



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 603 03 075 T2** 2006.09.14

(12)

Übersetzung der europäischen Patentschrift

(97) **EP 1 408 653 B1**

(51) Int Cl.⁸: **H04L 12/28** (2006.01)

(21) Deutsches Aktenzeichen: **603 03 075.0**

(96) Europäisches Aktenzeichen: **03 022 872.0**

(96) Europäischer Anmeldetag: **08.10.2003**

(97) Erstveröffentlichung durch das EPA: **14.04.2004**

(97) Veröffentlichungstag

der Patenterteilung beim EPA: **04.01.2006**

(47) Veröffentlichungstag im Patentblatt: **14.09.2006**

(30) Unionspriorität:

416528 P	08.10.2002	US
632807	04.08.2003	US

(84) Benannte Vertragsstaaten:

DE, FR, GB

(73) Patentinhaber:

Broadcom Corp., Irvine, Calif., US

(72) Erfinder:

**Lor, Kar-Wing Edward, Castro Valley California
94552, US; Martin, Richard, 95027 Morgan Hill
California, US; Hassen, Alarabi Omar, 92656 Aliso
Viejo California, US**

(74) Vertreter:

**Bosch, Graf von Stosch, Jehle
Patentanwalts-gesellschaft mbH, 80639 München**

(54) Bezeichnung: **Drahtloses LAN Vermittlungssystem für Unternehmen**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

HINTERGRUND DER ERFINDUNG

GEBIET DER ERFINDUNG

[0001] Die vorliegende Erfindung ist auf drahtlose lokale Netzwerke in Unternehmensumgebungen gerichtet, die eine leichte Installation und nahtlose Übergänge zwischen Abschnitten des drahtlosen lokalen Netzwerks bereitstellen. Insbesondere betrifft die vorliegende Erfindung ein Verfahren und eine Vorrichtung zur Kontrolle eines Datenflusses in einem drahtlosen lokalen Unternehmens-Netzwerk.

BESCHREIBUNG DES STANDES DER TECHNIK

[0002] Drahtlose lokale Netzwerke (WLANs; wireless local area networks) gewinnen immer mehr an Popularität als das System zur Vernetzung von Benutzern in dem Unternehmen. Die Vorteile, die WLANs gegenüber herkömmlichen verdrahteten LANs bereitstellen, sind Benutzermobilität, leichte Installation, nahtloser Übergang zwischen Unternehmensumgebungen und Telekommunikations-Provider-Umgebungen und die Konnektivität an öffentlichen Plätzen (wie z.B. Flughäfen, Bibliotheken und Konferenzen), sowie weitere Vorteile.

[0003] Es gibt viele Bereiche, in denen bestehende WLAN-Lösungen Raum für Verbesserungen bieten, und die WLAN-Netzwerke der nächsten Generation in der Unternehmensumgebung werden zusätzliche Leistungsmerkmale und Funktionalitäten bereitstellen müssen. Die Probleme, die mit der drahtlosen Unternehmens-LAN-Architektur verbunden sind, umfassen die Sicherheit, die Zugriffskontrolle, die Mobilität, das Netzwerkmanagement, den Lastausgleich und die Dienstgüte. Diese Bereiche stehen zwar in einer engen Beziehung zueinander, aber trotzdem stellt jeder von ihnen einzigartige Anforderungen, denen sich die Unternehmens-WLAN-Architektur widmet.

[0004] Der Artikel von P. Bahl et al, "PAWNS: Satisfying the need for ubiquitous secure connectivity and location services" (PAWNS: Befriedigung des Bedarfs nach allgegenwärtiger Sicherheit bei der Konnektivität und den ortsbezogenen Diensten), der in IEEE Wireless Communications, Band 9, Nr. 1, Seiten 40–48, im Februar 2002 veröffentlicht worden ist, bezieht sich auf öffentliche drahtlose Netzwerke (PAWNS; public area wireless networks) und erörtert die Probleme der Netzwerksicherheit, der Authentifizierung zum Schutz der Privatsphäre und des Mobilitätsmanagements in PAWNS. Ferner werden die Architektur, die Dienstmodelle und die ortsbezogenen Dienste eines PAWN, das von den Autoren des Artikels entwickelt worden ist, beschrieben.

[0005] Bestehende WLAN-Lösungen sind zur Verwendung in begrenzten Installationen wie z.B. in einem Büro zuhause oder in einem kleinen Büro bestimmt, aber sie mangeln immer noch in vielen Bereichen, wenn der Einsatz in großen Unternehmen erforderlich ist. Entsprechend besteht im Stand der Technik ein Bedarf nach einem Verfahren oder einem Mechanismus, die eine Unternehmens-WLAN-Architektur bereitstellen können, die für eine leichte Installation und Wartung, eine nahtlose Mobilität von drahtlosen Vorrichtungen bzw. Geräten in dem Unternehmen und für die Sicherheit des Unternehmens sorgt.

ZUSAMMENFASSUNG DER ERFINDUNG

[0006] Die vorliegende Erfindung strebt danach, die Nachteile der oben beschriebenen herkömmlichen Netzwerkvorrichtungen und -verfahren zu überwinden.

[0007] Zu diesem Zweck werden ein Verfahren und eine Netzwerkvorrichtung bereitgestellt, wie sie durch den Gegenstand der Nebenansprüche 1 und 6 dargelegt sind. Weitere vorteilhafte Merkmale der Erfindung sind in den Unteransprüchen definiert.

[0008] Gemäß einer Ausführungsform der vorliegenden Erfindung ist ein Verfahren zur Kontrolle eines Datenflusses in einem drahtlosen Netzwerk offenbart, das einen drahtlosen Zugriff auf das drahtlose Netzwerk durch drahtlose Vorrichtungen vorsieht. Daten werden von einer drahtlosen Vorrichtung mittels einer Netzwerkvorrichtung durch einen Zugangspunkt einer Vielzahl von Zugangspunkten in Kommunikation mit der Netzwerkvorrichtung empfangen, wobei eine Client-Identifizierung für die drahtlose Vorrichtung angezeigt wird. Die Client-Identifizierung wird zu einem Authentifikationsserver und der Netzwerkvorrichtung weitergeleitet, die die Authentifizierung der drahtlosen Vorrichtung mit dem Authentifikationsserver vermittelt hat. Danach werden die Datenpakete, die von Abschnitten des drahtlosen Netzwerks und von der Vielzahl von Zugangspunkten empfangen werden, ausgewertet, und die empfangenen Datenpakete werden zu Abschnitten des drahtlosen Netz-

werks und zu der Vielzahl von Zugangspunkten auf der Grundlage der Auswertung der empfangenen Datenpakete übermittelt. Außerdem fragt die Netzwerkvorrichtung periodisch einen Zustand bzw. Status der drahtlosen Vorrichtung von dem Zugangspunkt ab.

[0009] Alternativ dazu kann die Auswertung der Datenpakete das Filtern der empfangenen Datenpakete derart umfassen, dass die gefilterten Datenpakete fallengelassen werden können, um eine Wirksamkeit eines Dienstverweigerungsangriffs zu begrenzen. Außerdem kann der Schritt des Vermittels der Authentifizierung der drahtlosen Vorrichtung das Einschränken des Zugriffs auf das drahtlose Netzwerk durch die drahtlose Vorrichtung auf der Grundlage einer Benutzerkategorie, die aus der Client-Identifizierung ermittelt wird, auf der Grundlage eines Typs von Vorrichtung, zu dem die drahtlose Vorrichtung gehört, oder auf der Grundlage einer Stunde und eines Tages der Woche umfassen, in denen die Daten von der drahtlosen Vorrichtung empfangen wurden. Die Zugriffseinschränkung kann auf einem physischen Aufenthaltsort des einen Zugangspunkts einer Vielzahl von Zugangspunkten basieren oder auf einem Typ einer Anwendung basieren, die bei der drahtlosen Vorrichtung abläuft und die für die drahtlose Vorrichtung Zugriff auf das Netzwerk verlangt. Außerdem kann das Verfahren das Weiterleiten von Aktualisierungen für die Software und Konfigurationen der Vielzahl von Zugangspunkten zu der Vielzahl von Zugangspunkten ausgehend von einer einzigen Stelle in dem drahtlosen Netzwerk umfassen.

[0010] Auch an Stellen, an denen sich die Funkversorgungsbereiche für wenigstens zwei der Vielzahl von Zugangspunkten überlappen, kann das Verfahren auch eine Überwachung der Benutzung durch drahtlose Vorrichtungen der wenigstens zwei der Vielzahl von Zugangspunkten und die Aufforderung für die wenigstens zwei der Vielzahl von Zugangspunkten umfassen, die Verwendung durch die drahtlosen Vorrichtungen derart zu verändern, dass eine Last, die von den wenigstens zwei der Vielzahl von Zugangspunkten getragen wird, ausgeglichen wird. Die Last, die von den wenigstens zwei der Vielzahl von Zugangspunkten getragen wird, kann ermittelt werden durch wenigstens eine einer Anzahl von drahtlosen Vorrichtungen, die die wenigstens zwei der Vielzahl von Zugangspunkten verwendet, eine Anzahl von Paketen, die durch die wenigstens zwei der Vielzahl von Zugangspunkten übertragen und empfangen werden, eine durchschnittliche Bandbreite, die von den wenigstens zwei der Vielzahl von Zugangspunkten übertragen wird, die Prioritäten der Pakete, die vor kurzem von den wenigstens zwei der Vielzahl von Zugangspunkten übertragen und empfangen worden sind, einen Typ von Anwendung, der bei den drahtlosen Vorrichtungen abläuft und mit den wenigstens zwei der Vielzahl von Zugangspunkten kommuniziert, und eine Signalstärke, die den drahtlosen Vorrichtungen zugeführt wird, die von den wenigstens zwei der Vielzahl von Zugangspunkten bereitgestellt wird.

[0011] Gemäß einem anderen Ausführungsbeispiel der vorliegenden Erfindung kann eine Priorität, die durch die Datenpakete angezeigt wird, aufrechterhalten werden, und die Datenpakete können mit einem Prioritäts-Tag markiert werden, das von den Zugangspunkten ausgewertet werden soll. Alternativ dazu können Priorisierungs-Richtlinien auf der Grundlage der Filterung der Datenpakete eingerichtet werden, und die Datenpakete können mit einem Prioritäts-Tag markiert werden, das von den Zugangspunkten auf der Grundlage der eingerichteten Priorisierungs-Richtlinien ausgewertet werden soll. Es können auch Bandbreitennutzungs-Richtlinien für die drahtlosen Vorrichtungen eingerichtet werden, und die Vielzahl von Zugangspunkten kann so instruiert werden, dass sie den eingerichteten Bandbreitennutzungs-Richtlinien folgen.

[0012] In einem anderen Ausführungsbeispiel kann das Verfahren das Empfangen einer Reassoziierungsanforderung von einer übertragenden drahtlosen Vorrichtung durch einen neuen Zugangspunkt der Vielzahl von Zugangspunkten, wobei die übertragende drahtlose Vorrichtung vorher mit einem alten Zugangspunkt der Vielzahl von Zugangspunkten assoziiert war, das Bereitstellen der Sitzungsinformationen für die übertragende drahtlose Vorrichtung zu dem neuen Zugangspunkt, und das Aktualisieren einer Routing-Tabelle mit einer Routing-Lokalisierung der übertragenden drahtlosen Vorrichtung aufweisen. Außerdem können die empfangenen Datenpakete mit Internet-Protokoll-Informationen eingekapselt werden, die mit dem neuen Zugangspunkt assoziiert sind. Auch kann das Verfahren das Empfangen einer Reassoziierungsanforderung von einer übertragenden drahtlosen Vorrichtung durch einen neuen Zugangspunkt der Vielzahl von Zugangspunkten, wobei die übertragende drahtlose Vorrichtung vorher mit einem anderen Zugangspunkt in Kommunikation mit dem drahtlosen Netzwerk durch eine andere Netzwerkvorrichtung assoziiert war, das Senden einer Anforderung von Konfigurationsinformationen für die übertragende drahtlose Vorrichtung von der alternativen Netzwerkvorrichtung und das Weiterleiten von Zugangspunkt-Konfigurationsdaten, die aus den Konfigurationsinformationen für die übertragende drahtlose Vorrichtung ermittelt wurden, die von der anderen Netzwerkvorrichtung empfangen worden sind, zu dem neuen Zugangspunkt umfassen.

[0013] Außerdem kann die drahtlose Vorrichtung ein drahtloses Internet-Protokoll-Telefon sein, die Client-Identifizierung kann Verbindungsaufbaudaten sein, und Datenpakete mit Sprache über das Internet-Proto-

koll (voice over internet protocol data packets) (VoIP-Datenpakete) können zu Abschnitten des drahtlosen Netzwerks und zu der Vielzahl von Zugangspunkten auf der Grundlage der Auswertung der empfangenen VoIP-Datenpakete übermittelt werden. Außerdem kann das Verfahren das Senden eines Freizeichens, das von einem Internet-Protokoll-Telefon-Gateway empfangen wurde, zu dem einen Zugangspunkt und das Vermitteln einer Aushandlung von Netzwerkressourcen zwischen dem Internet-Protokoll-Telefon-Gateway und dem drahtlosen Internet-Protokoll-Telefon umfassen.

[0014] Gemäß einer Ausführungsform der Erfindung ist ein Verfahren zur Kontrolle eines Datenflusses in einem drahtlosen Netzwerk vorgesehen, das einen drahtlosen Zugriff auf das drahtlose Netzwerk durch drahtlose Vorrichtungen vorsieht, wobei das Verfahren folgendes aufweist:

Empfangen von Daten von einer drahtlosen Vorrichtung mittels einer Netzwerkvorrichtung durch einen Zugangspunkt einer Vielzahl von Zugangspunkten in Kommunikation mit der Netzwerkvorrichtung, wobei eine Client-Identifizierung für die drahtlose Vorrichtung angezeigt wird;

Weiterleiten der Client-Identifizierung zu einem Authentifikationsserver;

Vermitteln der Authentifizierung der drahtlosen Vorrichtung mit dem Authentifikationsserver;

Auswerten von Datenpaketen, die von Abschnitten des drahtlosen Netzwerks und von der Vielzahl von Zugangspunkten empfangen werden; und

Übermitteln der empfangenen Datenpakete zu Abschnitten des drahtlosen Netzwerks und zu der Vielzahl von Zugangspunkten auf der Grundlage der Auswertung der empfangenen Datenpakete;

wobei die Netzwerkvorrichtung periodisch einen Zustand der drahtlosen Vorrichtung von dem Zugangspunkt abfragt; und

wobei die Zugangspunkte und die Netzwerkvorrichtung Informationen bezüglich der Konfiguration, des Zustands und der Client-Sitzungs-Zustände der Zugangspunkte durch ein Messaging-Protokoll austauschen.

[0015] Vorteilhafterweise umfasst dieser Schritt des Auswertens von Datenpaketen das Filtern der empfangenen Datenpakete derart, dass die gefilterten Datenpakete fallengelassen werden können, um eine Wirksamkeit eines Dienstverweigerungsangriffs zu begrenzen.

[0016] Vorteilhafterweise umfasst der Schritt des Vermittelns der Authentifizierung der drahtlosen Vorrichtung das Einschränken des Zugriffs auf das drahtlose Netzwerk durch die drahtlose Vorrichtung auf der Grundlage einer Benutzerkategorie, die aus der Client-Identifizierung ermittelt wird.

[0017] Vorteilhafterweise basiert dieser Schritt des Einschränkens des Zugriffs auf das drahtlose Netzwerk auf einem Typ von Vorrichtung, zu dem die drahtlose Vorrichtung gehört.

[0018] Vorteilhafterweise weist dieser Schritt des Vermittelns der Authentifizierung der drahtlosen Vorrichtung das Einschränken des Zugriffs auf das drahtlose Netzwerk durch die drahtlose Vorrichtung auf der Grundlage einer Stunde und eines Tages der Woche auf, in denen die Daten von der drahtlosen Vorrichtung empfangen wurden.

[0019] Vorteilhafterweise basiert dieser Schritt des Einschränkens des Zugriffs auf das drahtlose Netzwerk auf wenigstens einem eines Typs von Vorrichtung, zu dem die drahtlose Vorrichtung gehört, und auf einer Benutzerkategorie, die aus der Client-Identifizierung ermittelt wird.

[0020] Vorteilhafterweise weist dieser Schritt des Vermittelns der Authentifizierung der drahtlosen Vorrichtung das Einschränken des Zugriffs auf das drahtlose Netzwerk durch die drahtlose Vorrichtung auf der Grundlage eines physischen Standorts des einen Zugangspunkts einer Vielzahl von Zugangspunkten auf.

[0021] Vorteilhafterweise weist dieser Schritt des Vermittelns der Authentifizierung der drahtlosen Vorrichtung das Einschränken des Zugriffs auf das drahtlose Netzwerk durch die drahtlose Vorrichtung auf der Grundlage eines Typs von Anwendung auf, die in der drahtlosen Vorrichtung abläuft und die einen Netzwerkzugriff für die drahtlose Vorrichtung verlangt.

[0022] Vorteilhafterweise weist dieser Schritt des Übermittelns der empfangenen Datenpakete das Weiterleiten von Aktualisierungen für die Software und Konfigurationen der Vielzahl von Zugangspunkten zu der Vielzahl von Zugangspunkten ausgehend von einer einzelnen Stelle in dem drahtlosen Netzwerk durch eine einzige Aktualisierung auf.

[0023] Vorteilhafterweise überlappen sich die Funkversorgungsbereiche für wenigstens zwei der Vielzahl von Zugangspunkten, und das Verfahren umfasst ferner folgendes:

Überwachen der Benutzung durch drahtlose Vorrichtungen der wenigstens zwei der Vielzahl von Zugangspunkten; und
 Auffordern der wenigstens zwei der Vielzahl von Zugangspunkten zur Änderung der Verwendung durch die drahtlosen Vorrichtungen derart, dass eine Last, die von den wenigstens zwei der Vielzahl von Zugangspunkten getragen wird, ungefähr ausgeglichen wird.

[0024] Vorteilhafterweise wird die Last, die von den wenigstens zwei der Vielzahl von Zugangspunkten getragen wird, mittels wenigstens einer Anzahl von drahtlosen Vorrichtungen, die die wenigstens zwei der Vielzahl von Zugangspunkten verwendet, einer Anzahl von Paketen, die durch die wenigstens zwei der Vielzahl von Zugangspunkten übertragen und empfangen werden, und einer durchschnittlichen Bandbreite bestimmt, die von den wenigstens zwei der Vielzahl von Zugangspunkten übertragen wird.

[0025] Vorteilhafterweise wird die Last, die von den wenigstens zwei der Vielzahl von Zugangspunkten getragen wird, durch wenigstens eine der Prioritäten von Paketen, die vor kurzem durch die wenigstens zwei der Vielzahl von Zugangspunkten übertragen und empfangen worden sind, einen Typ von Anwendung, der in den drahtlosen Vorrichtungen abläuft und mit den wenigstens zwei der Vielzahl von Zugangspunkten kommuniziert, und eine Signalstärke bestimmt, die den drahtlosen Vorrichtungen zugeführt wird, die von den wenigstens zwei der Vielzahl von Zugangspunkten bereitgestellt wird.

[0026] Vorteilhafterweise umfasst der Schritt des Übermittels der empfangenen Datenpakete das Aufrechterhalten einer Priorität, die von den Datenpaketen angezeigt wird, und das Markieren der Datenpakete mit einem Prioritäts-Tag, das von den Zugangspunkten ausgewertet werden soll.

[0027] Vorteilhafterweise umfasst der Schritt des Übermittels der empfangenen Datenpakete das Einrichten von Priorisierungs-Richtlinien auf der Basis der Filterung der Datenpakete und das Markieren der Datenpakete mit einem Prioritäts-Tag, das von den Zugangspunkten auf der Grundlage der eingerichteten Priorisierungs-Richtlinien ausgewertet werden soll.

[0028] Vorteilhafterweise umfasst das Verfahren ferner das Einrichten von Bandbreitennutzungs-Richtlinien für die drahtlosen Vorrichtungen und das Instruieren der Vielzahl von Zugangspunkten dahingehend, dass sie den eingerichteten Bandbreitennutzungs-Richtlinien folgen.

[0029] Vorteilhafterweise umfasst das Verfahren des Weiteren:
 Empfangen einer Reassoziierungsanforderung von einer übertragenden drahtlosen Vorrichtung durch einen neuen Zugangspunkt der Vielzahl von Zugangspunkten, wobei die übertragende drahtlose Vorrichtung vorher mit einem alten Zugangspunkt der Vielzahl von Zugangspunkten assoziiert war;
 Bereitstellen von Sitzungsinformationen für die übertragende drahtlose Vorrichtung zu dem neuen Zugangspunkt; und
 Aktualisieren einer Routing-Tabelle mit einer Routing-Lokalisierung der übertragenden drahtlosen Vorrichtung.

[0030] Vorteilhafterweise umfasst das Verfahren ferner das Einkapseln der empfangenen Datenpakete mit Internet-Protokoll-Informationen, die mit dem neuen Zugangspunkt assoziiert sind, und das Aktualisieren der Routing-Informationen in einer lokalen Routing-Tabelle.

[0031] Vorteilhafterweise umfasst das Verfahren des Weiteren folgende Schritte:
 Empfangen einer Reassoziierungsanforderung von einer übertragenden drahtlosen Vorrichtung durch einen neuen Zugangspunkt der Vielzahl von Zugangspunkten, wobei die übertragende drahtlose Vorrichtung vorher mit einem anderen Zugangspunkt in Kommunikation mit dem drahtlosen Netzwerk durch eine andere Netzwerkvorrichtung assoziiert war;
 Senden einer Anforderung nach Konfigurationsinformationen für die übertragende drahtlose Vorrichtung von der anderen Netzwerkvorrichtung; und
 Weiterleiten der Zugangspunkt-Konfigurationsdaten, die aus den Konfigurationsinformationen für die übertragende drahtlose Vorrichtung bestimmt wurden, die von der anderen Netzwerkvorrichtung empfangen wurden, zu dem neuen Zugangspunkt.

[0032] Vorteilhafterweise ist die drahtlose Vorrichtung ein drahtloses Internet-Protokoll-Telefon, die Client-Identifizierung besteht aus Verbindungsaufbaudaten, und der Schritt des Übermittels der empfangenen Datenpakete umfasst das Übermitteln von VoIP-Datenpaketen zu Abschnitten des drahtlosen Netzwerks und zu der Vielzahl von Zugangspunkten auf der Grundlage der Auswertung der empfangenen VoIP-Datenpakete.

