Sicherheitsrisiken in Ethernet, WEP und WAN-Techniken

Seminar 18.415:
Sicherheit in vernetzten Systemen

Christian Muus
0muus@informatik.uni-hamburg.de
Fachbereich Informatik
Universität Hamburg
WS 2002/2003

Übersicht

1. Ethernet
2. Wireless LAN´s
3. WEP
4. WAN
5. Literatur

1. Ethernet IEEE 802.3

1.1 Grundlagen

1.2 Standards

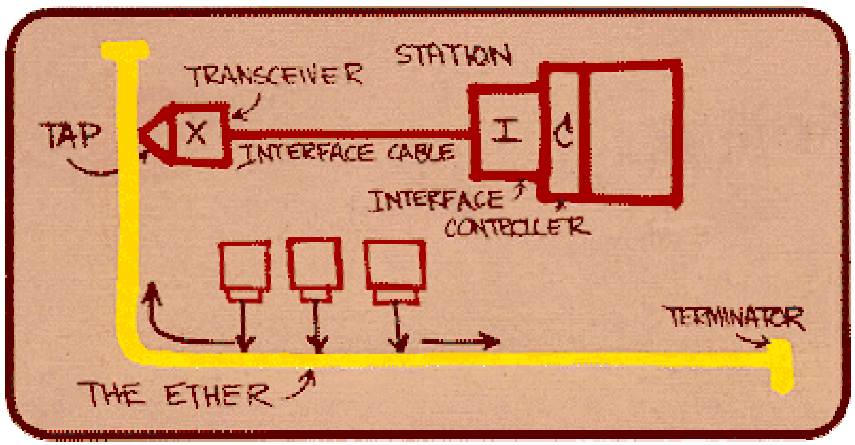
1.3 Schwachstellen

1.4 Absichern

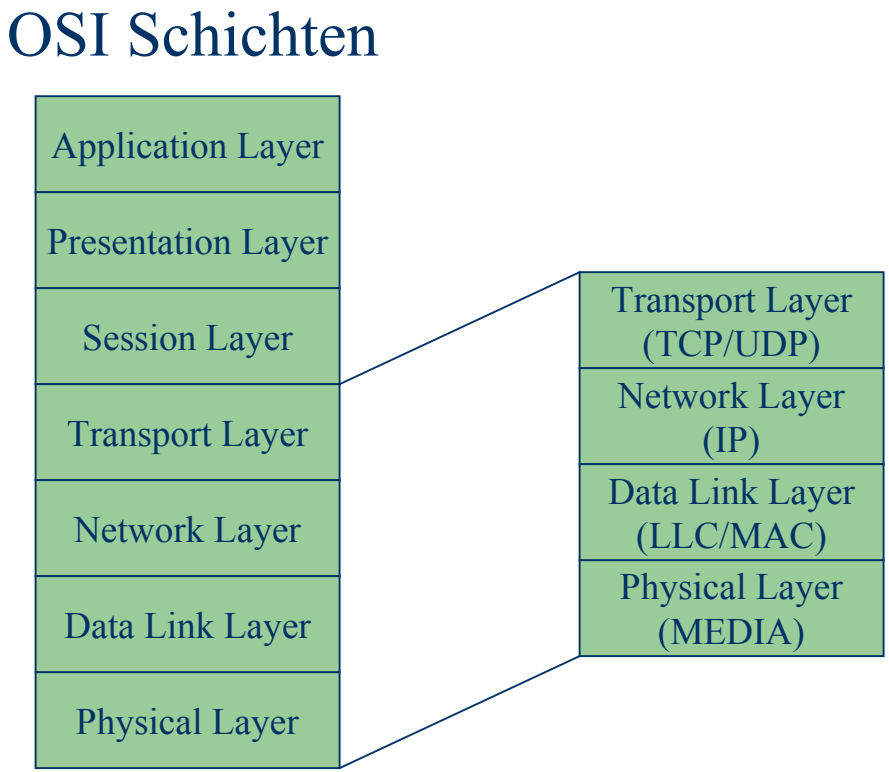
1.5 Ausblick

1.1 Grundlagen

- 70er Jahre bei Xerox entwickelt (3 Mbps)
- 1982 IEEE Standard 802 (10 Mbps)
- 1985 IEEE 802.3 mit CSMA/CD

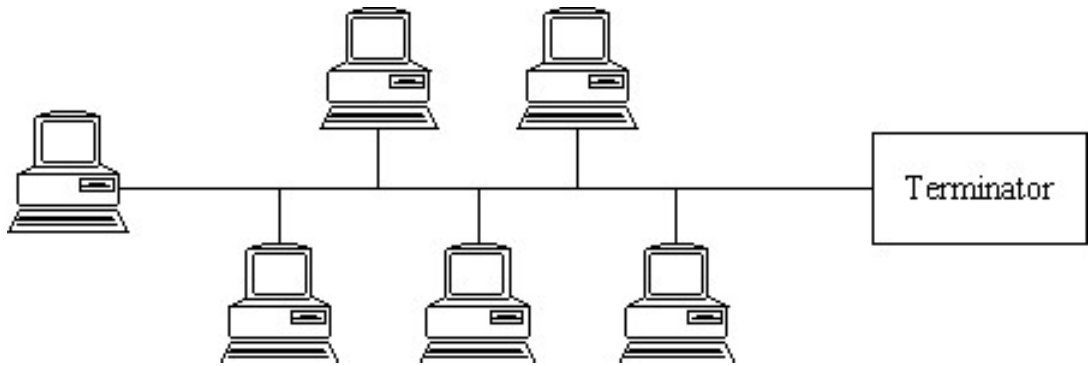


1.1 Schichten



In über 90% der implementierungen

1.1 Bus Topologie



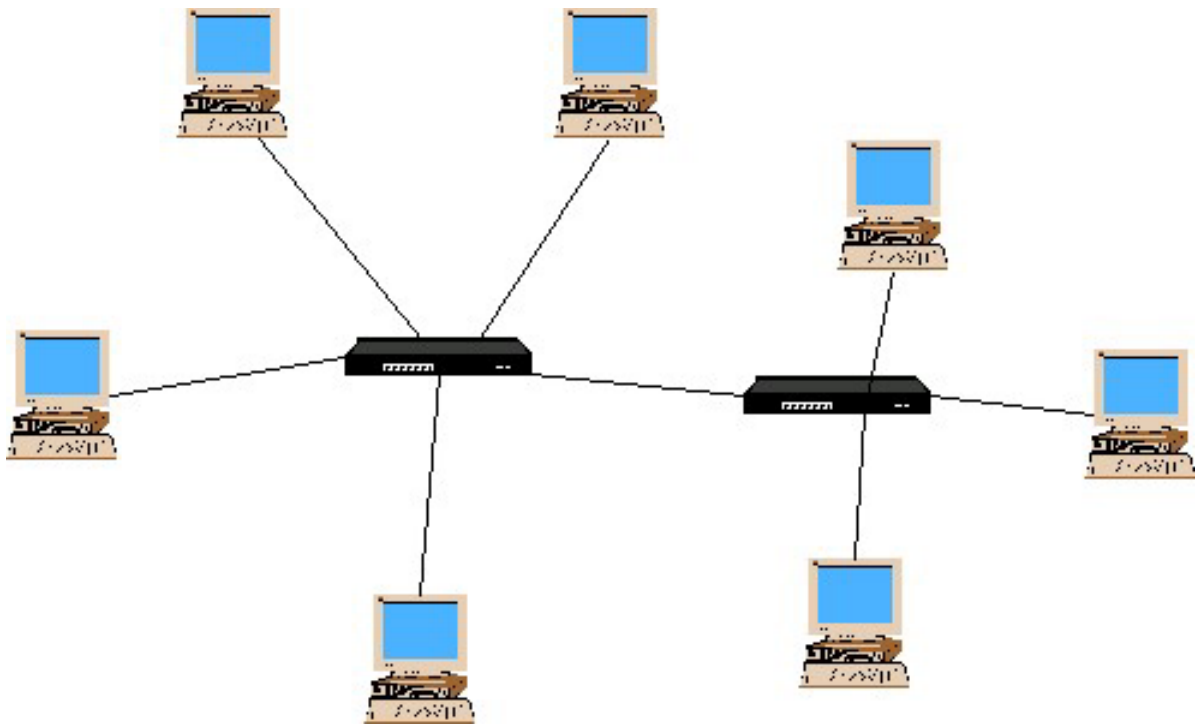
- 10 Base 5 „ThickNet“
- 10 Base 2 „ThinNet“

1.1 Switch/Hub

- Hub: „Bus in a box“
- Shared Medium
- Kein Vollduplex

- Switch: Gleichzeitige übertragund zu mehreren stationen
- Vollduplex

1.1 Stern/Baum Topologie



1.2 Ethernet Standards

- IEEE 802.3 10 Base(5,2,T,F)
- IEEE 802.3u 100 Base(TX,FX,T4)
- IEEE 802.3ab 1000 Base-T
- IEEE 802.3ae 10 GBase-T (Mitte, Ende 2004)

1.3 Schwachstellen

- Shared Medium
- Sniffing
- Keine Authentifizierung
- ARP-Spoofing
- MAC-Spoofing
- CAM-Attack

1.3.1 MAC-Attack / CAM Overflow

- CAM Table Overflow (Content Adressable Memory)
- Begrenzter Speicher
- Flooding the switch
- Broadcast wenn kein passender Eintrag

1.4 Absichern des Ethernet

- Physikalischer Schutz
- Switches statt Hubs
- Switches mit intruder protection und manuellen MAC einträgen
- Tools die das Netz ständig überprüfen z.B. arpwatch

1.5 Ausblick

- Optical Ethernet im Metro Netz
- 100GB Ethernet ...
- Ethernet on first/last mile

