die RC4-Streamverschlüsselung ist anfällig für Klartextangriffe
- Einige Implementierungen leiten WEP-Schlüssel von Kennwörtern ab
- Keine Unterstützung für erweiterte Authentifizierung, z. B. durch Tokenkarten, Zertifikate, Smartcards, One-Time-Kennwörter, biometrische Sicherheitsvorrichtungen usw.
- Probleme der Schlüsselverwaltung, z. B. erneute Verwendung globaler Schlüssel und keine dynamische, auf STA-Unicast-Sitzungen basierende Schlüsselverwaltung

Derzeitige Sicherheitsoptionen für IEEE 802.11

Die von IEEE 802.11 bereitgestellten Sicherheitsoptionen umfassen Authentifizierungs- und Verschlüsselungsdienste, die auf dem WEP-Algorithmus basieren. Der WEP-Algorithmus sieht für die Authentifizierung und Verschlüsselung die Verwendung eines geheimen 40-Bit-Schlüssels vor. Ergänzend zu dem geheimen 40-Bit-Schlüssel ermöglichen zahlreiche IEEE 802.11-Implementierungen die Verwendung von geheimen 104-Bit-Schlüsseln.

Beim Einsatz von IEEE 802.11 ist es nicht erforderlich, dass alle Stationen dieselben WEP-Schlüssel verwenden. Zudem ist es möglich, dass eine Station zwei Sätze gemeinsamer Schlüssel verwendet: einen stationsspezifischen Unicast-Sitzungsschlüssel und einen Multicast- oder globalen Schlüssel. Aktuelle IEEE 802.11-Implementierungen unterstützen in erster Linie Multicast- oder globale Schlüssel; in absehbarer Zeit kann jedoch auch mit der Unterstützung von stationsspezifischen Unicast-Sitzungsschlüsseln gerechnet werden.

Authentifizierungsdienste: Open System und Shared Key

IEEE 802.11 unterstützt zwei Arten von Authentifizierungsdiensten: Open System und Shared Key. Die Art der "aufgerufenen" Authentifizierung wird durch den **AuthenticationType**-Parameter gesteuert, während die Art der von einer Station "akzeptierten" Authentifizierung von Sicherheitsmechanismen gesteuert wird, die durch das MIB-Attribut (Management Information Base) **dot11AuthenticationType** definiert werden.

Open System ist ein Standardalgorithmus für die Null-Authentifizierung, der einen aus zwei Schritten bestehenden Prozess – die Identitätsassertion und eine Authentifizierungsanforderung – gefolgt von dem Authentifizierungsergebnis umfasst.

Shared Key unterstützt die Authentifizierung einer Station entweder als Mitglied derjenigen Stationen, denen ein gemeinsamer, geheimer Schlüssel bekannt ist, oder als Mitglied der Stationen, denen dieser Schlüssel nicht bekannt ist. Der Standard setzt derzeit voraus, dass der gemeinsame Schlüssel über einen sicheren, von IEEE 802.11 unabhängigen Kanal an die teilnehmenden Stationen übermittelt wird.

WEP stellt Verschlüsselungsdienste bereit, um autorisierte Benutzer eines drahtlosen LANs vor Abhörversuchen zu schützen, und stellt Attribute zur Gewährleistung der physischen Sicherheit bereit, die denen eines verkabelten LANs vergleichbar sind. WEP ist ein symmetrischer Algorithmus, in dem derselbe Schlüssel für die Ver- und Entschlüsselung verwendet wird. Der geheime Schlüssel wird mit einem Initialisierungsvektor (IV) verknüpft, was zu einem Anfangswert führt, der als Eingabe für einen Pseudozufallszahlen-Generator (Pseudo-Random Number Generator, PRNG) verwendet wird. Mithilfe des PRNGs wird die Schlüsselfolge generiert, die mathematisch mit dem Nachrichtentext kombiniert und mit dem Integritätsprüfwert (Integrity Check Value, ICV) verknüpft wird. Das Triplett {IV, Nachrichtentext, ICV} bildet die tatsächlichen Daten, die in einem IEEE 802.11-Datenrahmen gesendet werden.

Während der geheime Schlüssel über längere Zeit konstant bleibt, wird der IV regelmäßig, und zwar so häufig wie jede MAC-Protokolldateneinheit (MAC Protocol Data Unit, MPDU), geändert. Die Häufigkeit, mit der IV-Werte geändert werden, hängt vom Grad der Vertraulichkeit ab, die vom WEP-Algorithmus angefordert wird. Die Änderung des IVs nach jedem MPDU ist die optimale Methode zur Aufrechterhaltung der Wirksamkeit von WEP.

Fehlen eines WEP-Schlüsselverwaltungsprotokolls

Das Fehlen eines WEP-Schlüsselverwaltungsprotokolls stellt eine Einschränkung für die Bereitstellung von IEEE 802.11-Sicherheitsdiensten dar, insbesondere in drahtlosen Infrastrukturnetzwerken, die eine große Anzahl von Stationen aufweisen. Das Fehlen von Authentifizierungs- und Verschlüsselungsdiensten wirkt sich zudem auf den Betrieb in drahtlosen Ad-hoc-Netzwerken aus.

Die derzeit von IEEE 802.11 bereitgestellte Sicherheitsoption für die Zugriffssteuerung passt sich nicht angemessen an ausgedehnte Infrastrukturnetzwerke (z. B. Unternehmensgelände oder öffentliche Orte) oder an Ad-hoc-Netzwerke an. Beim Roaming von Stationen von einem Zugriffspunkt zu einem anderen führt das Fehlen eines zugriffspunktübergreifenden Protokolls (Inter-Access Point Protocol, IAPP) darüber hinaus zu weiteren Problemen hinsichtlich der Schlüsselverwaltung.

IEEE 802.1X

IEEE 802.1X ist der Entwurf für einen Standard für die anschlussbasierte Netzwerkzugriffssteuerung. Mithilfe dieses Standards soll der authentifizierte Netzwerkzugriff für Ethernet-Netzwerke ermöglicht werden. Die anschlussbasierte Netzwerkzugriffssteuerung verwendet die physischen Merkmale vermittelter LAN-Infrastrukturen, um eine Methode zur Authentifizierung von Geräten bereitzustellen, die an einen LAN-Anschluss angeschlossen sind, und um den Zugriff auf den Anschluss zu verhindern, falls der Authentifizierungsprozess fehlschlägt.

Authentifikator oder Endsystem (Supplicant)

Ein LAN-Anschluss, auch als Anschlusszugriffsentität (Port Access Entity, PAE) bezeichnet, kann im Rahmen der Interaktion zum Zwecke der Zugriffssteuerung eine von zwei Funktionen übernehmen: die des Authentifikators oder die des Endsystems.

Ein Authentifikator ist ein Anschluss, der die Authentifizierung "erzwingt", bevor er den Zugriff auf die über diesen Anschluss verfügbaren Dienste zulässt. Das Endsystem ist ein Anschluss, der den Zugriff auf die über den Anschluss des Authentifikators verfügbaren Dienste "anfordert".

Darüber hinaus übernimmt der Authentifizierungsserver ebenfalls die Authentifizierungsfunktion. Er überprüft die Anmeldeinformationen des Endsystems anstelle des Authentifikators und antwortet dem Authentifikator, indem er ihm mitteilt, ob das Endsystem befugt ist, auf die Dienste des Authentifikators zuzugreifen. Bei dem Authentifizierungsserver kann es sich um eine separate Entität handeln, seine Funktionalität kann sich jedoch auf derselben Entität wie der Authentifikator befinden.

Kontrollierte und nicht kontrollierte Anschlüsse

Die portbasierte Zugriffssteuerung des Authentifikators definiert über einen einzelnen physischen LAN-Anschluss zwei logische Zugriffspunkte für das LAN, wie in Abbildung 1 veranschaulicht wird.

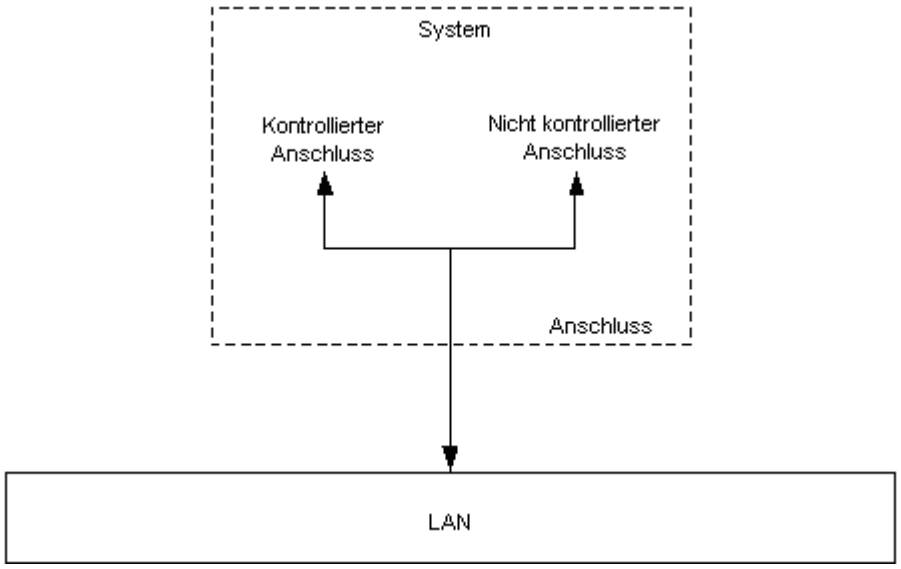

Abbildung 1: Kontrollierte und nicht kontrollierte Anschlüsse

Der erste logische Zugriffspunkt (der als "Nicht kontrollierter Anschluss" bezeichnete Anschluss) ermöglicht den unkontrollierten Austausch zwischen dem Authentifikator und anderen Systemen im LAN, unabhängig vom Autorisierungsstatus des jeweiligen Systems. Der zweite logische Zugriffspunkt (der als "Kontrollierter Anschluss" bezeichnete Anschluss) ermöglicht den Austausch zwischen einem System im LAN und den Diensten des Authentifikators nur dann, wenn das jeweilige System befugt ist, auf die Dienste zuzugreifen.

Verwenden von IEEE 802.1X für die drahtlose Authentifizierung

Mithilfe eines RADIUS-Servers (Remote Authentication Dial-In Service) für die Authentifizierung von Clientanmeldeinformationen kann IEEE 802.1X für die drahtlose Authentifizierung verwendet werden.

Damit Datenpakete eines bestimmten Clients zuverlässig von einem drahtlosen Zugriffspunkt identifiziert werden können, ist eine Erweiterung des IEEE 802.1X-Basisprotokolls erforderlich. Die Erweiterung erfolgt, indem dem Client und dem drahtlosen Zugriffspunkt im Rahmen des Authentifizierungsverfahrens ein Authentifizierungsschlüssel übergeben wird. Nur authentifizierte Clients kennen den Authentifizierungsschlüssel, mit dem sämtliche von einem Client gesendeten Pakete verschlüsselt werden.

Authentifizierung: Das Verfahren im Überblick

Die folgenden Schritte stellen überblicksartig das Verfahren dar, das von einem Zugriffspunkt und einem RADIUS-Server zur Authentifizierung einer Station verwendet wird.

Ohne einen gültigen Authentifizierungsschlüssel unterbindet ein Zugriffspunkt den gesamten Datenfluss, der über ihn erfolgt.

- Wenn eine drahtlose Station (ein Endsystem) in den Funkbereich eines drahtlosen Zugriffspunktes eintritt, gibt der drahtlose Zugriffspunkt eine Herausforderung an die drahtlose Station aus.
- Bei Erhalt der Herausforderung vom Zugriffspunkt antwortet die Station mit ihrer Identität.
- Der Zugriffspunkt leitet die Identität der Station dann an den RADIUS-Server (den Authentifizierungsserver) weiter, um die Authentifizierungsdienste aufzurufen.

Anschließend fordert der RADIUS-Server die Anmeldeinformationen für die Station an, wobei er den Typ der Anmeldeinformationen angibt, die erforderlich sind, um die Identität der Station zu bestätigen.

- Die Station sendet ihre Anmeldeinformationen an den RADIUS-Server.
- Werden die Anmeldeinformationen der Station validiert, übermittelt der RADIUS-Server einen Authentifizierungsschlüssel an den Zugriffspunkt. Der Authentifizierungsschlüssel ist verschlüsselt, so dass nur der Zugriffspunkt darauf zugreifen kann.

(Beachten Sie, dass Anforderungen, die zwischen der Station und dem RADIUS-Server gesendet werden, den "nicht kontrollierten Anschluss" des Zugriffspunktes passieren, da die Station nicht direkt mit dem RADIUS-Server kommunizieren kann. Der Zugriffspunkt lässt die Kommunikation über den "kontrollierten" Anschluss nicht zu, da die Station nicht über einen Authentifizierungsschlüssel verfügt.)

- Der Zugriffspunkt verwendet den vom RADIUS-Server erhaltenen Authentifizierungsschlüssel, um stationsspezifische Unicast-Sitzungsschlüssel und Multicast- bzw. globale Authentifizierungsschlüssel an die Station zu übermitteln.

Der globale Authentifizierungsschlüssel muss verschlüsselt sein. Um dies zu gewährleisten, muss die verwendete EAP-Methode (Extensible Authentication Protocol) in der Lage sein, im Rahmen des Authentifizierungsprozesses einen Verschlüsselungsschlüssel zu generieren.

Transportschichtsicherheit (Transport Level Security, TLS)

Transportschichtsicherheit (Transport Level Security, TLS) ermöglicht die gegenseitige Authentifizierung, die Aushandlung der verwendeten Verschlüsselungsmechanismen bei Gewährleistung der Integrität und den Schlüsselaustausch zwischen zwei Endpunkten. Vor diesem Hintergrund empfiehlt sich die Verwendung von EAP-TLS, um die TLS-Mechanismen innerhalb von EAP bereitzustellen.

Im Anschluss an die Authentifizierung sollte das Protokoll IEEE 802.1X so konfiguriert werden, dass die erneute Authentifizierung der Station in regelmäßigen, festgelegten Abständen angefordert wird.

