WLAN
Technik und Betrieb

Wilfried Speltacker
DL9NAM

DL9NAM

1

Internet Geschichte (Übersicht)

- **1969**
  - ARPAnet (*Advanced Research Projects Agency Network*), paket-vermitteltes Netz (Erstinstallation bei UCLA),
  - Entwickelt vom MIT im Auftrag des US DoD (seit 1962)
- **1974**
  - Aufsatz von Cerf/Kahn über „*Internetworking*“
  - Erste Vorstellung einer Sicherungsschicht (wurde später zu TCP)
- **1977**
  - ARPA Forschungsprogramm zu „*Internetworking*“
  - TCP/IP Prototyp
- **1983**
  - ARPA übernimmt TCP/IP und es wird US Mil-Standard
  - „Geburt“ des Internet
- **1985**
  - Internet für allgemeine akademische Anwendungen (USA, NSFnet)
  - Einfluss auf die Entwicklung von UNIX und der Programmiersprache C
- **1989**
  - Privatisierung des Internet (mit kommerzieller Ausprägung)
- **1991**
  - Einführung des World Wide Web (WWW) als Internet Anwendung (CERN)

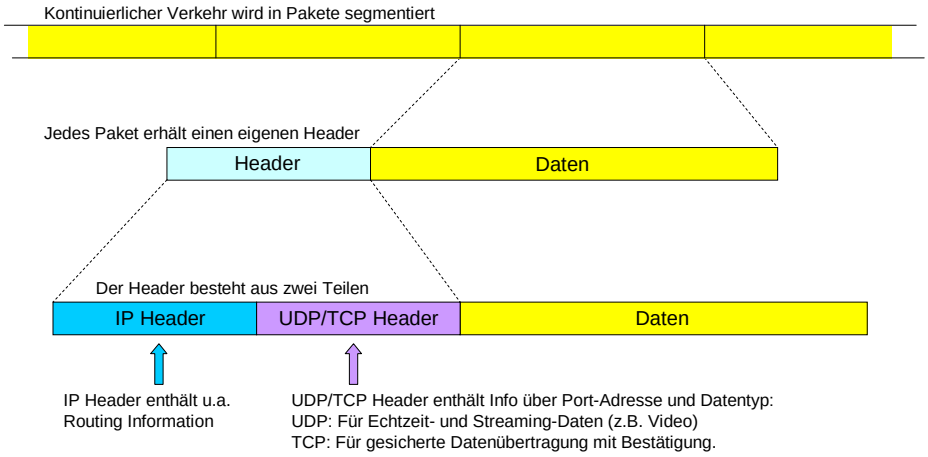
DL9NAM

2

Internet Verkehr (Prinzip)

Deutscher Amateur-Radio-Club e.V.

Der Internet ist paketorientiert, d.h. Daten werden in einzelne Abschnitte segmentiert und jedes einzelne Segment mit Zusatzinformationen (Header) zur Verwaltung und über Sender und Empfänger versehen.

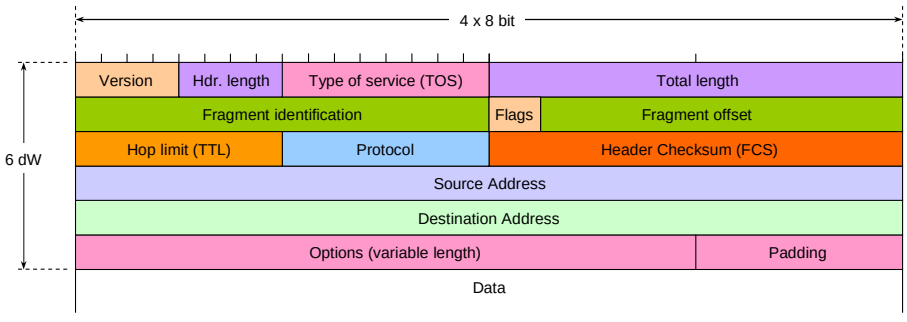


DL9NAM

3

IPv4 Header

Deutscher Amateur-Radio-Club e.V.