2. Wireless LAN´s

2.1 Grundlagen

2.2 Standards

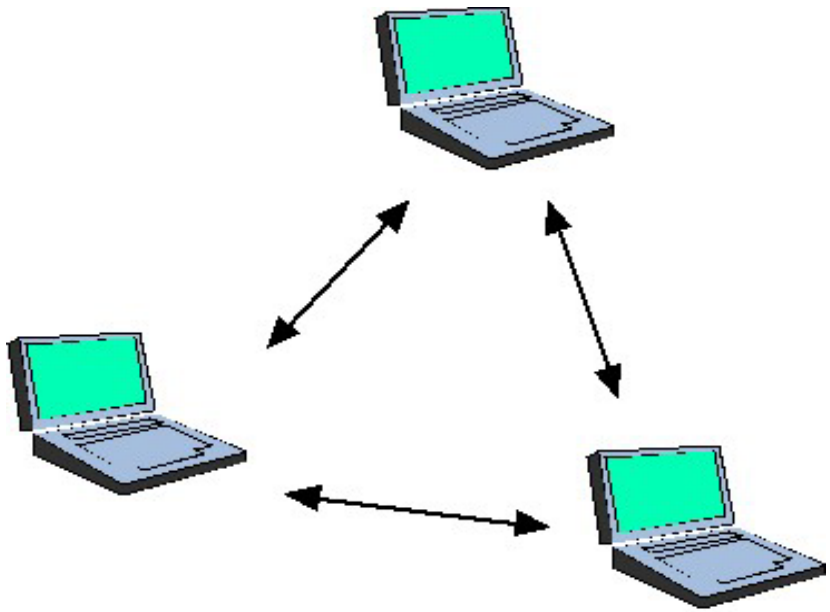
2.3 Schwachstellen

2.4 Absichern von WLANS

2.1 WLAN Grundlagen WLAN

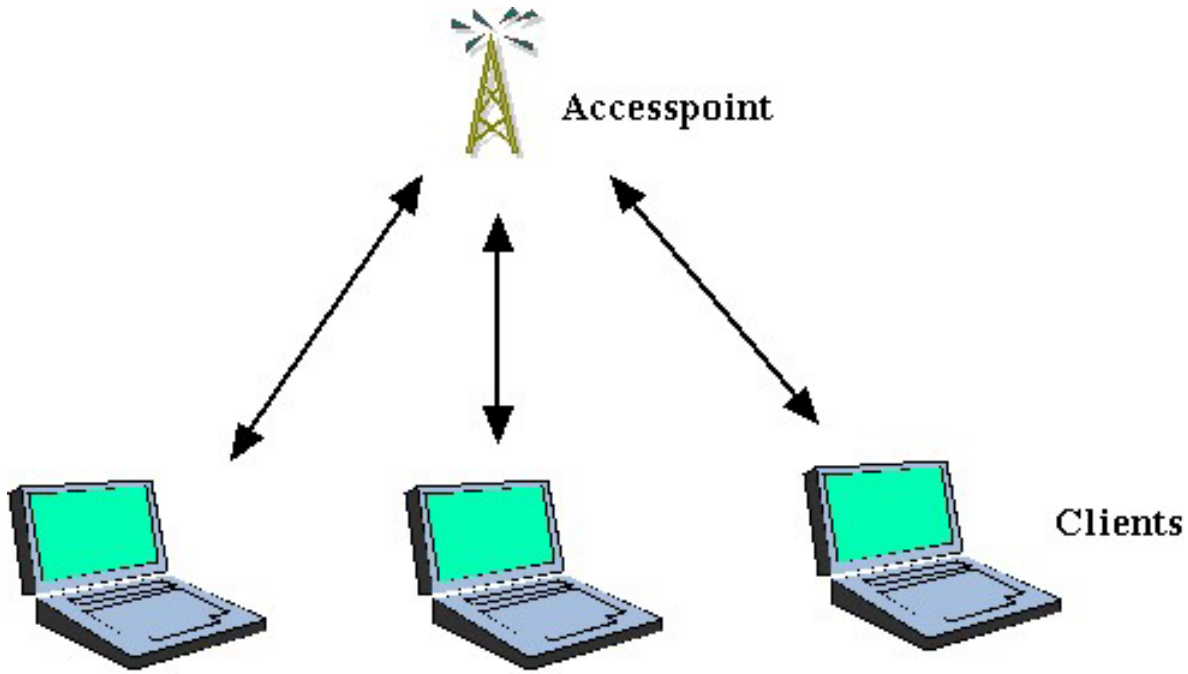
- Ad-Hoc-Modus (peer to peer)
- Infrastruktur-Modus
- Überlappende Funkzellen („Roaming“)
- Reichweite ca. 30 – 150m
- Einsatz als Repeater
- Funkbridges Reichweite mehrere Km

2.1 Ad-hoc-Modus



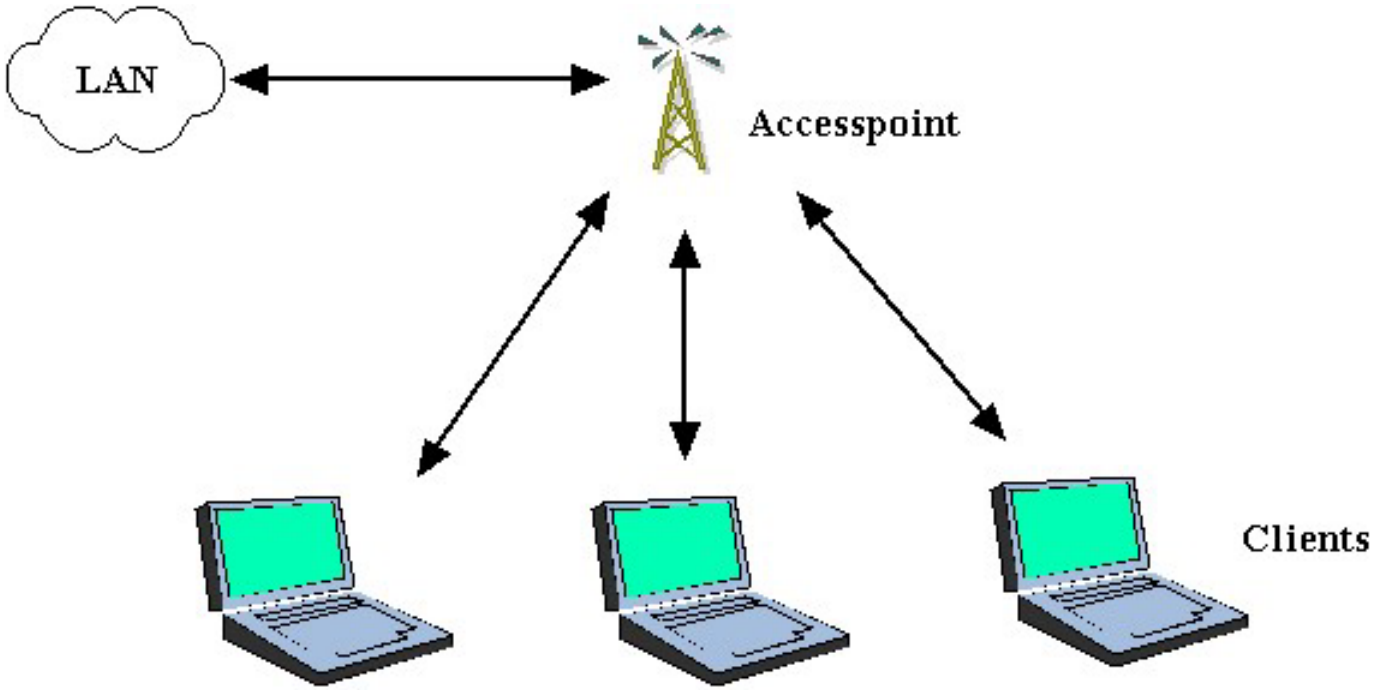
Ad-hoc-Modus (peer to peer)