Authentifizierung: Das Verfahren im Detail

- Der drahtlose Zugriffspunkt ist so konfiguriert, dass ohne gültige Authentifizierungsschlüssel keine Datenpakete an ein verkabeltes Netzwerk, z. B. ein Ethernet-Netzwerk, oder an eine andere drahtlose Station weitergeleitet werden. Der drahtlose Zugriffspunkt und die drahtlose Station müssen einen Multicast- bzw. globalen Authentifizierungsschlüssel unterstützen und können darüber hinaus die Unterstützung für einen stationsspezifischen Unicast-Sitzungsschlüssel bieten.
- Der drahtlose Zugriffspunkt verfügt über einen Prozess, der Abfragen im Hinblick auf IEEE 802.1X-Verkehr – mit oder ohne Authentifizierungsschlüssel – durchführt.
- Wenn der Zugriffspunkt eine neue Station ermittelt, die eine Funkverbindung herstellen möchte, übermittelt der IEEE 802.1X-Prozess des Zugriffspunktes eine EAP-Request-Nachricht (Identity) an die neue Station.
- Wenn der IEEE 802.1X-Prozess des Zugriffspunktes eine EAP-Start-Nachricht von einer Station empfängt, übermittelt der IEEE 802.1X-Prozess eine EAP-Request-Nachricht (Identity) an die entsprechende Station.
- Wenn eine Station eine Funkverbindung zu einem neuen Zugriffspunkt aufbauen möchte, übermittelt sie eine EAP-Start-Nachricht.
- Falls kein Benutzer an das Gerät angemeldet ist, übermittelt eine Station als Antwort auf eine EAP-Request-Nachricht (Identity) eine EAP-Response-Nachricht (Identity) mit dem Namen des Geräts. Falls ein Benutzer an das Gerät angemeldet ist, übermittelt eine Station als Antwort auf eine EAP-Request-Nachricht (Identity) eine EAP-Response-Nachricht (Identity) mit dem Namen des Benutzers.
- Der drahtlose Zugriffspunkt leitet die EAP-Response-Nachricht (Identity) an einen RADIUS-Server weiter.
- Als Antwort auf die EAP-Response-Nachricht (Identity) der Station sendet der RADIUS-Server eine EAP-Request-Nachricht (entweder MD5 Challenge oder TLS). (TLS ist für die drahtlose Kommunikation erforderlich. Andernfalls ist der RADIUS-Server nicht in der Lage, die sichere Übertragung der Multicast- bzw. globalen Authentifizierungsschlüssel und, falls erforderlich, der stationsspezifischen Sitzungsschlüssel an die Station zu gewährleisten).
- Der drahtlose Zugriffspunkt leitet die EAP-Request-Nachricht vom RADIUS-Server an die Station weiter.
- Die Station übermittelt eine EAP-Response-Nachricht mit ihren Anmeldeinformationen über den drahtlosen Zugriffspunkt an den RADIUS-Server.
- Der drahtlose Zugriffspunkt leitet die Anmeldeinformationen der Station an den RADIUS-Server weiter.
- Der RADIUS-Server überprüft die Anmeldeinformationen der Station und generiert eine Erfolgsnachricht für die Station. Die Antwort des RADIUS-Servers an den drahtlosen Zugriffspunkt enthält die Stationsnachricht und den Verschlüsselungsschlüssel, der vom EAP-TLS-Sitzungsschlüssel abgeleitet wurde.
- Der drahtlose Zugriffspunkt generiert den Multicast- bzw. globalen Authentifizierungsschlüssel, indem er eine Zufallszahl generiert oder ihn aus zuvor festgelegten Werten auswählt.
- Sobald der drahtlose Zugriffspunkt die Nachricht des RADIUS-Servers erhält, leitet er die Erfolgsnachricht an die Station weiter.
- Der drahtlose Zugriffspunkt übermittelt eine EAP-Key-Nachricht an die Station, die den Multicast- bzw. globalen Authentifizierungsschlüssel enthält, der mithilfe des sitzungsspezifischen Verschlüsselungsschlüssels verschlüsselt wurde.
- Wenn der drahtlose Zugriffspunkt und die drahtlose Station stationsspezifische Unicast-Sitzungsschlüssel unterstützen, verwendet der Zugriffspunkt den vom RADIUS-Server gesendeten Verschlüsselungsschlüssel als stationsspezifischen Unicast-Sitzungsschlüssel.

- Wenn der drahtlose Zugriffspunkt den Multicast- bzw. globalen Authentifizierungsschlüssel ändert, generiert er EAP-Key-Nachrichten: Jede Nachricht enthält den neuen Multicast- bzw. globalen Authentifizierungsschlüssel, der mit dem stationsspezifischen Unicast-Sitzungsschlüssel der jeweiligen Station verschlüsselt wurde.
- Falls die entsprechende Unterstützung vorhanden ist, fügt der drahtlose Zugriffspunkt den stationsspezifischen Unicast-Sitzungsschlüssel zur stationsspezifischen Liste der Unicast-Sitzungsschlüssel hinzu.
- Bei Erhalt der EAP-Key-Nachricht verwendet die Station den stationsspezifischen Unicast-Sitzungsschlüssel, um den Multicast- bzw. globalen Authentifizierungsschlüssel zu entschlüsseln.
- Wenn der drahtlose Zugriffspunkt und die drahtlose Station stationsspezifische Unicast-Sitzungsschlüssel unterstützen und ein Multicast- bzw. globaler Authentifizierungsschlüssel empfangen wurde, wird der vom EAP-TLS-Sitzungsschlüssel abgeleitete Sitzungsschlüssel als stationsspezifischer Unicast-Sitzungsschlüssel an die drahtlosen Station übergeben.
- Bei Erhalt der Authentifizierungsschlüssel muss der Treiber der drahtlosen Netzwerkkarte die Netzwerkkarte der drahtlosen Station programmieren. Sobald die Programmierung der Authentifizierungsschlüssel abgeschlossen ist, ruft die Station DHCP (Dynamic Host Configuration Protocol) auf, um den DHCP-Prozess neu zu starten.

Anforderungen für Netzwerkkarten

Die Einbeziehung von IEEE 802.11 sowohl im Infrastruktur- als auch im Ad-hoc-Netzwerkmodus kann durch die Reduktion der Komplexität der NIC-Konfiguration erheblich verbessert werden. Es wird empfohlen, die NIC-Konfiguration zu automatisieren, um eine Benutzerintervention so weit wie möglich zu vermeiden.

Aspekte der NIC-Konfiguration

Die zentralen Aspekte der NIC-Konfiguration, die besondere Beachtung erfordern, sind die folgenden:

- Konfiguration des Clients unter unterschiedlichen Betriebsszenarien
- Neukonfiguration des Clients beim Wechsel zwischen Betriebsszenarien
- Konfiguration des Clients zur Sicherung des Zugriffs auf drahtlose LANs

Erweiterungen für IEEE 802.11-NICs

Ergänzend zu den zuvor aufgeführten Konfigurationsaspekten sollte die IEEE 802.11-NIC die folgenden Erweiterungen umfassen:

- **WEP-Authentifizierung (Wireless Equivalent Privacy)** – Ergänzend zu den Authentifizierungsdiensten Open System und Shared Key sollte die IEEE 802.11-NIC in der Standardeinstellung eine dritte Authentifizierungsmethode unterstützen. Wenn die NIC vorab mit einem gemeinsamen WEP-Schlüssel konfiguriert wurde, versucht der Standard-Authentifizierungsalgorithmus zuerst die Shared Key-Authentifizierung von IEEE 802.11 durchzuführen. Falls diese Authentifizierung fehlschlägt oder die NIC nicht vorab mit einem gemeinsamen WEP-Schlüssel konfiguriert wurde, sollte die NIC auf die Open System-Authentifizierung zurückgreifen.
- **Stromversorgungsmodi** – Eine IEEE 802.11-NIC sollte zwei Einstellungen für die Stromversorgung unterstützen: eine für Geräte, die an eine Wechselstromquelle angeschlossen sind, und eine zweite Einstellung für Geräte, die eine Batterie verwenden. Der Standardmodus (Wechselstrom) sollte so konfiguriert sein, dass die Betriebsgeschwindigkeit des Geräts maximiert wird; die Einstellung für die Stromzufuhr mittels Batterie sollte so konfiguriert sein, dass der Stromverbrauch des Geräts minimiert wird.
- **Clientname** – Der Clientname wird an die IEEE 802.11-NIC übergeben und zu unterschiedlichen Zwecken eingesetzt. Viele Anbieter von 802.11-NICs und Zugriffspunkten verwenden diese Informationen, um Clientinformationen am Zugriffspunkt zu melden und auf diesem zu verwalten. Standardmäßig wird als Clientname der Name des Geräts verwendet.

- **Medienerkennung** – Die IEEE 802.11-NIC muss die Medienerkennung unterstützen und ein Medienverbindungsereignis anzeigen, sobald eine Funkverbindung zu einem neuen Zugriffspunkt aufgebaut wird. Das Verbindungsereignis weist den Transport darauf hin, dass er auf einen möglichen Subnetzwechsel achten muss. Ein Trennereignis ist nur dann erforderlich, wenn die NIC über keinerlei Konnektivität mehr verfügt.

NDIS-Änderungen

Im Folgenden werden die Änderungen umrissen, die an der Spezifikation für Netzwerkgeräte-Schnittstellen (Network Device Interface Specification, NDIS) vorgenommen wurden, um die zuvor beschriebenen NIC-Erweiterungen zu unterstützen.

- Der Gerätename wird während des Systemstarts an den NIC-Treiber übergeben. Diese Informationen werden von einigen NICs und Zugriffspunkten zu unterschiedlichen Verwaltungszwecken verwendet.
- Der Stromversorgungsstatus wird während des Systemstarts und bei jeder Statusänderung an den NIC-Treiber übergeben. Als Minimalanforderung muss erfüllt sein, dass dem NIC-Treiber ein Wechsel zur Wechselstromeinstellung oder zur Batterieeinstellung angezeigt wird.
- NDIS ruft **PnPEventNotifyHandler()** des Miniports auf, wodurch der Miniport bei Profiländerungen mit dem Stromversorgungsstatus D0 initialisiert oder auf diesen festgelegt wird. Der **PnPEvent**-Parameter entspricht **NdisDevicePnPEventPowerProfileChanged**, und **InformationBuffer** zeigt auf eine ULONG-Variable mit folgendem Inhalt:

```
typedef enum _NDIS_POWER_PROFILE
{
NdisPowerProfileBattery,
NdisPowerProfileAcOnLine
} NDIS_POWER_PROFILE, *PNDIS_POWER_PROFILE;
```

NDIS-Objektkennungen (Object Identifiers, OIDs)

Um die zuvor beschriebene neue Funktionalität zu ermöglichen, muss der IEEE 802.11-NDIS-Treiber eine Reihe neuer OIDs bereitstellen. Diese OIDs sind über Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI) verfügbar und müssen unterstützt werden. Diese Anforderung kann nur erfüllt werden, wenn die für das drahtlose LAN (Wireless LAN, WLAN) verwendete NIC-Hardware die entsprechende Funktionalität unterstützt.

In der folgenden Tabelle finden Sie eine Zusammenfassung der abhängigen Objekte für die drahtlose Kommunikation. Die NDIS-Typen, die mit diesen WLAN-OIDs verwendet werden, finden Sie in Anhang A.

WLAN-abhängige Objekte für die drahtlose Kommunikation

OID (Hexa-dezimalwert)	OID-Name	Status-anzeige	Abfragen	Festlegen	Obligatorisch
0D010101	OID_802_11_BSSID		X	X	X
0D010102	OID_802_11_SSID		X	X	X
0D010203	OID_802_11_NETWORK_ TYPES_SUPPORTED		X		
0D010204	OID_802_11_NETWORK_ TYPE_IN_USE		X	X	X
0D010205	OID_802_11_TX_POWER_LEVEL		X	X	
0D010206	OID_802_11_RSSI	X	X		X
0D010207	OID_802_11_RSSI_TRIGGER		X	X	

OID (Hexa-dezimalwert)	OID-Name	Status-anzeige	Abfragen	Festlegen	Obligatorisch
0D010108	OID_802_11_INFRASTRUCTURE_ MODE		X	X	X
0D010209	OID_802_11_FRAGMENTATION_ THRES HOLD		X	X	
0D01020A	OID_802_11_RTS_THRESHOLD		X	X	
0D01020B	OID_802_11_NUMBER_OF_ ANTENNAS		X		
0D01020C	OID_802_11_RX_ANTENNA_ SELECTED		X	X	
0D01020D	OID_802_11_TX_ANTENNA_ SELECTED		X	X	
0D01020E	OID_802_11_SUPPORTED_ RATES		X		X
0D010210	OID_802_11_DESIRED_RATES		X	X	
0D010211	OID_802_11_CONFIGURATION		X	X	X
0D020212	OID_802_11_STATISTICS		X		
0D010113	OID_802_11_ADD_WEP			X	X
0D010114	OID_802_11_REMOVE_WEP			X	X
0D010115	OID_802_11_DISASSOCIATE			X	X
0D010216	OID_802_11_POWER_MODE		X	X	
0D010217	OID_802_11_BSSID_LIST		X		X
0D01011A	OID_802_11_BSSID_LIST_SCAN			X	X
0D010118	OID_802_11_AUTHENTICATION_ MODE		X	X	X
0D010119	OID_802_11_PRIVACY_FILTER		X	X	

SSID-Verbindungsanforderung/-algorithmus (Service Set Identifier, Dienstsatzidentifizierung)

Die NIC sollte standardmäßig ohne Konfiguration eines Netzwerknamens installiert werden. Diese Konfiguration sollte den nachfolgend aufgeführten Algorithmus einhalten:

- Falls keine Funkverbindung zu einem Netzwerk besteht, sollte die NIC eine Funkverbindung zu jeder Netzwerkinfrastruktur aufbauen, die ihren Netzwerknamen mittels Beacon-Nachricht signalisiert.
- Falls der Verbindungsaufbau fehlschlägt, muss der Versuch unternommen werden, eine Funkverbindung zu einer anderen Netzwerkinfrastruktur, falls verfügbar, aufzubauen.
- Diese Vorgehensweise wird wiederholt, bis keine Infrastrukturen mehr verfügbar sind.

- Falls keine Funkverbindung aufgebaut werden konnte, sollte die NIC, falls zulässig, in den Ad-hoc-Netzwerkmodus wechseln, bis eine neue Infrastruktur verfügbar wird.
- Wenn bei bestehender Funkverbindung zu einem Netzwerk die festgelegte Dienstsatzidentifzierungs-OID aufgerufen wird, verhält sich die NIC so, als ob der Verbindungsaufbau zu diesem Netzwerk fehlgeschlagen wäre.

Durch Festlegen der Dienstsatzidentifizierung oder durch einen Aufruf von OID_802_11_INFRASTRUCTURE_MODE sollte diese Verbindungsanforderung/dieser Algorithmus zurückgesetzt werden.

Anforderungen für Zugriffspunkte

Für die Einbindung von Sicherheitsdiensten in Zugriffspunkte benötigt IEEE 802.1X zusätzliche Tools. Bei diesen Tools handelt es sich um Verwendung der SSID als EAP-Identity-Text und die RADIUS-Unterstützung.

SSID als EAP-Identity-Text

Die IEEE 802.11-SSID sollte in das EAP-Identity/Request-Nachrichtenfeld kopiert werden.

(Detailinformationen zur Verwendung der EAP-Request-Nachricht (Identity) wurden bereits zuvor in diesem Dokument bereitgestellt. Detailinformationen zur Verwendung der EAP-Identity/Request-Zeichenfolge finden Sie in Anhang B.)