TTL = Time To Live
FCS = Frame Check Sequence

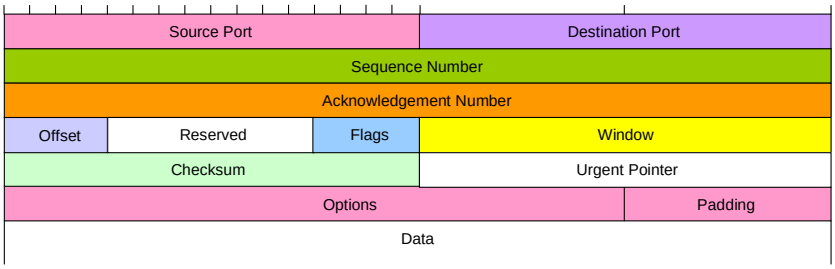
DL9NAM

4

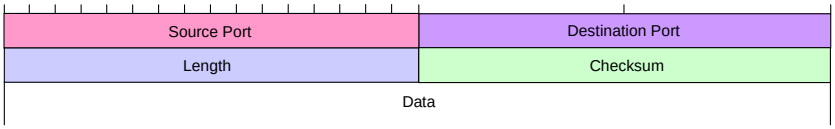
TCP und UDP Header

Deutscher Amateur-Radio-Club e.V.

TCP Header



UDP Header



TCP = Transport Control Protocol
UDP = User Datagram Protocol

DL9NAM

5

Internet Zugang

Deutscher Amateur-Radio-Club e.V.

Jeder Teilnehmer, der das Internet nutzen will benötigt einen geeigneten (physikalischen) Zugang.

Für große Unternehmen erfolgt das in der Regel über eine Mietleitung geeigneter Kapazität. Dem Unternehmen wird auch oft eine bestimmte Menge von IP Adressen fest zugewiesen.

Kleine Unternehmen und auch Privatpersonen (sog. SOHO Gruppen) erhalten den Zugang in der Regel über xDSL und die IP Adresse bzw. mehrere Adressen werden dabei fest (bei Unternehmen) oder dynamisch (bei Privatpersonen) zugewiesen.

Große Telekommunikationsunternehmen (sog. ISPs) haben sich bei der globalen IP Adressverwaltung eine große Anzahl von IP Adressen zuweisen lassen, die sie dann an ihre Kunden vergeben.

Bei SOHO Teilnehmern wird zumeist die Telefon-Anschlussleitung zum Internetzugang genutzt. Bei Unternehmen ist der Datenverkehr in Up- und Down-Link etwa gleich mächtig und es kommt die SDSL Technik zum Einsatz. Für Privatpersonen mit geringerem Uplink Verkehr ist hingegen die ADSL Technik geeigneter (d.h. billiger).

Um während der Internet-Nutzung den Telefonbetrieb zu ermöglichen wird die Telefon-Anschlussleitung in unterschiedliche Frequenzbereiche aufgeteilt und den Bereichen Telefon-, Uplink- und Downlink-Verkehr zugewiesen. Die Trennung der Frequenzbereiche erfolgt in der Regel in einem passiven Splitter.

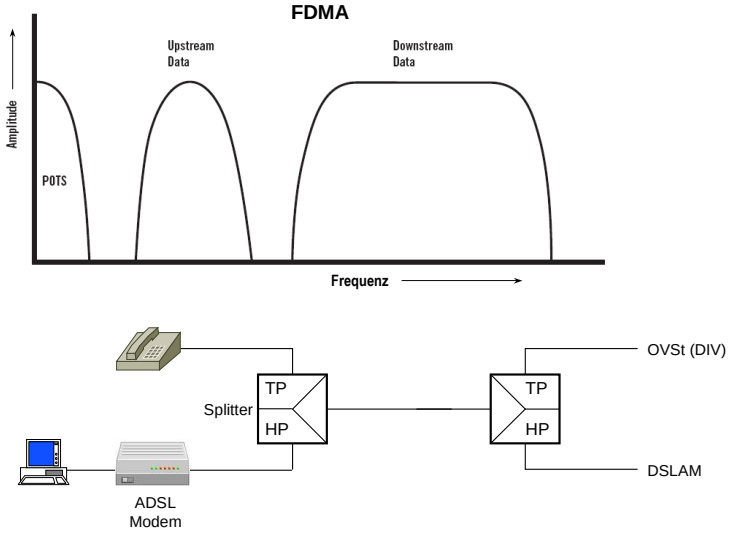
Zur Teilnahme am Internet benötigt jeder Teilnehmer eine entsprechende Authentifizierung (z.B. Zugangskennung und Passwort), die ihm von seinem ISP zugewiesen wird. Erst nach Abgleich dieser Daten ist er autorisiert den Dienst zu nutzen und erhält eine dynamische IP Adresse zugewiesen.

DL9NAM

6

ADSL Anschlussleitung

Deutscher Amateur-Radio-Club e.V.