- [0033]** Vorteilhafterweise umfasst dieser Schritt des Vermittelns der Authentifizierung der drahtlosen Vorrichtung mit dem Authentifizierungsserver die folgenden Schritte:
Senden eines Freizeichens, das von einem Internet-Protokoll-Telefon-Gateway empfangen wird, zu dem einen Zugangspunkt; und
Vermitteln einer Aushandlung von Netzwerkressourcen zwischen dem Internet-Protokoll-Telefon-Gateway und dem drahtlosen Internet-Protokoll-Telefon.
- [0034]** Gemäß einer anderen Ausführungsform der Erfindung ist eine Netzwerkvorrichtung zur Kontrolle eines Datenflusses in einem drahtlosen Netzwerk bereitgestellt, das einen drahtlosen Zugriff auf das drahtlose Netzwerk durch drahtlose Vorrichtungen bereitstellt, wobei die Netzwerkvorrichtung folgendes aufweist:
Empfangseinrichtungen zum Empfangen von Daten von einer drahtlosen Vorrichtung mittels der Netzwerkvorrichtung durch einen Zugangspunkt einer Vielzahl von Zugangspunkten in Kommunikation mit der Netzwerkvorrichtung, wobei eine Client-Identifizierung für die drahtlose Vorrichtung angezeigt wird;
Weiterleitungseinrichtungen zum Weiterleiten der Client-Identifizierung zu einem Authentifikationsserver;
Vermittlungseinrichtungen zum Vermitteln der Authentifizierung der drahtlosen Vorrichtung mit dem Authentifikationsserver;
Auswerteeinrichtungen zum Auswerten von Datenpaketen, die von Abschnitten des drahtlosen Netzwerks und von der Vielzahl von Zugangspunkten empfangen werden; und
Übermittlungseinrichtungen zum Übermitteln der empfangenen Datenpakete zu Abschnitten des drahtlosen Netzwerks und zu der Vielzahl von Zugangspunkten auf der Grundlage der Auswertung der empfangenen Datenpakete;
wobei die Netzwerkvorrichtung so konfiguriert ist, dass sie periodisch einen Zustand der drahtlosen Vorrichtung von dem Zugangspunkt abfragt; und
wobei die Zugangspunkte und die Netzwerkvorrichtung Informationen bezüglich der Konfiguration, des Zustands und der Client-Sitzungs-Zustände der Zugangspunkte durch ein Messaging-Protokoll austauschen.
- [0035]** Vorteilhafterweise weist die Auswerteeinrichtung Filtereinrichtungen zum Filtern der empfangenen Datenpakete derart auf, dass die gefilterten Datenpakete fallengelassen werden können, um eine Wirksamkeit eines Dienstverweigerungsangriffs zu begrenzen.
- [0036]** Vorteilhafterweise weist diese Vermittlungseinrichtung Beschränkungseinrichtungen zum Beschränken des Zugriffs auf das drahtlose Netzwerk durch die drahtlose Vorrichtung auf der Grundlage einer Benutzerkategorie auf, die aus der Client-Identifizierung ermittelt wird.
- [0037]** Vorteilhafterweise ist die Beschränkungseinrichtung so konfiguriert, dass sie den Zugriff auf der Grundlage eines Typs von Vorrichtung beschränkt, zu dem die drahtlose Vorrichtung gehört.
- [0038]** Vorteilhafterweise weist die Vermittlungseinrichtung Beschränkungseinrichtungen zum Beschränken des Zugriffs auf das drahtlose Netzwerk durch die drahtlose Vorrichtung auf der Grundlage einer Stunde und eines Tages der Woche auf, in denen die Daten von der drahtlosen Vorrichtung empfangen wurden.
- [0039]** Vorteilhafterweise ist die Beschränkungseinrichtung so konfiguriert, dass sie den Zugriff auf der Grundlage wenigstens eines Typs von Vorrichtung, zu dem die drahtlose Vorrichtung gehört, und einer Benutzerkategorie beschränkt, die aus der Client-Identifizierung bestimmt wird.
- [0040]** Vorteilhafterweise weist die Vermittlungseinrichtung Beschränkungseinrichtungen zum Beschränken des Zugriffs auf das drahtlose Netzwerk durch die drahtlose Vorrichtung auf der Grundlage eines physischen Standorts des einen Zugangspunkts einer Vielzahl von Zugangspunkten auf.
- [0041]** Vorteilhafterweise weist die Vermittlungseinrichtung Beschränkungseinrichtungen zum Beschränken des Zugriffs auf das drahtlose Netzwerk durch die drahtlose Vorrichtung auf der Grundlage eines Typs einer Anwendung auf, die in der drahtlosen Vorrichtung abläuft, die den Netzwerkzugriff für die drahtlose Vorrichtung verlangt.
- [0042]** Vorteilhafterweise weist die Übermittlungseinrichtung Weiterleitungseinrichtungen zum Weiterleiten von Aktualisierungen für die Software und Konfigurationen der Vielzahl von Zugangspunkten zu der Vielzahl von Zugangspunkten ausgehend von einer einzigen Stelle in dem drahtlosen Netzwerk durch eine einzige Aktualisierung auf.
- [0043]** Vorteilhafterweise überlappen sich Funkversorgungsbereiche für wenigstens zwei der Vielzahl von Zu-

gangspunkten, und die Netzwerkvorrichtung umfasst des Weiteren folgendes:

Überwachungseinrichtungen zum Überwachen der Benutzung durch drahtlose Vorrichtungen der wenigstens zwei der Vielzahl von Zugangspunkten; und

Aufforderungseinrichtungen zum Auffordern der wenigstens zwei der Vielzahl von Zugangspunkten zur Änderung der Verwendung durch die drahtlosen Vorrichtungen derart, dass eine Last, die von den wenigstens zwei der Vielzahl von Zugangspunkten getragen wird, ungefähr ausgeglichen wird.

[0044] Vorteilhafterweise wird die Last, die von den wenigstens zwei der Vielzahl von Zugangspunkten getragen wird, durch wenigstens eine einer Anzahl von drahtlosen Vorrichtungen, die die wenigstens zwei der Vielzahl von Zugangspunkten verwendet, eine Anzahl von Paketen, die durch die wenigstens zwei der Vielzahl von Zugangspunkten übertragen und empfangen werden, und eine durchschnittliche Bandbreite ermittelt, die von den wenigstens zwei der Vielzahl der Zugangspunkte übertragen wird.

[0045] Vorteilhafterweise wird die Last, die von den wenigstens zwei der Vielzahl von Zugangspunkten getragen wird, durch wenigstens eine der Prioritäten der Pakete, die vor kurzem von den wenigstens zwei der Vielzahl von Zugangspunkten übertragen und empfangen worden sind, einen Typ von Anwendung, der in den drahtlosen Vorrichtungen abläuft und mit den wenigstens zwei der Vielzahl von Zugangspunkten kommuniziert, und eine Signalstärke bestimmt, die den drahtlosen Vorrichtungen zugeführt wird, die von den wenigstens zwei der Vielzahl von Zugangspunkten bereitgestellt wird.

[0046] Vorteilhafterweise umfasst die Übermittlungseinrichtung Aufrechterhaltungseinrichtungen zum Aufrechterhalten einer Priorität, die von den Datenpaketen angezeigt wird, und zum Markieren der Datenpakete mit einem Prioritäts-Tag, das von den Zugangspunkten ausgewertet werden soll.

[0047] Vorteilhafterweise umfasst die Übermittlungseinrichtung Einrichtungseinrichtungen zum Einrichten von Priorisierungs-Richtlinien auf der Grundlage der Filterung der Datenpakete und zum Markieren der Datenpakete mit einem Prioritäts-Tag, das von den Zugangspunkten auf der Grundlage der eingerichteten Priorisierungs-Richtlinien ausgewertet werden soll.

[0048] Vorteilhafterweise umfasst die Netzwerkvorrichtung ferner Einrichtungseinrichtungen zum Einrichten von Bandbreitennutzungs-Richtlinien für die drahtlosen Vorrichtungen und zum Instruieren der Vielzahl von Zugangspunkten dahingehend, den eingerichteten Bandbreitennutzungs-Richtlinien zu folgen.

[0049] Vorteilhafterweise umfasst die Netzwerkvorrichtung ferner folgendes:

zweite Empfangseinrichtungen zum Empfangen einer Reassoziierungsanforderung von einer übertragenden drahtlosen Vorrichtung durch einen neuen Zugangspunkt der Vielzahl von Zugangspunkten, wobei die übertragende drahtlose Vorrichtung vorher mit einem alten Zugangspunkt der Vielzahl von Zugangspunkten assoziiert war;

Bereitstellungseinrichtungen zum Bereitstellen von Sitzungsinformationen für die übertragende drahtlose Vorrichtung zu dem neuen Zugangspunkt; und

Aktualisierungseinrichtungen zum Aktualisieren einer Routing-Tabelle mit einer Routing-Lokalisierung der übertragenden drahtlosen Vorrichtung.

[0050] Vorteilhafterweise umfasst die Netzwerkvorrichtung ferner Einkapselungseinrichtungen zum Einkapseln der empfangenen Datenpakete mit Internet-Protokoll-Informationen, die mit dem neuen Zugangspunkt assoziiert sind, und Aktualisieren von Routing-Informationen in einer lokalen Routing-Tabelle.

[0051] Vorteilhafterweise umfasst die Netzwerkvorrichtung des Weiteren folgendes:

zweite Empfangseinrichtungen zum Empfangen einer Reassoziierungsanforderung von einer übertragenden drahtlosen Vorrichtung durch einen neuen Zugangspunkt der Vielzahl von Zugangspunkten, wobei die übertragende drahtlose Vorrichtung vorher mit einem alternativen Zugangspunkt in Kommunikation mit dem drahtlosen Netzwerk durch eine andere Netzwerkvorrichtung assoziiert war;

Sendeeinrichtungen zum Senden einer Anforderung nach Konfigurationsinformationen für die übertragende drahtlose Vorrichtung ausgehend von der anderen Netzwerkvorrichtung; und

zweite Weiterleitungseinrichtungen zum Weiterleiten von Zugangspunkt-Konfigurationsdaten, die aus den Konfigurationsinformationen für die übertragende drahtlose Vorrichtung bestimmt wurden, die von der anderen Netzwerkvorrichtung empfangen worden sind, zu dem neuen Zugangspunkt.

[0052] Vorteilhafterweise ist die drahtlose Vorrichtung ein drahtloses Internet-Protokoll-Telefon, die Client-Identifizierung besteht aus Verbindungsaufbaudaten, und der Schritt des Übermittels der empfangenen

Datenpakete umfasst das Übermitteln von VoIP-Datenpaketen zu Abschnitten des drahtlosen Netzwerks und zu der Vielzahl von Zugangspunkten auf der Grundlage der Auswertung der empfangenen VoIP-Datenpakete.

[0053] Vorteilhafterweise umfasst die Vermittlungseinrichtung folgendes:

Sendeeinrichtungen zum Senden eines Freizeichens, das von einem Internet-Protokoll-Telefon-Gateway empfangen wird, zu dem einen Zugangspunkt; und

zweite Vermittlungseinrichtungen zum Vermitteln einer Aushandlung von Netzwerkressourcen zwischen dem Internet-Protokoll-Telefon-Gateway und dem drahtlosen Internet-Protokoll-Telefon.

[0054] Diese und weitere Aufgaben der vorliegenden Erfindung werden in der nachfolgenden Beschreibung der bevorzugten Ausführungsbeispiele beschrieben oder werden durch diese offenbart.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0055] Damit die vorliegende Erfindung leicht verständlich und ohne weiteres praktizierbar ist, werden nun bevorzugte Ausführungsbeispiele zum Zwecke der Veranschaulichung und nicht der Beschränkung im Zusammenhang mit den nachfolgenden Figuren beschrieben:

[0056] [Fig. 1](#) ist eine schematische Darstellung der Komponenten eines drahtlosen lokalen Unternehmens-Netzwerks gemäß einem Ausführungsbeispiel der vorliegenden Erfindung;

[0057] [Fig. 2](#) veranschaulicht eine schematische Darstellung der Linien der Sicherheitsdurchsetzungsdemarkationen in einem drahtlosen lokalen Unternehmens-Netzwerk gemäß einem Ausführungsbeispiel der Erfindung;

[0058] [Fig. 3](#) ist eine schematische Darstellung, die die Typen der Mobilitäts-Weiterreichung in einem drahtlosen lokalen Netzwerk veranschaulicht;

[0059] [Fig. 4](#) veranschaulicht die Nachrichtenaustauschsequenz für die Reassoziierung;

[0060] [Fig. 5](#) veranschaulicht eine Weiterreichung in einem einzelnen IP-Teilnetz;

[0061] [Fig. 6](#) veranschaulicht einen Heimatagenten (home agent) und ein Heimat-Teilnetz (home subnet);

[0062] [Fig. 7](#) veranschaulicht ein Beispiel der Tunnelung in einem mobilen IP zwischen Heimat-Teilnetzen und fremden Teilnetzen;

[0063] [Fig. 8](#) veranschaulicht ein Beispiel einer Upstream-Tunnelung in einem mobilen IP zwischen fremden und Heimat-Teilnetzen;

[0064] [Fig. 9](#) veranschaulicht die Nachrichtenaustauschsequenz für das Anmelden des Client (client login) gemäß einem Ausführungsbeispiel der vorliegenden Erfindung;

[0065] [Fig. 10](#) veranschaulicht die Nachrichtenaustauschsequenz für das Abmelden des Client (client logoff) gemäß einem Ausführungsbeispiel der vorliegenden Erfindung;

[0066] [Fig. 11](#) veranschaulicht die Nachrichtenaustauschsequenz für die Weiterreichung im gleichen Switch (same switch handoff) gemäß einem Ausführungsbeispiel der vorliegenden Erfindung;

[0067] [Fig. 12](#) veranschaulicht die Nachrichtenaustauschsequenz für die Weiterreichung quer durch Switches (across switch handoff) gemäß einem Ausführungsbeispiel der vorliegenden Erfindung;

[0068] [Fig. 13](#) veranschaulicht die Nachrichtenaustauschsequenz für die drahtlose IP-Telefon-Anrufinitiierung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung; und

[0069] [Fig. 14](#) veranschaulicht die Nachrichtenaustauschsequenz für die drahtlose IP-Telefon-Anrufbeendigung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung.

GENAUE BESCHREIBUNG VON BEVORZUGTEN AUSFÜHRUNGSBEISPIELEN

[0070] In einer drahtlosen Unternehmens-LAN-Umgebung sind die drahtlosen Vorrichtungen typischerweise an der Kante des Netzwerks positioniert. Die drahtlosen Vorrichtungen **120–129**, wie sie in [Fig. 1](#) gezeigt sind, sind mit dem Unternehmensnetzwerk über die Zugangspunkte **111–115** verbunden, die wiederum die Kanten-vorrichtungen des verdrahteten LAN sind. Die Zugangspunkte **111–115** sind mit dem LAN über Switches (Vermittlungsstellen) **106** und **107** verbunden. Diese Switches, die drahtlose LAN-Switches genannt werden, führen nicht nur das Schicht-2-Switching durch, sondern dienen auch als ein drahtloser Kantenmanager (edge manager). Sie stellen die zusätzlichen Funktionalitäten wie z.B. Zugriffskontrolle, Firewall-Funktionen, Verkehrsdatenschutz und Dienstgüte, Netzwerkmanagement und Lastausgleich bereit. Eine höhere Architektur eines drahtlosen Unternehmens-LAN, bei dem die Switches auch als die Kantenmanager dienen, ist in [Fig. 1](#) veranschaulicht. Ebenfalls veranschaulicht ist das größere LAN **101**, durch das die drahtlosen LAN-Switches **106** und **107** verbunden sind sowie auch mit einem Authentifizierungsserver **104** verbunden sind.

[0071] Bei dieser Architektur ist die drahtlose Übertragung zwischen dem Client und dem Zugangspunkt geschützt, während die verdrahtete Verbindung zwischen dem Zugangspunkt und dem Unternehmens-Switch ebenfalls geschützt ist. Der Switch und der ZP kommunizieren in gewöhnlichem Ethernet-Verkehr. Aus der Perspektive des Switch handelt es sich hier einfach um das Switching (Vermitteln) eines regulären Schicht-2-Rahmens. In dem Switch sitzen das Wissen eines WLAN und seine Managementintelligenz hauptsächlich in einem Controller für den Switch, der durch Software vermittelt wird.

[0072] Vom Standpunkt der Sicherheit des verdrahteten LAN aus kann der ZP als der verdrahtete/drahtlose Demarkationspunkt verwendet werden. Die Sicherheitsprobleme im Innern des verdrahteten Abschnitts des LAN werden hier nicht speziell angesprochen, da diese allgemein bekannt sind. Es wird erwartet, dass das WLAN Gesamt-Unternehmens-LAN-Sicherheitsrichtlinien entspricht, falls solche vorhanden sind, wie dies bei dem verdrahteten Abschnitt des LAN der Fall ist. Aber die Sicherheitsanforderungen, die nur den verdrahteten LAN betreffen, werden hier nicht angesprochen.

[0073] In der drahtlosen LAN-Umgebung kann der Unternehmens-Benutzer einen virtuellen Privatnetz-Extratunnel (extra virtual private network (VPN) tunnel) zwischen dem drahtlosen Client und dem Unternehmensnetzwerk einrichten. Dieser VPN-Tunnel wird an einem VPN-Server im Innern des LAN enden. Für ältere drahtlose Clients und ZP ist das VPN virtuell ein obligatorisches Verfahren, um die drahtlose Sicherheit zu gewährleisten. Aber da sich die Standards für drahtlose Sicherheit weiterentwickeln, kann der Informationstechnik-(IT)-Manager unterschiedliche Mechanismen auswählen, um die Sicherheit bereitzustellen. Da VPN-Tunnel keine obligatorische Maßnahme für die neue Generation von WLAN-Zugriff sind, und da es viele allgemein bekannte Nachteile bei der Durchsetzung eines Zugriffs auf VPN-Basis gibt, widmet sich die vorliegende Anmeldung nicht direkt obligatorischen VPN-Tunneln.

[0074] Im Allgemeinen können die Probleme, die mit der drahtlosen Unternehmens-LAN-Architektur der vorliegenden Erfindung verbunden sind, in sechs größere Bereiche unterteilt werden. Diese Bereiche umfassen die Sicherheit, die Zugriffskontrolle, die Mobilität, das Netzwerkmanagement, den Lastausgleich und die Dienstgüte. Diese Bereiche stehen in enger Beziehung zueinander, aber dennoch stellt jeder von ihnen einzigartige Anforderungen, denen sich die Unternehmens-WLAN-Architektur widmet. Die folgenden Unterabschnitte widmen sich diesen Bereichen im Hinblick auf Funktionalität, die Schnittstelle mit externen Entitäten und Performanzanforderungen.

SICHERHEIT

[0075] Ein drahtloses LAN sollte nicht weniger sicher sein als ein herkömmliches verdrahtetes LAN. Aufgrund der öffentlichen Natur des Mediums führt die Einführung von drahtlosen LAN-Segmenten in eine ansonsten sichere Infrastruktur auch eine Anzahl von potentiellen Sicherheitsproblemen ein, die folgendes umfassen: anonymespassives Abhören, unberechtigte Verbindung mit dem Netzwerk, Sitzungsübernahme und Verweigerung von Diensten durch Stau (jamming).

[0076] Viele solcher Angriffe werden durch Open Source Hacker-Werkzeuge erleichtert, die über das Internet einfach zur Verfügung stehen. Die breite Verfügbarkeit von drahtloser LAN-Technologie zu geringen Kosten führt eine weitere Bedrohung ein, nämlich die unberechtigte Verbindung einer drahtlosen Rogue-Basisstation, oftmals für gelegentliche persönliche Verwendung. Die Schwachstellen der WLAN-Sicherheit und die Gegenmaßnahmen werden erörtert, und ein Implementierungsansatz gemäß der vorliegenden Erfindung für Sicherheitsmechanismen wird ebenfalls erörtert.

[0077] Drahtlose LANs sind zwei Hauptkategorien von Angriffen ausgesetzt: sogenannte herkömmliche LAN-Angriffe und Angriffe, die auf drahtlose LANs spezialisiert sind. Eine der Bedrohungen, die sowohl die herkömmlich geschalteten verdrahteten LANs als auch die WLANs betreffen, sind die Man-in-the-Middle-Angriffe (Man-in-the-Middle attacks), die sowohl Router-Umleitung als auch ARP-Spoofing umfassen. Diese ermöglichen sowohl passive als auch aktive Angriffe, die die Paketmodifikation einschließen.

[0078] Ebenfalls in den "herkömmlichen" Typen von Angriffen eingeschlossen sind die TCP/IP-Dienstverweigerungsangriffe, die eine Klasse von Angriffen wie zum Beispiel das TCP-SYN-Flooding, das sich zufällig ändernde Quell-IP-Adressen verwendet, den Identitätswechsel, der das IP- oder MAC-Adressen-Spoofing verwendet, Kennwort-Schätz-Angriffe, Netzwerkablast- und Topologieerkennungsangriffe wie etwa Port-Abtastungen und Simple Network Management Protocol (SNMP; einfaches Netzwerkmanagement-Protokoll)-Angriffe umfassen.

[0079] Alternativ dazu nutzen viele Bedrohungen das Fehlen der physischen Verdrahtung in WLANs aus. Diese umfassen die Verwendung eines drahtlosen Schnüfflers (sniffer), bei dem der Angreifer den Raub über den Luftdatenverkehr durchführt und sensible Informationen wie etwa das Kennwort eines Benutzers erhält. Der Angreifer kann sich dann als legitimer Benutzer tarnen und Zugriff auf das Netzwerk erhalten. Hacker-Werkzeuge wie z.B. "dsniff" oder "airsnort" können die Bedrohung ermöglichen. Außerdem umfassen diese Verfahren auch das War Driving, das analog zum "War Dialing" ist und bei dem der Angreifer um ein Gebäude herum fährt, wobei er eine verstärkte Antenne verwendet, um "Hot Spots" und ungeschützte drahtlose Netzwerke zu lokalisieren, um diese anzugreifen. Auch ist die Verwendung von Rogue-Zugangspunkten umfasst, bei denen Benutzer zu ihrer eigenen Annehmlichkeit drahtlose Rogue-LANs errichten, aber Löcher in der Unternehmens-Netzwerkinfrastruktur öffnen.