RADIUS-Unterstützung

Der RADIUS-Client des Zugriffspunktes sollte die erneute Übertragung verloren gegangener Pakete implementieren. In Umgebungsszenarien (mittels EAP-TLS) mit hohem Störpegel, die zahlreiche Phasen des Datenaustauschs durchlaufen, wird es empfohlen, für den RADIUS-Client die erneute Übertragung basierend auf einem Timeout zu implementieren. (Der Timeout kann in Abhängigkeit von den Besonderheiten des Netzwerkes geändert werden). Hierfür ist es erforderlich, dass der RADIUS-Server den Status aufrecht erhält und in der Lage ist, erneuten Übertragungen Rechnung zu tragen.

Failoverschutz

Der RADIUS-Client des Zugriffspunktes sollte darüber hinaus den Failoverschutz implementieren. Dies erhöht die Zuverlässigkeit des Zugriffs des RADIUS-Clients auf den RADIUS-Server, indem es dem RADIUS-Client ermöglicht wird, seine Transaktionen an einen anderen RADIUS-Server zu richten, falls der primäre RADIUS-Server ausfällt. Hierdurch wird ein Einzelpunktversagen verhindert.

WEP-Schlüssel

Der WEP-Schlüssel kann im Zugriffspunkt konfiguriert oder vom Zugriffspunkt mithilfe eines Zufallszahlengenerators generiert werden. Durch die Konfiguration desselben WEP-Schlüssels in mehreren Zugriffspunkten kann jeder Zugriffspunkt eine Station sofort authentifizieren, sobald der Zugriffspunkt eine IEEE 802.11-Authentifizierung mit dem korrekten WEP-Schlüssel durchführt.

IEEE 802.1X-Schlüsselnachricht

Durch die Einbindung einer IEEE 802.1X-Schlüsselnachricht stellt IEEE 802.1X einen besser skalierbaren und verwaltbaren Mechanismus für die Zugriffssteuerung zur Verfügung. Nachdem die IEEE 802.1X-Authentifizierung erfolgreich abgeschlossen wurde, wird der EAPOL-Schlüssel (EAP-over-LAN) vom Zugriffspunkt an die Station gesendet. Diese Nachricht enthält einen WEP-Schlüssel, mit dessen Hilfe der von IEEE 802.11 verwendete Verschlüsselungsschlüssel generiert wird. Für diese Nachricht ist jedoch eine EAP-Authentifizierungsmethode, wie z. B. EAP-TLS, erforderlich.

Mithilfe dieses vom RADIUS-Server erstellten sitzungsspezifischen Schlüssels wird ein sitzungsspezifischer Verschlüsselungsschlüssel generiert, mit dem der WEP-Schlüssel verschlüsselt wird. Der RADIUS-Server berechnet den sitzungsspezifischen Verschlüsselungsschlüssel und übergibt ihn in der Erfolgsnachricht an den Zugriffspunkt. Der verschlüsselte WEP-Schlüssel wird dann vom Zugriffspunkt an die Station übermittelt. Wird IEEE 802.1X und WEP verwendet, ermöglichen Stationen und Zugriffspunkte den Empfang verschlüsselter und nicht verschlüsselter Datenpakete (wie im Standard IEEE 802.11 festgelegt).

Wenn die WEP-Schlüsselverteilung aktiviert ist, sollte der Zugriffspunkt eine weitere Überprüfung durchführen und alle nicht verschlüsselten Nicht-IEEE 802.1X-Datenpakete verwerfen. Es wird empfohlen, dass Zugriffspunkte diese zusätzliche Filterung vornehmen, um das Maß an Sicherheit über die Standardfilterung anhand von MAC-Adressen (Media Access Control) hinaus zu verbessern.

EAPOL–Key

Die EAPOL-Key-Nachricht (EAP-over-LAN) betrifft nur IEEE 802.11-Netzwerke. Sie ermöglicht es dem drahtlosen Zugriffspunkt, einen oder mehrere WEP-Schlüssel vom Zugriffspunkt an die Station zu senden. Zur Unterstützung der Vertraulichkeit benötigt jeder Zugriffspunkt einen einzelnen globalen WEP-Schlüssel. Dieser WEP-Schlüssel kann zufällig vom Zugriffspunkt generiert oder konfiguriert und mittels der EAPOL-Key-Nachricht an eine Station übergeben werden.

Der Zugriffspunkt sollte zwei globale Schlüssel verwenden, zwischen denen er wechselt, wenn der Schlüssel geändert wird. Nach der Authentifizierung können Zugriffspunkte jederzeit eine EAPOL-Key-Nachricht senden, um die WEP-Schlüssel auf den Stationen zu aktualisieren.

Der stationsspezifische Unicast-Sitzungsschlüssel wird erhalten, indem frühere Benutzerauthentifizierungsschlüssel wiederverwendet werden. Dies ist gemäß RFC 2548 zulässig, in der die Microsoft-Herstellerattribute definiert sind, die der RADIUS-Server an den RADIUS-Client des Zugriffspunktes sendet.

Der Zugriffspunkt kann den WEP-Schlüssel senden, um eine Datenübertragung von der Station zum Zugriffspunkt zu ermöglichen. Es ist jedoch möglich, dass der Zugriffspunkt den WEP-Schlüssel nicht sendet. Falls der Zugriffspunkt den WEP-Schlüssel nicht sendet, sollte die Station das **MS-MPPE-Send-Key**-Attribut als WEP-Schlüssel verwenden, um Datenübertragungen von der Station zum Zugriffspunkt zu ermöglichen.

Anmerkung Die Hersteller-ID von Microsoft ist 311. Weitere Informationen finden Sie in RFC 2548.

Wechseln zwischen Zugriffspunkten

Beim Wechsel zwischen Zugriffspunkten wird die Adresse des vorherigen Zugriffspunktes von der Station an den neuen Zugriffspunkt übergeben. Wenn die Zugriffspunkte keine zugriffspunktübergreifende Unterstützung bereitstellen, wird die Station für den neuen Zugriffspunkt mithilfe einer EAP-Start-Nachricht vom Zugriffspunkt erneut authentifiziert.

Es kann jedoch ein zugriffspunktübergreifendes Protokoll (Inter-Access Point Protocol, IAPP) definiert werden, das es dem neuen Zugriffspunkt ermöglicht, die Authentifizierungsinformationen von dem alten Zugriffspunkt zu erhalten und eine neue EAPOL-Key-Nachricht mit einem neuen Satz an WEP-Schlüsseln an die Station zu senden. Durch das IAPP sollten zudem ausreichende RADIUS-Server-Kontoinformationen an den neuen Zugriffspunkt übermittelt werden, damit der Zugriffspunkt weiterhin dieselben Kontendatensätze verwenden kann und keine neuen anlegen muss.

Verwendung der WEP-Authentifizierung

Wenn mehrere Zugriffspunkte mit demselben WEP-Schlüssel konfiguriert wurden, implementiert der Zugriffspunkt einen weiteren Optimierungsmechanismus. Die NIC versucht, mithilfe des WEP-Schlüssels, der von dem alten Zugriffspunkt als gemeinsamer Schlüssel erhalten wurde, eine IEEE 802.11-Authentifizierung durchzuführen. Ist diese Authentifizierung erfolgreich, fügt der Zugriffspunkt die Station sofort zur Liste der authentifizierten Stationen hinzu.

Schlägt die Authentifizierung fehl, nimmt die NIC eine Open System-Authentifizierung am Zugriffspunkt vor, und es erfolgt eine vollständige IEEE 802.1X-Authentifizierung. Der Zugriffspunkt muss unterscheiden können, ob eine Station mittels Open System oder unter Verwendung der Shared Key-Methode authentifiziert wurde.

Wird der Station unter Verwendung der Shared Key-Methode der Zugriff auf den neuen Zugriffspunkt gestattet, wird von dem neuen Zugriffspunkt weiterhin die IEEE 802.1X-Authentifizierung gestartet, um Kontendatensätze zu aktualisieren.

Indem die Stations-Netzwerkkonnektivität mittels Shared Key-Authentifizierung ermöglicht wird, während der neue Zugriffspunkt IEEE 802.1X ausführt, wird sichergestellt, dass an der Station keine Unterbrechung der Netzwerkkonnektivität auftritt. Wenn die IEEE 802.1X-Authentifizierung der Station am neuen Zugriffspunkt nicht erfolgreich abgeschlossen werden kann, wird die Netzwerkverbindung zu der Station über den kontrollierten Port des Zugriffspunktes beendet. Auf diese Weise wird die Sicherheit des Netzwerkes gewährleistet.

Anforderungen für den RADIUS-Server

Die Anforderungen für den RADIUS-Server lassen sich in zwei Kategorien unterteilen: Kontenverwaltung und Authentifizierung.

Anmerkung Die Zahlen in eckigen Klammern [ ] verweisen auf die Artikel, die weiter unten im Abschnitt "Referenzinformationen" aufgeführt sind; die Zahlen in runden Klammern ( ) verweisen auf bestimmte Attribute, Typen und Fehler, die in diesen Artikeln definiert sind.

Attribute der RADIUS-Kontenverwaltung

Bis auf wenige Ausnahmen haben die in [5] und [6] definierten Attribute der RADIUS-Kontenverwaltung innerhalb von IEEE 802.1X-Sitzungen und in Einwählsitzungen dieselbe Bedeutung, so dass keine weiteren Erläuterungen notwendig sind.

Die folgenden Attribute müssen jedoch genauer betrachtet werden:

- Acct-Terminate-Cause
- Acct-Multi-Session-Id
- Acct-Link-Count

Acct-Terminate-Cause

Wie in [5] beschrieben, zeigt dieses Attribut an, wie die Sitzung beendet wurde. Wenn dieses Attribut verwendet wird, entspricht die Abbruchsursache **User Request** (1) der Situation, in der die Sitzung aufgrund einer vom Endsystem erhaltenen EAPOL-Logoff-Nachricht beendet wurde.

Die Abbruchsursache **Lost Carrier** (2) weist darauf hin, dass die Sitzung aufgrund des Verlusts der physischen Verbindung, der jedoch nicht durch Roaming herbeigeführt wurde, beendet wurde. Wenn das Endsystem z. B. eine Point-to-Point-LAN-Verbindung trennt oder aus dem Funkbereich eines 802.11-Zugriffspunktes heraustritt, wird diese Abbruchsursache verwendet. Tritt für eine Sitzung ein Timeout aufgrund des Ablaufs eines Zeitgebers für Leerlaufzeit auf, wird die Abbruchsursache **Idle Timeout** (4) verwendet. Tritt der Timeout aufgrund des Ablaufs eines Sitzungszeitgebers auf, wird die Ursache **Session Timeout** (5) angezeigt.

Wenn eine Sitzung aufgrund von Roaming verlagert wird, wird die Abbruchsursache **NAS (Network Access Server) Request** (10) verwendet. Wird die Sitzung beendet, weil eine erneute Authentifizierung fehlgeschlagen ist, wird die Abbruchsursache **User Error** (17) angezeigt.

Acct-Multi-Session-Id

Dieses Attribut ermöglicht es, mehrere in Beziehung stehende Sitzungen miteinander zu verknüpfen. Während es innerhalb von IEEE 802.1X nicht möglich ist, Mehrfachverbindungsbündel zu erstellen, kann ein Endsystem, das mittels Roaming zwischen IEEE 802.11-Zugriffspunkten wechselt, veranlassen, dass mehrere Accounting-Stop-Pakete gesendet werden.

Sofern dies vom Zugriffspunkt unterstützt wird, wird das **Acct-Multi-Session-Id**-Attribut verwendet, um mehrere in Beziehung stehende Sitzungen eines das Roaming nutzenden Endsystems zu verknüpfen. Hierfür ist es erforderlich, dass das **Acct-Multi-Session-Id**-Attribut für alle Zugriffspunkte, Endsysteme und Sitzungen eindeutig ist. Um diese Eindeutigkeit sicherzustellen, wird empfohlen, dass **Acct-Multi-Session-Id** die folgende Form aufweist:

```
MAC-Adresse des ursprünglichen Zugriffspunktes | MAC-Adresse des Endsystems
| NTP-Timestamp
```

Die MAC-Adresse des ursprünglichen Zugriffspunktes entspricht der MAC-Adresse des Zugriffspunktes (in Hexadezimaldarstellung), bei dem die Sitzung begonnen wurde. Der NTP-Timestamp kennzeichnet den Beginn der ursprünglichen Sitzung. Um die Einheitlichkeit des **Acct-Multi-Session-Id**-Attributs zwischen IEEE 802.11-Roamingsitzungen sicherzustellen, kann die Multisitzungs-ID als Teil eines IAPPs zwischen den Zugriffspunkten verschoben werden.

Diese Form des **Acct-Multi-Session-Id**-Attributs stellt die Eindeutigkeit der ID für alle Zugriffspunkte, Endsysteme und Sitzungen sicher. Da der NTP-Timestamp nicht vom Systemstart ausgehend berechnet wird, besteht keine Möglichkeit, dass ein erneut gestarteter Zugriffspunkt einen Wert für **Acct-Multi-Session-Id** wählt, der mit dem Wert einer vorherigen Sitzung verwechselt werden kann.

Acct-Link-Count

Das Erstellen von Mehrfachverbindungsbündeln innerhalb von IEEE 802.1X ist nicht möglich. Dieses Attribut bietet somit keine Vorteile für IEEE 802.1X-Authentifikatoren.

RADIUS-Authentifizierung

Die folgenden in [8] und [10] definierten Attribute sind für IEEE 802.1X-Authentifikatoren relevant, die als RADIUS-Clients fungieren:

- User-Name
- User-Password, CHAP-Password, CHAP-Challenge
- NAS-IP-Address
- NAS-Port
- Service-Type
- Framed-Protocol
- Framed-IP-Address, Framed-IP-Netmask
- Framed-Routing
- Filter-Id
- Framed-MTU
- Framed-Compression
- Reply-Message
- Callback-Number, Callback-ID
- Framed-Route
- State
- Class
- Vendor-Specific
- Proxy-State
- Session-Timeout
- Idle-Timeout

- Termination-Action
- Called-Station-ID
- Calling-Station-ID
- NAS-Identifier
- NAS-Port-Type
- Port-Limit
- Password-Retry
- Connect-Info
- EAP-Message
- Message-Authenticator
- NAS-Port-Id
- Framed-Pool
- Tunnel-Medium-Type
- Tunnel-Assignment-Id

User-Name

In IEEE 802.1X gibt das Endsystem seine Identität üblicherweise mittels einer EAP-Response/Identity-Nachricht an. Die Identität des Endsystems wird sowohl in das **User-Name**-Attribut als auch in die RADIUS-Access-Request- und Access-Reply-Nachrichten eingeschlossen. In dem weiter unten in [8] aufgeführten Dokument wird dies näher angegeben.

Falls **Service-Type** dem Wert **Call Check** entspricht, enthält das **User-Name**-Attribut den Wert für **Calling-Station-ID**; dieser Wert wird auf die MAC-Adresse des Endsystems eingestellt und als ASCII-Wert ausgedrückt.