2.1 Infrastruktur-Modus



Infrastruktur-Modus

2.1 Infrastruktur-Modus im LAN

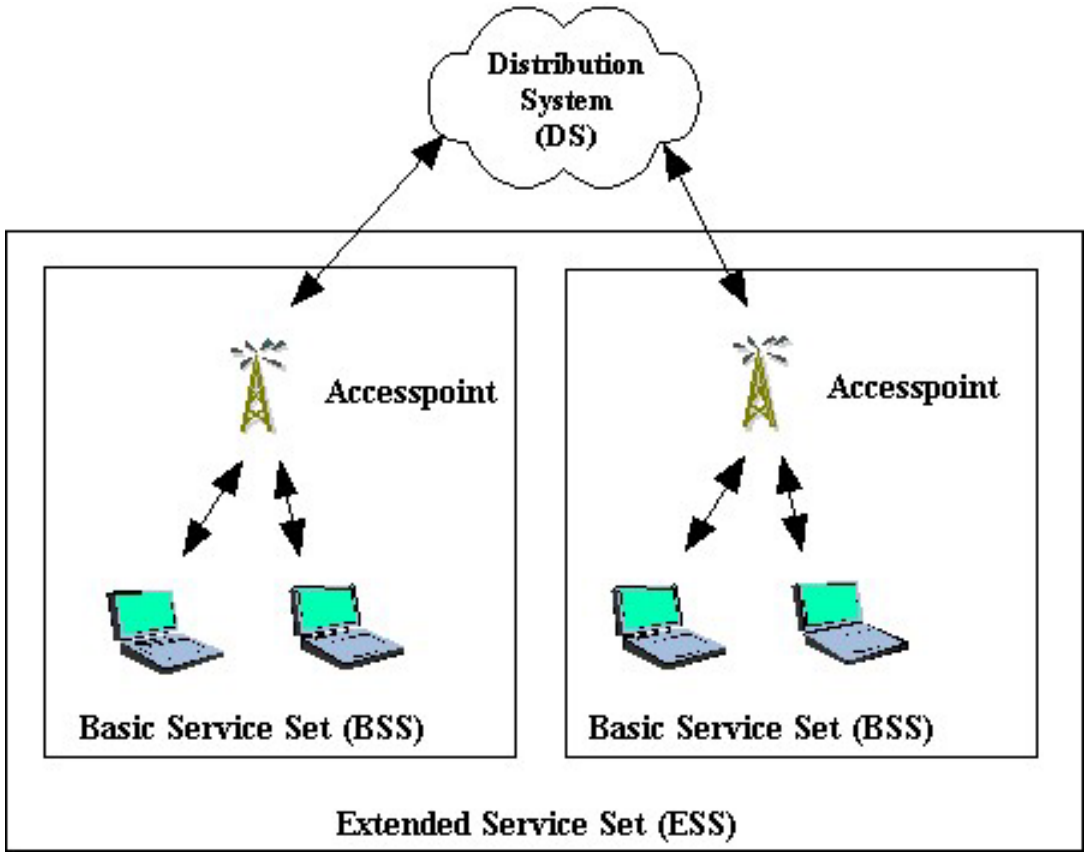


Infrastruktur-Modus mit LAN Anbindung

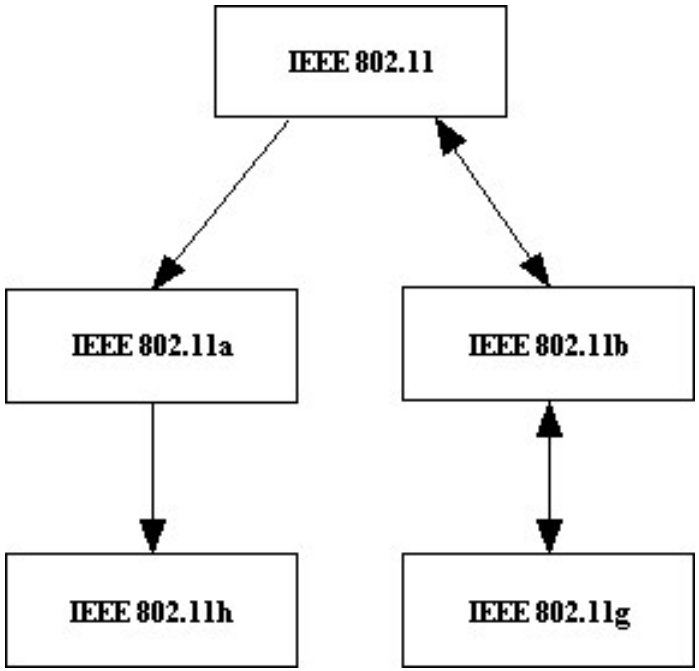
2.1 WLAN Grundlagen

- Basic Serves Set (BSS)
- Extended Service Set (ESS)
- Distribution System (DS)
- Basic Service Set transition (BSS-transition) (handover)

2.1 Extended Service Set and Distribution System



2.2 Migrations-Pfade



2.2 Standards - IEEE 802.11

- 2,4 GHz Frequenzband
- CSMA/CA
- Modulation: FHSS (Frequency Hopping Spread Spectrum) oder DSSS (Direct Sequence Spread Spectrum)
- Bruttodatenrate 1 bis 3 Mbps
- SSID (Service Set Identify) bzw. ESSID (Extended SSID)
- MAC-Adresse (Media Access Control)
- WEP

2.2 Standards - IEEE 802.11a

- 5,15 – 5,35 Ghz und 5,725 – 5,825 GHz
- Modulation: OFDM (Orthogonal Frequency Divison Multiplexing
- Bruttodatenrate bis 54 Mbps
- Störung durch Radar, Flugnavigationsdienste und Satellitenverbindungen
- 802.11h Erweiterung für Europäischen Markt , mit DFS (Dynamic Frequency Selection) und TPC (Transmission Power Control)

2.2 Standards - IEEE 802.11b

- 2,400 – 2,4835 GHz
- Modulation: DSSS (Direct Sequence Spread Spectrum),(CCK (Complimentary Code Keying) , PBCC (Packet Binary Convolutional Code))
- Bruttodatenrate bis 11 Mbps, mit PBCC bis 22Mbps
- Störungen durch andere ISM-Anwendungen

2.2 Standards - IEEE 802.11g

- Modulation: OFDM
- Abwärtskompatibel zu 802.11b durch Implementierung von CCK-OFDM und PBCC
- Bruttodatenraten bis 54Mbps

2.2 Standards - IEEE 802.11i

- TKIP (Temporary Key Integerity Protocol)
- AES
- Quality of Service
- Authentifizierung über Zertifikate, Username und Password oder SIM Karte (Subscriber Identification Module)

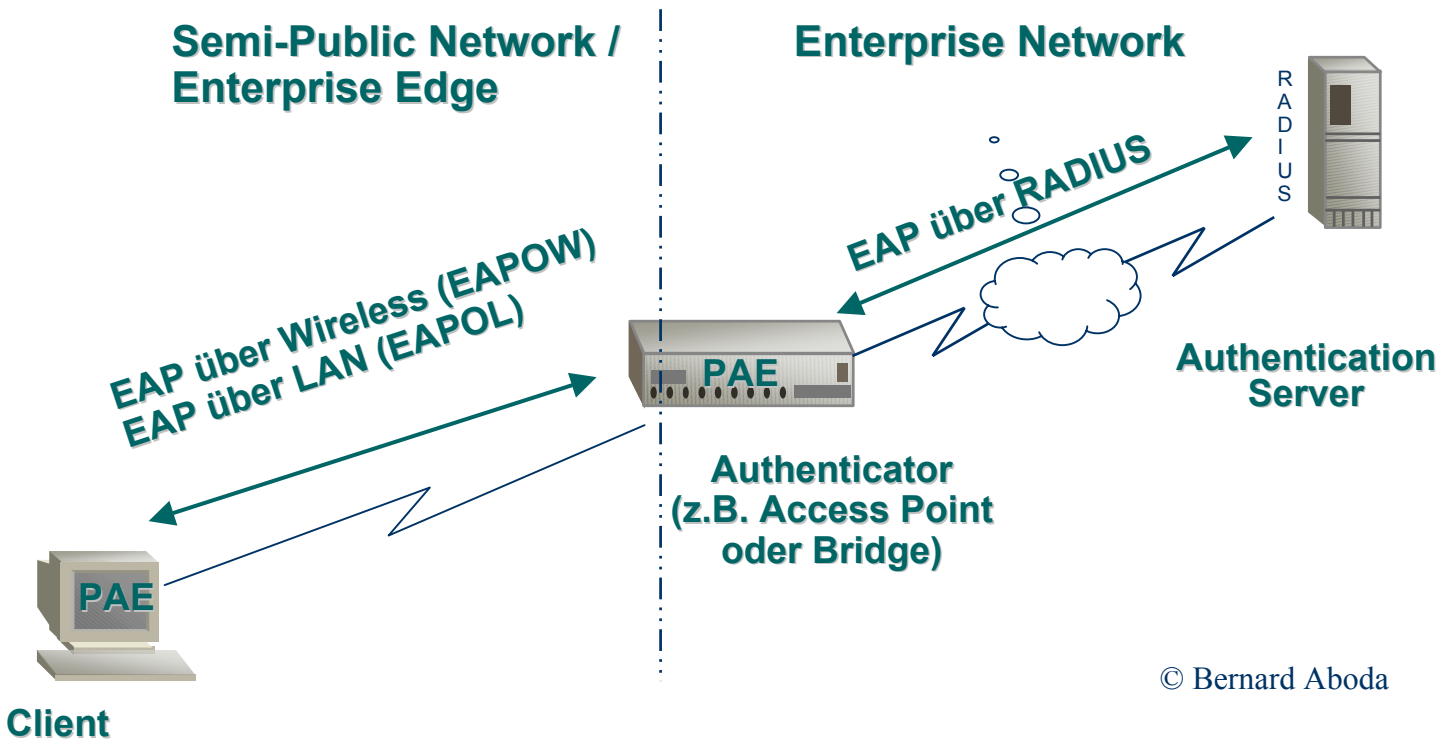
2.2 Temporal Key Integrity Protocol

- Re-Keying
- Per-Packet-Mixing
- Re-Sequencing
- Message Integrity Check (MIC)
- AES