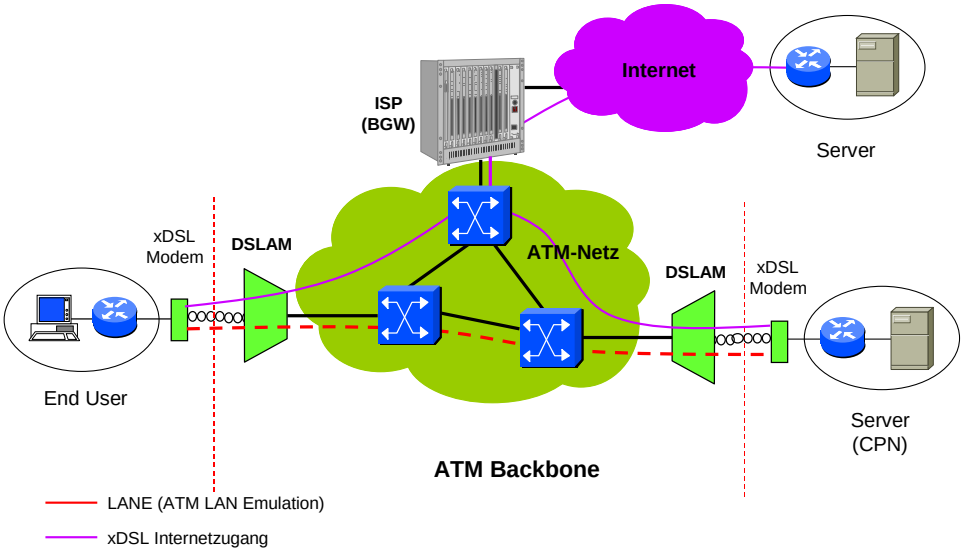


DL9NAM

7

Internet Zugang (xDSL)

Deutscher Amateur-Radio-Club e.V.



DL9NAM

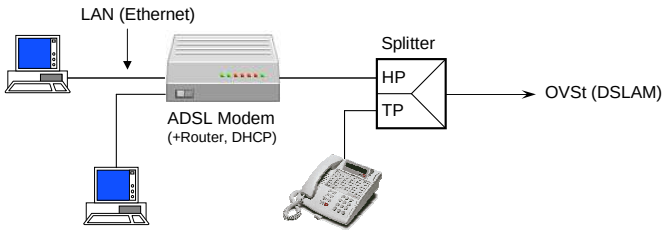
8

ADSL Anschluss

Deutscher Amateur-Radio-Club e.V.

Die Frequenzbereiche für Telefon und Internet-Zugang werden im sog. Splitter getrennt und dem normalen Telefon bzw. dem ADSL Modem zugeführt.

Die beiden Frequenzbereiche für Up- und Down-Link trennt das ADSL Modem und verbindet sie mit den unterschiedlichen Prozessoren für beide Richtungen. Die IP Pakete beider Richtungen werden dabei nicht direkt eingespeist, sondern in ein sog. PPP eingekapselt. Dieses PPP dient auch zur Authentifizierung des Teilnehmers beim ersten Anschluss.



Die meisten ADSL Modems verfügen heute auch über eine Router-Funktion, so dass mehrere Verbraucher (PCs) angeschlossen werden können. Dabei wird jedem vom eingebauten DHCP eine eigene, interne IP Adresse zugeordnet. Alle teilen sich dabei die öffentliche, beim ersten Anschluss vom ISP zugewiesene IP Adresse. Dieses Verfahren heißt NAT und hat in gewissem Umfang die Funktion eines Hardware-Firewall.

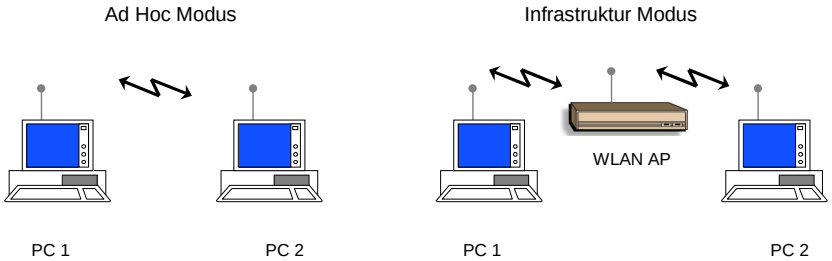
DL9NAM

9

WLAN Betriebs Modi

Deutscher Amateur-Radio-Club e.V.