User-Password, CHAP-Password, CHAP-Challenge

Da IEEE 802.1X keine Unterstützung für PAP (Password Authentication Protocol) oder CHAP (Challenge Handshake Authentication Protocol) für das Benutzerkennwort bietet, werden die Attribute **CHAP-Password** oder **CHAP-Challenge** nicht von IEEE 802.1X-Authentifikatoren verwendet, die als RADIUS-Clients fungieren.

NAS-IP-Address

Bei Verwendung von IEEE 802.1X enthält das **NAS-IP-Address**-Attribut die IP-Adresse der Brücke oder des Zugriffspunktes, die bzw. der als RADIUS-Client fungiert.

NAS-Port

Bei Verwendung von IEEE 802.1X, enthält das **NAS-Port**-Attribut ggf. die Anschlussnummer der Brücke oder des Zugriffspunktes. Da in IEEE 802.11 keine physischen Anschlüsse vorgesehen sind, wird dieses Attribut nicht von Zugriffspunkten gesendet.

Service-Type

Bei Verwendung von IEEE 802.1X haben nur die Werte **Framed** (2), **Authenticate-Only** (8) und **Call-Check** (10) eine Bedeutung.

- **Framed** weist darauf hin, dass für die Verbindung entsprechende 802-Rahmen verwendet werden sollen.
- **Authenticate-Only** (8) weist darauf hin, dass im Access-Accept-Paket keine Autorisierungsinformationen zurückgegeben werden müssen.

- **Call-Check**, wie in [8] beschrieben, wird in eine Access-Request-Paketanforderung an den RADIUS-Server eingebunden, um den Verbindungsversuch zuzulassen oder zurückzuweisen. Dies basiert üblicherweise auf dem **Called-Station-ID**-Attribut (das auf die MAC-Adresse der Brücke oder des Zugriffspunktes einstellt wird) oder auf dem **Calling-Station-ID**-Attribut (das auf die MAC-Adresse des Endsystems eingestellt wird). Wie in [8] aufgezeigt, wird in diesem Fall empfohlen, dass das **User-Name**-Attribut den Wert von **Calling-Station-ID** erhält.

Framed-Protocol

Da es keinen Wert für 802-Medien gibt, wird das **Framed-Protocol**-Attribut nicht von IEEE 802.1X-Authentifikatoren verwendet.

Framed-IP-Address, Framed-IP-Netmask

Da IEEE 802.1X keinen Mechanismus zur Zuweisung von IP-Adressen bereitstellt, werden die Attribute **Framed-IP-Address** und **Framed-IP-Netmask** nicht von IEEE 802.1X-Authentifikatoren verwendet.

Framed-Routing

Das **Framed-Routing**-Attribut gibt die Weiterleitungsmethode für das Endsystem an. Es betrifft somit nur IEEE 802.1X-Authentifikatoren, die als Geräte der Ebene 3 fungieren und die nicht von einer Brücke oder einem Zugriffspunkt verwendet werden können.

Filter-ID

Dieses Attribut gibt den Namen der Filterliste für das Endsystem an. Es wird von einem IEEE 802.1X.-Authentifikator verwendet und kann entweder auf Filter der Ebene 2 oder auf Filter der Ebene 3 hinweisen.

Framed-MTU

Dieses Attribut gibt die maximale Übertragungseinheit (Maximum Tranmission Unit, MTU) an. IEEE 802.1X-Authentifikatoren legen das **Framed-MTU**-Attribut auf den Wert der MTU des relevanten 802-Mediums fest und schließen es in das RADIUS-Access-Request-Paket ein.

Framed-Compression

IEEE 802.1X bietet keine Unterstützung für die Komprimierung, so dass dieses Attribut von 802.1X-Authentifikatoren nicht interpretiert werden kann.

Reply-Message

Dieses Attribut wird verwendet, um Text zu kennzeichnen, der dem Benutzer angezeigt wird. Ein IEEE 802.1X-Authentifikator, der dieses Attribut erhält, schließt die Zeichenfolge in eine EAP-Request/Notification-Nachricht ein, die an das Endsystem gesendet wird.

Callback-Number, Callback-ID

Diese Attribute können von IEEE 802.1X-Authentifikatoren nicht interpretiert werden.

Framed-Route

Das **Framed-Route**-Attribut stellt Routen bereit, die für das Endsystem konfiguriert werden. Es betrifft nur IEEE 802.1X-Authentifikatoren, die als Geräte der Ebene 3 fungieren. Brücken oder Zugriffspunkte können **Framed-Route** nicht interpretieren.

State, Class, Vendor-Specific, Proxy-State

Diese Attribute erfüllen denselben Zweck (vgl. das unter [8] angegebene Dokument).

Session-Timeout

Dieses Attribut gibt an, wie lange (in Sekunden) ein Dienst maximal bereitgestellt wird, bevor die Sitzung beendet wird. Welche Aktion bei Beendigung eingeleitet werden muss, wird im **Termination-Action**-Attribut festgelegt. Ein IEEE 802.1X-Authentifikator verwendet diesen Wert zum Auslösen einer regelmäßigen Neuauthentifizierung in den durch das Sitzungstimeout festgelegten Intervallen, um erfolgreich authentifizierte, anhaltende Sitzungen zu gewährleisten.

Idle-Timeout

Mit diesem Attribut wird festgelegt, wie lange (in Sekunden) ein Endsystem eine Verbindung im Leerlauf aufrechterhalten darf, bevor die Sitzung beendet wird. Sobald der durch **Idle-Timeout** angegebene Zeitraum verstrichen ist, wechselt eine IEEE 802.1X-Authentifikator-PAE (Port Access Entity, Anschlusszugriffseinheit) zum unverbundenen Status.

Termination-Action

Dieses Attribut gibt die Aktion an, die bei Beendigung der Bereitstellung des Dienstes erfolgen soll. Der Wert **Default** (0) gibt an, dass die Authentifikator-PAE zum unverbundenen Status wechselt. Der Wert **RADIUS-Request** (1) gibt an, dass die Authentifikator-PAE zum Neuauthentifizierungsstatus wechselt.

Called-Station-ID

Bei Verwendung durch IEEE 802.1X-Authentifikatoren wird in diesem Attribut die MAC-Adresse der Brücke oder des Zugriffspunktes im ASCII-Format gespeichert, wobei die Oktettwerte durch einen Bindestrich (-) getrennt sind. (Beispiel: "00-10-A4-23-19-C0")

Calling-Station-ID

Bei Verwendung durch IEEE 802.1X-Authentifikatoren wird in diesem Attribut die MAC-Adresse des Endsystems im ASCII-Format gespeichert, wobei die Oktettwerte durch einen Bindestrich (-) getrennt sind.

NAS-Identifier

Dieses Attribut enthält eine Zeichenfolge zur Identifizierung des IEEE 802.1X-Authentifikators, von dem das Access-Request-Paket stammt.

NAS-Port-Type

Bei Verwendung von IEEE 802.1X werden die **NAS-Port-Type**-Werte **Ethernet** (15) oder **Wireless - IEEE 802.11** (19) verwendet. Bei der Verwendung von IEEE 802.1X über Token Ring gibt es keinen entsprechenden Wert.

Port-Limit

Da IEEE 802.1X keine Unterstützung für Mehrfachverbindungsbündel bietet, hat dieses Attribut keinerlei Auswirkung, wenn es an einen IEEE 802.1X-Authentifikator gesendet wird.

Password-Retry

Dieses Attribut kann in ein Access-Reject-Paket eingebunden werden, um anzuzeigen, wie viele Authentifizierungsversuche ein Benutzer durchführen kann, bevor die Verbindung getrennt wird. Bei IEEE 802.1X-Systemen sollte dieses Attribut verwendet werden, um zu steuern, wann die Authentifikator-PAE zum Haltestatus wechselt.

Connect-Info

Dieses Attribut wird von einer Brücke oder einem Zugriffspunkt gesendet, um die Art der Verbindung des Endsystems anzuzeigen. Wird dieses Attribut in einem Access-Request-Paket gesendet, empfiehlt es sich, dass das Attribut Informationen zur Geschwindigkeit der Verbindung des Endsystems enthält, z. B. CONNECT 11 Mbps IEEE 802.11a.

Wird das Attribut in einer Accounting-Stop-Nachricht gesendet, kann es verwendet werden, um statistische Angaben zur Sitzungsqualität zusammenzufassen. In IEEE 802.11 kann das **Connect-Info**-Attribut beispielsweise Informationen zur Anzahl der erneuten Übertragungen über die Sicherungsschicht enthalten. Das genaue Format dieses Attributs hängt von der jeweiligen Implementierung ab.

EAP-Message

Da IEEE 802.1X wie in [2] und [3] beschrieben die Kapselung von EAPOL (EAP-over-LAN), bereitstellt, wird das **EAP-Message**-Attribut zur Kapselung von EAP-Paketen verwendet, die vom IEEE 802.1X-Authentifikator an den Authentifizierungsserver gesendet werden.

Da das IEEE keinen Ethernet-Typ für EAPOL-Rahmen veröffentlicht hat, werden die MAC-Adresse und der Ethernet-Typ zu Testzwecken derzeit folgendermaßen definiert:

```
BYTE Def_dest_mac_addr[]={0x01, 0x80, 0xc2, 0x00, 0x00, 0x0f};
BYTE Def_ethernet_type[]={0x81, 0x80};
```

Message-Authenticator

Wie in [10] aufgezeigt, muss das **Message-Authenticator**-Attribut verwendet werden, um alle Pakete zu schützen, die ein **EAP-Message**-Attribut enthalten.

NAS-Port-Id

Mithilfe dieses Attributs wird der IEEE 802.1X-Authentifikatoranschluss identifiziert, der das Endsystem authentifiziert. Da in IEEE 802.11 keine physischen Anschlüsse vorgesehen sind, wird dieses Attribut nicht von Zugriffspunkten gesendet.

Framed-Pool

Da IEEE 802.1X keine Unterstützung für die Adresszuweisung bietet, hat dieses Attribut keinerlei Bedeutung für einen IEEE 802.1X-Authentifikator.

Tunnel-Medium-Type

Falls die Zuweisung einer VLANID (Virtual Local Access Network ID) zum Anschluss eines IEEE 802.1X-Endsystems gewünscht ist, wird für das **Tunnel-Medium-Type**-Attribut der Wert 802 (6) verwendet.

Tunnel-Assignment-Id

In Kombination mit dem **Tunnel-Medium-Type**-Wert 802 dient dieses Attribut zum Senden der VLANID.

Roaming

Es gibt zwei Möglichkeiten zur Bereitstellung von Sicherheitsdiensten, wenn eine Station von einem Zugriffspunkt zum anderen wechselt.

Keine Koordination der Zugriffspunkte

Der erste Ansatz geht davon aus, dass die Zugriffspunkte die Übergaben der Station zwischen dem alten und dem neuen Zugriffspunkt nicht koordinieren. In diesem Fall muss die Station im Anschluss an die Übergabe sämtliche Phasen zum Aufbauen einer IEEE 802.11-Funkverbindung durchlaufen, an die sich die erneute IEEE 802.1X-Authentifizierung anschließt.

Während dieses Zeitraums, also des erneuten Verbindungsaufbaus und der erneuten Authentifizierung, ist der Zugriff der Station auf das Netzwerk unterbrochen. Auch wenn davon ausgegangen werden kann, dass dieser Prozess unter normalen Bedingungen nur wenige Sekunden in Anspruch nimmt, sind bestimmte Anwendungsbereiche vorstellbar, z. B. die Wiedergabe von Audio- oder Videostreams, in denen dies zu einer Leistungsbeeinträchtigung führt. Ein Vorteil dieses Ansatzes liegt jedoch darin, dass im Anschluss an die Übergabe der Station vom alten zum neuen Zugriffspunkt keine Änderungen am Stations- und Zugriffspunktbetrieb notwendig sind.

Koordination der Zugriffspunkte

Der zweite Ansatz geht davon aus, dass die Zugriffspunkte die Übergaben der Station koordinieren. Hierdurch wird eine schnelle Übergabe ermöglicht. Zudem werden Unterbrechungen der Netzwerkkonnektivität der Station während anhaltender Sitzungen vermieden. Hierfür ist die Definition eines IAPPs erforderlich, damit der alte und der neue Zugriffspunkt die Übergabe der Station koordinieren können.

Mithilfe eines IAPPs können im Anschluss an die Übergabe einer Station stationsspezifische Unicast-Schlüssel vom alten an den neuen Zugriffspunkt übermittelt werden. Darüber hinaus würde eine EAPOL-Key-Nachricht verwendet, um den gemeinsamen Schlüssel zu aktualisieren.

Zusätzliche Optimierung

Wenn mehrere Zugriffspunkte mit demselben WEP-Schlüssel konfiguriert wurden, kann der Zugriffspunkt einen zusätzlichen Optimierungsmechanismus nutzen.

Die NIC sollte mithilfe des WEP-Schlüssels, der von dem alten Zugriffspunkt als gemeinsamer Schlüssel erhalten wurde, versuchen, eine IEEE 802.11-Authentifizierung durchzuführen. Ist diese Authentifizierung erfolgreich, sollte der Zugriffspunkt die Station sofort zur Liste der authentifizierten Stationen hinzufügen.

Wird der Station unter Verwendung der Shared Key-Methode der Zugriff auf den neuen Zugriffspunkt gestattet, wird von dem neuen Zugriffspunkt weiterhin die IEEE 802.1X-Authentifizierung gestartet, um die Kontendatensätze zu aktualisieren. Indem die Stations-Netzwerkkonnektivität mittels Shared Key-Authentifizierung ermöglicht wird, während der neue Zugriffspunkt IEEE 802.1X ausführt, wird sichergestellt, dass an der Station keine Unterbrechung der Netzwerkkonnektivität auftritt.

Mehrere Zertifikate

Die EAP-TLS-Implementierung von RAS (Remote Access Server) ermöglicht beim ersten Mal die Auswahl eines Zertifikats; dieses Zertifikat wird anschließend wiederverwendet. Wird IEEE 802.1X in einem Szenario verwendet, in dem vom Roaming Gebrauch gemacht wird, wirft dieser Prozess einige Probleme auf. Bei RAS gibt es für jedes Ziel eine einzelne Verbindung. Bei IEEE 802.1X kann eine LAN-Verbindung an mehreren Standorten verwendet werden.

Verwenden mehrerer Standorte

Es kann durchaus begründet sein, an unterschiedlichen Standorten unterschiedliche Anmeldeinformationen anzugeben; um dies zu ermöglichen, muss ein Mechanismus zur Verfügung stehen, mit dessen Hilfe der jeweilige Standort erkannt werden kann. Bei IEEE 802.11 kann der Netzwerkname bzw. die Dienstsatzidentifizierung zur Standortidentifikation verwendet werden.

Beim Einsatz von Ethernet gibt es keine Möglichkeit, den Standort zu ermitteln, es sei denn, es würden Änderungen an IEEE 802.1X vorgenommen. (In Organisationsnetzwerken, z. B. Unternehmen und Universitäten, ist die Verwendung von IEEE 802.1X und Ethernet wahrscheinlich, da auf diese Weise die sichere Netzwerkkonnektivität bereitgestellt werden kann.)