[0080] Weitere Bedrohungen, die das Fehlen einer physischen Verdrahtung in WLANs ausnützen, umfassen das Zugangspunkt-Klonen, das eine Variante des klassischen Login Spoof ist, bei dem der Angreifer seinen eigenen ZP (mit einem stärkeren Signal) einführt und Benutzer-Kennworte stiehlt. Auch Client-zu-Client-Angriffe können eine Bedrohung sein, bei denen drahtlose Clients oftmals standardmäßig einen "Ad-Hoc"-Modus konfiguriert haben, der sie Angriffen ausgesetzt lassen kann, wie z.B. einem unautorisierten File Sharing. Außerdem gibt es Implementationsschwachstellen wie zum Beispiel die Ausnutzung von bekannten Schlüsselmanagement-Schwachstellen von Wired Equivalent Privacy (WEP), oftmals mit der Unterstützung von Hacker-Werkzeugen wie etwa "airsnort". Auch durch eine fehlerhafte Konfiguration können Zugangspunkte, bei denen die Sicherheitsmerkmale nicht eingeschaltet sind, zur Erlangung eines ungebührlichen Zugriffs verwendet werden.

[0081] Die vorliegende Erfindung verwendet mehrere Verfahren zur Abschwächung dieser Bedrohungen, wobei das erste Verfahren sichere Kommunikationsprotokolle umfasst. Unten ist eine Liste von Sicherheitsprotokollen enthalten, die verwendet werden können, um die oben genannten Sicherheitsbedrohungen abzuschwächen. Diese Protokolle umfassen IEEE 802.1x, das eine portbasierte Benutzerauthentifikation bereitstellt. Der vorgeschlagene IEEE 802.11i Standard spezifiziert die Erweiterungen zu dem 802.1x EAPOL (Extensible Authentication Protocol (EAP) over LAN) Protokoll, um gemeinsam genutzte kryptografische Kontexte zwischen dem Client (Supplicant) und dem ZP (Authenticator) einzurichten. Das EAP ist auch ein Internet Engineering Task Force (IETF) Standard, der einen universellen Authentifizierungsaustausch definiert. Das EAP unterstützt mehrere Authentifizierungsmechanismen, z.B. das Challenge Handshake Authentication Protocol (CHAP), die Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) und das Protected EAP (PEAP).

[0082] Ein weiteres Protokoll ist das TKIP (Temporal Key Integrity Protocol), das in dem vorgeschlagenen 802.11i Standard definiert ist. Das TKIP ist für den Zwischeneinsatz und die Nachrüstung von bestehenden WEP-Geräten gedacht. Das TKIP verwendet den gemeinsam genutzten Verschlüsselungskontext gemäß 802.1x und leitet Schlüssel pro Paket ab. Es verwendet einen neuen Algorithmus namens Michael für die Paket-Schicht-Integrität. Das TKIP wurde angeregt durch einen Bedarf, die berüchtigte Schlüsselableitung und die Paket-Integritäts-Schwächen des WEP zu überwinden. Es behält die WEP-Rahmenformate und die Verwendung des RC4-Algorithmus bei. Ein anderes Protokoll, das WRAP, ist in IEEE 802-11i als eine Langzeitsicherheitslösung vorgeschlagen. Wie das TKIP, so verwendet auch dieses Protokoll gemeinsam genutzte Verschlüsselungskontexte gemäß IEEE 802.1x und stellt ein Schlüsselmanagement und eine Integrität pro Paket bereit. Das WRAP verwendet den Advanced Encryption Standard (AES) Algorithmus sowohl für die Datenvertraulichkeit als auch für ihre Integrität. Zähler mit Cipher Block Chaining-Message Authentication Code (CCM) und Offset Codebook (OCB) sind Betriebsmodi, die die Verschlüsselung und die Integrität in einem einzigen Durchlauf kombinieren.

[0083] Andere Protokolle umfassen proprietäre WEP-Erweiterungen, die eine Benutzerauthentifizierung gekoppelt mit "dynamischen" WEP- Verschlüsselungs-Schlüsseln pro Station bereitstellen und die auf EAP und IEEE 802.1x aufgebaut sind. Diese sind zwar schon älter und werden zum größten Teil durch TKIP ersetzt werden, aber sie werden weiter in bestimmten Händlerangeboten existieren. Zum Beispiel wird LEAP von CISCO und Microsoft unterstützt, und EAP-TLS wird von Microsoft unterstützt. Außerdem gibt es eine Anzahl von EAP-Mechanismen, einschließlich EAP-TLS, die den TLS (Transport Layer Security) Protokoll-Einrichtung-Quittungsaustausch in EAP einbetten, um Schlüsselmanagementnachrichten zu verschlüsseln, und EAP-TTLS, welches ein Derivat von EAP-TLS und PEAP (Protected EAP) ist, das ebenfalls TLS-Quittungsaustauschnachrichten verwendet.

[0084] Ebenfalls in den Protokollen enthalten sind VPN-Protokolle, wobei IPsec das IETF IP Sicherheitsprotokoll ist, das in hohem Maße für VPNs verwendet wird. Dieser Lösungsweg behandelt das WLAN als komplett nicht vertrauenswürdig, eine sogenannte drahtlose entmilitarisierte Zone (DMZ; wireless demilitarized zone), und verlangt von den Benutzern, dass sich diese unter Benutzung eines VPN-Protokolls in das Unternehmensnetzwerk tunneln, wie sie das auch vom Internet aus tun würden. IPsec stellt eine Schicht-3-Sicherheit bereit. Auch das Punkt-zu-Punkt-Tunnelungs-Protokoll (PPTP; point-to-point tunneling protocol) ist ein proprietäres Sicherheitsprotokoll, das durch IPsec ersetzt worden ist, aber immer noch in hohem Maße für VPNs benutzt wird, da es sich in jedem Windows-Client befindet. Das PPTP stellt eine Schicht-2-Einkapselung über IP bereit.

[0085] Ein anderes Verfahren zur Bedrohungsabschwächung umfasst die Paketfilterung. Dieses verwendet das Universal-IP-Schicht-Eingangsfiltren zur Begrenzung oder Verhinderung von Dienstverweigerungsangriffen, wie zum Beispiel TCP SYN. Der Vorgang der Filterung in Netzwerkgeräten wird im US-Patent Nr. 6,335,935 erörtert.

ZUGRIFFSKONTROLLEN

[0086] Zugriffskontrollmechanismen stellen die Fähigkeit bereit, Sicherheitsrichtlinien bei der Netzwerkbenutzung durchzusetzen. Zugriffskontrollen sind auf der Benutzerebene am effektivsten und können mit verschiedenen Graden von Granularität angelegt werden. Zugriffskontrollmechanismen werden im Kontext der drahtlosen LANs immer wichtiger, da die öffentliche Natur des Mediums es wiederum möglich macht, Dienste wie etwa einen "Gast"-Zugriff bereitzustellen.

[0087] Der effizienteste Weg zur Implementierung der Zugriffskontrolle ist an der Kante des drahtlosen Mediums, d.h. an dem Zugangspunkt oder ZP. Aber die ZPs können mit akzeptablen Zugriffskontrolldurchsetzungsfähigkeiten ausgerüstet sein oder auch nicht. Falls sie nicht damit ausgerüstet sind, dient der WLAN-Switch als die zweite Verteidigungslinie oder als der Zugriffskontrollvollstrecker (access control enforcer).

[0088] Es gibt verschiedene Typen von Zugriffskontrollrichtlinien, die ein WLAN unterstützen sollte, einschließlich solcher auf der Basis der Client-Identität, auf der Basis von Zeit, auf der Basis der Position und auf der Basis der Anwendung. Der üblichere Fall würde eine Kombination aus diesen umfassen. Sie werden in den nachfolgenden Abschnitten beschrieben.

[0089] Zugriffskontrollen auf Client-Basis gewähren einem bestimmten Benutzer oder einer bestimmten Benutzerkategorie Zugriffsrechte auf der Grundlage der authentifizierten Identität. Beispiele von Benutzerkategorien umfassen reguläre Angestellte, Lieferanten, Unternehmenspartner, Besucher oder spezielle aufgezählte Gruppen. Jedem Typ von Benutzer können unterschiedliche Zugriffsrechte gewährt werden, zum Beispiel auf das gesamte Unternehmensnetzwerk oder nur auf ein bestimmtes Teilnetz, auf das Internet, auf bestimmte Anwendungen und/oder auf bestimmte Netzwerkdienste.

[0090] Zugriffsrichtlinien auf Client-Basis können von der verwendeten Vorrichtung unabhängig sein oder nicht von dieser unabhängig sein. Zum Beispiel könnte ein Benutzer mit zwei verschiedenen Laptops, der auf das WLAN unter Verwendung von zwei unterschiedlichen MAC-Adressen zugreifen würde, die gleichen Zugriffsrechte besitzen. Andererseits sind die Zugriffsrechte für den gleichen Benutzer von einem Laptop aus oder von einem IP-Telefon aus wahrscheinlich unterschiedlich. Einem Laptop sollte der Zugriff auf das gesamte Netzwerk gewährt werden. Da ein IP-Telefon nur eine Vorrichtung ist, die eine bestimmte Anwendung unterstützt, sollte diesem nur Zugriff auf diese Anwendung gewährt werden, und sie kann auf der Basis eines virtuellen lokalen Netzwerks (VLAN; virtual local area network), eines IP-Teilnetzes, eines Protokolls, eines Ports, etc. beschränkt sein, wie dies für die Sprache-über-IP-(VoIP; voice-over-IP)-Anwendung konfiguriert ist.

[0091] Die WLAN-Zugriffsrichtlinien können auf der Zeit des Tages oder auf dem Tag der Woche basieren. So

kann der WLAN-Zugriff zum Beispiel für Besucher während der Nicht-Arbeitsstunden und der Wochenenden gesperrt sein, da es nicht wahrscheinlich ist, dass sich während dieser Stunden Besucher auf dem Gelände befinden, um das WLAN zu benutzen. Angestellten und Lieferanten kann es verboten sein, während der Arbeitszeit auf bestimmte Streaming Video Server oder Datenbanken zuzugreifen, etc..

[0092] Zugriffsrichtlinien auf Zeitbasis können auch ein bestimmtes Zeitlimit spezifizieren, in dem ein Client auf das WLAN zugreifen kann. Dies kann als ein Sitzungs-Zeitlimit implementiert werden. Eine typische Verwendung dieses Mechanismus kann die Notwendigkeit umfassen, dass ein bestimmter Typ von Benutzer auf das Netzwerk nur für eine bestimmte Zeitspanne zugreifen kann, oder die Notwendigkeit, dass eine Sitzung aufgrund von Leerlauf beendet wird.

[0093] Die WLAN-Zugriffsrichtlinien können auf einer physischen Position basieren, das heißt, auf dem Standort des ZP basieren. Bestimmte Standorte in dem Gelände können weniger geschützt sein als andere, so dass es wünschenswert sein kann, den drahtlosen Zugriff von diesen Stellen aus einzuschränken. Zum Beispiel wird ein Schulungsraum oder eine Eingangs-Lobby oft von Besuchern frequentiert, und der Zugriff auf das öffentliche Internet von solchen Stellen aus kann wünschenswert sein, wobei der Zugriff auf das interne Unternehmensnetzwerk verhindert wird. Angestellte, die versuchen, von so einer Stelle aus Zugriff auf das Unternehmensnetzwerk zu bekommen, müssen unter Verwendung eines VPN durch das Internet gehen.

[0094] Zugriffskontrollrichtlinien können auf einer Anwendung basieren, da manche Anwendungen mehr Ressourcen benötigen als andere. Zum Beispiel kann das Herunterladen von Dateien des Peer-to-Peer-Typs und von Streaming Videos während der Arbeitszeit nicht besonders willkommen sein. Der Zugriff kann entweder bei dem ZP oder bei dem WLAN-Switch geregelt werden, indem die Paketinhalte inspiziert werden. Pakete aus unwillkommenem Verkehr werden somit verworfen. Im Falle all dieser Zugriffskontrollprozeduren wird die Zugriffskontrolle in den ZP oder den WLAN-Switch hinein über Konfigurationsskripte, Befehlszeilenschnittstellen oder netzbasierte Konsolen konfiguriert.

[0095] In Bezug auf sichere WLAN-Entitäten ist der drahtlose Client (Endstation, STA) der Benutzerauthentifizierungsagent, der als ein IEEE 802.1x Supplicant relativ zu dem IEEE 802.11i dient. Er muss den Authentifizierungsmechanismus unterstützen, um diesem zu ermöglichen, EAP zur Authentifizierung des Benutzers gegenüber einem Authentifizierungsserver (AS) zu verwenden. Der Client muss an seinem Ende eine Unterstützung für welches Datensicherheitsprotokoll auch immer, das unterstützt werden muss (z.B. TKIP, LEAP, VPN), bereitstellen.

[0096] In Bezug auf sichere WLAN-Entitäten ist der drahtlose Client (Endstation, STA) der Benutzerauthentifizierungsagent, der als ein IEEE 802.1x Supplicant relativ zu dem IEEE 802.11i dient. Er muss den Authentifizierungsmechanismus unterstützen, um diesem zu ermöglichen, EAP zur Authentifizierung des Benutzers gegenüber einem Authentifizierungsserver (AS) zu verwenden. Der Client muss an seinem Ende eine Unterstützung für welches Datensicherheitsprotokoll auch immer, das unterstützt werden muss (z.B. TKIP, LEAP, VPN), bereitstellen.

[0097] Eine andere sichere WLAN-Entität ist der Authentifizierungsserver AS, der die Benutzerauthentifizierungs-Datenbank verwaltet. An seinem Ende des Benutzerauthentifizierungsaustausches werden die EAP-Mechanismen benötigt. Durch 802.11i hat er die Fähigkeit, Schlüssel für gemeinsam genutzte Verschlüsselungskontexte zwischen Clients und ZPs bereitzustellen. Der AS ist normalerweise ein Remote Authentication Dial-In User Services (RADIUS) Server, aber die AS-Funktionalität könnte auch zusammengestellt mit irgendeiner anderen Netzwerkentität bereitgestellt werden, wie etwa dem ZP oder dem Switch.

[0098] Der Authentifizierungsserver verwaltet die Benutzerzugriffskontroll-Datenbank, die aus Zugriffskontrollregeln besteht, die in Zugriffskontrolllisten (ACLs; access control lists) organisiert sind. Ein proprietäres Protokoll kann notwendig sein, um ACLs auszutauschen, wenn der Berechtigungsserver nicht mit den Durchsetzungsfunktionen zusammen angeordnet ist. Der WLAN-Switch stellt eine feinkörnige Schicht-2/3/4-Zugriffskontrolldurchsetzung bereit. Es kann sein, dass eine VPN-Fähigkeit für eine sichere Verbindung zu den ZPs benötigt wird, wenn das LAN physisch nicht sicher ist. Die VPN-Tunnelung benötigt einen Upstream-VPN-Server, falls sie verwendet wird, um die Sicherheit des Client über den Äther bereitzustellen. Es sei angemerkt, dass das Keying ein Teil des VPN-Protokolls wäre (z.B. IKE für IPsec), unabhängig von dem AS.

[0099] Die Funktionen, die sich auf die WLAN-Sicherheit beziehen, und ihre Zuordnung lauten folgendermaßen:

Authentifizierung	Client, ZP, AS	Der Client kommuniziert mit dem AS zur Authentifizierung. Der AS kommuniziert mit dem ZP, um den authentifizierten Zugriff zu erlauben, und um gemeinsam genutzte Verschlüsselungskontexte bereitzustellen.
Zugriffskontrolle	Switch, Berechtigungs-Server	Der WLAN-Switch filtert den Verkehr mittels Richtlinienparameter wie etwa: Switch-Port, Anwendung, Tageszeit, Benutzerebene, auf der Grundlage von ACLs, die von dem Berechtigungs-Server empfangen werden.
Schlüsselmanagement	Client, ZP, AS	Gemeinsam genutzte Verschlüsselungskontexte ergeben sich als ein Nebenprodukt des Authentifizierungsaustausches.
Verschlüsselung/ Entschlüsselung	Client, ZP	Als Teil einer Sicherheit über den Äther muss der ZP mehrere Verschlüsselungsprotokolle unterstützen, einschließlich WEP, TKIP und die AES-Modi.
Verkehrssegregation	Switch	Beschränkt die ZPs, die das WLAN bilden, auf ein "drahtloses DMZ", Benutzerverkehr auf separate VLANs. Kann MAC auf der Basis von VLANs bereitstellen, zur Segregation des Benutzerverkehrs.
VPN-Tunnel-Terminierung	VPN-Gateway	Dies wird benötigt, wenn die Sicherheit über den Äther unter Verwendung von IPsec oder PPTP bereitgestellt wird.

TABELLE 1

[0100] Auf der Grundlage der obigen Arbeitsteilung wird die vorgeschlagene Demarkation der Sicherheitsmaßnahmen in einem drahtlosen LAN abgeleitet. Die Demarkationslinien zeigen an, wo die Sicherheitsmerkmale tatsächlich implementiert werden, anstatt dass sie anzeigen, wo die Sicherheitsentscheidungen getroffen werden. Zum Beispiel wird die Authentifizierungsdatenbank in einem Authentifizierungsserver aufbewahrt, aber die Verschlüsselung/Entschlüsselung wird in Wirklichkeit in dem Zugangspunkt durchgeführt. Die Demarkationsempfehlung basiert auf den allgemein bekannten Fähigkeiten der Vorrichtungen in dem Netzwerk. Aber dies schließt keine Ausführungsbeispiele aus, die alle Sicherheitsmerkmale in einer einzigen Einheit ausführen können.

[0101] Die Sicherheitsdurchsetzungsdemarkationen gemäß einem Ausführungsbeispiel der vorliegenden Erfindung sind in [Fig. 2](#) veranschaulicht. In [Fig. 2](#) sind die drahtlosen Vorrichtungen **220–229** mit den Zugangspunkten **211–215** verbunden. Auf der Ebene des Pfeils A findet die Benutzerauthentifizierung sowie die Verschlüsselung und die Entschlüsselung statt. Die Zugangspunkte **211–215** sind mit drahtlosen LAN-Switches **206** und **207** verbunden. Auf der Ebene von Pfeil B finden die Zugriffskontrolle und die Benutzersegregation statt. Die Switches **206** und **207** sind mit einem Router **203** verbunden, wobei der Letztere mit einem VPN-Gateway **202** verbunden ist. Auf der Ebene von Pfeil C findet die VPN-Tunnelung statt.

[0102] Zur Bereitstellung einer lebensfähigen Lösung für drahtlose Unternehmens-LANs hat der Unternehmens-Switch die folgenden Sicherheitsmerkmale: Unterstützung der 802.1x Authentifizierung, höhere Filterung zur Implementierung von Zugriffskontrollrichtlinien, einschließlich der Stateful Inspection, MAC-basierte VLANs, die die Benutzersegregation unterstützen, und die Unterstützung eines Messaging-Protokolls, das eine gegenseitige Erkennung zwischen dem Switch und dem ZP und den Transfer von Benutzerkontext zwischen Switches oder Switch-Ports erlaubt, damit sich der Benutzer nicht erneut authentifizieren muss. Der letztere Aspekt wird im nächsten Abschnitt genauer erläutert.

[0103] Es gibt zwei spezifische Mobilitätsmanagement-Designs in der drahtlosen LAN-Architektur, die hier erörtert werden. Diese Designs umfassen die Mobilitäts-Weiterreichung innerhalb des gleichen WLAN-Switch und die Weiterreichung (Handoff) quer durch die WLAN-Switches. Diese Designs sind analog zu der Inter-Basisstations-Weiterreichung und der Inter-Mobile-Vermittlungsstellen-Weiterreichung in einem zellularen Netz. Eine Weiterreichung in dem gleichen WLAN-Switch benötigt das Aktualisieren der Client-Informationen nur innerhalb des Switch von einem Switch-Port zu einem anderen. Die Weiterreichung quer durch die Switches erfordert eine Infrastruktur für Switches, damit sie Client-Sitzungsinformationen gemeinsam nutzen können. Die Client-Sitzungsinformationen sind entweder zentralisiert oder verteilt.

[0104] Die beiden Weiterreichungs-Szenarien sind in [Fig. 3](#) veranschaulicht. Das LAN **301** verbindet die drahtlosen Switches **306** und **307** und stellt auch eine Verbindung zu dem Authentifikationsserver **304** her. Der ZP **312** ist mit dem Switch **306** verbunden, und die ZPs **313–315** sind mit dem Switch **307** verbunden. Die Weiterreichung zwischen Switches ist veranschaulicht, wie die drahtlose Vorrichtung **322** zu der Position der drahtlosen Vorrichtung **323** hinüberwandert. Die Weiterreichung in dem gleichen WLAN-Switch ist veranschaulicht, wie die drahtlose Vorrichtung **326** zu der Position der drahtlosen Vorrichtung **327** hinüberwandert.

[0105] Es gibt zwei Typen von Persistenzanforderungen für die WLAN-Weiterreichung: Sitzungspersistenz und Anwendungspersistenz. Bei der Sitzungspersistenz sollte eine Weiterreichung eine Sitzung nicht unterbrechen. Mit anderen Worten, der drahtlose Client sollte keine erneute Authentifikation benötigen, wenn er von einem Zugangspunkt zu einem anderen wandert. Wenn die Sitzung von einem ZP zu einem anderen übertragen wird, sollten alle Attribute, die mit dieser Sitzung assoziiert sind, wie z.B. Client-basierte Bandbreitenbeschränkung, Zugriffsrechte etc., ebenfalls übertragen werden. Bei der Anwendungspersistenz sollte eine Weiterreichung eine Anwendung nicht unterbrechen. Mit anderen Worten, eine drahtlose Client-Anwendung sollte nicht abgebrochen und neu gestartet werden, wenn der drahtlose Client von einem ZP zu einem anderen wandert. Außerdem sollten Attribute, die mit dieser Anwendungssitzung assoziiert sind, ebenfalls auf den neuen ZP übertragen werden. Die Attribute umfassen Anwendungs-basierte Dienstgüte, Bandbreitenzuordnung, Zugriffskontrolle, etc..

[0106] Die signifikanten Punkte bei WLAN-Weiterreichungen umfassen die Reassoziierung mit dem Netzwerk sowie auch die Umleitung des Verkehrs zu dem Client an einem neuen physischen Standort. Diese beiden Punkte werden in den nachfolgenden Abschnitten angesprochen.

[0107] Wenn sich ein drahtloser Client von einer Zone zu einer anderen bewegt, wird der Client mit einem anderen ZP reassoziert. Diese Reassoziierung führt dazu, dass der alte ZP und der neue ZP die Client-Sitzungsinformationen austauschen. Wenn man dem Rahmenwerk von 802.11f oder dem Inter Access-Point Protocol (IAPP) folgt, können die Sitzungsinformationen oder der Verbindungskontext, die zwischen den ZPs ausgetauscht werden, Sitzungsinformationen wie zum Beispiel Verschlüsselungs-/Entschlüsselungs-Schlüssel, Service Set, etc. enthalten. Durch diesen Austausch kann der Client an der neuen Stelle die Kommunikation sofort wiederaufnehmen, womit die Notwendigkeit einer erneuten Authentifikation beseitigt ist.