Im sog. ad hoc Modus kann eine Verbindung zwischen zwei PCs ohne WLAN Access Point oder WLAN ADSL Modem realisiert werden. Dieser Modus muss an beiden Geräten eingestellt und beiden eine interne IP Adresse zugewiesen werden.



Der ad hoc Modus ist eine Punkt-zu-Punkt Alternative zum sog. Infrastruktur Modus, der immer einen zentralen WLAN Zugangsknoten (WLAN Access Point) erfordert. Die Einstellungen bezüglich Betriebsmodus (WEP, WPA), Zugangskennung (PSK) und Verschlüsselung muss bei beiden Rechnern identisch eingestellt werden. Er ist in der Regel nicht zum Internet-Zugang geeignet.

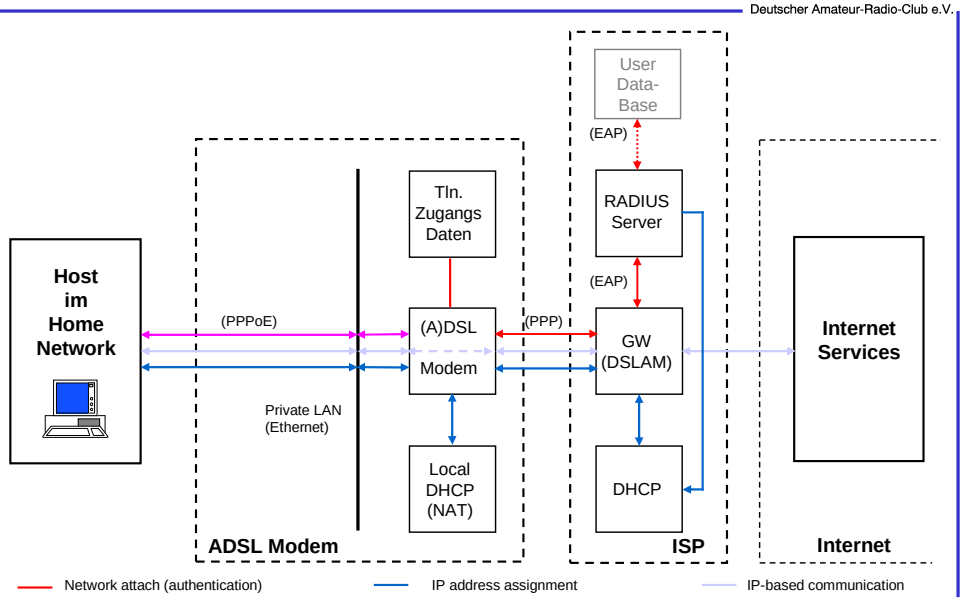
Im Infrastruktur Modus erfolgt die Verbindung zwischen den angeschlossenen Rechnern über den AP, der auch Verbindung zum Internet ermöglicht.

Ein wechselseitiger Zugriff auf Ordner/Dateien ist nur möglich, wenn diese freigegeben sind.

DL9NAM

10

Internet Zugang mittels ADSL



DL9NAM

11

PPP Link

Die Verbindung zum *Border-Gateway* des ISP wird mittels PPP (*Point-to-Point Protocol*) herzustellen und bildet einen Tunnel für die IP Pakete. Bei der Initialisierung wird es auch benutzt, um die Authentifizierungsdaten des Teilnehmers zu übertragen.

Die erforderlichen Zugangsdaten (User-Name und *Password*) werden dabei mittels PAP (*Password Authentication Protocol*) oder zumeist CHAP (*Challenge Handshake Authentication Protocol*) ausgetauscht. Die Authentifizierung erfolgt zumeist bereits beim Einschalten des ADSL Modems, seltener erst bei Aufrufen eines Internet Dienstes. Die notwendigen Zugangsdaten sind dabei (in der Regel) im Modem gespeichert.

Ist ein Teilnehmer als berechtigt erkannt, wird ihm vom DHCP (*Dynamic Host Configuration Protocol*) Server des ISP eine IP Adresse (temporär) zugewiesen.

PPPoA wird heute schrittweise durch PPPoE ersetzt und der DSLAM (*Digital Subscriber Line Access Multiplexer*) mit dem IP BGW (*Boarder Gateway*) zusammengefasst.