Standardzertifikat für jedes Netzwerk

Drahtlose Netzwerke werden zudem sehr häufig an öffentlichen Orten, z. B. an Flughäfen oder in Einkaufszentren, verwendet. Öffentliche Orte können die Verwendung von querverweisenden Anmeldeinformationen ermöglichen, in vielen Fällen ist jedoch die Verwendung anderer Anmeldeinformationen, z. B. eines Standardzertifikats für jedes Netzwerk, erforderlich.

Verwendung der EAP-Identity/Request-Zeichenfolge

Vorzuziehen ist, dass sowohl Ethernet- als auch IEEE 802.11-Netzwerke in der Lage sind, dem Client/der Station ihre aktuellen Standorte anzuzeigen, indem sie der EAP-Identity-Nachricht ein Attribut hinzufügen. Diese Nachricht könnte den Dienst angeben, der vom Netzwerk bereitgestellt wird. Falls dieses Attribut in IEEE 802.11-Netzwerken nicht verfügbar ist, sollte stattdessen standardmäßig die Dienstsatzidentifizierung verwendet werden.

Für die anzuzeigende nullterminierte Zeichenfolge und den durch Kommas getrennten Abschnitt der EAP-Identity-Nachrichtenzeichenfolge wird daher folgendes Format empfohlen:

```
Dies ist eine Anzeigenzeichenfolge\0networkid=<Netzwerkname>,nasid=<NAS-
Name>,portid=<Port-ID>
Wobei gilt:
<Netzwerkname> = :SSID für IEEE 802.11, jedoch eine beliebige Zeichenfolge
für Ethernet.
<NAS-Name> = : Name des IEEE 802.11-Zugriffspunktes oder Ethernet-Switches;
falls kein Name verfügbar ist, die MAC-Adresse des Zugriffspunktes oder
Ethernet-Switches.
<Port-ID> = : Anschlusskennung, über die diese IEEE 802.1X-Sitzung erfolgt.
```

Das IEEE 802.1X-Endsystem (Station) würde diese Zeichenfolge vor dem Null-Terminierungszeichen (\0) anzeigen, um Administratoren die Anzeige von Netzwerk-Identifikationsnachrichten zu ermöglichen.

Weitere Informationen zur Angabe der Identitätszeichenfolge in einer EAP-Identity-Request-Nachricht finden Sie in Anhang B.

Nicht authentifizierter Zugriff

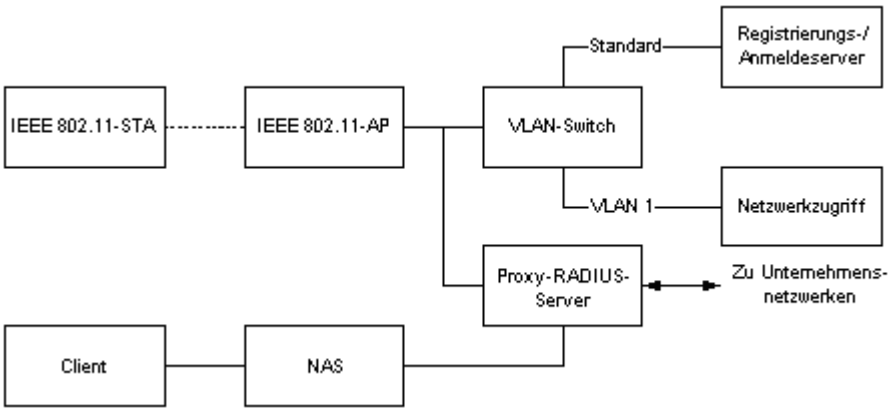

Abbildung 2: Typisches Netzwerkszenario für den nicht authentifizierten Zugriff

Die Verwendung von IEEE 802.11 an öffentlichen Orten, wie z. B.Flughäfen oder Einkaufszentren, würde eine zusätzliche Erweiterung des Standards IEEE 802.1X erforderlich machen. Derzeit erfolgt der IEEE 802.1X-Authentifizierungsprozess im Anschluss an den IEEE 802.11-Verbindungsaufbau. Abbildung 2 zeigt ein typisches Netzwerkszenario für nicht authentifizierten Zugriff.

Der nicht authentifizierte Zugriff durch Benutzer an öffentlichen Orten lässt sich in zwei Kategorien unterteilen:

- **Kunden mit einem bevorzugten Dienstanbieter**, wie z. B. Benutzer in Unternehmen, die über ein Standard-VLAN den Zugriff auf das Internet erhalten.
- **Kunden**, die beabsichtigen, sich bei dem Dienstanbieter anzumelden, um über ein VLAN den Zugriff auf das Internet zu erhalten.

Standard-VLANs

Benutzer in Unternehmen, die eine Verbindung zum Netzwerk herstellen, würden zuerst eine IEEE 802.11-Funkverbindung zwischen der Station und dem Zugriffspunkt herstellen. Im Anschluss an den Aufbau der IEEE 802.11-Funkverbindung folgt die IEEE 802.1X-Authentifizierung mithilfe des Proxy -RADIUS-Servers. Anschließend wird den authentifizierten Benutzern im Unternehmen der Netzwerkzugriff über das Standard-VLAN ermöglicht.

Dieser Ansatz ist mit der Methode vergleichbar, die derzeit eingesetzt wird, um Clients den Netzwerkzugriff über den Netzwerkzugriffsserver (Network Access Server, NAS) zu ermöglichen. Benutzer in Unternehmen, die eine Verbindung zu ihrem Intranet herstellen möchten, würden nun mithilfe eines Verfahrens zur Verwendung eines sicheren Tunnels, wie z. B. PPTP (Point-to-Point Tunneling Protocol), eine Verbindung zum Unternehmensfirewall aufbauen.

Öffentliche Internetszenarien

Benutzer, die beabsichtigen, einen Internetdienst zu abonnieren, müssten sich vor der Authentifizierung für den Netzwerkzugriff anmelden und registrieren. Aus diesem Grund müsste IEEE 802.1X so konzipiert sein, dass es den Zugriff auf die Anmeldungs- und Registrierungsserver ermöglicht, indem die Benutzerkommunikation an das entsprechende VLAN gelenkt wird. Mithilfe einer EAP-Notification-Nachricht kann der Benutzer darüber informiert werden, bei welchem Server die Anmeldung und Registrierung zum Zweck der Kontoverwaltung und Abrechnung erfolgen muss. Die Anmeldung und Registrierung muss stattfinden, bevor der Zugriff auf das Netzwerk gewährt wird.

Clientanforderungen

Für einen nicht authentifizierten Benutzer sollte ein IEEE 802.1X-Client in der EAP-Response/Identity-Nachricht eine Nullzeichenfolge als Identitätsangabe übermitteln. Als nicht authentifizierter Benutzer wird ein Benutzer bezeichnet, der auf dem Clientgerät nicht die erforderlichen Anmeldeinformationen bereitstellen kann, also z. B. ein Benutzer, der nicht über die erforderlichen Benutzerzertifikate für das Netzwerk verfügt, auf das er zuzugreifen versucht.

Anforderungen für Zugriffspunkte

Verarbeiten eines nicht authentifizierten Benutzers

Wenn der Zugriffspunkt eine EAP-Response/Identity-Nachricht von einem nicht authentifizierten Benutzer erhält, übermittelt er im Rahmen der Kommunikation mit dem RADIUS-Server die im Folgenden beschriebenen Informationen:

- Der RADIUS-Client des Zugriffspunktes gibt im RADIUS-Access-Request-Paket nicht das RADIUS-Attribut **User-Name** (Nummer 1) an.
- Der RADIUS-Client des Zugrifsspunktes gibt im RADIUS-Access-Request-Paket nicht das RADIUS-Attribut **EAP-Message** (Nummer 79) an.

Drei Ebenen des Netzwerkzugriffs

Ein Zugriffspunkt bietet dem Client drei Ebenen des Netzwerkzugriffs, die von der Authentifizierungsantwort des RADIUS-Servers abhängen. Es handelt sich um die folgenden drei Ebenen:

- **Vollständiger Netzwerkzugriff**. Dem Client wird der vollständige Zugriff auf alle Netzwerkressourcen ermöglicht, die für einen authentifizierten Benutzer verfügbar sind.
- **Beschränkter Netzwerkzugriff**. Dem Client wird der beschränkte Zugriff auf Netzwerkressourcen ermöglicht. So können z. B. Übertragungen vom Client auf eine bestimmte Gruppe von Zieladressen begrenzt sein, während Übertragungen zu anderen Zieladressen durch den Zugriffspunkt unterbunden werden.
- **Unterbinden des Netzwerkzugriffs**. Der Client kann auf keine Netzwerkressource zugreifen.

Authentifizierungsantworten

Bei Erhalt einer Authentifizierungsantwort vom RADIUS-Server wendet der Zugriffspunkt eines der folgenden Netzwerk-Autorisierungsverfahren an:

Access-Accept-Paket mit EAP-Success-Nachricht (RADIUS-Paket enthält ein **EAP-Message**-Attribut)

- Vollständiger Netzwerkzugriff wird ermöglicht
- Bereitstellung des beschränkten Netzwerkzugriffs wird aufgehoben

Access-Reject-Paket mit EAP-Failure-Nachricht (RADIUS-Paket enthält ein **EAP-Message**-Attribut)

- Bereitstellung des vollständigen Netzwerkzugriffs wird aufgehoben
- Bereitstellung des beschränkten Netzwerkzugriffs wird aufgehoben

Access-Reject-Paket mit EAP-Success-Nachricht (RADIUS-Paket enthält ein **EAP-Message**-Attribut)

- Bereitstellung des vollständigen Netzwerkzugriffs wird aufgehoben
- Bereitstellung des beschränkten Netzwerkzugriffs wird aufgehoben

Access-Accept-Paket (RADIUS-Paket enthält *kein* **EAP-Message**-Attribut)

- Bereitstellung des vollständigen Netzwerkzugriffs wird aufgehoben
- Bereitstellung des beschränkten Netzwerkzugriffs wird aufgenommen

Access-Reject-Paket (RADIUS-Paket enthält *kein* **EAP-Message**-Attribut)

- Bereitstellung des vollständigen Netzwerkzugriffs wird aufgehoben
- Bereitstellung des beschränkten Netzwerkzugriffs wird aufgehoben

IEEE 802.11 im Ad-hoc-Modus

Im Ad-hoc-Netzwerkmodus von IEEE 802.11 können Stationen innerhalb eines Basisdienstsatzes (Basic Service Set, BSS) direkt mit Peer-Stationen innerhalb desselben BSS kommunizieren.

Das IEEE 802.1X-Authentifizierungsprozess wird von Peer-Stationen mithilfe einer EAPOL-Interaktion ausgelöst. Alle Stationen innerhalb des BSS müssen sich untereinander gegenseitig authentifizieren. Hierfür ist ein Algorithmus erforderlich, um einen Authentifikator auszuwählen.

Gegenseitige Authentifizierung

Da im Ad-hoc-Netzwerkmodus kein RADIUS-Server für die Authentifizierung verwendet wird, müssen die Anmeldeinformationen der Benutzer auf den Stationen gespeichert werden. Dies hat zur Folge, dass für die Schlüsselverwaltung im Ad-hoc-Netzwerkmodus eine kennwortgestützte gegenseitige Authentifizierung und eine sichere Schlüsselgenerierung erforderlich sind.

Zwei Ansätze

Derzeitige EAP-Methoden stellen zwei Ansätze für die gegenseitige Authentifizierung zur Verfügung:

- **EAP-TLS** unterstützt die gegenseitige Authentifizierung und die Schlüsselgenerierung, geht jedoch davon aus, dass beide Benutzer über ein Zertifikat verfügen.
- **EAP-GSS** unterstützt die gegenseitige Authentifizierung, geht jedoch davon aus, dass die Serverseite mit einem Schlüsselverteilungscenter (Key Distribution Center, KDC) in Verbindung steht.

Im Ad-hoc-Netzwerkmodus kann IEEE 802.1X nur mit der Shared Key-Authentifizierung verwendet werden. In einige Szenarien wird die gegenseitige Authentifizierung bevorzugt, es dürfte jedoch eine neue EAP-Methode notwendig sein, um dieser Anforderung angemessen gerecht zu werden.

Unterstützung drahtloser LANs durch Windows 2000 und Windows XP

Windows 2000 bietet zahlreiche wichtige Funktionen zur Unterstützung und Erweiterung des drahtlosen Einsatzes von Computern. Die neuen Medienerkennungsfunktionen im TCP/IP-Stack erleichtern das Roaming von einem Zugriffspunkt zum nächsten, ohne dass die Gefahr besteht, dass Verbindungen unterbrochen oder Daten ausgespäht werden.

Die NDIS-Schnittstelle von Windows 2000 unterstützt drahtlose Netzwerkadapter und die zugehörigen Treiber. Im Lieferumfang von Windows 2000 sind zahlreiche Treiber für Karten für drahtlose LANs enthalten. Zudem stellen die meisten Geräte für drahtlose LANs Treiber für Windows 2000 zur Verfügung, so dass das Einrichten und Verwenden drahtloser Geräte für das bzw. mit dem Betriebssystem völlig unproblematisch ist. Die meisten der drahtlosen Geräte, die in Windows 2000 unterstützt werden, implementieren Sicherheitsmechanismen, indem sie einen gemeinsamen Schlüssel oder WEP (Wired Equivalent Privacy) verwenden.

Durch die Erweiterung des Betriebssystems um IEEE 802.11 sowie verbesserte konfigurationsfreie Verbindungen und Roamingfunktionalität vereinfacht Windows XP die Verwaltung drahtloser Geräte.

Zusammenfassung

Durch die Unabhängigkeit von Kabelverbindungen und die einfachere Netzwerkinstallation stellen IEEE 802.11-basierte, drahtlose Netzwerke eine ausgesprochen attraktive Lösung dar. Aufgrund unterschiedlicher Beschränkungen, vor allem jedoch aufgrund von Sicherheitsbedenken, waren Administratoren von Unternehmensnetzwerken bei der Bereitstellung drahtloser Netzwerke bislang eher zurückhaltend. Durch die Erweiterung von IEEE 802.11-basierten Netzwerken um IEEE 802.1X-Standards wird die Sicherheit jedoch sogar über das in verkabelten Netzwerken übliche Maß hinaus erweitert, so dass dem Einsatz im Unternehmen nichts mehr im Wege steht. Diese Sicherheitsfeatures können auch für andere IEEE 802-Netzwerke, z. B. in 802.3 Ethernet-Netzwerken, verwendet werden, um die netzwerkweite Zugriffssicherheit zu verbessern.

Weitere Informationen

Aktuelle Informationen zu Windows 2000 und Windows XP finden Sie unter http://www.microsoft.com/germany/ms/windows2000/ oder unter http://www.microsoft.com/windows2000/ (englischsprachig) sowie unter http://www.microsoft.com/germany/ms/windowsxp/ oder unter http://www.microsoft.com/windowsxp/ (englischsprachig).