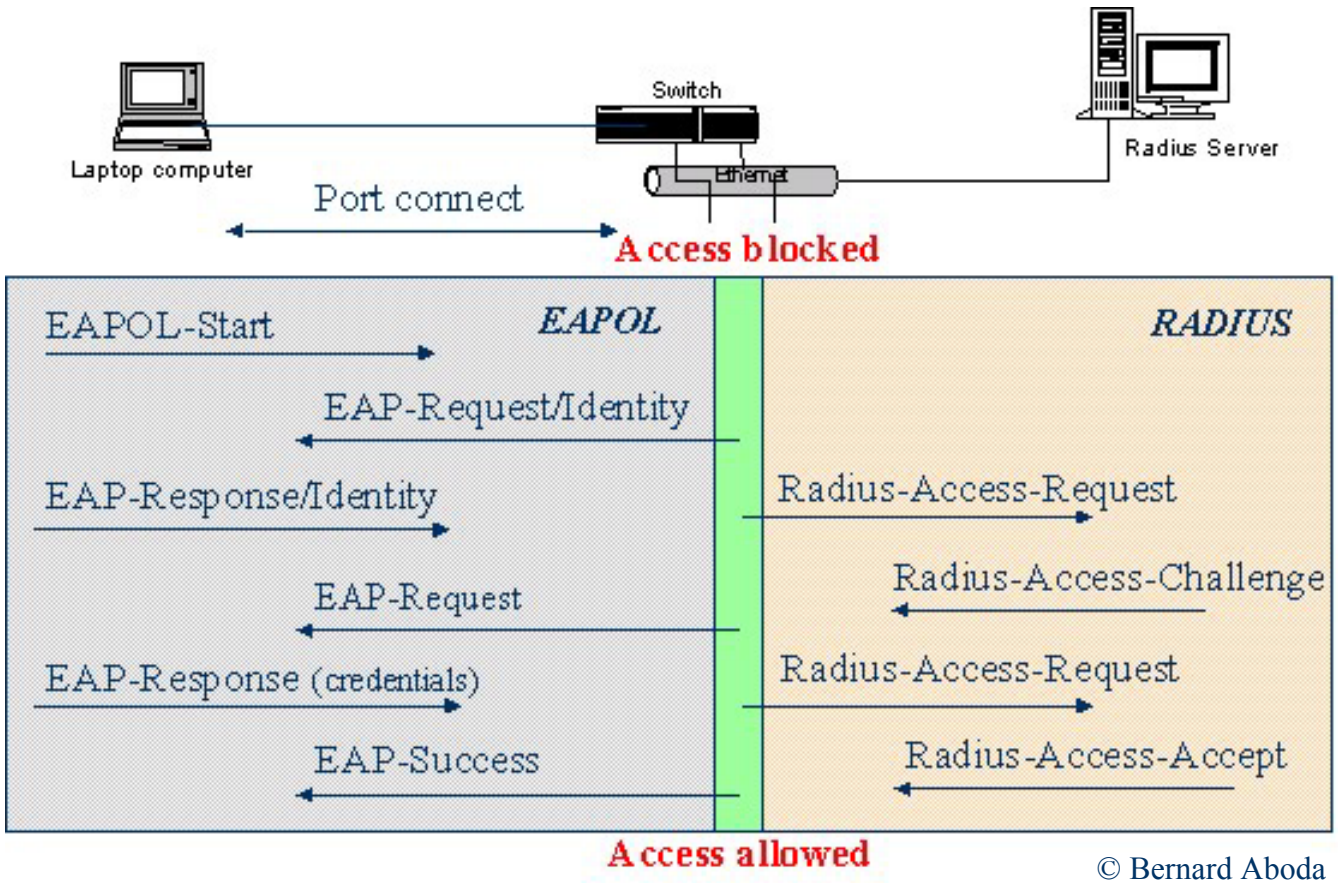
2.2 Standards – IEEE 802.1x

- Für Ethernet , WLan, Token Ring
- Benutzer basierte Authentifizierung
- Zentrale Authentifizierung und Administration (RADIUS)
- Dynamisches Key-Managemen
- EAP (Extensible Authentication Protocol)

2.2 Standards – IEEE 802.1x



2.2 Standards - EAP



2.3 Schwachstellen

- Shared Medium
- Räumlich nicht begrenzt
- Schlechte Grundkonfiguration
- (E)SSID
- Keine WEP Verschlüsselung im ad-hoc-Modus
- WEP ist nicht sicher

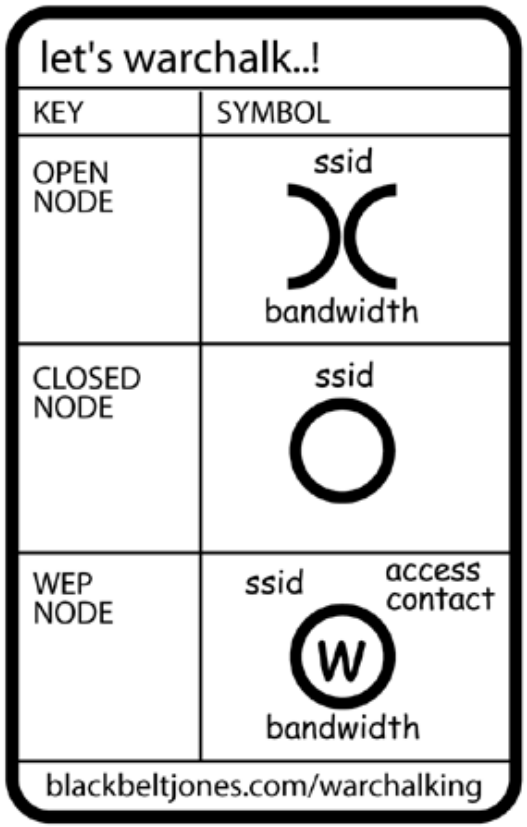
2.3.1 Angriffsmöglichkeiten

- Sniffing und monitoring
- Brute Force attack against Access Point Passwords
- denial of service
- jamming
- Hijacking / MITM
- client to client attack

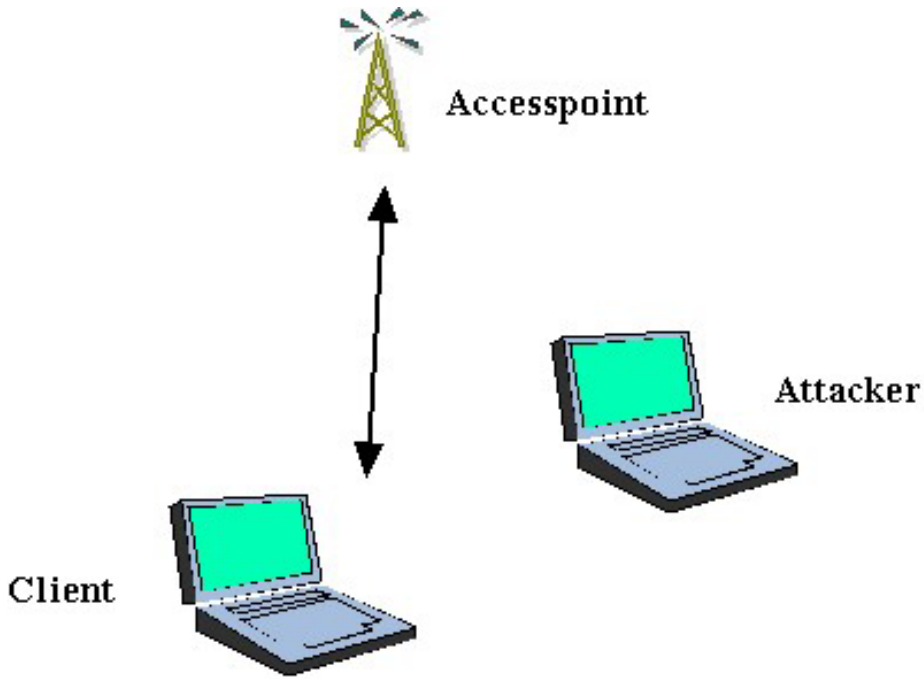
2.3.1 Sniffing

- Sniffing z.B. Netstumbler, Airopeek, Kismet ...
- WarDriving mit GPS Positionsaufzeichnung