Die meisten ADSL Modems für SOHO Anwendungen verwenden NAT (*Network Address Translation*). Dabei wird die zugeteilte, öffentliche IP Adresse vom eigenen DHCP des Modems auf eine interne Adresse eines nicht öffentlichen Bereichs abgebildet (z.B.: **192.168.x.x** oder 10.x.x.x bzw. 172.16.x.x).

DL9NAM

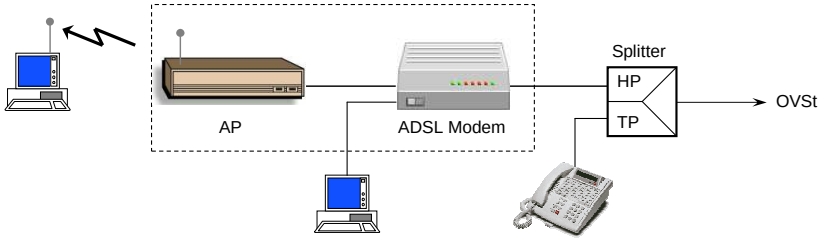
12

WLAN Anschluss

Deutscher Amateur-Radio-Club e.V.

Für eine größere Flexibilität und zur Vermeidung einer leitungsgebundenen LAN Installation wurde speziell für SOHO Anwendungen ein drahtloser LAN Anschluss konzipiert.

Dafür wird ein lizenzfreies Spektrum im Bereich 2.4 GHz und 5 GHz verwendet. In beiden Bereichen werden mehrere, teilweise überlappende Kanäle definiert. Als Modulationsart kommt CDMA bzw. OFDM zur Anwendung.



Die WLAN Basisstation (*Access Point* = AP) kann mit dem LAN Ausgang des ASDL Modems verbunden werden, so dass dieses den Internet-Zugang und interne IP Adressvergabe auch für die drahtlos angebundenen Geräte ermöglicht. Oft sind auch beide Funktionen in einem einzigen Gerät zusammengefasst.

Zur Realisierung des WLAN Anschlusses stehen verschiedene Technologien zur Verfügung.

DL9NAM

13

WLAN Standards (1)

Deutscher Amateur-Radio-Club e.V.

	802.11a	802.11b	802.11g	802.11n
Frequenzbereich	5 GHz	2.4 GHz	2.4 GHz	2.4 / 5 GHz
Brutto Datenrate	54 Mbit/s	11 Mbit/s	54 Mbit/s	600 Mbit/s
Netto Datenrate	32 Mbit/s	5 Mbit/s	32 Mbit/s	74 Mbit/s
Sendeleistung	30 mW	100 mW	100 mW	
Versorgungsradius	30 m	35 – 110 m	35 – 110 m	100 – 200 m
Anwendung	Indoor	Indoor/outdoor	Indoor/outdoor	Indoor/outdoor
Kanäle	19	13 (3 *)	13 (3 *)	
QoS	ffs	ffs	ffs	ffs

* Nicht überlappend

DL9NAM

14

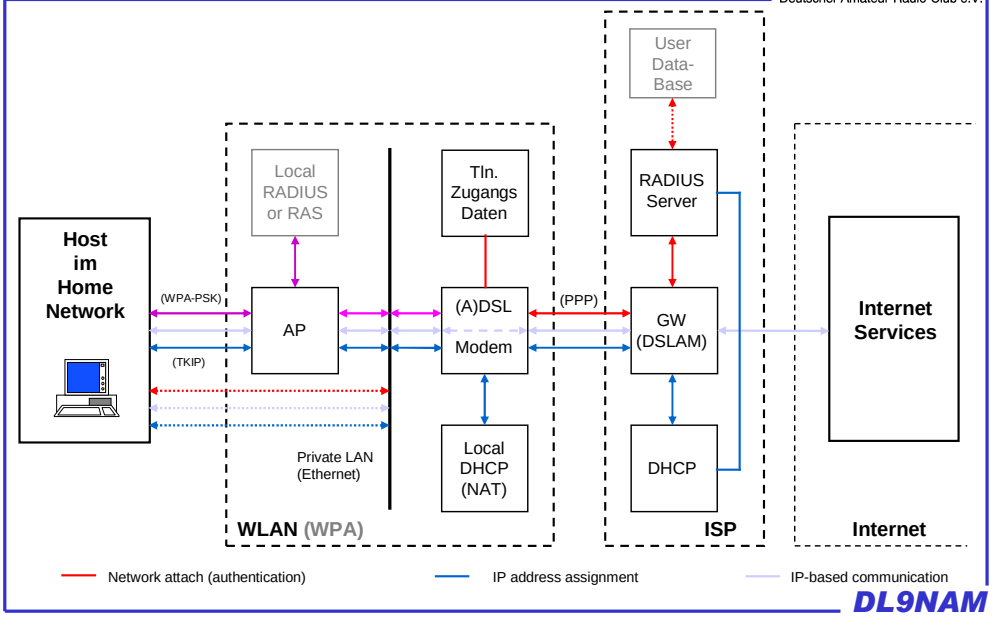
WLAN Standards (2)