[0108] Der Informationsaustausch zwischen den in Beziehung zueinander stehenden Entitäten, einschließlich des Client, des alten und des neuen ZP und des Authentifikationsservers, in einem Reassoziierungsprozess ist in dem Nachrichtensequenzdiagramm in [Fig. 4](#) veranschaulicht. Die Nachrichten, die ausgetauscht werden, sind entweder IEEE 802.11 oder 802.11f Nachrichten.

[0109] Bei diesem Nachrichtenaustausch sendet der Client eine Reassoziierungsanforderung, die die Basis Service Set Identifikation (BSSID; basic service set ID) des alten ZP umfasst, an den neuen ZP. An diesem Punkt besitzt der neue ZP keinerlei Informationen darüber, wo dieser Client her kommt, aber er wird die BSSID in einer Zugriffsanforderungs-Nachricht zu dem Authentifikationsserver schicken, der Informationen in Bezug auf den alten ZP, einschließlich seiner IP-Adresse, zurückschicken wird.

[0110] Eine Transferkontrollprotokoll-(TCP; transfer control protocol)-Verbindung wird dann zwischen dem neuen und dem alten ZP eingerichtet. Wenn in dieser Verbindung Sicherheit erwünscht ist, werden die beiden ZPs optionale Verschlüsselungsinformationen in einem Sicherheitsblock-Sende-(Send-Security-Block)- und Sicherheitsblock-Bestätigungs-(Ack-Security-Block)-Nachrichtenpaar austauschen. In diesen beiden Nachrichten einigen sich die beiden ZPs auf einen Verschlüsselungsschlüssel in den Nachrichten zwischen ihnen. Danach wird der neue ZP eine Bewegungsanforderungs-(Move-Request)-Nachricht an den alten ZP senden, der mit einer Bewegungsantwort-(Move-Response)-Nachricht antworten wird, die den Verbindungskontext

enthält.

[0111] In der Unternehmens-WLAN-Architektur der vorliegenden Erfindung wird die Reassoziierung auch bewirken, dass auf den Switch bezogene Sitzungsinformationen zwischen Switches ausgetauscht werden, wenn die Weiterreichung mehr als einen Switch beansprucht. Derartige Informationen können die Berechtigung, Zugriffsrechte, Dienstgüteparameter, Bandbreitenmanagementparameter, etc. umfassen.

[0112] Dieser Weiterreichungs-Mechanismus in dem Unternehmens-WLAN wird unten erörtert. Es gibt wenigstens zwei Lösungswege, den Verkehr nach den Weiterreichungen umzuleiten. Die folgenden Unterabschnitte widmen sich diesen beiden Lösungswegen gemäß zwei Designs. Bei beiden Lösungswegen wird angenommen, dass die VPN-Tunnelung nicht für den Client verwendet wird, um eine geschützte drahtlose Verbindung zu gewährleisten. Dieses Ziel wird durch das neuere Verschlüsselungsverfahren, den Advanced Encryption Standard (AES), erreicht, der bei der drahtlosen Übertragung verwendet wird.

[0113] Bei dem Lösungsweg mit einem einzigen Teilnetz wird das gesamte Unternehmen auf ein einziges IP-Teilnetz begrenzt. Alle mobilen Clients werden IP-Adressen in diesem Teilnetz zugewiesen. Wenn sich ein Client von einer ZP-Zone zu einer anderen ZP-Zone bewegt, bleibt die IP-Adresse des Client identisch. Es wird der Switching- oder Routing-Vorrichtung überlassen, ihre interne Tabelle so zu aktualisieren, dass alle nachfolgenden Pakete korrekt zu dem Client vermittelt oder geroutet werden. Die beiden Szenarien der Weiterreichung im gleichen Switch und der Weiterreichung quer durch Switches werden unten angesprochen.

[0114] Bei der Weiterreichung im gleichen Switch sind der alte und der neue ZP mit dem gleichen Switch verbunden. Der alte ZP muss den Switch informieren, dass der Client nicht mehr länger mit ihm assoziiert ist, während der neue ZP den Switch informieren muss, dass der Client neu mit ihm assoziiert ist. Der Switch muss seine L2-Switching-Tabelle derart aktualisieren, dass die nachfolgenden Pakete für den Client korrekt nach draußen vermittelt werden. Dies wird dadurch erzielt, dass der existierende Eintrag des mobilen Client in der L2-Tabelle entfernt wird. Das nächste Paket, das für den mobilen Client bestimmt ist, wird somit einen unbekannten Unicastinduzieren, so als ob das Paket von dem Switch in der Downstream-Richtung zum ersten Mal bearbeitet worden ist.

[0115] Bei der Weiterreichung quer durch die Switches gibt es einen Eintrag in der Routing-Tabelle in dem Router, der die IP-Adresse der mobilen Station zu der Schnittstelle zu dem alten Switch oder SW1, **506**, in [Fig. 5](#) abbildet. Der Switch SW1 **506** ist bei A mit dem Router **503** verbunden und der Switch SW2 **507** ist bei B mit dem Router **503** verbunden. Der mobile Client **522**, der sich zu AP2 **513** bewegt, sollte es erlauben, dass der Routing-Tabelleneintrag ablaufen kann, da jedes Paket, das für den mobilen Client bestimmt ist und zu der Schnittstelle A weitergeleitet wird, sein Ziel nicht erreichen würde. Normalerweise würde bei einem Unicast der Routing-Tabelleneintrag von {192.168.3.11, 23.EC.EB.14.1A.51, A} mit {192.168.3.11, 23.EC.EB.14.1A.51, B} aktualisiert, wenn eine der vier Situationen auftreten würde.

[0116] Die Routing-Tabelle kann aktualisiert werden, wenn der mobile Client 192.168.3.11 ein Paket zu dem Netzwerk über den Router sendet oder wenn der ARP-Eintrag des mobilen Client abläuft und eine neue Address Resolution Protocol (ARP)-Anforderung rundsendet. Die Routing-Tabelle kann auch aktualisiert werden, wenn eine bestehende TCP-Verbindung zwischen dem mobilen Client und einer anderen Entität in dem Netzwerk derart besteht, dass jeder nachfolgende stromabwärtige TCP-Verkehr nicht korrekt geroutet wird. Die unterbrochene TCP-Verbindung wird den Router dazu veranlassen, eine ARP-Anfrage an das Teilnetz zu senden und somit die Routing-Tabelle mit dem neuen Folgesprung des mobilen Client zu aktualisieren. Die Routing-Tabelle kann auch dann aktualisiert werden, wenn sowohl SW1 **506** als auch SW2 **507**, die sich beide der Weiterreichung bewusst sind, proprietäre Nachrichten an den Router **503** senden, um dem Router mitzuteilen, dass er den Eintrag aktualisieren soll. Wenn eine proprietäre Nachricht nicht erwünscht ist, kann ein Paket von SW2, das die MAC/IP-Adressen des mobilen Client fingiert, ausreichen, um eine Aktualisierung bei dem Router zu bewirken. Wenn mehrere Router zwischen SW1 und SW2 vorhanden sind, müssen alle betroffenen Zwischenrouter ebenfalls aktualisiert werden. Wenn die Routing-Tabelle aktualisiert ist, werden alle nachfolgenden Pakete, die für 192.168.3.11 bestimmt sind, korrekt zu SW2, AP2 und dann zu dem mobilen Client geleitet.

[0117] Das Verfahren mit einem einzigen Teilnetz ist ein einfaches Verfahren, um die Mobilität des drahtlosen Client zu unterstützen. Der Nachteil bei diesem Verfahren ist aber, dass dieses Verfahren nicht skalierbar ist. Es hat nur eine begrenzte Anzahl von Teilnetz-Adressen (bei einem Teilnetz von 192.168.3.x liegt die Anzahl der unterstützten drahtlosen Clients bei 254). Es kann kein Unternehmen unterstützen, das eine größere Anzahl von drahtlosen Verbindungen benötigt.

[0118] Eine flexiblere, skalierbare Lösung für die WLAN-Mobilität ist das mobile IP. Als ein Internet Engineering Task Force (IETF) Standard ist das mobile IP ein Mechanismus, der es erlaubt, dass eine permanente IP-Adresse eines mobilen Client in unterschiedlichen IP-Teilnetzen verwendet werden kann, wenn sich der Client in dem mobilen Netzwerk herumbewegt, das von unterschiedlichen ZPs abgedeckt ist.

[0119] Das mobile IP verwendet das Konzept eines Heimatnetzwerks und eines fremden Netzwerks für den Client. Das Heimnetzwerk ist dasjenige, in dem der mobile Client seine IP-Adresse bekommt. In dem Heimteilnetz **601**, wie es in [Fig. 6](#) veranschaulicht ist, gibt es einen Knoten, der Heimatagent (home agent) **602** genannt wird, der als die Care-of-Adresse des mobilen Client dient. Der Heimatagent empfängt den gesamten Datenverkehr für den Client **603**. Solange der Client in dem Heimnetzwerk bleibt, leitet der Heimatagent den Verkehr einfach an den Client weiter. Für gewöhnlich spielt ein Router in dem Heimteilnetz die Rolle des Heimatagenten.

[0120] Wenn sich der mobile Client **703** von einem Teilnetz in ein anderes bewegt, d.h. von **701** zu **703**, wie in [Fig. 7](#) veranschaulicht ist, bleibt die IP-Adresse des Client gleich. Da er sich physisch in einem anderen Teilnetz befindet, kann der Verkehr, der für den Client bestimmt ist, nicht normal durch das Unternehmens-LAN zu dem Client geroutet werden. Ein Tunnelungs-Mechanismus wird benötigt, um den Verkehr von dem alten oder Heimnetzwerk zu dem neuen oder fremden Netzwerk umzuleiten. Dem Heimatagenten **702** ähnlich, weist auch das fremde Netzwerk **705** eine Entität auf, die der Fremdagent (foreign agent) **706** genannt wird, der sich um den umgeleiteten Verkehr für den mobilen Client kümmert. Jeder Agent hat einen zugeordneten ZP, **712** und **713**. Der Tunnel, der zwischen dem Heimatagenten und dem Fremdagenten errichtet wird, ist in [Fig. 7](#) veranschaulicht.

[0121] Der getunnelte Verkehr wird in einem anderen Standardprotokoll, entweder IP-in-IP oder minimale Kapselung, eingekapselt. Der Heimatagent ist verantwortlich für die Kapselung des Verkehrs, der für den mobilen Client bestimmt ist, und für das Weiterleiten dieses Verkehrs zu dem Fremdagenten. Der Fremdagent ist verantwortlich für das Entfernen der Verkapselungsform des getunnelten Verkehrs und für das Weiterleiten des Verkehrs zu dem mobilen Client.

[0122] In der Veranschaulichung von [Fig. 7](#) weist der mobile Client eine IP-Adresse von 192.168.3.11 auf, die er von dem Teilnetz 192.168.3.x erhalten hat. Wenn sich der Client in das Teilnetz 192.168.22.x bewegt, wird der Heimatagent, der der Schnittpunkt für den gesamten Verkehr für den Client ist, den Verkehr zu dem Fremdagenten weiterleiten, der im Augenblick mit dem Client assoziiert ist, welches der Fremdagent in dem Teilnetz 192.168.22.x ist. Unter Verwendung von IP-in-IP wird ein getunneltes Paket die IP-Adresse des Heimatagenten (192.168.3.5) als die Quelladresse, die IP-Adresse des Fremdagenten (192.168.22.4) als die Zieladresse, und den Protokoll-Typ von 4 (IP-in-IP) aufweisen. Das Originalpaket wird dann die Nutzlast dieses IP-in-IP-Pakets sein.

[0123] Die kritischen Aspekte des mobilen IP sind die Agentenentdeckung und die Agentenregistrierung. Wenn der mobile Client eine neue mobile Zone betritt, muss er den Agenten dieses Teilnetzes entdecken, der als der Fremdagent der mobilen Clients dient. Er muss auch seinem eigenen Heimatagenten den gegenwärtigen Fremdagenten mitteilen, damit der Heimatagent weiß, wohin er den Verkehr leiten soll.

[0124] Bei dem Lösungsweg mit dem mobilen IP sind der Router und der Client die einzig relevanten Spieler in der Infrastruktur. Der Router muss die Fähigkeit bezüglich eines mobilen IP aufweisen, während das Protokollprofil in dem Client auch in der Lage sein muss, das mobile IP zu unterstützen. Es ist bekannt, dass die Verwendung des mobilen IP in Unternehmensnetzwerken nicht weit verbreitet ist und dass Router und Clients aktualisiert werden müssten, um das mobile IP unterstützen zu können.

[0125] Da das mobile IP nicht notwendigerweise bei älteren Routern verwendet wird, ist ein alternativer Lösungsweg, dass der WLAN-Switch die Tunnelung für den umherwandernden Client durchführt. Wie bei dem mobilen IP kann es viele IP-Teilnetze geben, von denen jedes eine oder mehrere ZP-Zonen abdeckt.

[0126] Das alternative Tunnelungs-Verfahren stammt von dem Konzept des mobilen IP. Der einzige Unterschied liegt darin, dass die Agenten nicht mehr die Router sind, sondern die Unternehmens-WLAN-Switches. Als eine Folge davon werden die Tunnel zwischen den WLAN-Switches statt zwischen den Routern errichtet.

[0127] Wenn sich der mobile Client zu einer anderen ZP-Zone bewegt, die in einem anderen IP-Teilnetz konfiguriert ist, empfängt der Heimatagent, der WLAN-Switch in dem Heimateilnetz, immer noch die Pakete für die mobile Station. Da der mobile Client nicht drahtlos mit dem Heimatagenten verknüpft ist, wird ein Fremda-

gent in dem neuen Teilnetz benötigt, um die Pakete zuzustellen.

[0128] Der Fremdagent ist ein anderer WLAN-Switch in dem neuen IP-Teilnetz, in das sich der mobile Client hineinbewegt. Da der mobile Client seine IP-Adresse nicht ändert, werden die Pakete nicht zu dem neuen Teilnetz weitergeleitet. Wie bei dem mobilen IP wird ein Tunnel zwischen den beiden WLAN-Switches errichtet. Unter Verwendung dieses Tunnels leitet der Heimatagent alle Pakete zu dem Fremdagenten weiter, der die Pakete wiederum zu dem mobilen Client liefert. Das Originalpaket, das für den mobilen Client bestimmt war, wird einfach unter Verwendung eines Standard-Tunnelungs-Protokolls wie IP-in-IP oder minimale Kapselung in dem getunnelten IP-Paket eingebettet. Beim Empfangen des Pakets vermittelt der Fremdagent die Pakete einfach auf der Basis seiner MAC-Adresse weiter.

[0129] Es sei angenommen, dass die Vorrichtungen die folgenden IP-Adressen aufweisen:

Heimatagent –	192.168.3.15
Fremdagent –	192.168.22.71
mobiler Client –	192.168.3.11

[0130] Ein Beispiel der Tunnelungs-Operation für stromabwärtigen Verkehr ist in [Fig. 7](#) veranschaulicht. Der Mechanismus zum Senden von stromaufwärtigem Verkehr ist gleich dem des stromabwärtigen Verkehrs und ist in [Fig. 8](#) veranschaulicht. Das Verfahren wird einfach umgekehrt. Pakete von dem mobilen Client **803** werden bei dem Fremdagenten **806** verarbeitet, nämlich bei dem Unternehmens-WLAN-Switch, durch den ZP2 **813** des fremden Teilnetzes **805**. Der Switch wird das aktuelle stromaufwärtige Paket in ein IP-in-IP-Paket verkapseln und dieses zu dem Heimatagenten **802** durch den Tunnel senden. Der Heimatagent **802** bedient das Teilnetz **801** durch den ZP2 **812**. Der Heimatagent, der der WLAN-Switch ist, mit dem der mobile Client ursprünglich assoziiert war, wird den IP-in-IP-Header entfernen und das tatsächliche Paket zu dem Netzwerk senden.

[0131] Die Tunnelung ist ein zuverlässiges, skalierbares Modell zur Umleitung von Verkehr in der WLAN-Mobilität. Aber bei diesem Modell wird eine zusätzliche Verarbeitungsleistung in dem WLAN-Switch benötigt, um die Tunnelung zu handhaben, sowie auch eine extra Bandbreite in dem verdrahteten LAN benötigt, weil der Verkehr mit einem extra Sprung wandert.

[0132] Eine Weiterreichung sollte eine nahtlose Operation sein. Die Sitzung und die Anwendungen sollten während einer Weiterreichung nicht unterbrochen werden. In einer gewöhnlichen Anmelde-Sitzung oder in einer normalen verbindungsorientierten Anwendung wie FTP ist mehr Spielraum in der Performanz vorhanden. Aber in nicht verbindungsorientierten, verzögerungsempfindlichen Anwendungen wie VoIP ist eine schnelle Weiterreichung der Sitzungs- und Anwendungsinformationen zwingend. Wenn eine Liste von neuen ZP-Kandidaten an einer Stelle in dem Client vorhanden wäre, würde dies den Weiterreichungs-Overhead in hohem Maße verbessern.

[0133] Bei VoIP ist das relevante Performanzproblem der stromabwärtige (WLAN zum Client) Paketverlust, wenn das drahtlose IP-Telefon von einer ZP-Zone zu einer anderen wandert. Während einer Weiterreichung im gleichen Switch würde die Entscheidung des Switch, die Sprachpakete von einem physikalischen Port zu einem anderen zu vermitteln, eine infinitesimale Zeit benötigen. Aber eine Weiterreichung quer durch Switches ist viel komplizierter und zeitaufwendiger. Der alte WLAN-Switch muss die Sprachpakete zu dem neuen WLAN-Switch erneut senden, während er gleichzeitig dem beliebigen Zwischenrouter mitteilen muss, dass er das Paket zu dem neuen WLAN-Switch derart umleiten muss, dass es wieder in die Richtung des alten Switch geleitet würde. Alle diese Aktionen müssen innerhalb einer Zeitspanne stattfinden, in der der Endbenutzer keine unterbrochene Konversation wahrnimmt.

[0134] Diese Zeitspanne wird von den Sprachcodecs bestimmt, die in dem IP-Telefon benutzt werden, da die meisten Sprachkompressions-Algorithmen die Fähigkeit haben, die Sprache bedingt durch verlorene Pakete abzugleichen. Die Zeitspanne dieser Abgleichung oder die Abtastwertinterpolation variiert von Codecs-Implementation zu Codecs-Implementation. Als eine Daumenregel kann man sagen, dass die wahrgenommene Sprachqualität leidet, wenn 3–5% der Pakete verloren gehen. So wäre zum Beispiel bei einem Satz von 3 Sekunden 90–150 ms an verlorenen Sprachrahmen nicht bemerkbar. Eine Abtastwertinterpolation ist vor allem dann ineffektiv, wenn das Sprachmuster von Schweigen zu Sprache übergeht. In einer WLAN-Umgebung wird eine Weiterreichung zwischen ZPs für gewöhnlich in einstelligen Millisekunden erledigt.

[0135] Dadurch, dass sich drahtlose LANs in Unternehmen so weit verbreitet haben, wird das Management aller Zugangspunkte zu einer Hauptangelegenheit für die IT-Manager. Das Managementproblem wird noch akuter in großen Unternehmen mit mehreren Standorten. Zum größten Teil wurden Zugangspunkt-Managementlösungen in einfacheren Zeiten entwickelt, wie zum Beispiel dann, wenn man nur ein halbes Dutzend dieser Vorrichtungen in einem Büro hat. Aber jetzt, da die Firmen drahtlose Produkte der Unternehmensklasse in Unternehmensmengen kaufen, ist das begrenzte Management nicht ausreichend. Zusammen mit einer drahtlosen Installation der Unternehmensklasse wird auch ein Unternehmensklassen-Management benötigt. Vorzugsweise ergänzt sich dieses Unternehmensklassen-Management nahtlos mit den LAN-Management-Werkzeugen, die bereits in dem Unternehmen verwendet werden.

[0136] Bei herkömmlichen drahtlosen LANs weisen diese Systeme kein herstellernertrales Management (Multi-Vendor-Management) auf, und eine herstellernertrale WLAN-Management-Schnittstelle wäre hilfreich dabei, es einem Administrator zu erlauben, das gesamte Unternehmen zu managen. Gegenwärtige WLAN-Management-Werkzeuge stellen keine globale Sicht der drahtlosen Netzwerkaktivität bereit, aber sie können einen einfachen Zugriff auf Informationen über jeden drahtlosen Zugangspunkt in dem Netzwerk bereitstellen. Für jede Vorrichtung können Paketstatistiken betrachtet werden, um zu bestimmen, wie viele Pakete welchen Typs hindurchgewandert sind. Auch die Brücken- und Adressenauflösungstabellen können betrachtet werden, und in einem Zustandsbereich kann man die Alarmsignale und die allgemeinen Betriebsbedingungen betrachten (wie z.B., ob der Zugangspunkt eingeschaltet ist). Aber in dem Fall von drahtlosen Unternehmens-Netzwerken werden bessere Management-Werkzeuge benötigt, um alle Vorrichtungen zu managen, die das Netzwerk benutzen.

[0137] Die Verwendung von WLAN-Lösungen in dem Unternehmen kann von der Fähigkeit der IT-Manager abhängen, WLAN-Netzwerke der Unternehmensklasse managen zu können. Leistungsmerkmale, die in WLAN-Management-Werkzeugen der Unternehmensklasse enthalten sein können, fallen in zwei Hauptkategorien: Installationsleistungsmerkmale und Wartungsleistungsmerkmale. In Bezug auf die Installationsleistungsmerkmale erlaubt die WLAN-Netzwerk-Topologieerkennung, dass die Auto-Discovery-Fähigkeiten die Zugangspunkte (ZPs) in "Plug-and-Play"-Vorrichtungen umwandeln. Wenn ein ZP mit dem Netzwerk verbunden wird, entdeckt ihn der WLAN-Manager sofort, selbst wenn er nicht konfiguriert ist. Außerdem können die Installationsleistungsmerkmale die automatische Verteilung von vordefinierten Einstellungen, wie z.B. die IP-Adresse, die Netzadresse und andere Konfigurationsparameter, die allen ZPs zu eigen sind, sowie auch die Erfassung von nicht autorisierten ZPs umfassen, indem ein Netzwerk-"Kennwort" für neue Vorrichtungen verwendet wird, die sich dem drahtlosen LAN anschließen.