2.3.1 Warchalk Symbole

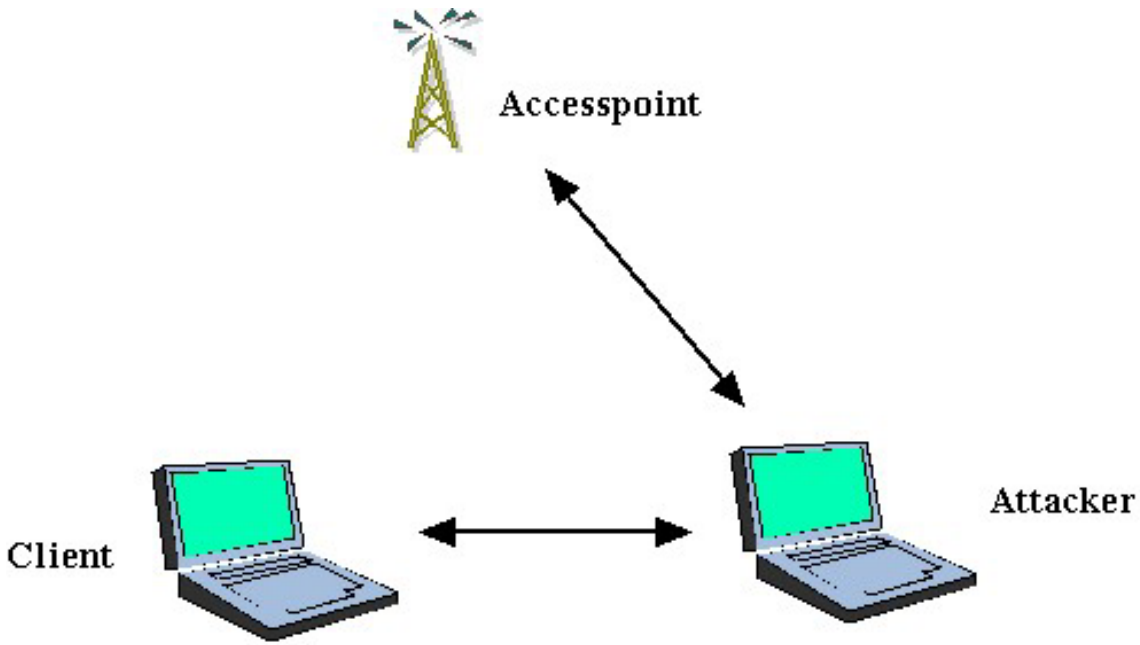


2.3.1 Hijacking / MITM



Normale Verbindung

2.3.1 Hijacking / MITM

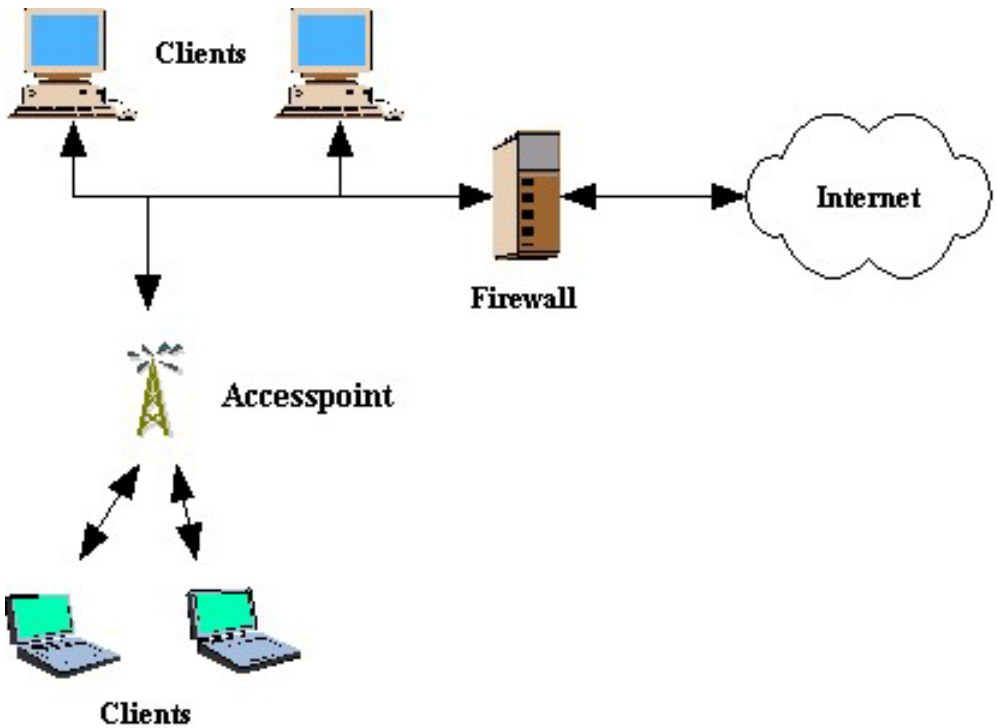


Hijacking einer Verbindung

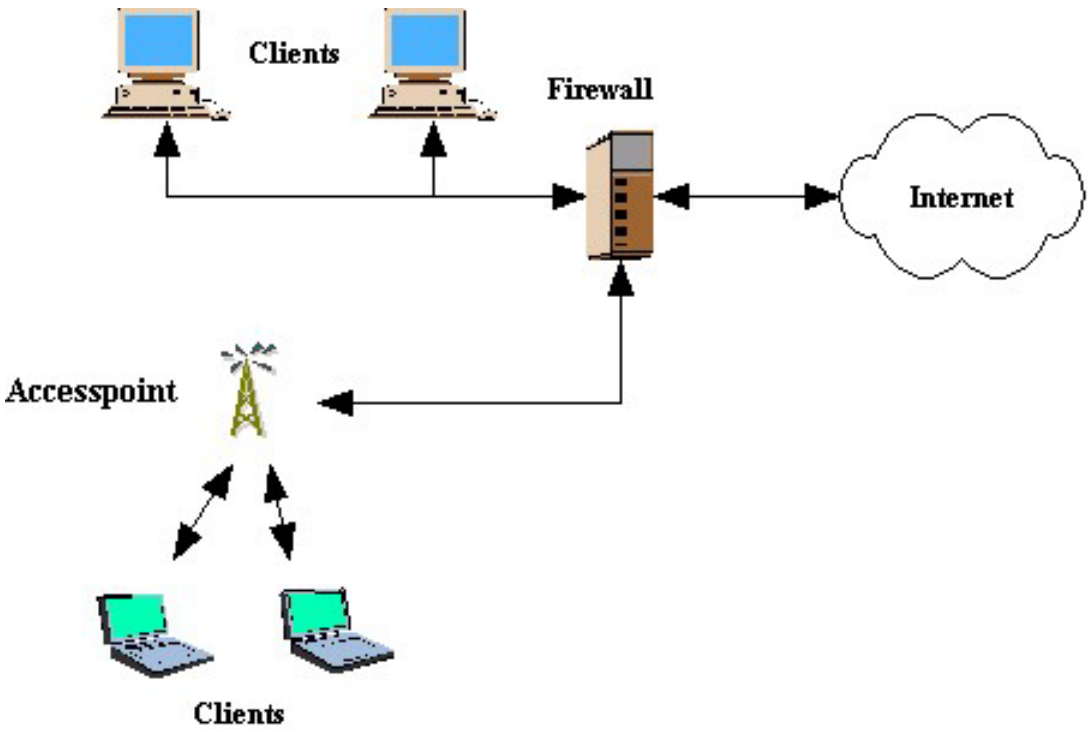
2.4 Absichern

- MAC Adressen Filtern, werden aber auch im Klartext übertragen
- Keine Beacons senden, SSID evtl. ausschalten
- WLAN behandeln wie externes Internet
- WEP benutzen
- EAP (Extensible Authentication Protocol) und RADIUS (Remote Authentication Dial in User Service), in IEEE 802.1x
- Layer 3 VPN über IPSEC
- Client: Personal Firewall verwenden

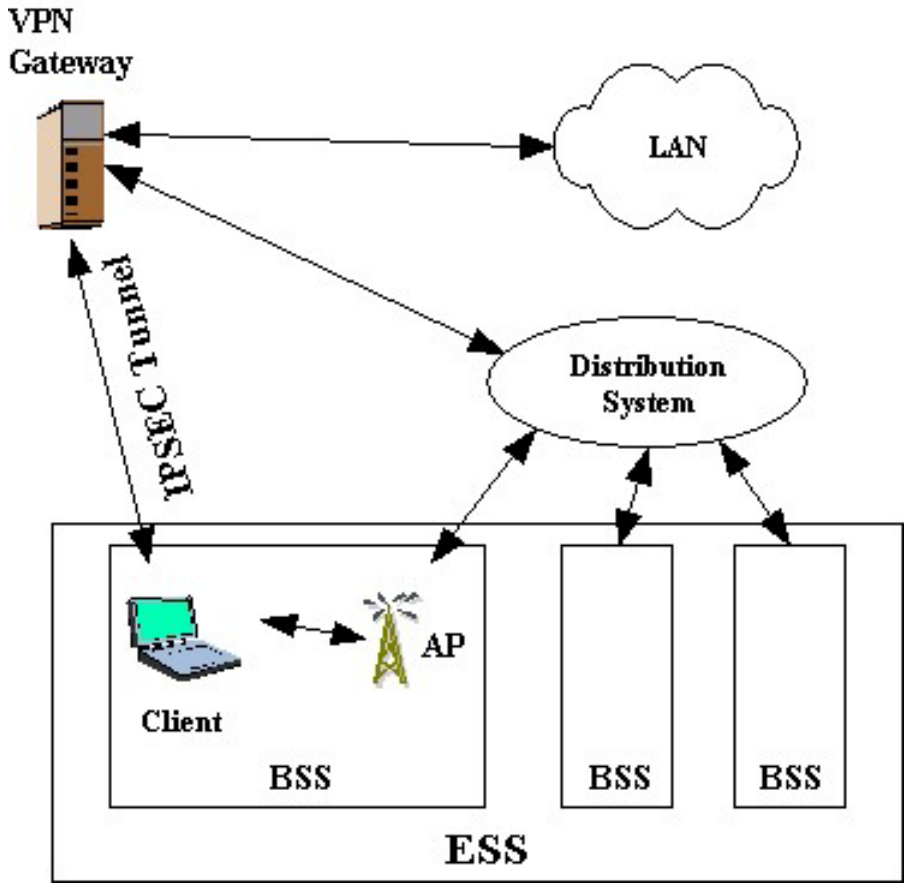
2.4.1 Netzarchitektur (falsch)



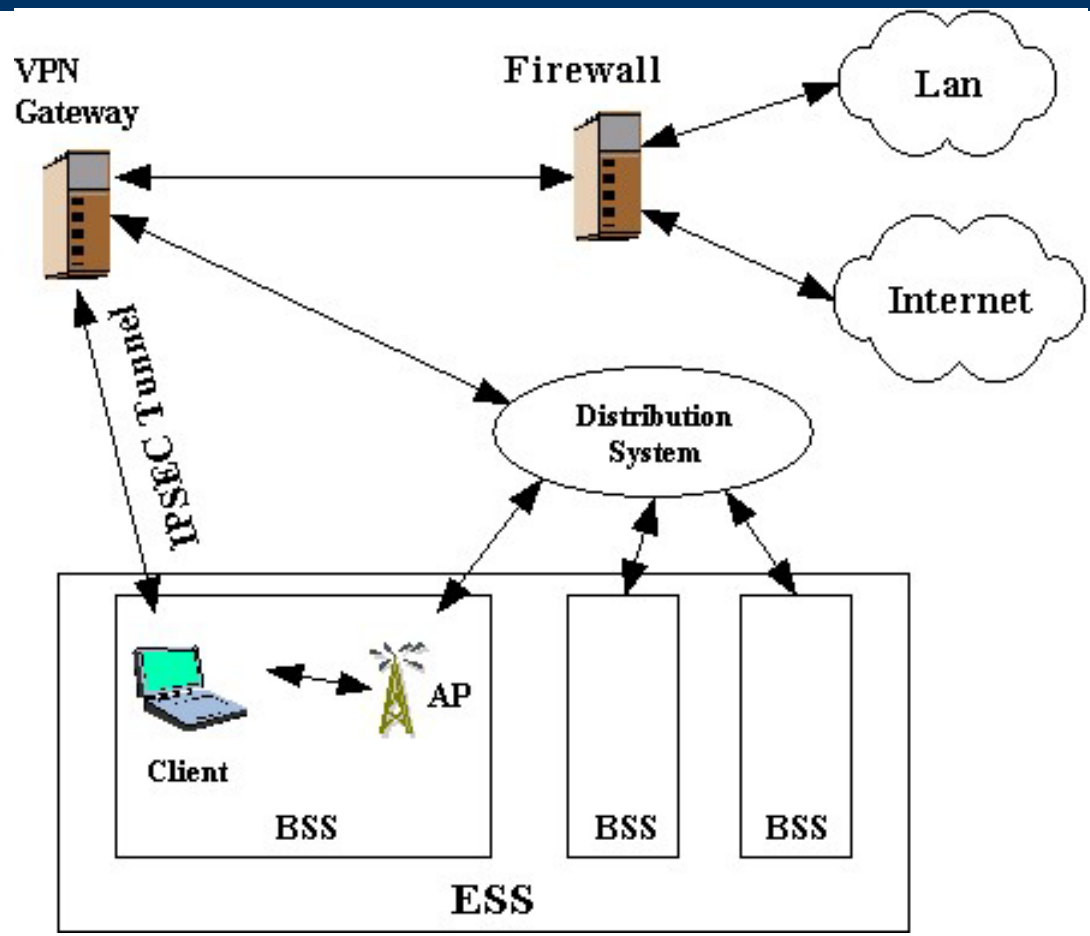
2.4.1 Netzarchitektur (besser)