- **WEP** (*Wired Equivalent Privacy*)
  - PSK mit geringer Länge (8 Zeichen),
  - Schwache Verschlüsselung auf der Luftschnittstelle.
- **WPA** (*Wi-Fi Protected Accesss*)
  - Subset von IEEE 802.11i
  - Neue Verschlüsselung auf der Luftschnittstelle mittels TKIP (*Temporal Key Integrity Protocol*) und MIC (*Message Integrity Check*) nach RC4 (Stromchiffre).
  - SOHO Mode mit Authentifizierung mittels PSK (*Pre-Stared Key* mit bis zu 63 Zeichen).
  - Enterprise Mode mit Authentifizierung nach IEEE 802.1x/EAP (RADIUS).
- **WPA-2**
  - Wie WPA nur mit weitgehender Implementierung von IEEE 802.11i (TKIP bzw. CCMP) und Verschlüsselung nach AES.

DL9NAM

15

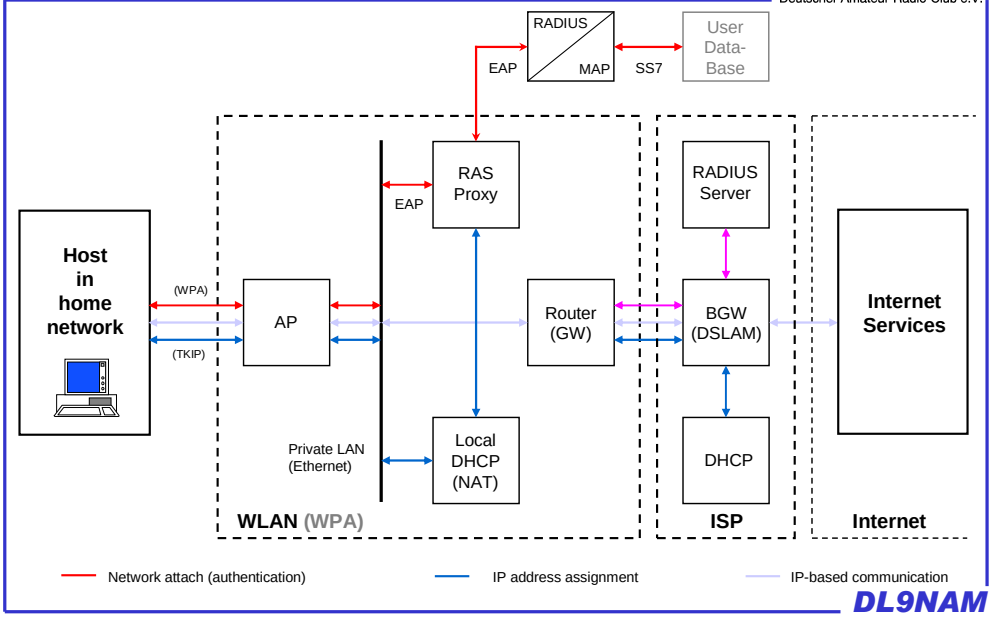
WPA(2) SOHO Mode



DL9NAM

16

WPA(2) Enterprise Mode



DL9NAM

17

WPA Übersicht

Mode	WPA	WPA2
Enterprise Mode (Business and Government)	Authentication: IEEE802.1x/EAP Encryption: TKIP/MIC	Authentication: IEEE802.1x/EAP Encryption: AES-CCMP
Personal Mode (SOHO/personal)	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

TKIP	Temporal Key Integrity Protocol (RC4)
MIC	Message Integrity Check
PSK	Pre-Stared Key (max 62 Characters)
AES	Advanced Encryption Standard
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
EAP	Extensible Authentication Protocol

DL9NAM

18

WLAN Sicherheit (1)

Deutscher Amateur-Radio-Club e.V.

Wenn ein neuer WLAN Access Point bzw. ein WLAN-ADSL Modem in Betrieb genommen wird, sind sofort die standardmäßig eingestellten Daten zu ändern, um Fremden die Möglichkeit zu nehmen, Informationen zum eigenen Gerät zu ermitteln.