[0138] In Bezug auf die Wartungsleistungsmerkmale umfassen diese Merkmale eine Überprüfung des Zustands/Status jedes Zugangspunkts in dem gemanagten WLAN ausgehend von einer zentralen Management-Konsole. Ebenfalls enthalten ist die Fähigkeit, die Einstellungen jedes Zugangspunkts in dem gemanagten WLAN, wie z.B. Rundsendeeinstellungen, Funkfrequenzen und Geräteabschalt- und -startzeiten, ändern zu können, und die Fähigkeit, ZP-Software-Upgrades in einer automatisierten Art und Weise verteilen zu können. Das Wartungsleistungsmerkmal kann auch die Fähigkeit umfassen, Vorrichtungskonfigurationen und -software schreiben und sichern zu können, eine globale Ansicht der WLAN-Verwendung bereitzustellen zu können und überlastete und zu wenig benutzte Zugangspunkte identifizieren zu können und eine schnelle Entdeckung eines WLAN-Performanz-Leistungsrückgangs und von Zugangspunktfehlern bereitstellen zu können.

[0139] Andere Wartungsleistungsmerkmale umfassen das Management des Netzwerkzugriffs und die Verwendung auf der Grundlage der Benutzerposition, das Management des Zugriffs auf gemeinsam genutzte Netzwerkressourcen wie zum Beispiel Drucker, Fax und Projektoren und die Sammlung von höheren Verkehrsstatistiken auf der Grundlage von SNMP, RMON und RMON2. Verwendungsmuster und Netzwerkaktivitätsmessungen sind entscheidend bei der Bestimmung der optimalen Platzierung von Zugangspunkten, des richtigen Lastausgleichs, was schließlich zu einer besseren Netzwerkperformanz führt. Außerdem ist die Multi-Vendor-Unterstützung bei großen Unternehmen entscheidend, in denen heterogene Geräte sowohl in den verdrahteten als auch in den drahtlosen Teilen des Netzwerks verwendet werden können. IT-Manager werden eine WLAN-Lösung auswählen, die unter Verwendung der Werkzeuge, die ihnen bereits in dem Unternehmen zur Verfügung stehen, gemanagt werden kann. In Bezug zum Letzteren steht das Management von drahtlosen LANs an entfernt gelegenen Stellen ausgehend von einem zentralisierten Standort unter Verwendung des Standard-Unternehmens-Netzwerks.

[0140] In Zusammenhang mit den Management-Werkzeugen steht die Schlüsselrolle, die der WLAN-Switch

in mehreren Bereichen des WLAN-Managements spielt. Diese umfassen das Sammeln von Statistiken, wobei der ZP begrenzte Zähler aufweist, und folglich ist der Switch eine Entität, die das Sammeln von höheren Statistiken und Topologieerkennung ermöglicht, wobei der Switch die logische Wahl für die zentrale Entität in dem Topologieerkennungsprozess ist. Ebenfalls wichtig ist die Multi-Vendor-Unterstützung, bei der der Switch die Upstream-Management-Informationen in dem zentralen Manager vereinigen kann und die Downstream-Informationen in einer händlerspezifischen Art und Weise verteilen kann, wodurch eine einfache, kostengünstige Multi-Vendor-Unterstützung bereitgestellt wird. Des Weiteren stellt der WLAN-Switch das Management des Zugriffs auf gemeinsam genutzte Netzwerkressourcen unter Verwendung der höheren Filterungsfähigkeiten und das Fernmanagement bereit, wobei die höheren Filterungsleistungsmerkmale in dem Switch das Management von WLAN-Netzwerken quer durch mehrere Standorte sicher ermöglichen können.

LASTAUSGLEICH

[0141] In den meisten WLAN-Umgebungen bekommt ein drahtloser Client eine stabile Signalstärke von mehreren ZPs, so dass sich der drahtlose Client mit dem ZP assoziieren will, der die beste Performanz bereitstellen kann. Es ist entscheidend für den Ausgleich der Last der ZPs, dass allen Clients eine optimale Performanz gegeben wird, weil dies eine skalierbare Unternehmenslösung erlaubt, die die zur Verfügung stehende Bandbreite effizient ausnutzt. Es gibt zwei mögliche Netzwerkkonfigurationen, die einen Lastausgleich ermöglichen, und zwar entweder wird eine ZP-Reihe in einer WLAN-Zone installiert, oder die ZPs werden strategisch so angeordnet, dass jedes Paar von benachbarten ZPs einen beträchtlichen überlappenden Bereich aufweisen würde. Das Ergebnis des Lastausgleichs liegt darin, dass man nicht einige ZPs hat, die überlastet sind, während andere ZPs zu wenig ausgelastet sind, wenn diese ZPs die gleiche Zone abdecken.

[0142] Es gibt zwei Lösungswege für den Lastausgleich, einen verteilten Lösungsweg und einen zentralisierten Lösungsweg. Bei einem verteilten Lösungsweg treffen der Client und die ZPs gemeinschaftlich die Entscheidung, welcher ZP mit dem Client assoziiert werden soll. In einem zentralisierten Lösungsweg sammelt ein zentraler Lastausgleichsmanager verschiedene Netzwerkstatistiken und -zustände und trifft die Lastausgleichsentscheidung. Die Anforderungen beider Lösungswege werden in diesem Abschnitt besprochen.

[0143] Beim verteilten Lastausgleich wird die Lastausgleichsentscheidung zwischen dem drahtlosen Client und den ZPs ausgehandelt. Bei der Standardmethode läuft es so, dass der Client auf der Grundlage des gegenwärtigen Verkehrsstatus des ZP entscheidet, mit welchem ZP er assoziiert werden will. Dieser verteilte Lösungsweg schiebt die Verantwortlichkeit hinunter zu dem drahtlosen LAN, somit benötigt er keine Ressourcen in dem LAN, um Statistiken von verschiedenen ZPs zu sammeln und derartige Entscheidungen zu treffen.

[0144] Beim verteilten Lastausgleich besitzt der Client eine Liste von ZP-Kandidaten, von denen er adäquate Signale bekommt. Es ist der Client, der entscheidet, mit welchem ZP er assoziieren will. In einem WLAN, das keinen Lastausgleich unterstützt, kann der Client einen ZP zufällig auswählen, nämlich den ersten ZP, den er entdeckt, den letzten ZP, den er entdeckt, oder denjenigen mit dem stärksten Signal, etc.. Aber diese beliebige Vorgehensweise führt nicht zu der optimalen Performanz in dem WLAN.

[0145] Ein effizienterer Lösungsweg besteht darin, dass der Client die Last der verschiedenen ZPs untersucht und sich mit dem ZP assoziiert, der ihm die beste Performanz geben wird. In den meisten Fällen wird er den ZP mit der leichtesten Last auswählen. Um dem Client Daten bereitzustellen, müssen die ZPs in der Lage sein, verschiedene Statistiken zu sammeln und zu verwalten. Abtastwertstatistiken können die Anzahl an assoziierten Clients, die Anzahl von übertragenen oder empfangenen Paketen, die durchschnittliche ankommende und abgehende Bandbreite, die in der jüngsten Vergangenheit verbraucht wurde, und Prioritäten des jüngsten Verkehrs umfassen. Es wird also ein Mechanismus für den ZP und den Client benötigt, um Lastinformationen auszutauschen, was unten beschrieben werden wird.

[0146] Es muss einen Kommunikationsmechanismus für den ZP und den Client geben, um die Lastinformationen derart zu kommunizieren, dass der Client eine intelligente Entscheidung bezüglich der Assoziierung mit einem ZP treffen kann. Ein Schicht-2-Protokoll ist erwünscht, da solche Kommunikationen sogar stattfinden können, bevor der Client in dem Netzwerk authentifiziert ist, d.h. sogar bevor der Client eine IP-Adresse erfasst. Der Client kann dann den Lastzustand und die Signalstärken von verschiedenen ZPs sammeln und die Assoziierungsentscheidung auf der Grundlage von mehreren Parametern treffen.

[0147] Ein virtueller Kanal (VC; virtual channel) ist ein Mechanismus für den ZP und den Client, um Lastinformationen zu kommunizieren. Ein VC ist ein Mechanismus für normkonforme Vorrichtungen, um miteinander in der Schicht 2 zu kommunizieren. Mit anderen Worten, drahtlose Clients und ZPs, die aus normkonformen

drahtlosen Vorrichtungen aufgebaut sind, sind mit einem Vorteil versehen, dass der verteilte Lastausgleich unterstützt wird.

[0148] Das Ziel des Lastausgleichs liegt darin, zu gewährleisten, dass die Clients optimale WLAN-Zugriffe erhalten. Zur Beurteilung der Auswirkungen des Lastausgleichs müssen die meisten, wenn nicht alle Clients optimale Dienste erhalten. Dies kann gemessen werden durch Clients, die die angeforderte Bandbreite erhalten, die Anzahl an fallengelassenen Paketen aufgrund der ZP/WLAN-Switch-Überlastung und der drahtlosen Kollision, und ob Pakete die entsprechende Priorisierung erhalten. Ähnlich wie das Mobilitäts-Problem, so ist eine andere Anforderung bei dem Lastausgleich sehr ähnlich zu dem bei der Mobilitäts-Weiterreichung. Die gleichen Prinzipien der Sitzungspersistenz und der Anwendungspersistenz gelten auch hier. Eine Dienstunterbrechung sollte auf einem Minimum gehalten werden.

[0149] Bei dem zentralisierten Lastausgleich wird die Lastausgleichsentscheidung von einem Lastausgleichsmanager getroffen. Dieser Manager kann irgendwo in dem LAN platziert sein; er kann auch zusammen mit dem WLAN-Switch angeordnet sein. Der Grund für den zentralisierten Ansatz liegt darin, Gesamtnetzwerk-Lastausgleichs-Richtlinien zu folgen. Es ist den Clients nicht erlaubt, irgendeinen beliebigen ZP, den sie wollen, auszuwählen. Verschiedene Aspekte der Lastausgleichsanforderungen werden unten erörtert.

[0150] Beim ZP-Lastausgleich kann ein Pool von Client-Stationen, die auf das WLAN von einer Zone aus zugreifen, durch einen oder mehrere ZPs den Zugriff erhalten. Es ist die ungleichmäßige Verteilung von Clients pro ZP, die nach einem Lastausgleich ruft. Die Kriterien, die Last auszugleichen, sind durch den WLAN-Administrator konfigurierbar. Der Lastausgleich kann auf einer Verkehrslast, einer Signalstärke, Client-Typen, etc. basieren. Die Entscheidung, die Verkehrsbelastung ausgehend von einer ZP-Zone sowie auch ihre benachbarten Zonen zu überwachen, gehört zu einem Lastausgleichsmanager, der in dem WLAN-Switch angeordnet sein kann. Der Lastausgleichsmanager untersucht die Verkehrskapazität verschiedener ZPs in einer Zone und trifft eine Entscheidung, ausgewählte Clients von einem ZP zu einem anderen zu vermitteln.

[0151] Ein Lastausgleichsmanager (LBM; load balancing manager) verwaltet den Lastausgleich. Er kann ein proaktiver oder ein reaktiver Mechanismus sein. In dem proaktiven Modus überprüft der LBM die Netzwerkbedingung periodisch, um den Bedarf nach einem Ausgleich der Last zu bestimmen; während er in einem reaktiven Modus ist, warnt der Netzwerkmanager den LBM, wenn bestimmte Statistiken vorbestimmte Schwellwerte erreichen. Um eine Last-Switching-Entscheidung zu treffen, untersucht er zwei Typen von Parametern; statische und dynamische Parameter.

[0152] Statische Parameter sind Parameter, die programmiert werden, wenn das WLAN konfiguriert wird. Diese Parameter sind höchstwahrscheinlich in einer Datenbank gespeichert. Einige statische Parameter umfassen die Netzwerktopologie von ZPs, wobei diese Datenbank von Informationen anzeigt, welche ZP-Zonen sich überlappen, dass Clients in der Zone von einem ZP zu einem anderen übertragen werden können. Andere statische Parameter umfassen ZP-Ressourcen, die die ZP-Fähigkeiten anzeigen, vor allem die ZP-Kapazitäten, die Bandbreitenmanagementgranularität des ZP, die ZP-MAC-Adressen, sowie auch zur Verfügung stehende Frequenzen.

[0153] Dynamische Parameter sind Parameter, die sich ändern, wenn das WLAN mit Clients arbeitet, die auf das WLAN zugreifen. Diese Parameter werden hauptsächlich aus dem Netzwerkmanagement MIB in dem WLAN erhalten. Einige dynamische Parameter umfassen die Signalstärke von Client-Stationen, wobei dann, wenn eine Client-Station von einem ZP zu einem anderen transferiert wird, die Signalstärke, die der neue ZP von dem Client empfängt, einen vorbestimmten Schwellwert überschreiten muss. Ein anderer dynamischer Parameter ist die ZP-Verkehrsbelastung. Aus diesem Parameter bestimmt der Lastausgleichsprozess, welcher ZP in einer Zone überladen ist und welcher ZP zu wenig ausgelastet ist. Ein anderer Typ von dynamischem Parameter ist die Client-Verkehrsbelastung, wobei dieser Parameter das Client-Verkehrsprofil untersucht, sowohl die durchschnittliche Bitrate als auch die Spitzen-Bitrate, sowie auch Bandbreitenmanagementparameter, um zu bestimmen, welche Client-Stationen die besten Kandidaten sind, um bewegt zu werden. Ebenfalls enthalten sind anwendungsbasierte Parameter, die bestimmen, wie Anwendungen auf ZPs verteilt werden, vor allem in einer ZP-REIHE. Anstatt eine Entscheidung auf der Basis einer Verkehrsbelastung zu treffen, beruht diese Entscheidung auf Anwendungen. Richtlinien können verzögerungssensitiven Anwendungen (z.B. VoIP, Streaming Media, etc.) eine höhere Priorität geben, zu einem ZP mit einer leichteren Last bewegt zu werden; andere Richtlinien können einen ZP für nicht-verzögerungssensitive, bandbreitenverbrauchende Anwendungen zuordnen (z.B. das Herunterladen von Filmen des Peer-to-Peer-Typs), während sie leichtere Lasten auf anderen ZPs durchführen. Die dynamischen Parameter können auch Client-basiert sein. Wie das anwendungsbasierte Kriterium kann auch dieses Kriterium aktive Clients auf der Grundlage ihrer Identitäten neu ver-

teilen. Diese Clients umfassen Angestellte, deren LAN-Zugriff bedeutsam für den Auftrag ist, leitende Angestellte, etc.. Indem die MAC-Adressen oder Login-IDs von ausgewählten Clients erkannt werden, kann der Lastausgleichsprozess entscheiden, diese Clients zu ZPs mit leichter Last zu bewegen. Im Allgemeinen sind die Performanzanforderungen für einen zentralisierten Lösungsweg gleich denen des verteilten Lösungswegs.

Dienstgüte

[0154] Es gibt zwei Aspekte der Dienstgüte (QoS; quality of service) in einem drahtlosen LAN, die wichtig für die vorliegende Erfindung sind, nämlich das drahtlose Medium und das verdrahtete Medium. Die Qos des drahtlosen Mediums wird von dem IEEE 802.11e Standard abgedeckt, einer Verbesserung des IEEE 802.11 Standards, während die Qos der Schicht 2 des verdrahteten Mediums von IEEE 802.1p abgedeckt wird. Zur Bereitstellung von Ende-zu-Ende-Qos für Vorrichtungen in dem Unternehmens-WLAN sollten sowohl das drahtlose als auch das verdrahtete Medium Qos-fähig sein.

[0155] Zwei Qos-Mechanismen sollten in dem WLAN unterstützt werden; dies sind die Verkehrspriorisierung und das Bandbreitenmanagement. Die Verkehrspriorisierung umfasst das Erkennen bestimmter Typen von Verkehr und das Bereitstellen einer bevorzugten Behandlung für diesen meistens verzögerungssensitiven Verkehr. Das Bandbreitenmanagement umfasst das Bereitstellen einer minimalen Bandbreitenzuordnung und einer maximalen Grenze für bestimmte Verkehrsströme derart, dass diese Ströme einer vorher vereinbarten Dienstebenenvereinbarung (SLA; service level agreement) entsprechen.

[0156] Die Verkehrspriorisierung ist wichtig für den verzögerungssensitiven Verkehr wie etwa Sprach- oder Videoverkehr. Dieser Typ von Verkehr hat eine kleine Latenzzeit, um sein Ziel ohne Performanzleistungsrückgang zu erreichen. Mit anderen Worten, verzögerungssensitiver Verkehr in einem Switch, der mit regulärem Datenverkehr überlastet ist, würde seine Zustellung zu dem Ziel enorm beeinträchtigen, was zu einer unterbrochenen Sprache oder einem unterbrochenen Video führen würde, das bei dem Client angezeigt wird.

[0157] Ein WLAN-Switch sollte die Einrichtungen zur Unterstützung der Verkehrspriorisierung derart aufweisen, dass der verzögerungssensitive Verkehr eine höhere Priorität genießen würde als reguläre Daten, wenn er in dem Switch verarbeitet wird. Es gibt zwei Lösungswege für die Verkehrspriorisierung: Achten der früheren Priorität oder Einrichten neuer Prioritätsrichtlinien.

[0158] Das Achten der Priorität, die mit dem verzögerungssensitiven Verkehr kommt, setzt voraus, dass der verzögerungssensitive Verkehr speziell markiert wäre, bevor er bei dem Switch ankommt. Die spezielle Markierung kann in der Form einer IEEE 802.1p Priorität kommen. In einer WLAN-Umgebung kann die Priorität eine IEEE 802.11e Priorität sein, erzeugt von dem drahtlosen Client, die der ZP als eine IEEE 802.1p Priorität enthält, wenn er die drahtlosen Rahmen in einen Ethernet-Rahmen umwandelt.

[0159] Durch das Achten der vorgekennzeichneten Priorität des Verkehrs nimmt der Switch an, dass die Clients und der ZP vertrauenswürdig sind, d.h. den mit einer Priorität gekennzeichneten Paketen wird getraut. Aber dieser Lösungsweg hat seinen Nachteil, einfach deswegen, weil der drahtlose Client das Vertrauen, das der Switch schenkt, missbrauchen kann. Er kann seinen gesamten Verkehr ungeachtet des Verkehrstyps mit einer höheren Priorität kennzeichnen. Dies würde zu einem Missbrauch der Priorisierungs-Richtlinien und somit zu einer alternativen Lösung führen.

[0160] Alternativ dazu kann ein WLAN-Switch seine eigenen Priorisierungs-Richtlinien einrichten. Eine Alternative zu dem Switching des Achtens der vorgekennzeichneten Prioritäten des Pakets liegt darin, dass man den Switch die Priorisierungs-Richtlinien einstellen lässt. Bei diesem Lösungsweg nimmt der Switch an, dass die Pakete ungekennzeichnet ankommen und richtet die Richtlinien unter Verwendung seiner Paketfilterungsfähigkeit ein. Der Switch sollte in der Lage sein, Pakete von VoIP- oder Streaming-Media-Anwendungen, die verzögerungssensitiv sind, zu erkennen, und diesen Paketen höhere Prioritäten zuzuweisen. Mit anderen Worten, der Switch betrachtet alle ankommenden Pakete von einem Qos-Standpunkt aus als nicht vertrauenswürdig.

[0161] In dem IEEE 802.11e Standard kann der Client auch einen Verkehrsstrom registrieren und bestimmte Qos-Hinweise für diesen Strom in dem drahtlosen Medium anfordern. In einem Netzwerk, dem nicht getraut wird, sollte dieser Strom mit den Qos-Richtlinien des WLAN derart querverwiesen werden, dass die Qos, die für den Strom angefordert wird, mit den Gesamt-WLAN-Richtlinien dieses Stroms konform geht. Der WLAN-Switch sollte in der Lage sein, beide Qos-Lösungswege zu unterstützen. Ob er nun die vormarkierte Paketpriorität achtet, seine eigenen Richtlinien einrichtet, oder eine Kombination aus beiden verwendet, sollte

durch den Netzwerkadministrator konfigurierbar sein.

[0162] Zur Unterstützung der Verkehrspriorisierung erwartet ein WLAN, dass Verkehr in dem Teil des Netzwerks, dem vertraut wird, unter Verwendung eines IEEE 802.1p Prioritäts-Tag priorisiert wird. Wenn der Switch der Qos-Markierung der Pakete nicht traut und seine eigenen Priorisierungs-Richtlinien einrichtet, kann die Paketfilterung nur bei nicht verschlüsselten Paketen durchgeführt werden. Mit anderen Worten, um den Inhalt der Pakete zu erfassen, um diese zu priorisieren, dürfen die Pakete nicht in einem IPSec- oder VPN-Tunnel eingekapselt sein.

[0163] In dem drahtlosen Schenkel des Verkehrs kann die Qos durch IEEE 802.11e freigegeben sein, die eine MAC-Ebenen-Weiterentwicklung von IEEE 802.11, 802.11b, 802.11a und 802.11g ist. Das WLAN kann einheitliche Qos-Richtlinien wirksam einsetzen, indem es 802.11e auf der drahtlosen Seite und 802.1p auf der verdrahteten Seite koordiniert. Jede Qos-Konfiguration kann zwischen dem WLAN-Switch und dem ZP derart kommuniziert werden, dass beide Vorrichtungen die gleiche Priorität und Bandbreitenbegrenzung für den gleichen Verkehrsstrom freigeben können. Damit drahtlose Clients die Qos in dem drahtlosen Medium nutzen können, müssen die Clients mit dem IEEE 802.11e Standard konform sein. Mit anderen Worten, er kann sich nicht konträr zu dem Standard verhalten. Zum Beispiel kann ein Verkehr in einer niedrigeren Verkehrskategorie (TC; traffic category) keine Priorität gegenüber einer höheren TC aufweisen.