Aktuelle Informationen zu IEEE 802.11-Standards finden Sie unter http://standards.ieee.org/wireless/ (englischsprachig)

Referenzinformationen

1. Teil 11: Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications, Draft International Standard ISO/IEC 8802-11, IEEE 802.11/D10, 14. Januar 1999 (englischsprachig).
2. Standards for Local and Metropolitan Area Networks: Port-based Network Access Control, Draft International Standard ISO/IEC 8802-11, IEEE Draft P802.1X/D8, 16. Oktober 2000 (englischsprachig).
3. L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", IETF RFC 2284, März 1998 (englischsprachig).
4. B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol", IETF RFC 2716, Oktober 1999 (englischsprachig).
5. C. Rigney, A. Rubens, W. A. Simpson, S. Willens, "Remote Authentication Dial-In User Service (RADIUS)", IETF RFC 2138, April 1997 (englischsprachig).
6. C. Rigney, "RADIUS Accounting", IETF RFC 2139, April 1997 (englischsprachig).
7. G. Zorn, "Microsoft Vendor-specific RADIUS Attributes", IETF RFC 2548, März 1999 (englischsprachig).
8. C. Rigney, S. Willens, A. Rubens, W. A. Simpson, "Remote Authentication Dial-In User Service (RADIUS)", IETF RFC 2865, Juni 2000 (englischsprachig).
9. C. Rigney, "RADIUS Accounting", IETF RFC 2866, Juni 2000 (englischsprachig).
10. C. Rigney, W. Willats, P. Calhoun, "RADIUS Extensions", IETF RFC 2869, Juni 2000 (englischsprachig).
11. G. Zorn, D. Leifer, A. Rubens, J. Shriver, M. Holdrege, I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", IETF RFC 2868, Juni 2000 (englischsprachig).
12. G. Zorn, D. Mitton, B. Aboba, "RADIUS Accounting Modifications for Tunnel Protocol Support", IETF RFC 2867, Juni 2000 (englischsprachig).
13. J. Linn, "Generic Security Service Application Program Interface, Version 2, Update 1", IETF RFC 2743, Januar 2000 (englischsprachig).
14. G. Zorn, "Microsoft Vendor-specific RADIUS Attributes", IETF RFC 2548, März 1999 (englischsprachig).

Anhang A: NDIS-Definitionen und Objektkennungen

Im Folgenden finden Sie eine kurze Beschreibung der NDIS-Definitionen, die mit den neuen NDIS-OIDs für die Unterstützung drahtloser LANs verwendet werden. Diese Typen finden Sie auch in den Headerdateien und in der Dokumentation zum Windows DDK (Driver Developers Kit).

NDIS-Definitionen

typedef enum _NDIS_802_11_NETWORK_TYPE

{

Ndis802_11FH,

Ndis802_11DS,

Ndis802_11NetworkTypeMax // kein echter Typ, ist als oberer Grenzwert definiert

} NDIS_802_11_NETWORK_TYPE, *PNDIS_802_11_NETWORK_TYPE;

typedef struct _NDIS_802_11_NETWORK_TYPE_LIST

{

ULONG NumberOfItems; // gemäß nachfolgender Liste, mindestens 1

NDIS_802_11_NETWORK_TYPE NetworkType [1];

} NDIS_802_11_NETWORK_TYPE_LIST, *PNDIS_802_11_NETWORK_TYPE_LIST;

typedef enum _NDIS_802_11_POWER_MODE

{

Ndis802_11PowerModeCAM,

Ndis802_11PowerModeMAX_PSP,

Ndis802_11PowerModeFast_PSP,

Ndis802_11PowerModeMax // kein echter Modus, ist als oberer Grenzwert definiert

} NDIS_802_11_POWER_MODE, *PNDIS_802_11_POWER_MODE;

typedef ULONG NDIS_802_11_TX_POWER_LEVEL; // in Milliwatt

//

// Anzeige für die Stärke des empfangenen Signals (Received Signal Strength Indication, RSSI)

//

typedef LONG NDIS_802_11_RSSI; // RSSI in dBmW

typedef struct _NDIS_802_11_CONFIGURATION_FH

{

ULONG Length; // Länge der Struktur

ULONG HopPattern; // gemäß Definition in 802.11, MSB festgelegt

```
ULONG HopSet; // entspricht 1 bei Nichtübereinstimmung mit 802.11
ULONG DwellTime; // Einheiten sind in Kusec angegeben
} NDIS_802_11_CONFIGURATION_FH, *PNDIS_802_11_CONFIGURATION_FH;
typedef struct _NDIS_802_11_CONFIGURATION
{
ULONG Length; // Länge der Struktur
ULONG BeaconPeriod; // Einheiten sind in Kusec angegeben
ULONG ATIMWindow; // Einheiten sind in Kusec angegeben
ULONG DSConfig; // Frequenz, Einheiten sind in KHz angegeben
NDIS_802_11_CONFIGURATION_FH FHConfig;
} NDIS_802_11_CONFIGURATION, *PNDIS_802_11_CONFIGURATION;
typedef struct _NDIS_802_11_STATISTICS
{
ULONG Length; // Länge der Struktur
LARGE_INTEGER TransmittedFragmentCount;
LARGE_INTEGER MulticastTransmittedFrameCount;
LARGE_INTEGER FailedCount;
LARGE_INTEGER RetryCount;
LARGE_INTEGER MultipleRetryCount;
LARGE_INTEGER RTSSuccessCount;
LARGE_INTEGER RTSFailureCount;
LARGE_INTEGER ACKFailu reCount;
LARGE_INTEGER FrameDuplicateCount;
LARGE_INTEGER ReceivedFragmentCount;
LARGE_INTEGER MulticastReceivedFrameCount;
LARGE_INTEGER FCSErrorCount;
} NDIS_802_11_STATISTICS, *PNDIS_802_11_STATISTICS;
typedef ULONG NDIS_802_11_KEY_INDEX;
```

```
typedef struct _NDIS_802_11_WEP
{
ULONG Length; // Länge der Struktur
ULONG KeyIndex; // 0 ist der clientspezifische Schlüssel, 1-N sind die
// globalen Schlüssel
ULONG KeyLength; // Länge des Schlüssels in Bytes
UCHAR KeyMaterial[1]; // variable Länge in Abhängigkeit von dem vorherigen Feld
} NDIS_802_11_WEP, *PNDIS_802_11_WEP;
typedef UCHAR NDIS_802_11_MAC_ADDRESS[6];
typedef struct _NDIS_802_11_SSID
{
ULONG SsidLength; // Länge des SSID-Informationsfeldes in Oktetten
UCHAR Ssid[32]; // SSID-Informationsfeld, umfasst 0 bis 32 Byte
} NDIS_802_11_SSID, *PNDIS_802_11_SSID;
typedef struct _NDIS_WLAN_BSSID
{
ULONG Length; // Länge der Struktur
NDIS_802_11_MAC_ADDRESS MacAddress; // BSSID
UCHAR Reserved[2];
NDIS_802_11_SSID Ssid; // SSID
ULONG Privacy; // erforderliche WEP-Verschlüsselung
NDIS_802_11_RSSI Rssi; // RSSI
// in dBmW
NDIS_802_11_NETWORK_TYPE NetworkTypeInUse; // Network_Type_In_Use
NDIS_802_11_CONFIGURATION Configuration; // Konfiguration
NDIS_802_11_NETWORK_INFRASTRUCTURE InfrastructureMode; // Infrastructure_Mode
NDIS_802_11_RATES SupportedRates; // Supported_Rates
} NDIS_WLAN_BSSID, *PNDIS_WLAN_BSSID;
```

```
typedef struct _NDIS_802_11_BSSID_LIST
{
ULONG NumberOfItems; // gemäß nachfolgender Liste, mindestens 1
NDIS_WLAN_BSSID Bssid[1];
} NDIS_802_11_BSSID_LIST, *PNDIS_802_11_BSSID_LIST;
typedef enum _NDIS_802_11_NETWORK_INFRASTRUCTURE
{
Ndis802_11IBSS,
Ndis802_11Infrastructure,
Ndis802_11AutoUnknown,
Ndis802_11InfrastructureMax // kein echter Wert, ist als oberer Grenzwert definiert
} NDIS_802_11_NETWORK_INFRASTRUCTURE, *PNDIS_802_11_NETWORK_INFRASTRUCTURE;
typedef enum _NDIS_802_11_AUTHENTICATION_MODE
{
Ndis802_11AuthModeOpen,
Ndis802_11AuthModeShared,
Ndis802_11AuthModeAutoSwitch,
Ndis802_11AuthModeMax // kein echter Modus, ist als oberer Grenzwert definiert
} NDIS_802_11_AUTHENTICATION_MODE, *PNDIS_802_11_AUTHENTICATION_MODE;
typedef ULONG NDIS_802_11_FRAGMENTATION_THRESHOLD;
typedef ULONG NDIS_802_11_RTS_THRESHOLD;
typedef ULONG NDIS_802_11_ANTENNA;
typedef UCHAR NDIS_802_11_RATES[8]; // Satz aus 8 Raten, wobei jeder Oktettwert eine Datenrate darstellt
typedef enum _NDIS_802_11_PRIVACY_FILTER
{
Ndis802_11PrivFilterAcceptAll,
Ndis802_11PrivFilter8021xWEP
} NDIS_802_11_PRIVACY_FILTER, *PNDIS_802_11_PRIVACY_FILTER;
```

NDIS-Objektkennungen

(Weiter oben finden Sie eine Liste der WLAN-abhängigen Objekte für die drahtlose Kommunikation.)

OID_802_11_BSSID

Dieses Objekt entspricht der MAC-Adresse des verbundenen Zugriffspunktes. Diese Einstellung kann im Rahmen von Scanvorgängen hilfreich sein.

Datentyp:	NDIS_802_11_MAC_ADDRESS
Abfrage:	Gibt die MAC-Adresse des aktuellen Zugriffspunktes zurück.
Festlegen:	Legt die MAC-Adresse des gewünschten Zugriffspunktes fest.
Statusanzeige:	Nicht unterstützt

OID_802_11_SSID

Dieses Objekt definiert die Dienstsatzidentifizierung (Service Set Identifier, SSID). Die Dienstsatzidentifizierung ist eine maximal 32 Zeichen umfassende Zeichenfolge. Sie identifiziert einen Satz untereinander verbundener Basisdienstsätze (Basic Service Sets, BSS). Wird in dieser OID-Anforderung eine leere Zeichenfolge übergeben, wird der NIC hierdurch mitgeteilt, dass mit dem Verbindungsaufbau nicht die Verfügbarkeit eines bestimmten Zugriffspunktes abgewartet, sondern eine Verbindung zu einem beliebigen Zugriffspunkt aufgebaut werden soll.

Das Festlegen einer Dienstsatzidentifizierung führt zur Aufhebung der Verbindung, wenn diese Dienstsatzidentifizierung bereits anderweitig vergeben ist. Die Aufhebung der Verbindung kann Folgendes bewirken: Aktivieren des Transceivers, wenn dieser bislang deaktiviert war, Festlegen der Dienstsatzidentifizierung auf den angegebenen Wert oder Festlegen der Dienstsatzidentifizierung auf einen beliebigen Wert (falls kein Wert angegeben wurde) und Versuch des Verbindungsaufbaus zur angegebenen Dienstsatzidentifizierung.

Datentyp:	NDIS_802_11_SSID
Abfrage:	Gibt die SSID zurück.
Festlegen:	Legt die SSID fest.
Statusanzeige:	Nicht unterstützt

OID_802_11_NETWORK_TYPES_SUPPORTED

Datentyp:	NDIS_802_11_NETWORK_TYPE_LIST
Abfrage**:**	Gibt ein Array aller vom Treiber und Gerät unterstützten NDIS_802_11_NETWORK_TYPE(s) zurück.
Festlegen:	Nicht unterstützt
Statusanzeige:	Nicht unterstützt

OID_802_11_NETWORK_TYPE_IN_USE

Datentyp:	NDIS_802_11_NETWORK_TYPE
Abfrage**:**	Gibt den momentan vom Gerät verwendeten NDIS_802_11_NETWORK_TYPE zurück.
Festlegen:	Legt den Netzwerktyp fest, der für den Treiber verwendet werden soll.
Statusanzeige:	Nicht unterstützt

OID_802_11_TX_POWER_LEVEL

Übertragungspegel in mW

Datentyp:	NDIS_802_11_TX_POWER_LEVEL
Abfrage:	Gibt den aktuellen NDIS_802_11_TX_POWER_LEVEL-Wert zurück.
Festlegen:	Legt den aktuellen NDIS_802_11_TX_POWER_LEVEL-Wert fest. Kontrollpegel werden vom Gerät nicht überschritten.
Statusanzeige:	Nicht unterstützt

OID_802_11_RSSI

Gibt die RSSI (Received Signal Strenght Indication) in dBmW zurück.

Datentyp:	NDIS_802_11_RSSI
Abfrage:	Gibt den aktuellen RSSI-Wert zurück.
Festlegen:	Nicht unterstützt
Statusanzeige:	Wenn die Statusanfrage aktiviert ist, wird, basierend auf dem festgelegten Wert, ein Ereignis ausgelöst.

OID_802_11_RSSI_TRIGGER

Diese OID fragt einen Triggerwert für das RSSI-Ereignis ab oder legt einen entsprechenden Wert fest.

Wenn der Triggerwert den aktuellen RSSI-Wert unterschreitet (<), erfolgt die Statusanzeige, sobald der aktuelle Wert größer oder gleich (>=) dem Triggerwert ist.

Wenn der Triggerwert den aktuellen RSSI-Wert überschreitet (>), erfolgt die Statusanzeige, sobald der aktuelle Wert kleiner oder gleich (<=) dem Triggerwert ist.

Wenn der Triggerwert dem aktuellen Wert entspricht, erfolgt die Statusanzeige sofort.

NdisMIndicateStatus wird aufgerufen, wobei der **GeneralStatus**-Parameter auf NDIS_STATUS_MEDIA_SPECIFIC_INDICATION festgelegt wird und **StatusBuffer** auf einen NDIS_802_1_RSSI-Puffer zeigt.

Datentyp:	NDIS_802_11_RSSI
Abfrage:	Gibt den aktuellen RSSI-Triggerwert zurück.
Festlegen:	Legt den RSSI-Triggerwert für ein Ereignis fest.
Statusanzeige:	Nicht unterstützt

OID_802_11_INFRASTRUCTURE_MODE

Diese OID fragt ab oder legt fest, wie eine 802.11-NIC eine Verbindung zum Netzwerk herstellt. Sie bewirkt darüber hinaus das Zurücksetzen des Netzwerkverbindungsalgorithmus.