- **Vorgegebenes Passwort zum Einstellen der Daten ändern**
  Dieses dient zum Zugang zur Einstellung der persönlichen Daten wie ISP Zugang, SSID, HF-Kanal, Betriebsmodus und PSK, etc.
- **Vorgegebene SSID ändern**
  Diese lässt im Auslieferzustand zumeist auf den Hersteller des Gerätes schließen und sollte durch einen unverdächtigen Namen geändert werden (sollte auch nicht auf den Betreiber verweisen).
- **HF Kanal ändern**
  Die meisten Geräte werden mit voreingestelltem Kanal 6 (bei 802.11b/g) ausgeliefert. Dieser sollte geändert werden, möglichst auf einen, der in der Nachbarschaft nicht belegt ist (kann mit geeigneter Software getestet werden).
- **Betriebsmodus einstellen**
  Hier sollte WPA2 ausgewählt werden. Falls nicht möglich auch WPA. WEP ist auf jeden Fall zu vermeiden.
- **PSK eingeben**
  Bei WPA und WPA2 ist das eine (ASKII) Zeichenfolge mit bis zu 63 Zeichen (bei WEP nur 8). Diese sollte möglichst zufällig sein und nicht aus einem leicht merkbaren Satz oder persönlichen Daten bestehen.
- **Zugangsdaten eingeben**
  Ist der WLAN AP gleichzeitig auch ADSL Modem, dann muss noch der User-Name vom ISP und das ISP Zugangs-Passwort eingegeben werden. Diese Daten wurden vom ISP zugeteilt, das Zugangspasswort muss ggf. nach der ersten Benutzung geändert werden (nicht mit dem Passwort zur Eingabe der Daten oder dem PSK verwechseln).
- **Master PC definieren**
  Falls möglich einen (Master) PC mit fester IP Adresse innerhalb des NAT Bereichs als einzigen Berechtigten zur Änderung der WLAN-Daten festlegen. Dieser Bereich fester IP Adressen sollte für WLAN Benutzer gesperrt sein. Beispiel: Gesamtbereich 192.168.1.1 bis 192.168.1.255 davon für feste Adressen reserviert (nur LAN) 192.168.1.1 bis 192.168.1.32 und alle anderen dynamisch für LAN und WLAN.

DL9NAM

19

WLAN Sicherheit (2)

Deutscher Amateur-Radio-Club e.V.

Zusätzlich zu TKIP/CCMP und PSK bzw. IEEE 802.1x/EAP können weitere Maßnahmen zur Erhöhung der Sicherheit vorgesehen werden (auch bei WEP)

- **Hidden SSID** (Service Set ID = AP Name)
  - Broadcast der SSID wird unterdrückt
  - AP wird von unberechtigten Stationen nicht gesehen (theoretisch)
  - Bei allen berechtigten Rechnern muss dann die Option „Verbindung auch herstellen, wenn kein Broadcast gesendet wird“ aktiviert sein (unter „Systemsteuerung“ → „Netzwerkverbindung“ → Eigenschaften von „Drahtlose Netzwerkverbindungen“ → „Drahtlosnetze“ <eigene SSID> → „Eigenschaften“)
- **MAC Filterung**
  - Nur die Mobilstationen deren MAC Adresse im AP gespeichert ist erhalten Zugang (PSK ist dennoch erforderlich)
  - AP muss MAC Filterung unterstützen und MAC Adressen aller PCs, die über den AP arbeiten dürfen müssen eingetragen sein.
  - MAC Adresse eines PC kann in der DOS-Box mittels „ipconfig –all“ für den WLAN Anschluss ermittelt werden (weicht von der Ethernet-LAN MAC Adresse ab).
- **IPSec**
  - Erlaubt Ende-zu-Ende Verschlüsselung (z.B. IKE nach RFC2409)
  - Nicht immer sicher (man-in-the-middle Problem)
- **VPN**
  - Es wird Ende-zu-Ende ein verschlüsselter (IP) Tunnel aufgebaut
  - Verschlüsselung mittels symmetrischem Schlüsselpaar (DES, 3DES)
  - Nicht alle (WLAN) ADSL Modems unterstützen VPN und wenn ja ist zumeist eine spezielle Software (bei manchen Herstellern kostenlos) erforderlich.

DL9NAM

20

Frequenz-/Kanal-Zuweisung

Deutscher Amateur-Radio-Club e.V.