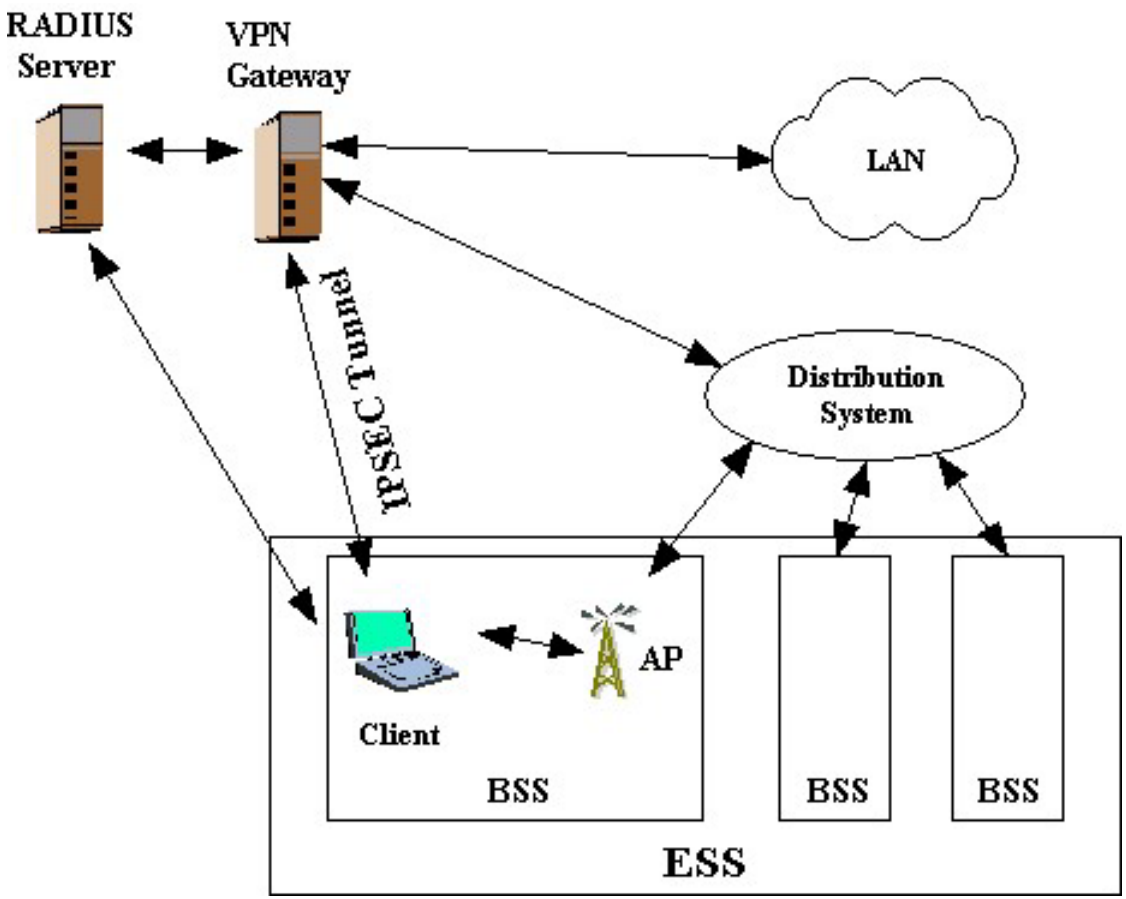
2.4.1 VPN über IPSEC



2.4.1 VPN über IPSEC mit Firewall



2.4.1 EAP mit Radius Server



3. WEP – Wired Equivalent Privacy

3.1 Grundlagen

3.2 Schwachstellen

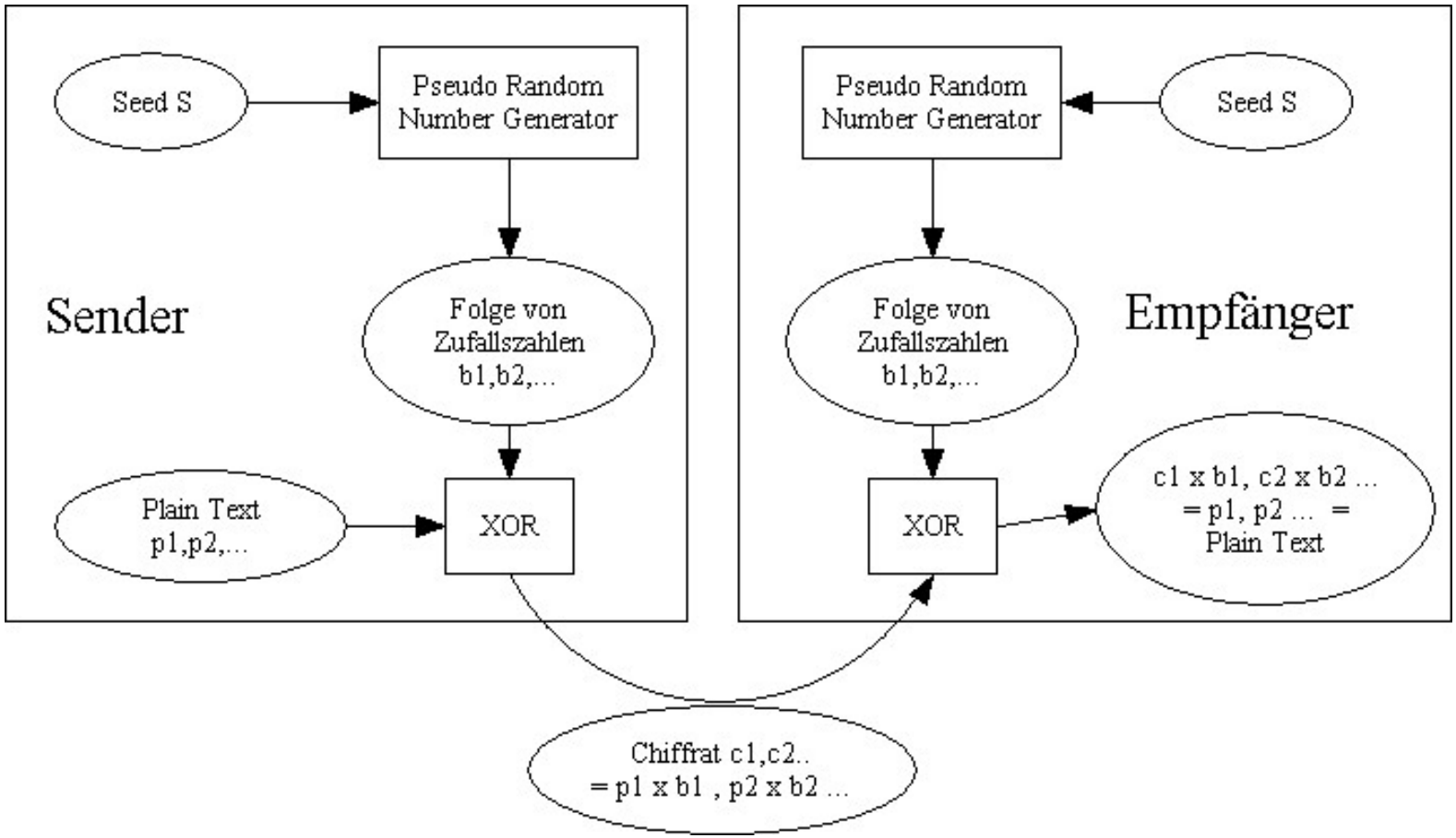
3.3 Angriffe

3.4 Absichern von WEP

3.1 WEP Grundlagen

- RC4 – symmetrisches Verschlüsselungsverfahren
- 40 und 104 Bit Schlüssel werden mit einem 24 Bit Initialisierungsvektor (IV) verknüpft, dadurch Schlüssellängen von 64 und 128 Bit
- Mit einem Seed wird ein Pseudozufallszahlengenerator initialisiert