Datentyp:	NDIS_802_11_NETWORK_INFRASTRUCTURE
Abfrage:	Gibt den Wert für einen der Modi **Infrastruktur**, **IBSS** (Independent Basic Service Set, Unabhängiger Basisdienstsatz) oder **Unbekannt** zurück.
Festlegen:	Legt den Modus **Infrastruktur** oder **IBSS** fest oder wechselt automatisch zwischen diesen beiden Modi.
Statusanzeige:	Nicht unterstützt

OID_802_11_FRAGMENTATION_THRESHOLD

Pakete, die diesen Schwellenwert überschreiten, werden vom WLAN fragmentiert. Durch die Einstellung Null wird die Fragmentierung beseitigt.

Datentyp:	NDIS_802_11_FRAGMENTATION_THRESHOLD
Abfrage:	Gibt den aktuellen Schwellenwert für die Fragmentierung zurück.
Festlegen:	Legt den Schwellenwert für die Fragmentierung fest.
Statusanzeige:	Nicht unterstützt

OID_802_11_RTS_THRESHOLD

Pakete, deren Größe diesen Schwellenwert überschreiten, führen zum Aufrufen des RTS/CTS-Mechanismus durch das WLAN. Der Wert **Null** bedeutet, dass RTS/CTS für alle Pakete angewendet wird.

Datentyp:	NDIS_802_11_RTS_THRESHOLD
Abfrage:	Gibt den aktuellen RTS-Schwellenwert zurück.
Festlegen:	Legt den RTS-Schwellenwert fest.
Statusanzeige:	Nicht unterstützt

OID_802_11_NUMBER_OF_ANTENNAS

Gibt die Anzahl der Antennen des Transceivers zurück.

Datentyp: Abfrage:	ULONG Gibt die Anzahl der Antennen des Transceivers zurück.
Festlegen:	Nicht unterstützt
Statusanzeige:	Nicht unterstützt

OID_802_11_RX_ANTENNA_SELECTED

Gibt die Antenne zurück, die am Transceiver für den Empfang ausgewählt wurde.

Datentyp:	NDIS_802_11_ANTENNA
Abfrage:	Gibt die Antenne zurück, die für den Empfang ausgewählt wurde.
Festlegen:	Legt die Antenne fest, die für den Empfang verwendet wird.
Statusanzeige:	Nicht unterstützt

Anmerkung Der Wert **-1** ist gleichbedeutend mit der Auswahl aller Antennen, also der Einstellung **Diversity** (Vielfalt).]

OID_802_11_TX_ANTENNA_SELECTED

Gibt die Antenne zurück, die am Transceiver für die Übertragung ausgewählt wurde.

Datentyp:	NDIS_802_11_ANTENNA
Abfrage:	Gibt die Antenne zurück, die für die Übertragung ausgewählt wurde.
Festlegen:	Legt die Antenne fest, die für die Übertragung verwendet wird.
Statusanzeige:	Nicht unterstützt

Anmerkung Der Wert **-1** ist gleichbedeutend mit der Auswahl aller Antennen, also der Einstellung **Diversity** (Vielfalt).]

OID_802_11_SUPPORTED_RATES

Hierbei handelt es sich um einen Satz unterstützter Datenraten, mit denen der Transceiver betrieben werden kann. Datenraten werden in Form von 8 Oktetten codiert, wobei jedes Oktett eine einzelne unterstützte Rate in Einheiten von 0,5 Mbit/s definiert.

Unterstützte Raten, die zum Satz der Basisraten des BSS (BSSBasicRateSet) gehören, werden für Rahmen, wie z. B. Steuerungs- und Broadcastrahmen, verwendet. Jede unterstützte Rate, die zum BSSBasicRateSet gehört, wird als Oktett codiert, wobei das MSB (Bit 7) auf 1 festgelegt wird. So wird beispielsweise eine Rate von 1 Mbit/s, die zum BSSBasicRateSet gehört, als 0x82 codiert.

Raten, die nicht zum BSSBasicRateSet gehören, werden codiert, indem das MSB auf 0 festgelegt wird. So wird beispielsweise eine Rate von 2 Mbit/s, die nicht zum BSSBasicRateSet gehört, als 0x04 codiert.

Datentyp:	NDIS_802_11_RATES
Abfrage:	Gibt den Satz der unterstützten Datenraten zurück, mit der der Transceiver betrieben werden kann.
Festlegen:	Nicht unterstützt
Statusanzeige:	Nicht unterstützt

OID_802_11_DESIRED_RATES

Hierbei handelt es sich um einen Satz von Datenraten, die für den Betrieb des Transceivers gewünscht sind. Datenraten werden in Form von 8 Oktetten codiert, wobei jedes Oktett eine einzelne Rate in Einheiten von 0,5 Mbit/s definiert. Rahmen, die an den Transceiver gerichtet werden, können mit anderen als den unterstützten Raten, die zum BSSBasicRateSet gehören, gesendet werden.

Datentyp:	NDIS_802_11_RATES
Abfrage:	Gibt den Satz der Datenraten zurück.
Festlegen:	Legt den Satz der Datenraten fest.
Statusanzeige:	Nicht unterstützt

OID_802_11_CONFIGURATION

Konfiguriert die Parameter des Transceivers.

Datentyp:	NDIS_802_11_CONFIGURATION
Abfrage:	Gibt die aktuelle Konfiguration des Transceivers zurück.
Festlegen:	Legt die Konfiguration des Transceivers fest.
Statusanzeige:	Nicht unterstützt

OID_802_11_STATISTICS

Ruft die aktuellen statistischen Informationen ab.

Datentyp:	NDIS_802_11_STATISTICS
Abfrage:	Gibt die aktuellen statistischen Informationen zurück.
Festlegen:	Nicht unterstützt
Statusanzeige:	Nicht unterstützt

OID_802_11_ADD_WEP

Der WEP-Schlüssel sollte nicht im permanenten Speicher abgelegt werden. Er sollte nicht mehr verfügbar sein, sobald die Karte die Funkverbindung zu allen BSSIDs trennt oder wenn die Shared Key-Authentifizierung mithilfe des WEP-Schlüssels fehlschlägt. Durch einen zweiten Aufruf desselben Indexes muss der vorherige Wert überschrieben werden.

Datentyp:	NDIS_802_11_WEP
Abfrage:	Nicht unterstützt
Festlegen:	Legt den gewünschten WEP-Schlüssel fest.
Statusanzeige:	Nicht unterstützt

OID_802_11_REMOVE_WEP

Der WEP-Schlüssel sollte nicht im permanenten Speicher abgelegt werden. Er sollte nicht mehr verfügbar sein, sobald die Karte die Funkverbindung zu allen BSSIDs trennt.

Datentyp:	NDIS_802_11_KEY_INDEX
Abfrage:	Nicht unterstützt
Festlegen:	Entfernt den gewünschten WEP-Schlüssel.
Statusanzeige:	Nicht unterstützt

OID_802_11_DISASSOCIATE

Trennt die Funkverbindung zur aktuellen Dienstsatzidentifizierung und deaktiviert den Transceiver.

Datentyp:	Diesem Satz ist kein Datentyp zugeordnet.
Abfrage:	Nicht unterstützt
Festlegen:	Trennt die Funkverbindung zur aktuellen Dienstsatzidentifizierung und deaktiviert den Transceiver.
Statusanzeige:	Nicht unterstützt

OID_802_11_POWER_MODE

Datentyp:	NDIS_802_11_POWER_MODE
Abfrage:	Gibt den aktuellen NDIS_802_11_POWER_MODE-Wert zurück.
Festlegen:	Legt den aktuellen NDIS_802_11_POWER_MODE-Wert fest.
Statusanzeige:	Nicht unterstützt

OID_802_11_BSSID_LIST

Diese OID gibt die Liste aller ermittelten BSSIDs einschließlich ihrer in der Datenstruktur angegebenen Attribute zurück. Die zurückgegebene Liste der BSSIDs entspricht der zwischengespeicherten Liste, die in der Datenbank der IEEE 802.11-NIC gespeichert wird. Die Liste der BSSIDs in der Datenbank der IEEE 802.11-NIC entspricht dem Satz der BSSs, die von der IEEE 802.11-NIC während des letzten Scanvorgangs im Hinblick auf mögliche BSSs ermittelt wurden. Ein Aufruf dieser OID sollte zu einer sofortigen Rückgabe der Liste der BSSIDs in der Datenbank der IEEE 802.11-NIC führen.

Wenn diese OID ohne vorherigen Aufruf von OID_802_11_BSSID_LIST_SCAN aufgerufen wird und die IEEE 802.11-NIC aktiv ist, kann eine Liste mit BSSIDs zurückgegeben werden, die auf diejenigen BSSIDs beschränkt ist, die gemäß der aktuellen Konfiguration der IEEE 802.11-NIC als gültig angesehen werden. Wenn diese OID jedoch direkt auf einen Aufruf von OID_802_11_BSSID_LIST_SCAN folgt, sollte die Liste der BSSIDs sämtliche BSSIDs umfassen, die von OID_802_11_BSSID_LIST_SCAN ermittelt wurden.

Datentyp:	NDIS_802_11_BSSID_LIST
Abfrage:	Gibt die NDIS_802_11_BSSID_LIST-Struktur zurück.
Festlegen:	Nicht unterstützt
Statusanzeige:	Nicht unterstützt

OID_802_11_BSSID_LIST_SCAN

Ein Aufruf dieser OID führt dazu, dass die IEEE 802.11-NIC einen Scanvorgang im Hinblick auf mögliche BSSs anfordert. Hierbei werden die folgenden Parameter verwendet:

- BSSType = sowohl Infrastruktur-BSSs als auch unabhängige BSSs
- BSSID = Broadcast-BSSID
- SSID = Broadcast-SSID
- ScanType = entweder aktiv, passiv oder eine Kombination aus dem passiven und dem aktiven Scanverfahren
- ChannelList = alle zugelassenen Frequenzkanäle

Beim Aufruf dieser OID führt die IEEE 802.11-NIC einen Scanvorgang aus (wobei das aktive oder passive Scanverfahren oder eine Kombination aus aktivem und passivem Scanverfahren zum Einsatz kommt), um die Liste der BSSIDs in der Datenbank der IEEE 802.11-NIC zu aktualisieren. Um einen Aufruf dieser OID abzuschließen, ist das aktive Scannen vorzuziehen, da es das schnelle Auffüllen der von der NIC geführten Datenbank ermöglicht. Das passive Scannen führt zu Verzögerungen, da der Eingang von Ankündigungen abgewartet werden muss.

Wenn die IEEE 802.11-NIC momentan mit einer bestimmten BSSID und SSID verbunden ist, die nicht in der von diesem Scan generierten Liste der BSSIDs enthalten sind, sollte die Beschreibung der momentan verbundenen BSSID und SSID zur Liste der BSSIDs in der Datenbank der IEEE 802.11-NIC hinzugefügt werden. Antworten sämtlicher BSSs auf Frequenzkanälen, die in dem jeweiligen Funkbereich, in dem die IEEE 802.11-NIC momentan betrieben wird, zulässig sind, sollten in die Liste der BSSIDs in der Datenbank der IEEE 802.11-NIC aufgenommen werden.

Datentyp:	Diesem Satz ist kein Datentyp zugeordnet.
Abfrage:	Nicht unterstützt
Festlegen:	Führt einen Scanvorgang im Hinblick auf mögliche BSSs durch.
Statusanzeige:	Nicht unterstützt

OID_802_11_ AUTHENTICATION _MODE

Legt den IEEE 802.11-Authentifizierungsmodus fest.

Datentyp:	NDIS_802_11_AUTHENTICATION_MODE
Abfrage:	Aktueller Modus
Festlegen:	Legt den Authentifizierungsmodus Open System oder Shared Key oder den automatischen Wechsel zwischen diesen beiden Modi fest.
Statusanzeige:	Nicht unterstützt

OID_802_11_PRIVACY_FILTER

Legt den IEEE 802.1X-Vertraulichkeitsfilter fest.

Datentyp:	NDIS_802_11_PRIVACY_FILTER
Abfrage:	Aktueller Modus
Festlegen:	Legt den offenen Filtermodus oder die 802.1X-Filterung fest (0 entspricht der offenen, 1 der 802.1X-Filterung).
Statusanzeige:	Nicht unterstützt

Anhang B: Angabe einer Identitätszeichenfolge in einer EAP-Identity-Request-Nachricht

Die im Folgenden beschriebenen Informationen wurden einem von Microsoft verfassten Internetentwurf entnommen, der im Jahr 2000 beim IETF eingereicht wurde.

In diesem Anhang wird definiert, wie die Zeichenfolge in einer EAP-Identity-Nachricht zum Bereitstellen der Informationen verwendet werden muss, die ein Client benötigt, um zu entscheiden, welche Anmeldeinformationen er angeben muss.

Übersicht

EAP ist ein erweiterbares Authentifizierungsprotokoll, das im Rahmen der PPP-Authentifizierung (Point-to-Point Protocol) und der IEEE 802.1X-Authentifizierung verwendet wird. IEEE 802.1X ermöglicht den authentifizierten Zugriff auf die folgenden LANs: Ethernet, Token Ring und IEEE 802.11. Wenn PPP verwendet wird, ist das Ziel normalerweise bekannt, so dass die zu verwendenden Anmeldeinformationen ebenfalls bekannt sind. Wird IEEE 802.1X verwendet, ist das Ziel nicht im Voraus bekannt, so dass die erforderlichen Anmeldeinformationen ebenfalls nicht bekannt sind.

EAP-Identitätszeichenfolge

EAP ermöglicht es, eine Zeichenfolge zur EAP-Identity-Request-Nachricht hinzuzufügen; diese Zeichenfolge wird jedoch nicht auf die übliche Weise verwendet. Mit IEEE 802.1X können, basierend auf dem Inhalt dieser Zeichenfolge, einige nützliche Ergebnisse erzielt werden; so könnte z. B. eine Netzwerkbezeichnung gesendet werden, der die Auswahl der geeigneten Anmeldeinformationen ermöglicht. Auf diese Weise wird das Roaming ermöglicht, ohne dass paarweise Übereinstimmungen erforderlich sind.

Verwenden von EAP

Als Antwort auf eine Identitätsanforderung wird eine Nachricht gesendet, die den Namen des Benutzers enthält, der den Zugriff auf das Netzwerk anfordert.

Format der EAP-Identitätszeichenfolge

Diese Zeichenfolge sollte das folgende Format aufweisen:

- Eine durch Null beendete, anzuzeigende Zeichenfolge – die Anzeige für den Benutzer.
- Eine durch Kommas getrennte Liste mit Namen – die Wertepaare.

NetworkID-Name

Bei dem Wert von **NetworkID** kann es sich z. B. um einen RADIUS-Bereich handeln. Die folgende Zeile enthält ein Beispiel für eine mögliche Anzeige:

```
Zeichenfolge\0networkid=Microsoft.com,networkid=exchange.Microsoft.com,foo=bar.
```

Sicherheitsaspekte

Die Nachrichtenformatierung und die Verwendungsregeln werfen keine neuen Sicherheitsprobleme auf.