IEEE 802.11b/g

Kanal	Frequenz
1	2412 MHz
2	2417 MHz
3	2422 MHz
4	2427 MHz
5	2432 MHz
6	2437 MHz
7	2442 MHz
8	2447 MHz
9	2452 MHz
10	2457 MHz
11	2462 MHz
12	2467 MHz
13	2472 MHz

IEEE 802.11a/n

Kanal	Frequenz
36	5180 MHz
40	5200 MHz
44	5220 MHz
48	5240 MHz
52	5260 MHz
56	5280 MHz
60	5300 MHz
64	5320 MHz
100	5500 MHz
104	5520 MHz
108	5540 MHz
112	5560 MHz
116	5580 MHz
120	5600 MHz
124	5620 MHz
128	5640 MHz
132	5660 MHz
136	5680 MHz
140	5700 MHz

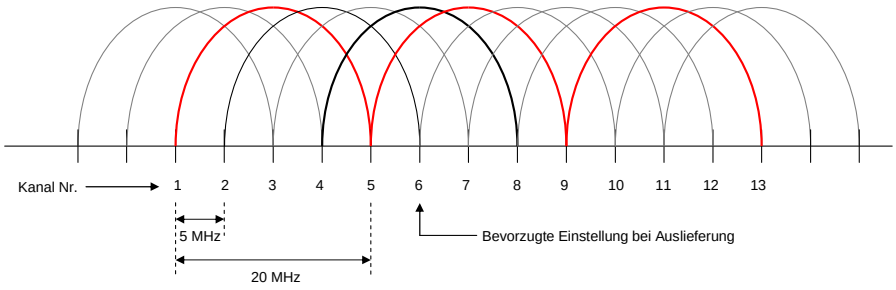
Das Kanalraster ist einheitlich 5 MHz. Die belegte Bandbreite je Kanal ist allerdings 20 MHz, so dass benachbarte Kanäle überlappt werden (Interferenz). Wegen des verwendeten Modulationsverfahren (CDMA bei b und g bzw. OFDM bei a und n) kann das toleriert werden, wenn die Feldstärke der eigenen Station hinreichend ist.

DL9NAM

21

IEEE 802.11b/g Kanalraster

Deutscher Amateur-Radio-Club e.V.

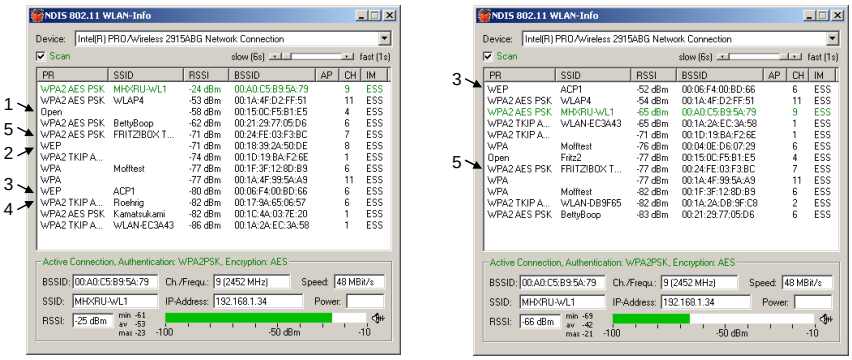


13 Kanäle im 2.4 GHz Bereich aber nur 3 davon nicht-überlappend

DL9NAM

22

Beispiele



Fehler:

1: Keine Zugangskontrolle und Verschlüsselung. Verbergen der SSID nicht ausreichend!

2: Zugangskontrolle und Verschlüsselung nur WEP. Verbergen der SSID nicht ausreichend!

3: Zugangskontrolle und Verschlüsselung nur WEP und offene SSID. Sehr unsicher!

4: Zugangskontrolle und Verschlüsselung nach WPA2 aber TKIP. SSID sollte nicht der Familienname sein!

5: Zugangskontrolle und Verschlüsselung nach WPA2 ok. SSID sollte nicht den AP Typ erkennen lassen!

DL9NAM

23

Links

Produkte mit Wi-Fi Zertifikat findet man unter

http://www.wi-fi.org/certified_products.php

Wi-Fi Standards:

http://www.wi-fi.org/knowledge_center_overview.php

TCP/IP Grundlagen:

http://www.netzmafia.de/skripten/netze/netz8.html

WLANInfo Download:

http://rrznt1.uni-regensburg.de/systemsw/TOOLS/wlaninfo.htm

DL9NAM

24