3.1 Verschlüsselung mit Zufallszahlen



3.1 WEP Verschlüsselung Beispiel

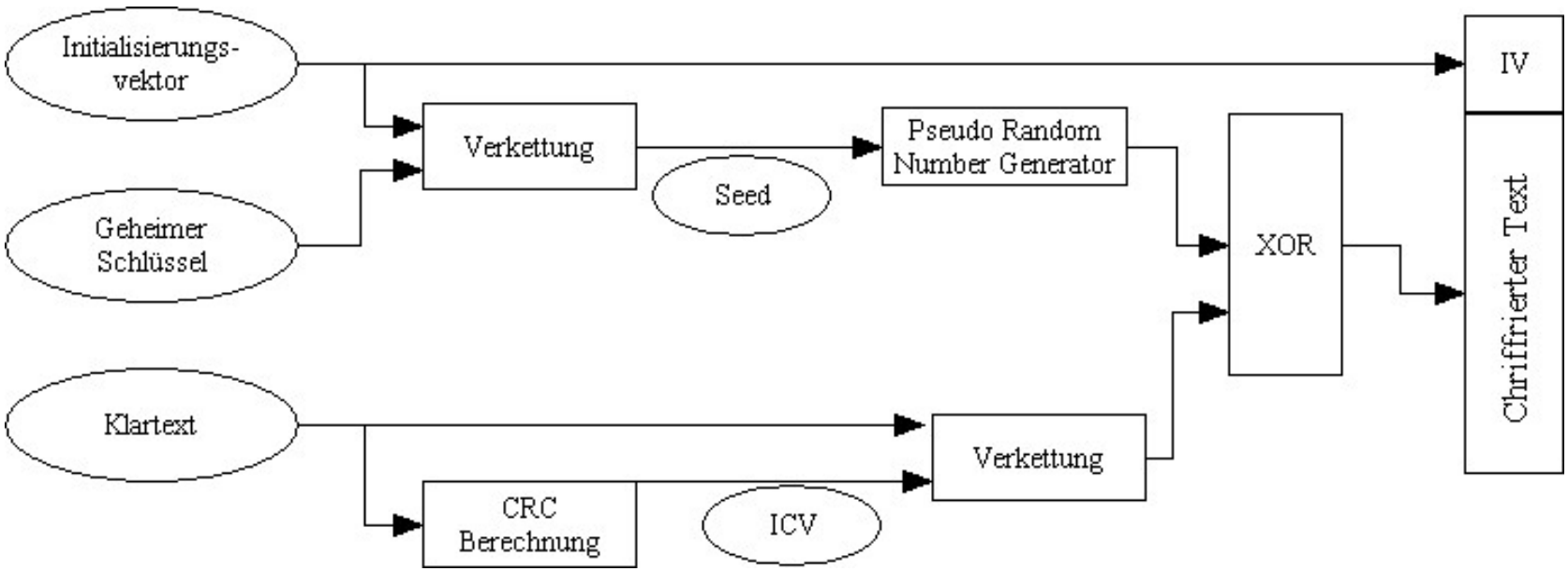
	Data
Buchstabe "a" Klartext	01100001
Buchstabe "n" secret key	01101110
XOR "a"	00001111

	Data
Buchstabe "b" Klartext	01100010
Buchstabe "n" secret key	01101110
XOR "b"	00001100

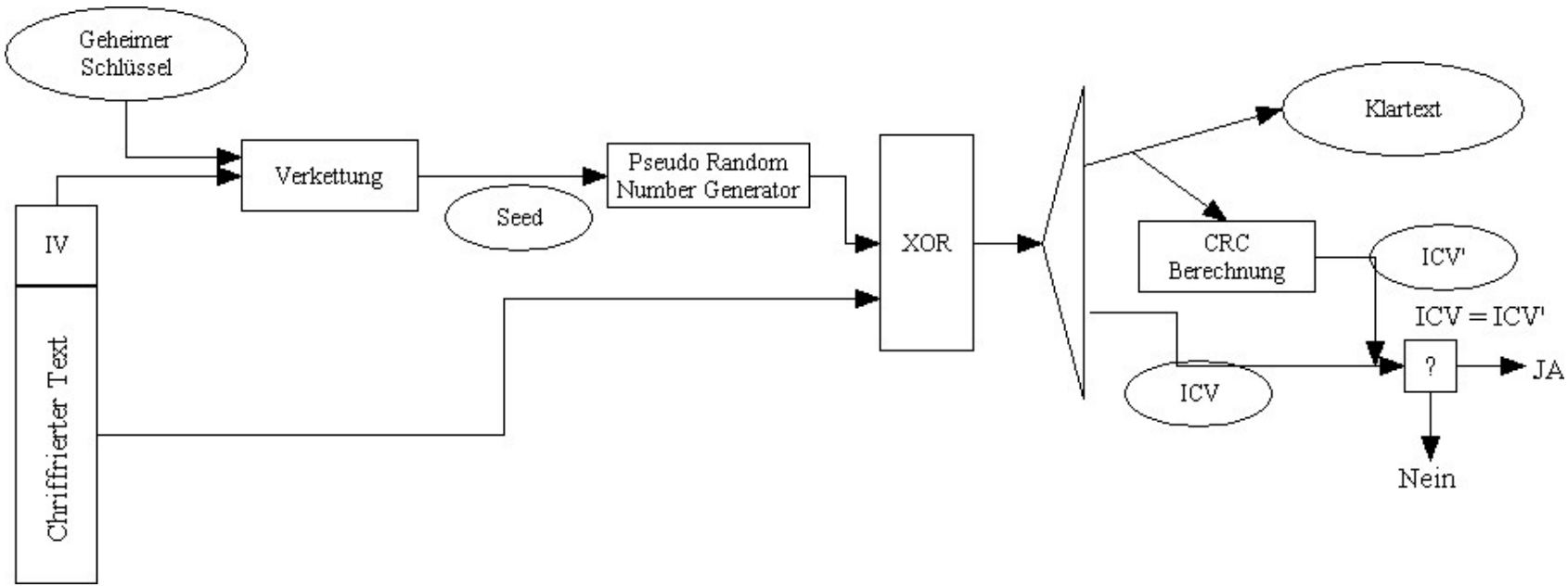
	Data
XOR "a"	00001111
XOR "b"	00001100
XOR - "a" & "b"	00000011

	Data
Buchstabe "a" Klartext	01100001
Buchstabe "b" Klartext	01100010
XOR - "a" & "b"	00000011

3.1 Verschlüsselung mit WEP



3.1 Entschlüsselung mit WEP



3.2 Schwachstellen in WEP

- Kein Schlüsselmanagement
- IV mit 24 Bit zu klein
- Einige Hersteller setzen den IV bei jeder Initialisierung auf 0 zurück und Inkrementieren dann um 1
- CRC32 ist linear
- RC4 schlecht implementiert

3.2.1 Schwachstellen - CRC

	Data	CRC8
Buchstabe "b" Klartext	01100010	00101001
Buchstabe "n" secret key	01101110	01101110
XOR Verschlüsselung	00001100	01000111

	Data	CRC8
XOR encryption	00001100	01000111
Change	00000011	00001001
Geänderte XOR Verschlüsselung	00001111	01001110

	Data	CRC8
Geänderte XOR Verschlüsselung	00001111	01001110
Buchstabe "n" secret key	01101110	01101110
Entschlüsselt : Buchstabe "a"	01100001	00100000

Checksumme für Buchstabe „a“ = 00100000 !!!

3.2.1 Initialisierungsvektor

Nur 2^24 Möglichkeiten = 16777216 IV´s

11Mbps / (1024 bytes per packet * 8)= 1342 packets per second

2^24 / 1342 packets per second = 12501 s

= 3,4 stunden !!!

3.3 Angriffe

- Passive attack to decrypt Traffic
- Active attack to Inject Traffic
- Active attack from Both Ends
- Table based attack

3.3.1 Passive attack

- Bestimmte Anzahl von Paketen mit demselben Schlüssel aber unterschiedlichen IV
- 1. Byte des IV Wert zwischen 3 und 15 , im 2ten Byte 255
- Davon ca 60 verschiedene IV‘s für jeden Wert zwischen 3 und 15
- Dadurch Berechnung des Schlüssels möglich
- Ca 4-6 Millionen Pakete Notwendig

3.3.1. Passive attack

	512 Byte	1024 Byte	2048 Byte
2.000.000	0,95	1,91	3,81
4.000.000	1,91	3,81	7,63
6.000.000	2,86	5,72	11,44
8.000.000	3,81	7,63	15,26

	5 Mbps	1 Mbps
0,95	3 min	16 min
1,91	7 min	33 min
2,86	10 min	49 min
3,81	13 min	65 min
5,72	20 min	98 min
7,63	26 min	130 min
11,44	39 min	195 min
15,26	52 min	260 min

3.3.1 Active attack to Inject Traffic

- Klartext einer verschlüsselten Nachricht bekannt
- Neue Nachricht machen, CRC32 berechnen und bits flippen (3.2.1)
- RC4(X) xor X xor Y = RC4(Y)
- Dadurch korrekt verschlüsselte Pakete die der AP akzeptiert

3.3.1 Active attack from Both Ends

- Manipulieren der Header
- IP Adresse wird geändert, dann Umleitung auf kontrollierten Rechner (durch Bit flippen)
- AP entschlüsselt und sendet weiter
- Dadurch Klartext auf dem Rechner

3.3.1 Table based attack

- Tabelle mit allen möglichen IV‘s
- Ca 15 GB
- Danach möglich alles zu entschlüsseln wenn einige Klartexte bekannt