IANA-Überlegungen

Hinsichtlich der IANA (Internet Assigned Numbers Authority) müssen keine besonderen Aspekte beachtet werden.

Weitere Informationen

Eine ausführliche Darstellung von EAP finden Sie in: Blunk, L. und J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, März 1998.

MS-MPPE-Send-Key

Beschreibung

Das **MS-MPPE-Send-Key**-Attribut enthält einen Sitzungsschlüssel für die Verwendung durch das MPPE-Protokoll (Microsoft Point-to-Point Encryption). Wie der Name schon andeutet, dient der Schlüssel zur Verschlüsselung von Paketen, die vom NAS an den Remotehost gesendet werden. Dieses Attribut wird nur in Access-Accept-Pakete eingebunden.

Im Folgenden finden Sie eine Zusammenfassung des Formats des **MS-MPPE-Send-Key**-Attributs. Die Felder werden von links nach rechts übertragen.

0 1 2 3

1 2 3 4 5 6 7 8 9 0 1

+-+

| Vendor-Type | Vendor-Length | Salt

+-+

String...

+-+

Vendor-Type

16 für MS-MPPE-Send-Key.

Vendor-Length

> 4

Salt

Die Länge des **Salt**-Feldes beträgt zwei Oktette. Das Feld stellt die Eindeutigkeit der Schlüssel sicher, die verwendet werden, um jedes der in einem Access-Accept-Paket verwendeten verschlüsselten Attribute zu verschlüsseln. Das MSB (Most Significant Bit, werthöchstes Bit), also das am weitesten links befindliche Bit des **Salt**-Feldes, muss auf (1) festgelegt werden. Der Inhalt jedes **Salt**-Feldes in einem Access-Accept-Paket muss eindeutig sein.

String

Das Klartextfeld **String** setzt sich aus drei logischen Unterfeldern zusammen: den Feldem **Key-Length** und **Key** (beide erforderlich) und dem optionalen **Padding**-Unterfeld. Das **Key-Length**-Unterfeld ist ein Oktett lang und gibt die Länge des unverschlüsselten **Key**-Unterfeldes an. Das **Key**-Unterfeld enthält den eigentlichen Verschlüsselungsschlüssel. Wenn die zusammengefasste Länge (in Oktetten) der unverschlüsselten Unterfelder **Key-Length** und **Key** kein gerades Mehrfaches von 16 ist, muss das **Padding**-Unterfeld vorhanden sein. Wenn diese Feld vorhanden ist, ist seine Länge variabel und beläuft sich auf einen Wert zwischen 1 und 15 Oktetten. Vor der Übertragung muss das **String**-Feld folgendermaßen verschlüsselt werden:

- Bilden Sie eine Klartextversion des **String**-Feldes, indem Sie die Unterfelder **Key-Length** und **Key** verketten. Füllen Sie gegebenenfalls die sich daraus ergebende Zeichenfolge auf, bis ihre Länge (in Oktetten) ein gerades Vielfaches von 16 ergibt. Es wird empfohlen, für das Auffüllen Null-Oktette (0x00) zu verwenden. Nennen Sie diese Klartextversion P.

Nennen Sie den gemeinsamen geheimen Schlüssel S, den aus einer 128-Bit-Pseudo-Zufallszahl bestehenden Request Authenticator (aus dem entsprechenden Access-Request-Paket) R und den Inhalt des **Salt**-Feldes A. Unterteilen Sie die Klartextversion in 16-Oktett-Blöcke p(1), p(2)...p(i), wobei i = Länge(P)/16. Nennen Sie die Blöcke mit verschlüsseltem Text c(1), c(2)...c(i) und den endgültigen verschlüsselten Text C. Die Zwischenwerte b(1), b(2)...c(i) sind erforderlich.

Die Verschlüsselung erfolgt folgendermaßen ('+' kennzeichnet eine Verkettung):

b(1) = MD5(S + R + A) c(1) = p(1) xor b(1) C = c(1)
b(2) = MD5(S + c(1)) c(2) = p(2) xor b(2) C = C + c(2)
. .
. .
. .
b(i) = MD5(S + c(i-1)) c(i) = p(i) xor b(i) C = C + c(i)

Das resultierende verschlüsselte **String** Feld enthält Folgendes:

c(1)+c(2)+...+c(i).

Beim Empfang wird dieser Prozess umgekehrt, um die Klartextversion der Zeichenfolge zu erhalten.

Hinweise zur Implementierung

Es ist möglicht, dass der zurückgegebene Schlüssel länger ist, als für das verwendete Verschlüsselungsschema erforderlich ist. In diesem Fall muss der RADIUS-Client die erforderliche Kürzung vornehmen.

Mithilfe dieses Attributs kann ein Schlüssel von einem externen Server (z. B. EAP) an den RADIUS-Server übergeben werden. In diesem Fall ist es dem externen Server eventuell nicht möglich, den Schlüssel korrekt zu verschlüsseln, da der gemeinsame geheime RADIUS-Schlüssel möglicherweise nicht verfügbar ist. Der externe Server sollte das Attribut dennoch wie zuvor definiert zurückgeben; das **Salt**-Feld sollte mit Nullen ausgefüllt und das **String**-Feld wie erforderlich aufgefüllt werden.

Wenn der RADIUS-Server das Attribut vom externen Server empfängt, muss er das **Salt**-Feld korrekt festlegen und das **String**-Feld verschlüsseln, bevor er das Attribut an den RADIUS-Client übermittelt. Wenn der für die Übermittlung des **MS-MPPE-Send-Key**-Attributs verwendete Kanal nicht abhörsicher ist, muss das Attribut durch Verschlüsselung geschützt werden.

MS-MPPE-Recv-Key

Beschreibung

Das **MS-MPPE-Recv-Key**-Attribut enthält einen Sitzungsschlüssel für die Verwendung durch das MPPE-Protokoll (Microsoft Point-to-Point Encryption). Wie der Name schon andeutet, dient der Schlüssel zur Verschlüsselung von Paketen, die der NAS vom Remotehost erhält. Dieses Attribut wird nur in Access-Accept-Pakete eingebunden.

Im Folgenden finden Sie eine Zusammenfassung des Formats des **MS-MPPE-Recv-Key**-Attributs. Die Felder werden von links nach rechts übertragen.

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+

| Vendor-Type | Vendor-Length | Salt

+-+

String...

+-+

Vendor-Type

17 für MS-MPPE-Recv-Key.

Vendor-Length

> 4

Salt

Die Länge des **Salt**-Feldes beträgt zwei Oktette. Das Feld stellt die Eindeutigkeit der Schlüssel sicher, die verwendet werden, um jedes der in einem Access-Accept-Paket verwendeten verschlüsselten Attribute zu verschlüsseln. Das werthöchste Bit (Most Significant Bit, MSB), also das am weitesten links befindliche Bit des **Salt**-Feldes, muss auf (1) festgelegt werden. Der Inhalt jedes **Salt**-Feldes in einem Access-Accept-Paket muss eindeutig sein.

String

Das Klartextfeld **String** setzt sich aus drei logischen Unterfeldern zusammen: den Feldern **Key-Length** und **Key** (beide erforderlich) und dem optionalen **Padding**-Unterfeld. Das **Key-Length**-Unterfeld ist ein Oktett lang und gibt die Länge des unverschlüsselten **Key**-Unterfeldes an. Das **Key**-Unterfeld enthält den eigentlichen Verschlüsselungsschlüssel. Wenn die zusammengefasste Länge (in Oktetten) der unverschlüsselten Unterfelder **Key-Length** und **Key** kein gerades Mehrfaches von 16 ist, muss das **Padding**-Unterfeld vorhanden sein. Wenn dieses Feld vorhanden ist, ist seine Länge variabel und beläuft sich auf einen Wert zwischen 1 und 15 Oktetten. Vor der Übertragung muss das **String**-Feld folgendermaßen verschlüsselt werden:

- Bilden Sie eine Klartextversion des **String**-Feldes, indem Sie die Unterfelder **Key-Length** und **Key** verketten. Füllen Sie gegebenenfalls die sich daraus ergebende Zeichenfolge auf, bis ihre Länge (in Oktetten) ein gerades Vielfaches von 16 ergibt. Es wird empfohlen, für das Auffüllen Null-Oktette (0x00) zu verwenden. Nennen Sie diese Klartextversion P.

Nennen Sie den gemeinsamen geheimen Schlüssel S, den aus einer 128-Bit-Pseudo-Zufallszahl bestehenden Request Authenticator (aus dem entsprechenden Access-Request-Paket) R und den Inhalt des **Salt**-Feldes A. Unterteilen Sie die Klartextversion in 16-Oktett-Blöcke p(1), p(2)...p(i), wobei i = Länge(P)/16. Nennen Sie die Blöcke mit verschlüsseltem Text c(1), c(2)...c(i) und den endgültigen verschlüsselten Text C. Die Zwischenwerte b(1), b(2)...c(i) sind erforderlich. Die Verschlüsselung erfolgt folgendermaßen ('+' kennzeichnet eine Verkettung):

b(1) = MD5(S + R + A) c(1) = p(1) xor b(1) C = c(1)
b(2) = MD5(S + c(1)) c(2) = p(2) xor b(2) C = C + c(2)
. .
. .
. .
b(i) = MD5(S + c(i-1)) c(i) = p(i) xor b(i) C = C + c(i)

Das resultierende verschlüsselte **String**-Feld enthält Folgendes:

c(1)+c(2)+...+c(i).

Beim Empfang wird dieser Prozess umgekehrt, um die Klartextversion der Zeichenfolge zu erhalten.

Hinweise zur Implementierung

Es ist möglich, dass der zurückgegebene Schlüssel länger ist, als für das verwendete Verschlüsselungsschema erforderlich ist. In diesem Fall muss der RADIUS-Client die erforderliche Kürzung vornehmen.

Mithilfe dieses Attributs kann ein Schlüssel von einem externen Server (z. B. EAP) an den RADIUS-Server übergeben werden. In diesem Fall ist es dem externen Server eventuell nicht möglich, den Schlüssel korrekt zu verschlüsseln, da der gemeinsame geheime RADIUS-Schlüssel möglicherweise nicht verfügbar ist. Der externe Server sollte das Attribut dennoch wie zuvor definiert zurückgeben; das **Salt**-Feld sollte mit Nullen ausgefüllt und das **String**-Feld wie erforderlich aufgefüllt werden.

Wenn der RADIUS-Server das Attribut vom externen Server empfängt, muss er das **Salt**-Feld korrekt festlegen und das **String**-Feld verschlüsseln, bevor er das Attribut an den RADIUS-Client übermittelt. Wenn der für die Übermittlung des **MS-MPPE-Recv-Key**-Attributs verwendete Kanal nicht abhörsicher ist, muss das Attribut durch Verschlüsselung geschützt werden.

MS-MPPE-Encryption-Policy

Beschreibung

Mithilfe des **MS-MPPE-Encryption-Policy**-Attributs kann gekennzeichnet werden, ob die Verwendung der Verschlüsselung zulässig oder erforderlich ist. Wenn das **Policy**-Feld dem Wert **1** entspricht (**Encryption-Allowed**) kann eine beliebige oder keine der im **MS-MPPE-Encryption-Types**-Attribut angegebenen Verschlüsselungsarten verwendet werden. Wenn das **Policy**-Feld dem Wert **2** entspricht (**Encryption-Required**) kann eine beliebige der im **MS-MPPE-Encryption-Types**-Attribut angegebenen Verschlüsselungsarten verwendet werden; die Verwendung einer dieser Verschlüsselungsarten ist jedoch erforderlich.

Im Folgenden finden Sie eine Zusammenfassung des Formats des **MS-MPPE-Encryption-Policy**-Attributs. Die Felder werden von links nach rechts übertragen.

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+

| Vendor-Type | Vendor-Length | Policy

+-+

Policy (Fortsetzung) |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Vendor-Type

7 für MS-MPPE-Encryption-Policy.

Vendor-Length

6

Policy

Die Länge des **Policy**Feldes beträgt vier Oktette. Folgende Werte sind definiert:

- Encryption-Allowed
- Encryption-Required

Zum Entschlüsseln des **Radius**-Attributs wird folgender Code verwendet:

```
DWORD DecryptMPPESendRecvKeys(
IN RADIUSSERVER UNALIGNED * pRadiusServer,
IN PBYTE pRequestAuthenticator,
IN DWORD dwLength,
IN OUT PBYTE pEncryptionKeys
)
{
BYTE * pbValue = (BYTE *)pEncryptionKeys + 2;
BYTE abCipherText[16];
struct MD5Context MD5c;
struct MD5Digest MD5d;
```

```
DWORD dwIndex;
DWORD dwBlock;
DWORD dwNumBlocks;
dwNumBlocks = ( dwLength - 2 ) / 16;
//
// Durchlaufen der Blöcke
//
for ( dwBlock = 0; dwBlock < dwNumBlocks; dwBlock++ )
{
MD5Init( &MD5c );
MD5Update( &MD5c, (PBYTE)(pRadiusServer->szSecret), pRadiusServer-
>cbSecret);
if ( dwBlock == 0 )
{
//
// Verwenden des Request Authenticators und des Salt-Feldes für den ersten
Block
//
MD5Update( &MD5c, pRequestAuthenticator, 16 );
MD5Update( &MD5c, pEncryptionKeys, 2 );
}
else
{
//
// Verwenden des vorherigen Blocks mit verschlüsseltem Text
//
MD5Update( &MD5c, abCipherText, 16 );
}
MD5Final( &MD5d, &MD5c );
//
// Speichern des verschlüsselten Textes aus diesem Block.
//
CopyMemory(abCipherText, pbValue, sizeof(abCipherText));
for ( dwIndex = 0; dwIndex < 16; dwIndex++ )
{
*pbValue ^= MD5d.digest[dwIndex];
pbValue++;
}
}
return( NO_ERROR );
}
```

Generieren der EAPOL-Key-Nachricht

Zum Generieren der EAPOL-Key-Nachricht müssen Sie Folgendes verwenden:

- **Recvkey** für die md5-Signatur und **IV+sendkey** für die rc4-Verschlüsselung. (Beachten Sie, dass die Schlüssel **MPPE-Send** und **Recv** länger als notwendig sein können. In diesem Fall verwenden Sie die ersten X Byte, die Sie benötigen.)
- RC4_KEYSTRUCT rc4key
- BYTE keybuffer[48]
- memcpy(keybuffer, IV, 16)
- memcpy(&keybuffer[16], mppesendkey, 32);
- rc4_key(&rc4, 48, keybuffer)
- rc4(&rc4, KeyLength, KeyMaterial);

Generieren der MD5-Signatur

Zum Generieren der MD5-Signatur müssen Sie Folgendes verwenden:

- Das Paket, das bei der EAPOL-Protokollversion beginnt und dies e umfasst, bis zum Ende des Pakets, einschließlich des ENCRYPTED-Schlüsselmaterials;
- Beispiel: das Paket nach dem Ethernet-Header, wie er mit Signatur 0 gesendet wird.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

4/2001