[0164] IEEE 802.11e spezifiziert zwei Qos-Konfigurationen, nämlich die Enhanced Distributed Coordination Function (EDCF) und die Hybrid Coordination Function (HCF). Die EDCF ist eine Peer-to-Peer-Qos, bei der jeder Client, einschließlich des ZP, in dem drahtlosen Medium das Recht zur Übertragung hat; die Clients lösen den Konflikt selber, wenn eine Konkurrenz vorliegt; ein Paket mit einer höheren Priorität hat einfach eine bessere Chance, die Konfliktlösung zu gewinnen als ein Paket mit einer niedrigeren Priorität. Andererseits ist die HCF eine zentrale gesteuerte Qos-Konfiguration, wobei der ZP als Koordinator dient. Der ZP weist den anderen drahtlosen Stationen Übertragungsmöglichkeiten (TXOP; transmission opportunities) zu. Auf der Basis des IEEE 802.11e Standards und der beiden Qos-Konfigurationen wird eine vorgeschlagene Aufteilung der Verantwortlichkeiten zwischen dem Switch und dem ZP bei der Unterstützung der Verkehrspriorisierung in der nachfolgenden Tabelle beschrieben:

	EDCF		HCF	
	Rolle des ZP	Rolle des Switch	Rolle des ZP	Rolle des Switch
Upstream (stromaufwärts)	Alle drahtlosen Vorrichtungen, einschließlich des ZP, müssen mit dem IEEE 802.11e konform gehen, um Qos nutzen zu können	entfällt	ZP ist allein verantwortlich für die Zuweisung von TXOP für Clients	Richtet die Prioritätsrichtlinien unter Clients ein und instruiert ZP, diesen Richtlinien zu folgen
Downstream (stromabwärts)	Die ZPs priorisieren den Verkehr in verschiedene TC-Warteschlangen	Markiert Pakete mit IEEE 802.1p Prioritäts-Tags derart, dass dies ZP achten kann	Das interne Scheduling der ZPs stellt dem Verkehr mit höherer Priorität TXOP bereit	Markiert Pakete mit IEEE 802.1p Priorität derart, dass dies ZP achten kann.

TABELLE 2

[0165] Für die Verkehrspriorisierung muss die Filterungsmaschine des WLAN-Switch in der Lage sein, unterschiedliche Filter für jeden einzelnen Client zu schaffen. Das Performanzlimit bei der Bereitstellung der Qos für Verkehrsströme basiert auf der Größe der Filterungsmaschine, d.h. der Anzahl von Filtern, die erlaubt ist. Wenn der ZP ebenfalls in der Lage ist, eine Verkehrsklassifizierung durchzuführen, wie von der IEEE 802.11e vorgeschlagen, aber nicht spezifiziert worden ist, dann wird die Anzahl von Verkehrsströmen, die die Verkehrspriorisierung nutzen kann, durch die geringere Größe der WLAN-Switch-Filterungsmaschine und den ZP-Klassifizierer bestimmt.

[0166] Ein anderes Qos-Merkmal, dass ein WLAN anbieten sollte, ist das Bandbreitenmanagement. Das Bandbreitenmanagement umfasst das Anbieten einer minimalen Bandbreite und/oder einer maximalen Bandbreite für jeden Verkehrsstrom. In diesem Kontext ist ein Verkehrsstrom aller Wahrscheinlichkeit nach mit einer bestimmten drahtlosen Client-Vorrichtung assoziiert.

[0167] Bei einem maximalen Übertragungsratenlimit sollte die gesamte Bandbreite für alle potentiellen Clients nicht die physikalische Grenze der drahtlosen Übertragung überschreiten. Für IEEE 802.11b ist dies 11 Mbps, für IEEE 802.11a oder 802.11g ist dies 54 Mbps. Wenn man annimmt, dass alle Benutzer gleich sind, sollte in einem drahtlosen ZP für 8 Benutzer, der IEEE 802.11a unterstützt, jeder Benutzer in der idealen Bedingung bezüglich der Übertragungsrate auf etwa 6 Mbps begrenzt sein, während in IEEE 802.11b jeder Benutzer in der idealen Bedingung bezüglich der Übertragungsrate auf etwa 1 Mbps begrenzt sein sollte. Die Übertragungsratenbegrenzung ist notwendig, um zu gewährleisten, dass jeder Benutzer nicht die gesamte Bandbreite in Beschlag nimmt und eine Verhungerungssituation schafft. Eine Minimumübertragungsratengarantie gewährleistet, dass jeder drahtlose Client eine gewisse minimale Bandbreite besitzt, um Daten zu übertragen.

[0168] In einem WLAN kann das Bandbreitenmanagement sowohl in dem ZP als auch in dem Switch ausgeführt werden. Der Switch kann die Übertragungsratenbegrenzung eines Downstream-Verkehrs (z.B. Herunterladen von Peer-to-Peer-Anwendungsdateien) eines bestimmten Stroms durchsetzen, während der Switch und der ZP einander koordinieren müssen, um eine minimale Bandbreitenzuordnung für diesen Strom zu gewährleisten. Für eine minimale garantierte Bandbreite und Übertragungsratenbegrenzung des Upstream-Verkehrs muss dies erst bei dem ZP ausgeführt werden.

[0169] Die zweite Schnittstellenanforderung bei der Verkehrspriorisierung trifft auch hier zu. Um das Bandbreitenmanagement nutzen zu können, muss der Verkehrsstrom identifiziert werden. Wenn der Strom durch eine IP-Header-Information identifiziert wird, dann kann das Paket nicht in einem IPSec-/VPN-Tunnel eingekapselt werden. Außerdem müssen die drahtlosen Client zu dem IEEE 802.11e Standard konform sein, damit das Bandbreitenmanagement wirken kann.

[0170] Wieder wird eine vorgeschlagene Aufteilung von Verantwortlichkeiten zwischen dem Switch und dem ZP bei der Unterstützung der Verkehrspriorisierung auf der Basis des IEEE 801.11e Standards und der Qos-Konfiguration von HCF in der nachfolgenden Tabelle beschrieben. Die Qos-Konfiguration von EDCF ist aufgrund ihrer Peer-to-Peer-Natur nicht in der Lage, das Bandbreitenmanagement zu unterstützen.

	EDCF		HCF	
	Rolle des ZP	Rolle des Switch	Rolle des ZP	Rolle des Switch
Upstream (stromaufwärts)	entfällt	entfällt	ZP ist allein verantwortlich für die Zuweisung von TXOP zu Clients, im Hinblick auf # von TXOP und Dauer, um die Bandbreitenanforderungen zu erfüllen	Richtet die Bandbreitenrichtlinien unter Clients ein und instruiert ZP, diesen Richtlinien zu folgen
Downstream (stromabwärts)	entfällt	entfällt	Der interne Klassifizierer und das interne Scheduling des ZP spezifizieren # von TXOP und die Dauer für ihren eigenen Downstream-Verkehr, um die Bandbreitenanforderungen zu erfüllen	Verwendet Übertragungsratenbegrenzung zur Regelung der Downstream-Bandbreite

TABELLE 3

[0171] Die Filterungsmaschine des WLAN-Switch muss in der Lage sein, unterschiedliche Filter für jeden einzelnen Client zu schaffen, um die Bandbreitenbegrenzung zu unterstützen. Das Performanzlimit bei der Bereitstellung des Bandbreitenmanagements für Client-Stationen basiert auf der Größe der Filterungsmaschine, d.h. der Anzahl von zugelassenen Filtern.

MESSAGING-PROTOKOLL

[0172] Ein Messaging-Protokoll (MP) ist ein proprietäres Protokoll, das für die Kommunikation zwischen normkonformen drahtlosen Netzwerkvorrichtungen gedacht ist. Die Beschreibung des MP hier konzentriert sich auf die MP-Interaktionen zwischen dem ZP und dem WLAN-Switch. Die Informationen, die zwischen diesen beiden Vorrichtungen ausgetauscht werden, umfassen die Konfigurations- und Statusinformationen der Einheit sowie auch die Client-Sitzungsinformationen. Derartige Informationen werden ausgetauscht, um die sechs Merkmale in dem WLAN zu ermöglichen, die in den vorhergehenden Abschnitten erwähnt wurden.

[0173] Das MP läuft über die TCP- oder UDP-Protokolle, die die allgemein bekannte Portanzahl verwenden, die in dem Rahmen eines Vorrichtungskommunikationsprotokolls (DCP; device communication protocol) spezifiziert sind. Unter dem DCP-Schirm gibt es mehrere Unterprotokolle, die für den Zweck der Kommunikationen in anderen Broadcom-Produkten definiert sind. Das MP ist nur ein neues Protokoll unter dem DCP für drahtlose Vorrichtungen und WLAN-Vorrichtungen.

[0174] Das MP wird für die Kommunikation von Informationen zwischen WLAN-Vorrichtungen verwendet. Es gibt fünf Kategorien von Nachrichten in dem MP, die wie folgt aufgelistet sind. Die ZP-Zustandsnachrichten vom ZP zu einem Switch oder einem ZP zeigen die ZP-Kapazität, die Bandbreitenzuordnung, # angeschlossene Clients, Signalstärke etc. an. Die ZP-Konfigurations-Nachrichten vom Switch zum ZP zur Konfigurierung des ZP, um einen Client zu erfassen, einschließlich der IEEE 802.11e Qos, Sicherheitsinformationen, etc.. Die Switch-Zustandsnachrichten von Switch zu Switch, die eine Assoziierung eines Switch mit Clients anzeigen, einschließlich der Sitzungsinformationen des Client, der Zugriffskontrolle, der Qos-Parameter, etc.. Die Switch-Konfigurations-Nachrichten von Switch zu Switch zur Konfigurierung eines WLAN-Switchs, um einen Client zu erfassen, einschließlich Zugriffskontrolle, Qos-Konfiguration, etc.. Die Client-Zustandsnachrichten vom ZP zum Switch sind Nachrichten, die Informationen eines Client anzeigen, einschließlich der Identifikation, der assoziierten MAC-Adresse, des Sitzungsstatus, der Verbindungsposition, etc..

[0175] In jeder Nachrichtenkategorie weist die Nachricht drei Nachrichten-Untertypen auf Anforderung, Daten und Bestätigung (ack). Diese Untertypen repräsentieren die Anforderung von Daten, die Übertragung der Daten selber, und eine Bestätigung des Empfangs der Daten. In einigen Fällen besteht der Austausch aus einer Anforderung und einer Antwort, während in einigen anderen Fällen die Daten freiwillig gesendet werden, woraufhin eine Bestätigung folgen sollte.

ANWENDUNGEN

[0176] Dieser Abschnitt widmet sich einigen Anwendungsszenarien in den drahtlosen Unternehmens-LANs gemäß mehreren Ausführungsbeispielen der vorliegenden Erfindung. Bei diesen Anwendungen werden die Sequenz der Ereignisse in verschiedenen Operationen wie zum Beispiel Anmeldung, Abmeldung, Weiterreichung, etc. beschrieben. Diese Anwendungen repräsentieren nicht alle der Anwendungen der vorliegenden Erfindung, aber sie sind repräsentativ für die vielen Anwendungsausführungsbeispiele, die von der vorliegenden Erfindung umfasst werden.

[0177] Zwei weit verbreitete Anwendungen in der drahtlosen LAN-Umgebung sind die reguläre Datenverarbeitung mit einem drahtlosen Laptop und ein drahtloses IP-Telefon. Sie werden in dem Rest dieses Abschnitts genauer beschrieben.

[0178] Das drahtlose Unternehmens-LAN wurde dafür geplant, für eine drahtlose Verbindung von Laptop-Computern mit dem LAN verwendet zu werden, so dass der drahtlose Client auf Dateien und Dienste in dem Unternehmens-LAN sowie auch auf das öffentliche Internet zugreifen kann. Mit diesem Ziel sind Verbindungen zu Laptop-Computern zunächst die wichtigste Anwendung in einer drahtlosen LAN-Umgebung. Die Verwendungsszenarien bei der Laptop-Datenverarbeitung werden in den folgenden Unterabschnitten beschrieben.

[0179] Das erste Szenario ist eine Sitzungsinitiierung oder eine Client-Anmeldung bei dem drahtlosen LAN. Vor dieser Operation wird angenommen, dass der ZP Beacon-Frames zu allen drahtlosen Vorrichtungen in seiner Nachbarschaft rundsenden wird, um seine Anwesenheit und seine MAC-Adresse bekannt zu geben. Somit weiß jede Client-Vorrichtung, die versucht, sich anzuschließen, Wohin sie die Anforderung senden muss.

[0180] Eine Liste von Ereignissen ist unten aufgeführt. Clients senden eine Verbindungsanforderung zu dem ZP, und der ZP stellt fest, dass dies ein neuer Client ist und sendet ihm eine Anmeldeaufforderung. Der Client antwortet mit der Identität, und der ZP sendet die Client-Identität zu dem Authentifikationsserver. Der Authentifikationsserver antwortet mit einer Einmalkennwort-(OTP; one-time password)-Abfrage und der ZP sendet die OTP-Abfrage zu dem Client. Der Client antwortet dem ZP mit einem Kennwort, der ZP leitet das Client-Kennwort zu dem Authentifikationsserver, und bei einer erfolgreichen Authentifikation antwortet der Authentifikationsserver mit einem Verschlüsselungsschlüssel. Der ZP leitet den Verschlüsselungsschlüssel zu dem Client, der ZP leitet auch den Client-Status (Identität, MAC-Adresse, etc.) zu dem WLAN-Switch, und der WLAN-Switch aktiviert eine zusätzliche Zugriffskontrolle für den Client, z.B. ein Teilnetz, Zeitdauer, Position, Qos, etc..

[0181] Die Sequenz von Nachrichten, die zwischen Client, ZP, Authentifikationsserver und WLAN-Switch ausgetauscht werden, ist in dem Nachrichtensequenzdiagramm von [Fig. 9](#) veranschaulicht. In dieser Austauschsequenz gibt es zwei Typen von Nachrichten. Das Extensible Authentication Protocol (EAP) von IEEE 802.1x für die Sitzungsauthentifizierung, und das Messaging-Protokoll (MP) für die Kommunikation der Sitzungsinformationen zwischen dem Broadcom-befähigten ZP und dem Broadcom-befähigten WLAN-Switch.

[0182] Die Sitzung kann durch die Client-Abmeldung, durch Sitzungsleerlauf, durch Zugriffsrichtlinien und durch explizite Aktion durch den Netzwerkadministrator beendet werden. Die Sequenz der Ereignisse bei einer Client-Abmeldung ist wie folgt aufgelistet. Der Client sendet eine Abmeldeanforderung zu dem ZP und der ZP sendet eine Bestätigung. Der ZP sendet die Abmeldeanforderung zu dem Authentifikationsserver, der Authentifikationsserver bestätigt, und der ZP sendet den Client-Status (Abmelden) zu dem WLAN-Switch. Der WLAN-Switch sendet eine Bestätigung und der WLAN-Switch beseitigt Sitzungsinformationen, die für diesen Client eingerichtet worden sind. Die Sequenz von Nachrichten, die zwischen Client, ZP, Authentifikationsserver und WLAN-Switch ausgetauscht werden, sind in dem Nachrichtensequenzdiagramm veranschaulicht, das in [Fig. 10](#) bereitgestellt ist.

[0183] Die Weiterreichung ist eine Pseudo-Sitzungsinitiierung/-beendigung, aber ohne die Notwendigkeit einer Authentifikation. Die Weiterreichung wird durch die Erfassung eines starken neuen Signals und den Leis-

tungsrückgang des alten Signals ausgelöst, zusätzlich zu dem Empfangen des Rundsende-Beacon des neuen ZP. In dem Unternehmens-WLAN gibt es zwei Typen von Weiterreichung, nämlich die Weiterreichung zwischen zwei ZPs, die mit dem gleichen WLAN-Switch verbunden sind, und die zwischen zwei ZPs, die mit unterschiedlichen WLAN-Switches verbunden sind. Das letztere Szenario ist ein wenig komplizierter, weil es das Übertragen von Informationen zwischen den beiden Switches umfasst.

[0184] Für die Weiterreichung in dem gleichen Switch ist die Sequenz der Ereignisse unten wie folgt aufgelistet. Der Client sendet eine Anforderung an den alten ZP zur Disassoziiierung und an den neuen ZP zur Reassoziiierung. Der neue ZP sendet eine Bewegungsbenachrichtigungsnachricht an den alten ZP und der alte ZP antwortet mit einer Bewegungsantwort mit einem Sitzungskontext. Der alte ZP sendet auch die Sicherheitsdaten (z.B. den Verschlüsselungsschlüssel) des Client zu dem neuen ZP und der ZP bestätigt. Der neue ZP sendet Weiterreichungs-Informationen zu dem WLAN-Switch und der WLAN-Switch wird die Switching-Informationen von einem Port (der mit dem alten ZP verbunden ist) zu einem anderen (der mit dem neuen ZP verbunden ist) transferieren. Das Nachrichtensequenzdiagramm für die Weiterreichung im gleichen Switch zwischen dem alten ZP, dem neuen ZP, dem Client und dem WLAN-Switch ist in [Fig. 11](#) veranschaulicht.

[0185] Für die Weiterreichung quer durch Switches wird es einfach ein paar zusätzliche Aktivitäten zwischen den beiden Switches geben. Diese sind wie folgt aufgelistet. Der Client sendet eine Anforderung an den alten ZP zur Disassoziiierung und an den neuen ZP zur Assoziiierung, und der neue ZP sendet eine Bewegungsbenachrichtigungsnachricht an den alten ZP. Der alte ZP antwortet mit einer Bewegungsantwort mit einem Sitzungskontext, und der alte ZP sendet auch die Sicherheitsdaten (z.B. den Verschlüsselungsschlüssel) des Client zu dem neuen ZP. Der ZP bestätigt und der neue ZP sendet den Client-Status (Weiterreichung) an den neuen WLAN-Switch. Der neue WLAN-Switch fordert die Switch-Konfiguration für den Client von dem alten WLAN-Switch an, der alte WLAN-Switch wird mit der Switch-Konfiguration antworten. Der neue WLAN-Switch wird die Switching-Intelligenz (Qos, Zugriffsrichtlinien, etc.) für den Client freigeben. Die Nachrichtenaustauschsequenz zwischen dem Client, dem alten ZP, dem neuen ZP, dem alten WLAN-Switch und dem neuen WLAN-Switch ist in [Fig. 12](#) veranschaulicht.

[0186] Die drahtlose IP-Telefonanwendung ist der drahtlosen Laptop-Datenverarbeitungsanwendung in dem Sinne ähnlich, dass sie einfach eine spezielle Anwendung in der drahtlosen Datenverarbeitung ist, bei der eine spezielle Vorrichtung verwendet wird. Aber es gibt keine Unterschiede in den Operationsszenarien, die einen separaten Abschnitt zur Besprechung rechtfertigen.

[0187] Ein Hauptunterschied liegt darin, dass dann, wenn die drahtlosen IP-Telefone die Verwendung von Funktelefonen kopieren sollen, eine Funktelefonkonvention geachtet werden muss, nämlich dass dann, wenn das Telefon eingeschaltet wird, es bereit zum Wählen ist; keine Anmeldung und kein Kennwort werden benötigt. Mit anderen Worten, jegliche Authentifikation muss selbstverständlich auf der Basis der MAC-Adresse durchgeführt werden. Eine andere Imitation des Funktelefons ist diejenige, dass die gesamte Nummer gefolgt von einer SENDE-Taste gewählt wird. Somit benötigt das Telefon selber keinen ausgehängten Zustand/Wählton-Zustand, wie dies bei verdrahteten IP-Telefonen zu sehen ist.

[0188] Ein weiterer Unterschied liegt darin, dass das drahtlose IP-Telefon öfter von Zone zu Zone wandert, ob das Telefon nun benutzt wird oder ob es einfach nur in Wartestellung ist. Ein Telefon in Wartestellung ist einfach nur eine Live-Sitzung, bei der das Telefon auf einen ankommenden Anruf wartet, während bei einem Telefon, das gerade benutzt wird, eine Telefongespräch läuft. In beiden Fällen entspricht das Telefon einer aktiven Sitzung des drahtlosen Laptop-Computers. Während ein Telefon, das zwar eingeschaltet, aber nicht verwendet wird, mit einer geringen Verzögerung bei der Weiterreichung behandelt werden kann, muss eine gerade stattfindende Konversation nahtlos mit einer minimalen Verzögerung weitergereicht werden.

[0189] Neben den normalen Vorrichtungen in einem WLAN muss ein WLAN, das ein IP-Telefon unterstützt, auch ein IP-Telefon-Gateway (IPG; IP phone gateway) aufweisen, um Anrufe vermitteln zu können. Das IPG kann ein Server oder eine IP-Wählanlage (IP PBX) in dem LAN sein. Es wird die Schnittstelle benötigt, um den Anruf zu verbinden, wenn das Anrufziel in dem öffentlichen Fernsprechwahlnetz (PSTN; public switched telephone network) liegt.

[0190] Dieser Abschnitt widmet sich zwei Operationsszenarien, nämlich der Anrufverbindung und der Anrufbeendigung. In beiden Fällen kann jede Partei die Verbindung oder die Beendigung initiieren. Der Typ von Station an dem anderen Ende des Anrufs ist irrelevant. Es kann eine Nummer im öffentlichen Fernsprechwahlnetz, eine IP-Telefonstation innerhalb des Unternehmens, ein IP-Telefon außerhalb des Unternehmens, ein älteres Telefon innerhalb der Unternehmens-Wählanlage, und schließlich ein anderes IP-Telefon in dem gleichen

WLAN sein.

[0191] Es gibt zwei einfache Voraussetzungen bezüglich der Form der Nummern, die gewählt werden: 1) wenn die Nummer eine interne Nummer ist, entweder eine Nebenstelle einer älteren Wählanlage, ein internes IP-Telefon oder ein internes drahtloses IP-Telefon, dann wird eine Nummer mit 5 Ziffern benutzt. Die fünfstellige Nummer beginnt mit einem vorbestimmten Präfix, gefolgt von der 4-stelligen Durchwahl. 2) Wenn die Nummer eine externe Nummer ist, entweder eine Nummer in dem öffentlichen Fernsprechwahlnetz oder eine Nummer in einem externen IP-Telefonnetzwerk, dann wird das E.164-Nummernformat verwendet. Die E.164-Nummer kann eine 10-stellige Nummer, die mit der Ortskennziffer beginnt, oder eine 7-stellige Nummer ohne Ortskennziffer sein. In beiden Fällen geht der Nummer ein Hinauswahl-Präfix voraus, welches die Nummer "9" ist, wie dies in den meisten Unternehmens-Wählanlagen konfiguriert ist. Die verschiedenen Operationsszenarien werden in den folgenden Abschnitten besprochen.

[0192] Das erste Szenario ist die Sitzungsinitiierung für ein drahtloses IP-Telefon zu dem drahtlosen LAN. Die gleiche Voraussetzung wie für die drahtlose Datenverarbeitung gilt auch hier, nämlich dass der ZP Beacon-Frames hinaus zu allen drahtlosen Vorrichtungen in seiner Nachbarschaft rundsenden wird, um sein Vorhandensein und seine MAC-Adresse zu verkünden. Bei der Sitzungsinitiierung kann ein Kennwort benötigt werden oder auch nicht, wenn das Telefon eingeschaltet wird.