3.4 Absichern

- Schlüsselmanagement
- Mindestens 104 Bit , 40 ist durch Brute Force brechbar

4. WAN

4.1 Grundlagen und Technik

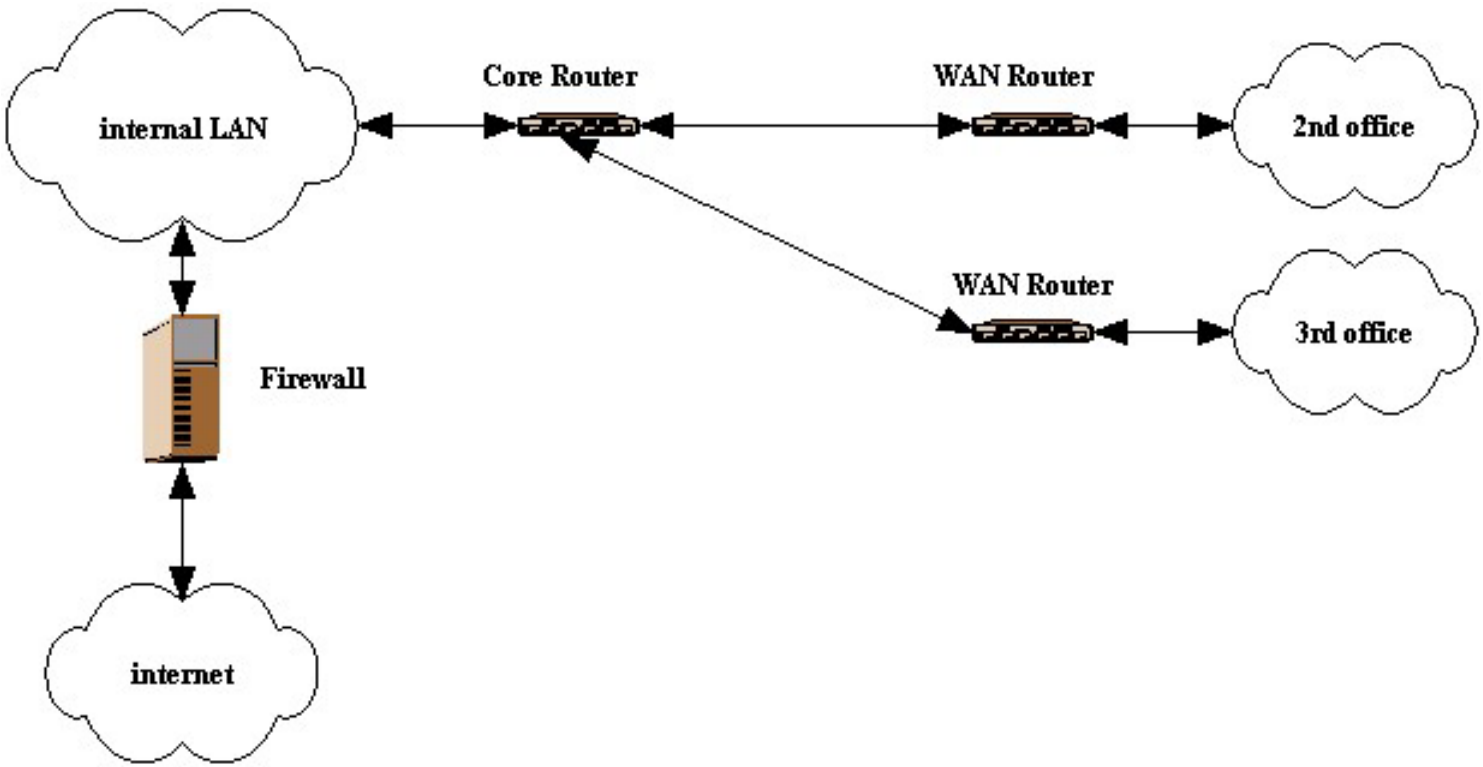
4.2 Sicherheitsrisiken

4.3 Absichern

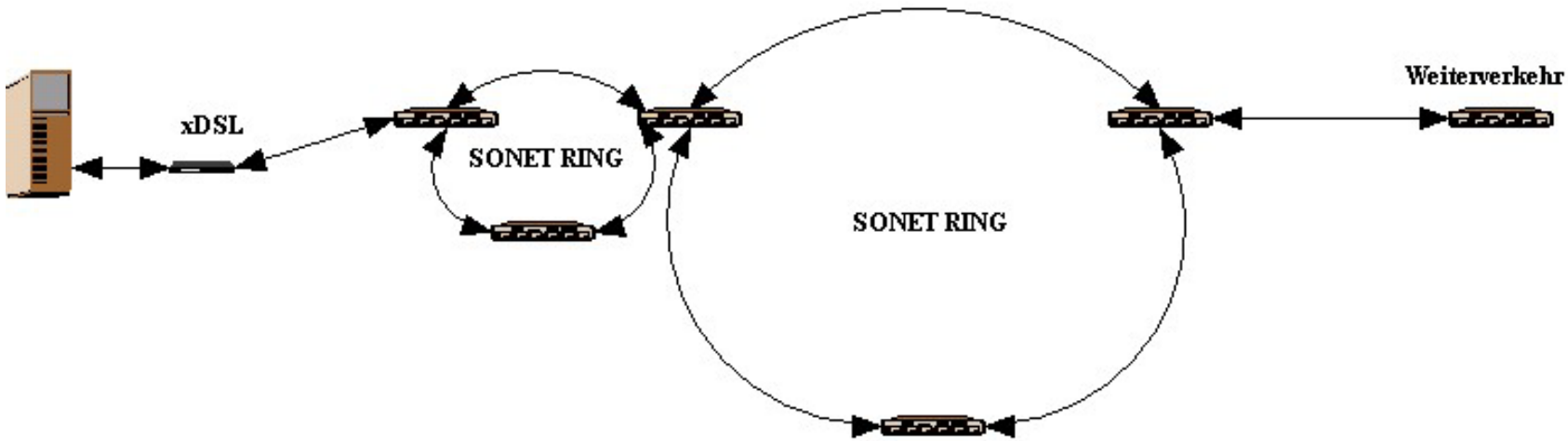
4.1 WAN Grundlagen

- WAN (Wide Area Network)
- SONET/SDH (Synchronous Optical NETwork / Synchronous Digital Hierarchy)
- ATM (Asynchronous Transfer Mode)
- Ethernet (Optical)

4.1 WAN Architektur (schlecht)



4.1 SONET Ring



4.1 SONET/SDH

Optical Level	Line Rate Mbps
OC-1	51.840
OC-3	155.520
OC-12	622.080
OC-48	2488.320
OC-192	9953.280
OC-768	39813.120

- Aufwendig
- Teuer
- Für Sprache
- > 40 Gbps

4.1 ATM

- Teuer
- > 622 Mbps

4.1 Ethernet

- Kostengünstig
- Leicht skalierbar
- Besser beherrschbar, da bekannter

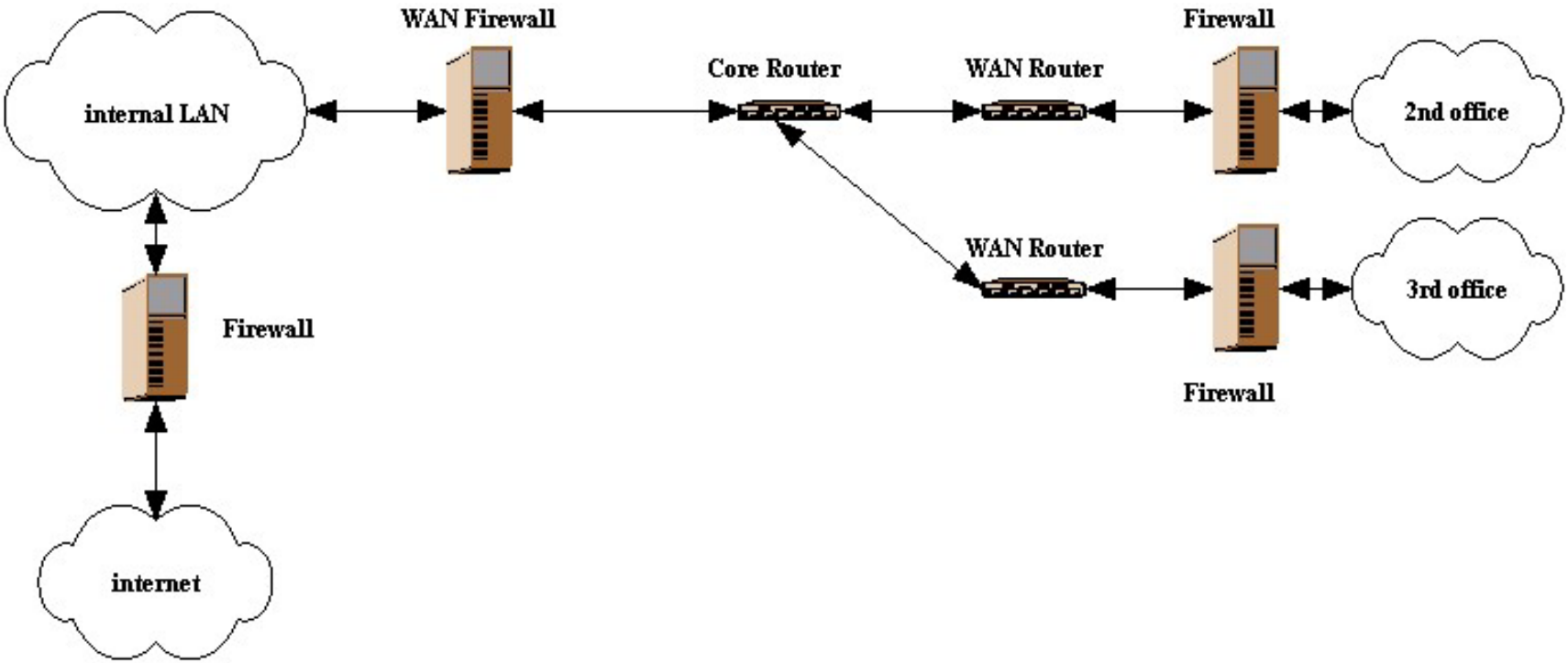
4.2 Sicherheitsrisiken

- Unerlaubters eindringen
- Spoofing etc...

4.3 WAN Absichern

- Firewall
- Authentifikation

4.3 WAN Architektur (besser)



5. Literatur

Ich habe zur Recherche meist PDF Dateien gelesen, in folgenden Links sind die wichtigsten aus verlinkt:

- http://www.drizzle.com/~aboba/IEEE/
- http://www.netalarms.com/cgi-bin/display_article.cgi?1210
- http://www.ethermanage.com/ethernet/ethernet.html

Bücher:

[1] Wireless LAN – Protokolle und Anwendungen , Axel Sikora, Addison-Wesley

Wer es genauer wissen möchte kann eine e-Mail an mich schicken und bekommt dann eine genaue Angabe der Literatur: 0muus@informatik.uni-hamburg.de

Vielen Dank