[0193] Die Liste der Ereignisse ist wie folgt aufgelistet. Die Ereignisse, die kursiv aufgelistet sind, sind optional, da sie einem Authentifikationsprozess entsprechen, der ein Kennwort benötigt. Der Client sendet eine Verbindungsanforderung zu dem ZP und der ZP bestimmt diesen als einen neuen IP-Telefon-Client und sendet eine Anforderung an das IP-Telefon bezüglich der Identität. Das IP-Telefon antwortet mit der Identität (Telefonnummer) und der ZP sendet die Client-Identität zu dem Authentifikationsserver. Der Authentifikationsserver antwortet mit einer Einmal-Kennwort(OTP; one-time password)-Abfrage und der ZP sendet die OTP Abfrage zu dem IP-Telefon. Das IP-Telefon antwortet dem ZP mit dem Kennwort, und der ZP leitet das IP-Telefon-Kennwort zu dem Authentifikationsserver. Bei einer erfolgreichen Authentifikation antwortet der Authentifikationsserver mit einem Verschlüsselungsschlüssel, der ZP übermittelt den Verschlüsselungsschlüssel dem Client, und der ZP übermittelt auch den Client-Zustand (Identität, MAC-Adresse, etc.) zu dem WLAN-Switch. Die Nachrichtenaustauschsequenz bei der Sitzungsinitiierung ist dann, wenn ein Kennwort benötigt wird, identisch zu dem Diagramm, das in [Fig. 12](#) veranschaulicht ist. Wenn kein Kennwort benötigt wird, werden die Pfeile, die der OTP-Abfrage und ihrer Antwort entsprechen, einfach entfernt.

[0194] Dieser Abschnitt widmet sich einem Anrufinitiierungsszenario. Angenommen, das VoIP-Protokoll ist ein standardbasiertes Protokoll, dann sind alle Nachrichten, die in diesem Abschnitt ausgetauscht werden, Schicht-5-VoIP-Protokoll-Nachrichten über TCP/IP oder UDP/IP. Das Protokoll kann auf H.323, H.248 (MGCP), SIP, etc. beschränkt sein, muss aber nicht. Bei diesem Szenario initiiert das drahtlose IP-Telefon (WIPP; wireless IP phone) selber den Anruf.

[0195] Die Liste der Ereignisse wird wie folgt aufgelistet. Das WIPP sendet eine Anruf-Aufbau-Anforderung (Verbindungsversuch mit einer internen Nebenstellenummer oder E.164-Nummer) zu dem IPG, und das IPG bestimmt, ob die Nummer eine interne IP-Telefonnummer oder eine ältere Nummer ist, dann ordnet es die Nummer entweder einer IP-Adresse oder einer älteren Telefonnummer zu. Das IPG sendet die Verbindungsanforderung zu der Zielstation (DSTA; destination station), das IPG sendet den Verbindungsstatus zu dem WIPP und das WIPP erzeugt einen Rufton. Das IPG empfängt das Aushänge-Signal von dem DSTA, das IPG handelt Ressourcen mit dem WIPP aus, und wenn die Ressourcenaushandlung fertig ist, startet das Gespräch. Der WLAN-Switch hört alle VoIP-Protokollnachrichten ab, der WLAN-Switch aktiviert die Switching-Qos für die Konversation, das WLAN übermittelt die Anrufinformationen zum ZP und der ZP aktiviert die IEEE 802.11e Qos für diesen Anruf. Die Nachrichtenaustauschsequenz in diesem Szenario ist in der [Fig. 13](#) veranschaulicht.

[0196] Dieser Abschnitt widmet sich einem Anrufbeendigungsszenario. Wenn man wieder voraussetzt, dass das drahtlose IP-Telefon selber den Anruf initiiert, werden die Operationsszenarien wie folgt beschrieben. Das WIPP sendet eine Anruftrennanforderung an das IPG, und das IPG sendet die Verbindungsanforderung zu der Zielstation (DSTA). Das IPG sendet die Trennanforderung zu der DSTA, und das IPG sendet eine Trenn-Bestätigung zu dem WIPP. Das IPG gibt Ressourcen für die Anruffsitzung frei, der WLAN-Switch hört alle VoIP-Protokollnachrichten ab, und der WLAN-Switch gibt Ressourcen (QoS-Aktivierung) für diese Anruffsitzung frei. Das WLAN übermittelt die Anrufinformationen zu dem ZP, der ZP gibt Ressourcen (802.11e Qos) für diese Anruffsitzung frei, und das WIPP kehrt zu einem Einhängenzustand zurück. Die Nachrichtenaustauschsequenz ist in [Fig. 14](#) veranschaulicht.

[0197] Die oben diskutierte Konfiguration der Erfindung ist in einem Ausführungsbeispiel auf einem Halbleitersubstrat wie z.B. Silizium mit geeigneten Halbleiterherstellungstechniken und auf der Basis eines Schaltungs-Layouts verwirklicht, wie dies auf der Grundlage der oben diskutierten Ausführungsbeispiele den Fachleuten auf diesem Gebiet offenkundig wäre. Ein Fachmann auf dem Gebiet in Bezug auf Halbleiterdesign und -herstellung wäre in der Lage, die verschiedenen Module, Schnittstellen und Komponenten etc. der vorliegenden Erfindung auf der Grundlage der oben diskutierten Architekturbeschreibung auf einem einzigen Halbleitersubstrat zu implementieren. Es läge ebenfalls im Schutzbereich der Erfindung, die offenbarten Elemente der Erfindung in diskreten elektronischen Bauteilen zu implementieren, wodurch man die funktionalen Aspekte der Erfindung ausnutzen könnte, ohne die Vorteile durch die Nutzung eines einzigen Halbleitersubstrats zu maximieren. Außerdem kann die vorliegende Erfindung vollständig oder teilweise durch Software implementiert werden.

[0198] Des Weiteren kann die Erfindung auf viele Typen von Netzwerkdaten übertragen werden, obwohl der Begriff Paket in der Beschreibung der vorliegenden Erfindung verwendet worden ist. Für die Zwecke der vorliegenden Erfindung umfasst der Begriff 'Paket' Paket, Zelle, Rahmen, Datagramm, Brückenprotokolladateneinheit, Paketdaten und alle Äquivalente davon.

[0199] Um die Grenzen der Erfindung zu bestimmen, soll Bezug auf die angehängten Ansprüche genommen werden.

Patentansprüche

1. Verfahren zur Kontrolle eines Datenflusses in einem drahtlosen lokalen Unternehmens-Netzwerk (**101**), das einen drahtlosen Zugriff auf das drahtlose Netzwerk (**101**) durch drahtlose Vorrichtungen (**120–129**) vorsieht, wobei das Verfahren folgendes aufweist:

Empfangen von Daten von einer drahtlosen Vorrichtung (**120–129**) mittels einer Netzwerkvorrichtung durch einen Zugangspunkt (**111–115**) einer Vielzahl von Zugangspunkten (**111–115**) in Kommunikation mit der Netzwerkvorrichtung, wobei eine Client-Identifizierung für die drahtlose Vorrichtung (**120–129**) angezeigt wird;

Weiterleiten der Client-Identifizierung zu einem Authentifikationsserver (**104**);

Vermitteln der Authentifizierung der drahtlosen Vorrichtung (**120–129**) mit dem Authentifikationsserver (**104**);

dadurch gekennzeichnet, dass das Verfahren des Weiteren folgendes aufweist:

Auswerten von Datenpaketen, die von Abschnitten des drahtlosen Netzwerks (**101**) und von der Vielzahl von Zugangspunkten (**111–115**) empfangen werden; und

Übermitteln der empfangenen Datenpakete zu Abschnitten des drahtlosen Netzwerks (**101**) und zu der Vielzahl von Zugangspunkten (**111–115**) auf der Grundlage der Auswertung der empfangenen Datenpakete;

wobei die Netzwerkvorrichtung periodisch einen Zustand der drahtlosen Vorrichtung (**120–129**) von dem Zugangspunkt (**111–115**) abfragt; und

wobei die Zugangspunkte (**111–115**) und die Netzwerkvorrichtung Informationen bezüglich der Konfiguration, des Zustands und der Client-Sitzungs-Zustände der Zugangspunkte (**111–115**) durch ein Messaging-Protokoll austauschen.

2. Verfahren nach Anspruch 1, wobei der Schritt des Auswertens von Datenpaketen das Filtern der empfangenen Datenpakete derart umfasst, dass die gefilterten Datenpakete fallengelassen werden können, um eine Wirksamkeit eines Dienstverweigerungsangriffs zu begrenzen.

3. Verfahren nach Anspruch 1, wobei der Schritt des Vermittelns der Authentifizierung der drahtlosen Vorrichtung (**120–129**) das Einschränken des Zugriffs auf das drahtlose Netzwerk (**101**) durch die drahtlose Vorrichtung (**120–129**) auf der Grundlage einer Benutzerkategorie aufweist, die aus der Client-Identifizierung ermittelt wird.

4. Verfahren nach Anspruch 3, wobei der Schritt des Einschränkens des Zugriffs auf das drahtlose Netzwerk (**101**) auf einem Typ von Vorrichtung basiert, zu dem die drahtlose Vorrichtung (**120–129**) gehört.

5. Verfahren nach Anspruch 1, wobei der Schritt des Vermittelns der Authentifizierung der drahtlosen Vorrichtung (**120–129**) das Einschränken des Zugriff auf das drahtlose Netzwerk (**101**) durch die drahtlose Vorrichtung (**120–129**) auf der Grundlage einer Stunde und eines Tages der Woche aufweist, in denen die Daten von der drahtlosen Vorrichtung (**120–129**) empfangen wurden.

6. Netzwerkvorrichtung zur Kontrolle eines Datenflusses in einem drahtlosen lokalen Unternehmens-Netzwerk (**101**), das den drahtlosen Zugriff auf das drahtlose Netzwerk (**101**) durch drahtlose Vorrichtungen

(120–129) vorsieht, wobei die Netzwerkvorrichtung folgendes aufweist:
 Empfangsmittel zum Empfangen von Daten von einer drahtlosen Vorrichtung (120–129) mittels der Netzwerkvorrichtung durch einen Zugangspunkt (111–115) einer Vielzahl von Zugangspunkten (111–115) in Kommunikation mit der Netzwerkvorrichtung, wobei eine Client-Identifizierung für die drahtlose Vorrichtung (120–129) angezeigt wird;
 Weiterleitungsmittel zum Weiterleiten der Client-Identifizierung zu einem Authentifikationsserver (104);
 Vermittlungsmittel zum Vermitteln der Authentifizierung der drahtlosen Vorrichtung (120–129) mit dem Authentifikationsserver (104);
 dadurch gekennzeichnet, dass die Netzwerkvorrichtung des Weiteren folgendes aufweist:
 Auswertemittel zum Auswerten von Datenpaketen, die von Abschnitten des drahtlosen Netzwerks (101) und von der Vielzahl von Zugangspunkten (111–115) empfangen werden; und
 Übermittlungsmittel zum Übermitteln der empfangenen Datenpakete zu Abschnitten des drahtlosen Netzwerkes (101) und zu der Vielzahl von Zugangspunkten (111–115) auf der Grundlage der Auswertung der empfangenen Datenpakete;
 wobei die Netzwerkvorrichtung so konfiguriert ist, dass sie periodisch einen Zustand der drahtlosen Vorrichtung (120–129) von dem Zugangspunkt (111–115) abfragt; und
 wobei die Zugangspunkte (111–115) und die Netzwerkvorrichtung Informationen bezüglich der Konfiguration, des Zustands und der Client-Sitzungs-Zustände der Zugangspunkte (111–115) durch ein Messaging-Protokoll austauschen.

7. Netzwerkvorrichtung nach Anspruch 6, wobei die Auswertemittel Filtermittel zum Filtern der empfangenen Datenpakete derart aufweisen, dass die gefilterten Datenpakete fallengelassen werden können, um eine Wirksamkeit eines Dienstverweigerungsangriffs zu begrenzen.

8. Netzwerkvorrichtung nach Anspruch 6, wobei die Vermittlungsmittel Beschränkungsmittel zum Beschränken des Zugriffs auf das drahtlose Netzwerk (101) durch die drahtlose Vorrichtung (120–129) auf der Grundlage einer Benutzerkategorie aufweisen, die aus der Client-Identifizierung ermittelt wird.

9. Netzwerkvorrichtung nach Anspruch 8, wobei die Beschränkungsmittel so konfiguriert sind, dass sie den Zugriff auf der Grundlage eines Typs von Vorrichtung beschränken, zu dem die drahtlose Vorrichtung (120–129) gehört.

10. Netzwerkvorrichtung nach Anspruch 6, wobei die Vermittlungsmittel Beschränkungsmittel zum Beschränken des Zugriffs auf das drahtlose Netzwerk (101) durch die drahtlose Vorrichtung (120–129) auf der Grundlage einer Stunde und eines Tages der Woche aufweisen, in denen die Daten von der drahtlosen Vorrichtung (120–129) empfangen wurden.

Es folgen 8 Blatt Zeichnungen

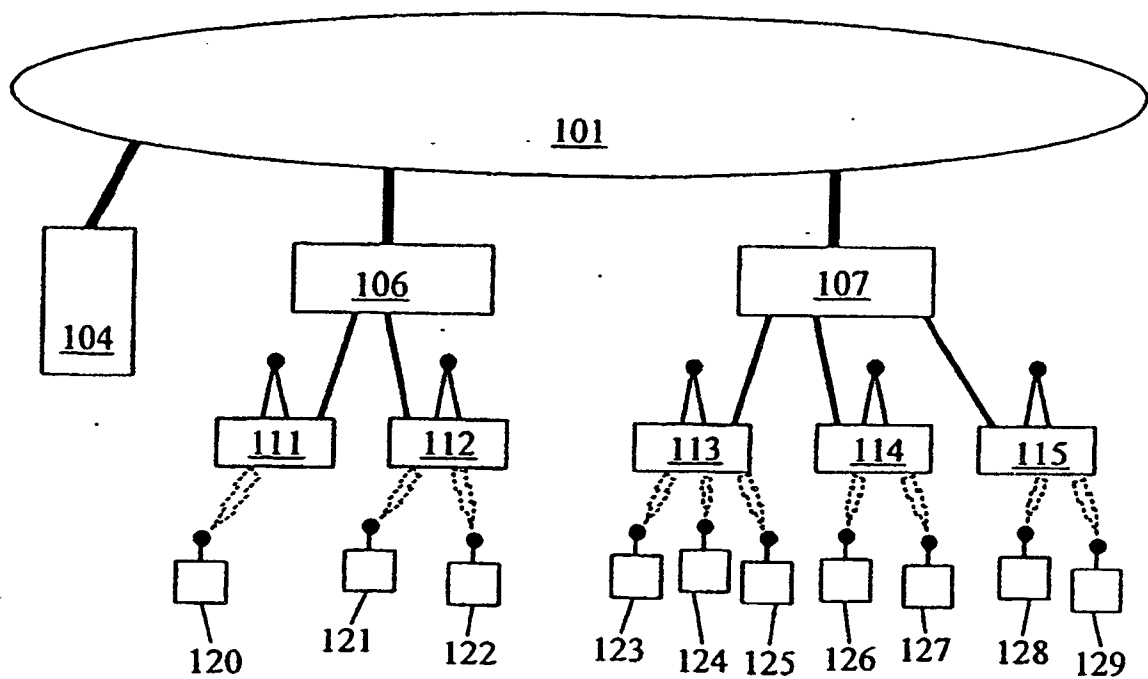


Fig. 1

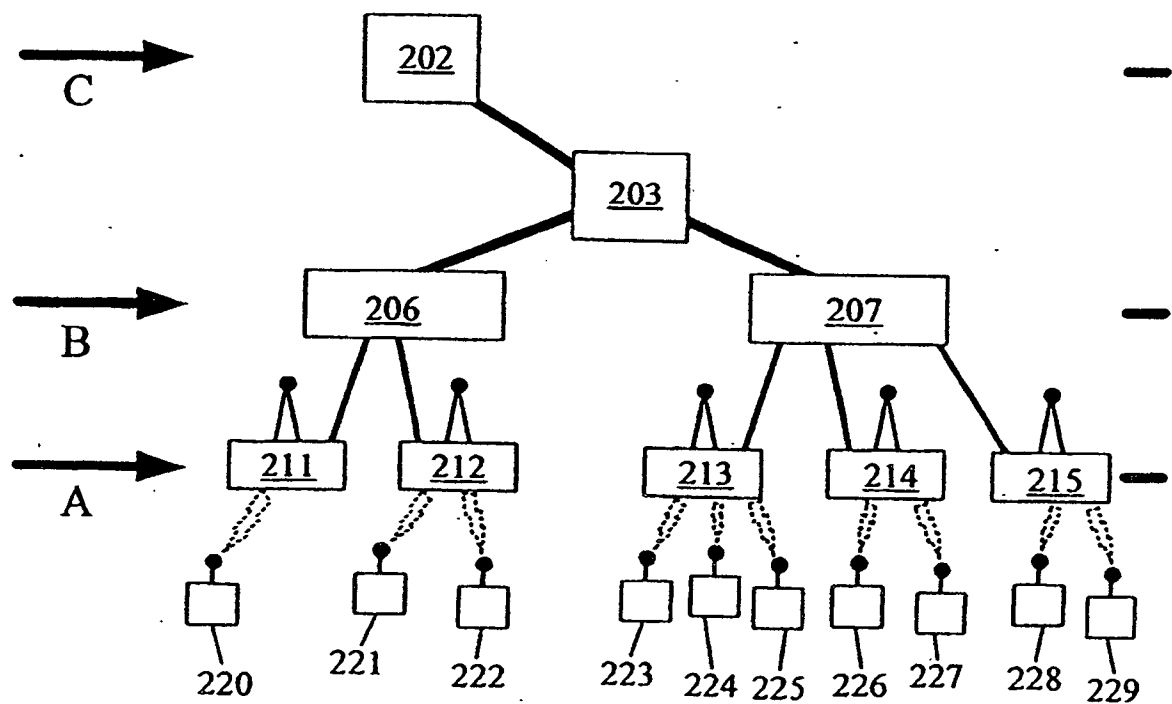


Fig. 2

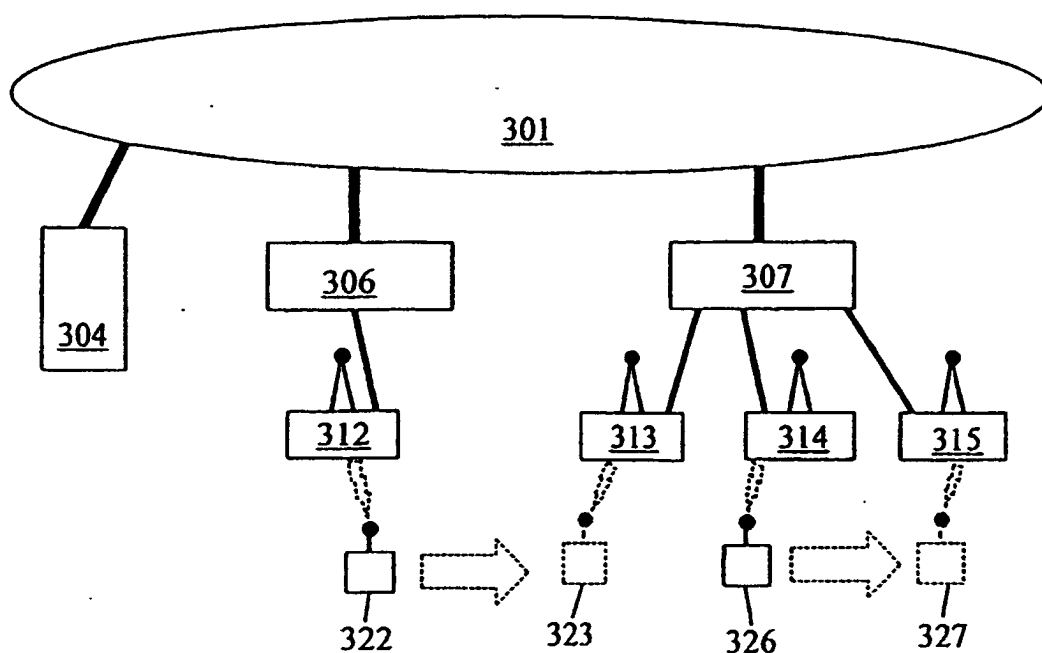


Fig. 3

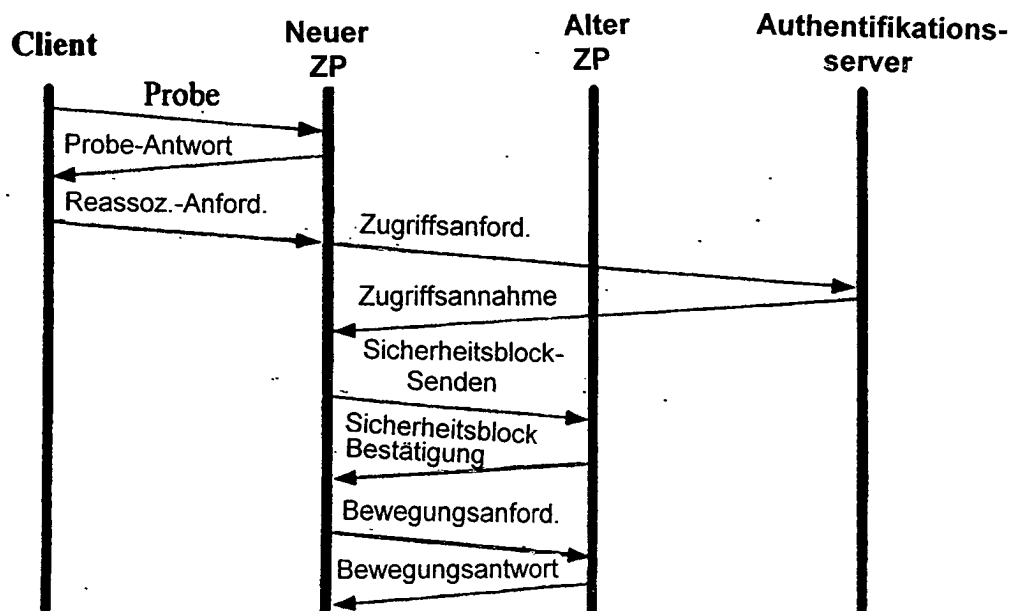


Fig. 4

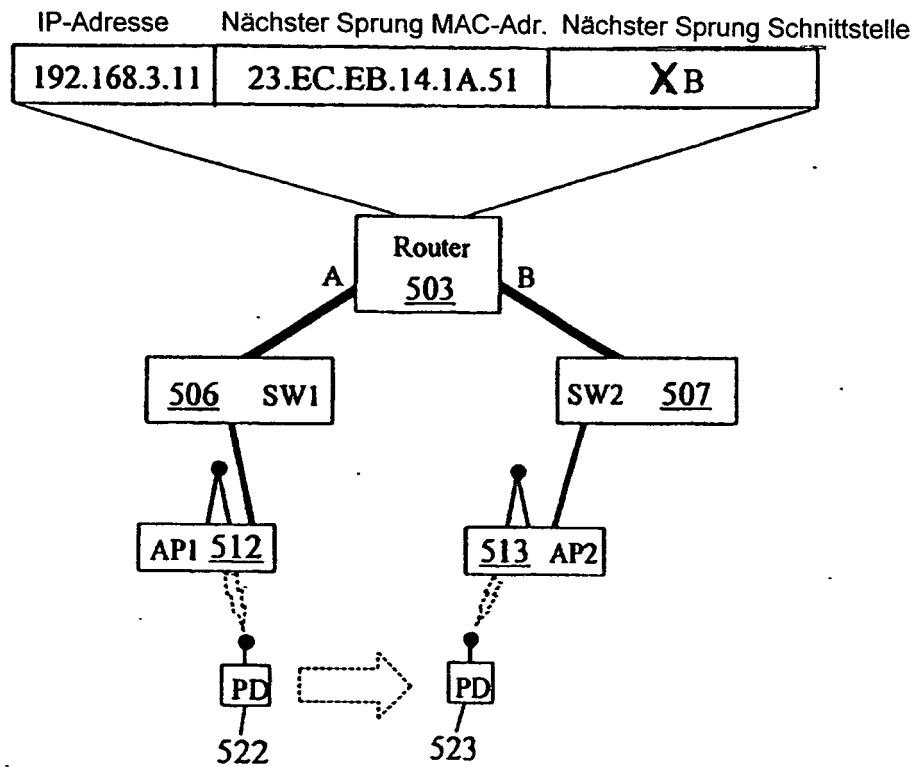


Fig. 5

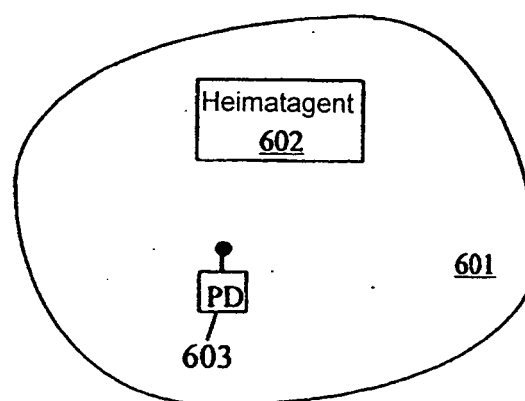


Fig. 6

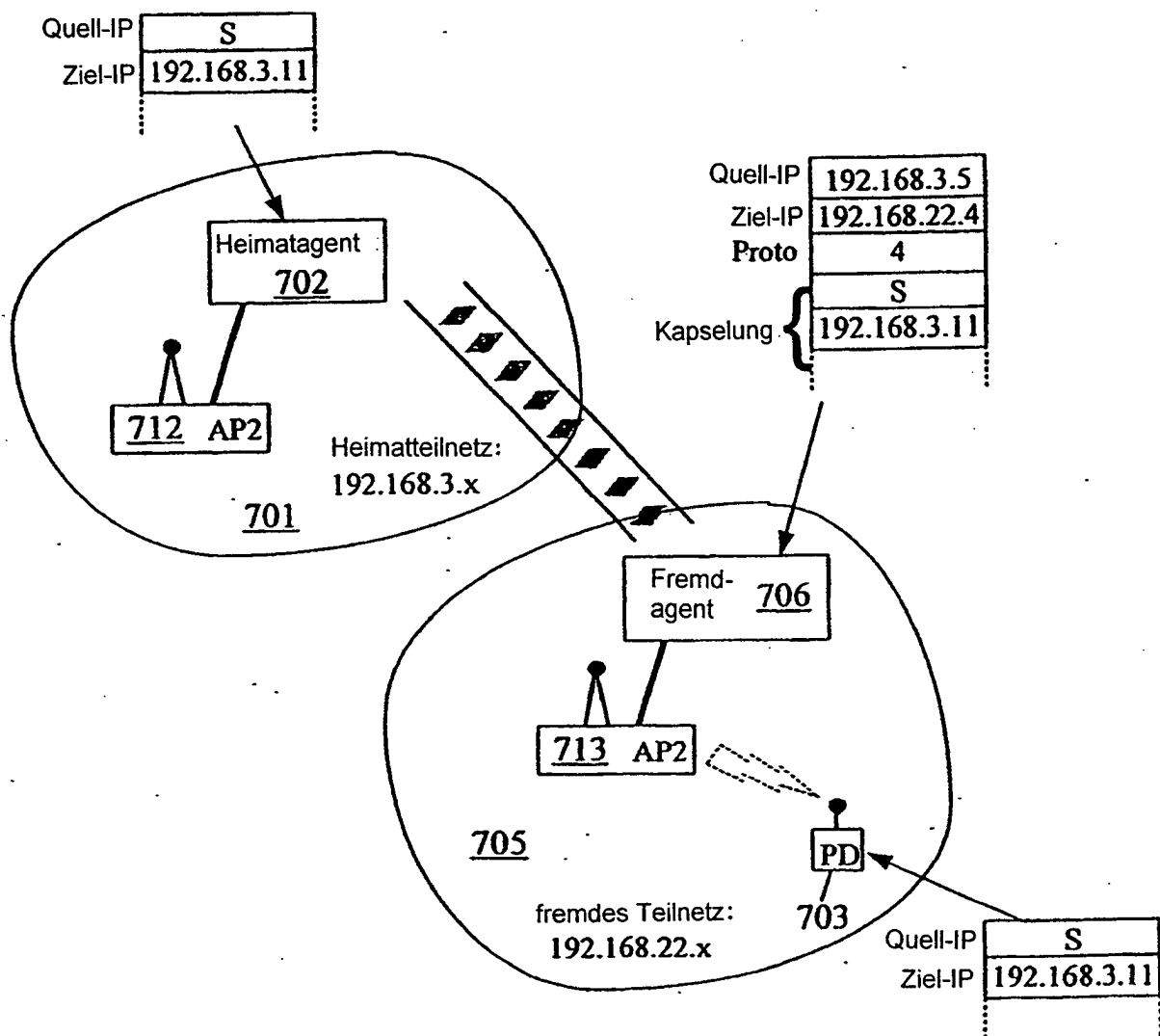


Fig. 7

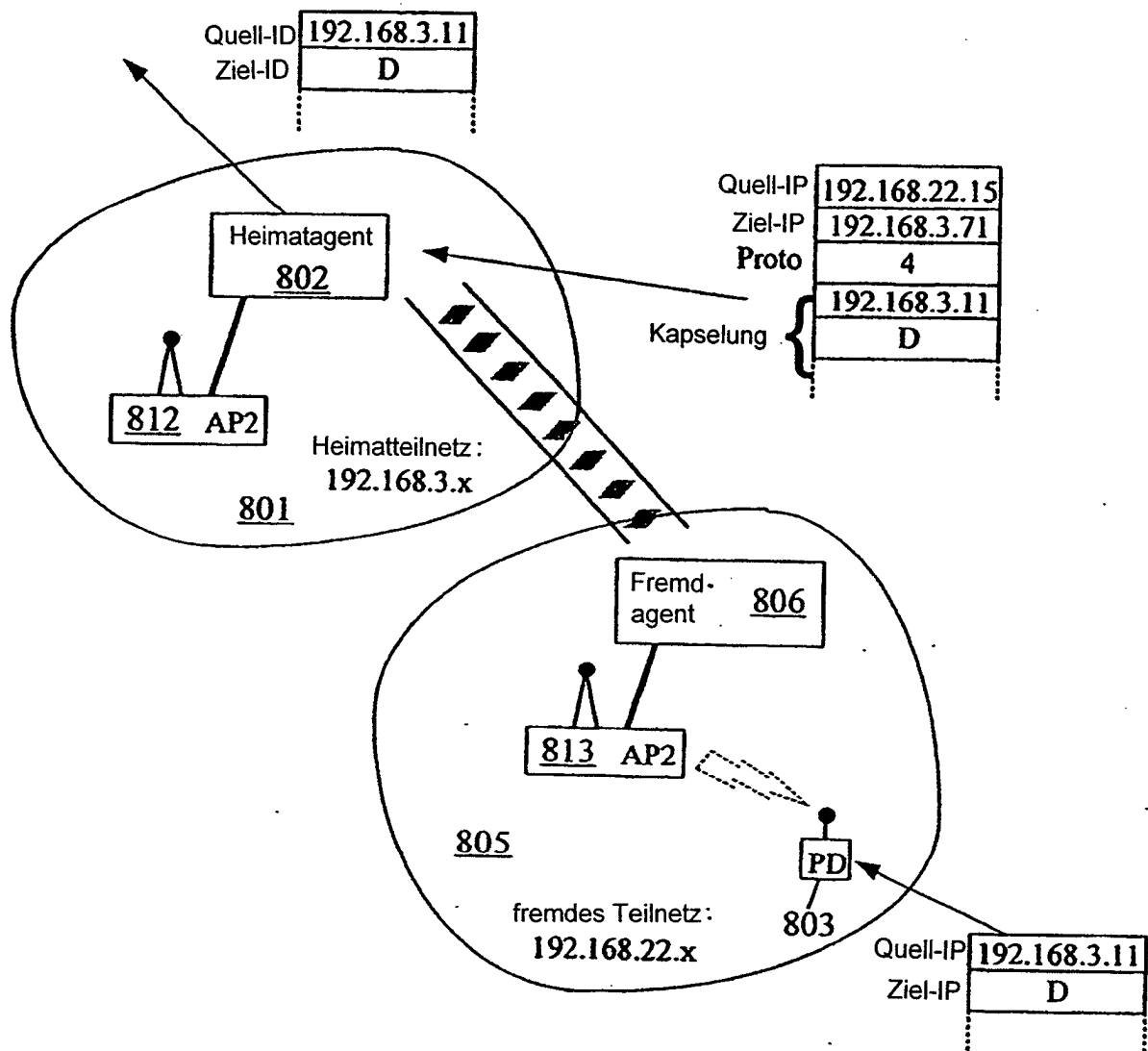


Fig. 8

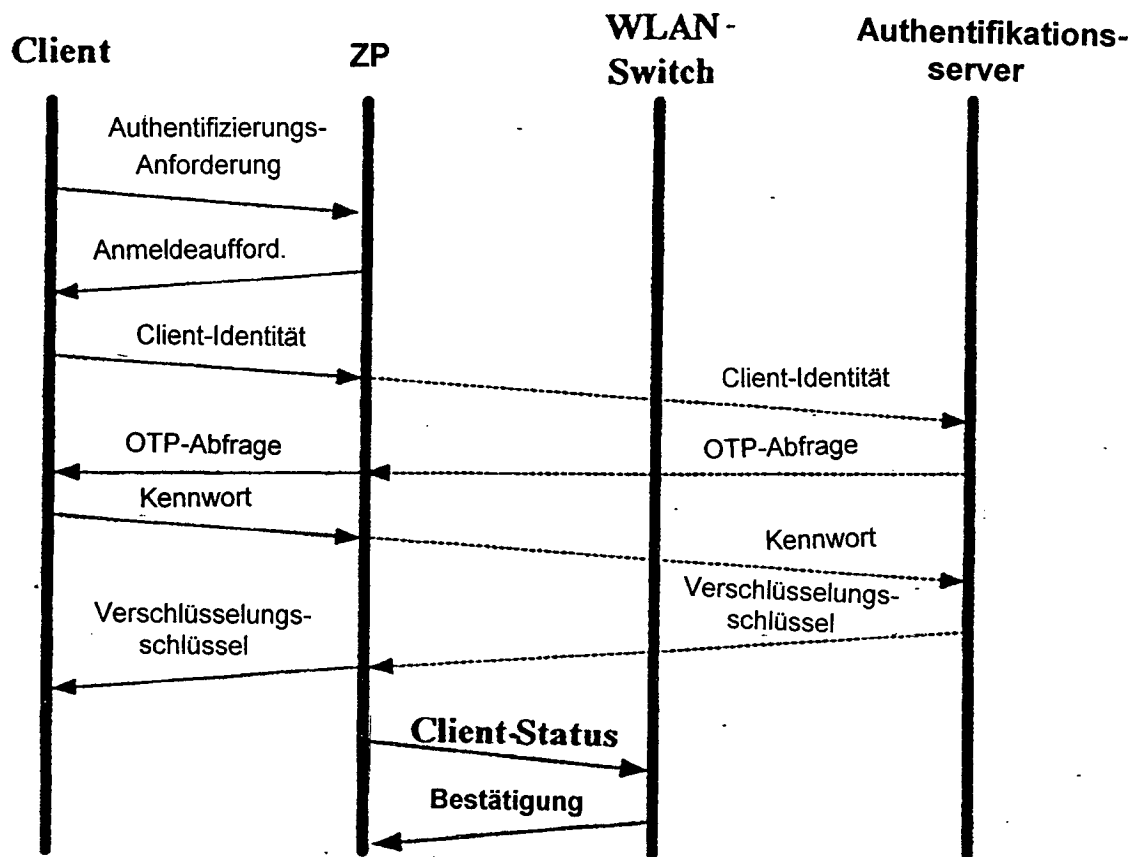


Fig. 9

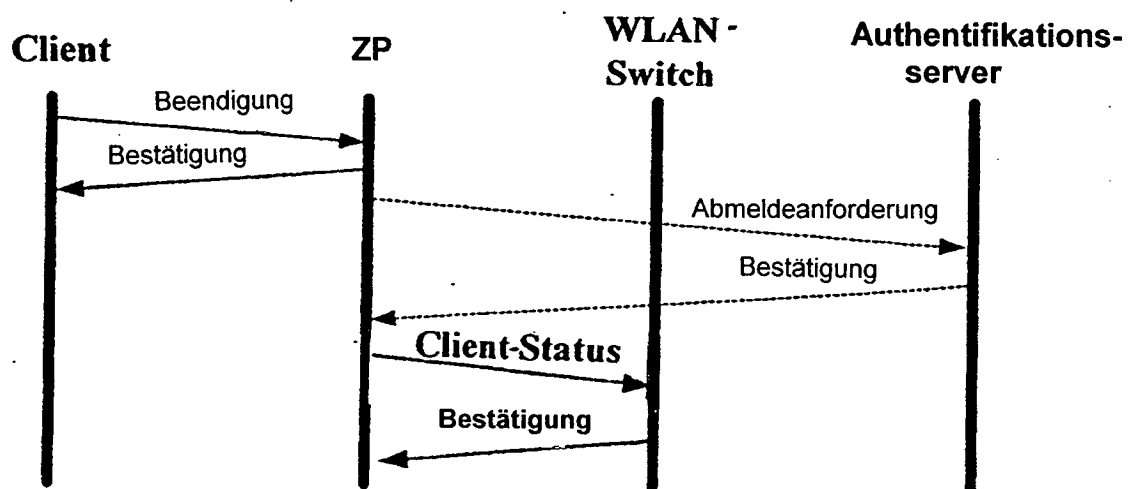


Fig. 10

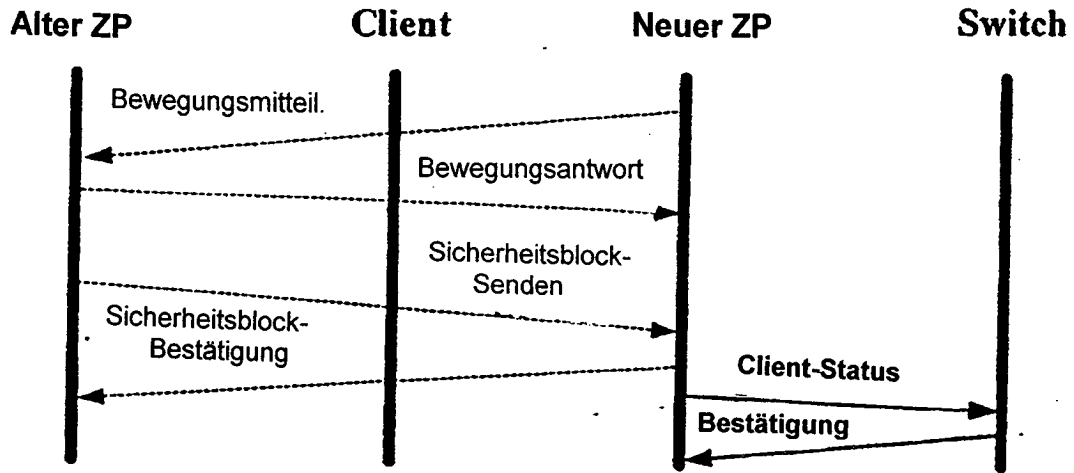


Fig. 11

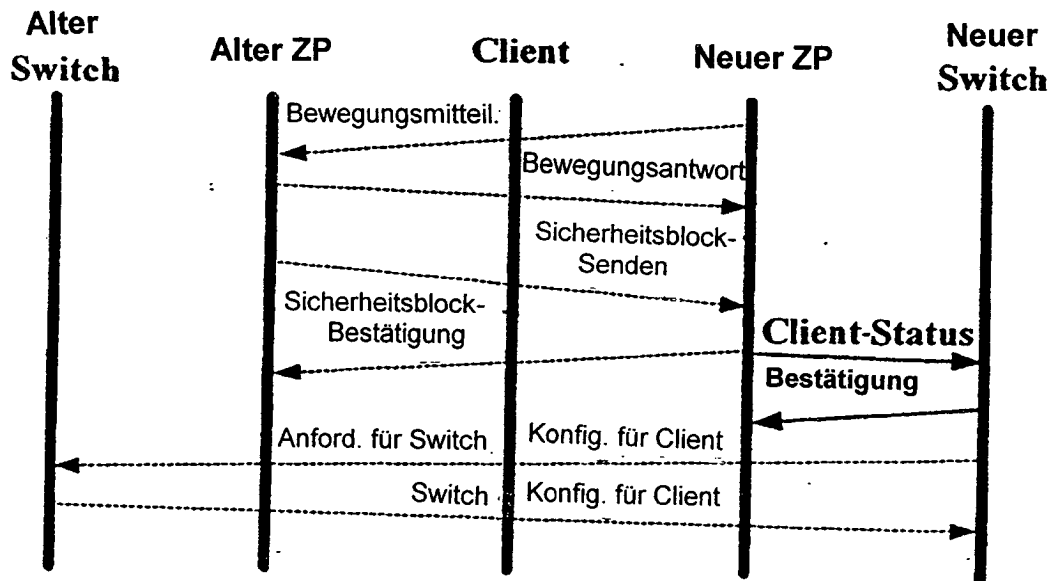


Fig. 12

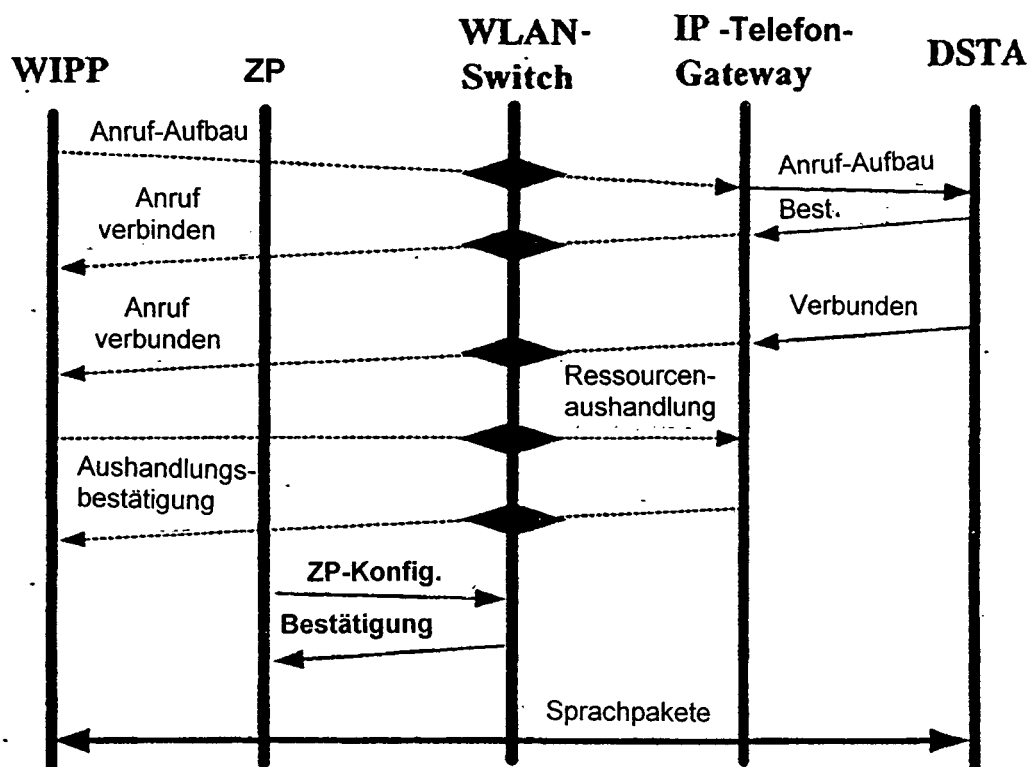


Fig. 13

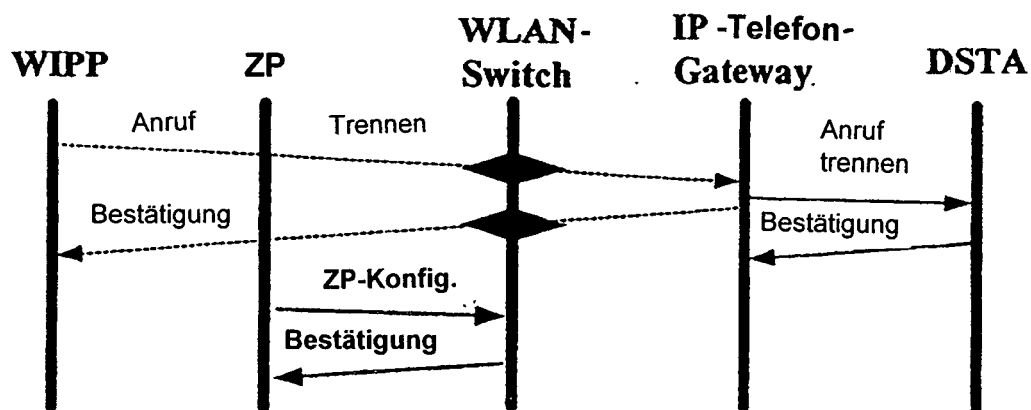


Fig. 14