UMRnet

WLAN-Zugang für Laptops

Stand: *02.03.2006*

Suchen, Neues, akt. Nachrichten

Für den Zugang zum UMRnet/Internet mit einem privaten Laptop gab es innerhalb der Universität bisher nur den drahtgebundenen **LAN-Zugang**, wobei der Laptop via Kabel an eine Anschlussdose des Datennetzes anzuschließen ist; derartige Anschlussdosen gibt es vor allem in PC-Sälen, Hörsälen und Bibliotheken. Das HRZ hat jetzt ein Betriebskonzept erarbeitet, das auch den drahtlosen Zugang erlaubt; **WLAN**
steht für Wireless Local Area Network. Der drahtlose Zugang erfolgt über Funk zwischen Laptop und sogenannten Access Points, die nicht nur in Räumen, sondern auch in Fluren, Foyers oder außerhalb von Gebäuden installiert werden können; diese Bereiche werden als Hotspots bezeichnet. Der WLAN-Zugang kann sowohl von Studierenden als auch von Professoren und Mitarbeitern genutzt werden; erforderlich ist ein entsprechender Internet-Account des HRZ. Der Laptop muss mit einem Funkadapter (WLAN-Karte) ausgestattet sein.

Das Betriebskonzept umfasst nicht nur den Zugang zum UMRnet/Internet von einem Standort in Marburg aus, sondern auch von anderen Hochschulstandorten, soweit dort eine entsprechende Infrastruktur installiert ist. Grundlage ist das WiN des DFN-Vereins, das Konzept trägt die Bezeichnung **DFN-Roaming**: Wissenschaftler und Studierende sollen von Hochschulstandorten in Deutschland per WLAN auf das Hochschulnetz ihrer Hochschule zugreifen können, insb. bei Tagungen und Konferenzen; die gastgebende Hochschule stellt dabei die Zugangstechnik bereit, die Berechtigungsprüfung erfolgt anhand der Accounts der eigenen Hochschule.

Der LAN-Zugang ist dem WLAN-Zugang hinsichtlich Sicherheit und Störungsfreiheit, vor allem aber hinsichtlich Bandbreite überlegen. Beim LAN-Zugang steht dem Nutzer die Bandbreite (10 Mbit/s) voll zur Verfügung, beim WLAN-Zugang muss er sich die Bandbreite (11 bzw. 54 Mbit/s) mit anderen teilen.

Inhalt

▲ Zugang, Voraussetzungen, Nutzung, Infrastruktur, Hotspots

WLAN-Zugang

Der WLAN-Zugang für Laptops ist in den Internet-Zugang integriert und unterliegt damit der Benutzungsordnung. Dabei

- darf der Laptop nur als Client und für die in § 2 Abs. 1 der Benutzungsordnung genannten Aufgaben genutzt werden
- ist der Betrieb von Servern (insb. WWW-/MP3-Upload-Servern) ausdrücklich untersagt
- kann bei Missbrauch der Internet-Account gesperrt werden

Die IP-Adresse wird dynamisch zugeteilt. Verbindungsdaten (wie z.B. Username, IP-Adresse, Datum/Uhrzeit der Session, übertragenes Datenvolumern) werden wie beim Modem-/ISDN- und LAN-Zugang aufgezeichnet und max. 6 Monate aufbewahrt.

▲ Zugang, Voraussetzungen, Nutzung, Infrastruktur, Hotspots

Voraussetzungen für die Nutzung

Internet-Account (Username, Passwort) des HRZ für Studierende bzw. Professoren und Mitarbeiter und **Laptop** mit (onboard- oder PCMCIA-) Funkadapter inkl. Treiber-Software:

- Funkadapter gemäß IEEE Standard 802.11b/g (11Mbit/s bzw. 54 Mbit/s im 2,4 GHz-Bereich) und/oder 802.11a (54 Mbit/s im 5 GHz-Bereich) sowie Unterstützung des WPA-Sicherheitsstandards der Wi-Fi Alliance
- Unterstützung des Authentisierungs-Standards IEEE 802.1x durch das Betriebssystem
- Unterstützung des Authentisierungs-Protokolls EAP-TTLS durch eine spezielle Client-Software (z.B. OpenSource-Produkt SecureW2, Installationsanleitung)
- Wurzelzertifikat der DFN-Zertifizierungsinstanz (wie für die Browser-Nutzung mit Verschlüsselung)
- Bei Windows 98, ME, 2000 und XP müssen die TCP/IP-Eigenschaften auf "IP-Adresse automatisch beziehen" eingestellt sein.
- Der Laptop muss sich innerhalb des Bereichs eines Hotspots befinden; wo solche Hotspots in der Universität vorhanden sind, finden Sie in der Tabelle am Ende dieses Dokuments.

Es bedeuten:
IEEE: Institute of Electrical and Electronics Engineers (Standardisierungsorganisation)
Wi-Fi Alliance: Herstellervereinigung
WEP: Wired Equivalent Privacy (gilt nicht mehr als sicher)
WPA: Wi-Fi Protected Access (Nachfolge zu WEP, Teilmenge von IEEE 802.11i)
IEEE 802.11i: Standard für sichere Funkübertragung
IEEE 802.1x: Authentisierungs-Standard mit verschiedenen Authentisierungs-Protokollen (u.a. EAP-TTLS)
EAP: Extensible Authentication Protocol
TTLS: Tunneled Transport Layer Security

▲ Zugang, Voraussetzungen, Nutzung, Infrastruktur, Hotspots

Nutzung des WLAN-Zugangs

Zur Nutzung des WLAN-Zugangs müsssen Sie sich innerhalb des Bereichs eines Hotspots befinden; wo solche Hotspots in der Universität vorhanden sind, finden Sie in der Tabelle am Ende dieses Dokuments.

Schalten Sie Ihren Laptop ein, aktivieren Sie Ihren Funkadapter und stellen Sie sicher, das folgende Parameter richtig eingestellt sind:

- Internetprotokoll (TCP/IP): IP-Adresse automatisch beziehen
- Netzwerk-SSID: **UMRnet_staff** bzw. **UMRnet_students**
- Netzwerkauthentifizierung über **802.1x** und **EAP-TTLS-PAP**
- Verschlüsselung mit **WPA/TKIP**
- für EAP-TTLS verfügbares **DFN Toplevel Zertifikat**

Verbinden Sie sich nun mit dem WLAN:

- **Studierende** der Philipps-Universität Marburg nutzen die SSID UMRnet_students
- **Professoren und Mitarbeiter** der Philipps-Universität Marburg nutzen die SSID UMRnet_staff

und geben Ihren Benutzernamen mit dem richtigen Passwort ein.

- **Teilnehmer am DFN-Roaming**
  benutzen bitte zum Verbinden mit dem WLAN die SSID UMRnet_students und geben ihren Benutzernamen mit dem s.g. Radius "Realm" ein (z.B. mueller@uni-giessen.de)

Nach erfolgreicher Authentisierung erhält Ihr Laptop automatisch eine dynamisch generierte IP-Adresse zugewiesen. Sie können jetzt beliebige TCP/IP-Client-Anwendungen (wie z.B. Web-Browser, eMail-Programm, Telnet, SSH, FTP, News, IRC, u.a.) nutzen.

Sollten Sie sich aus der Reichweite des Hotspots entfernen, wird die Verbindung getrennt. Sie müssen sich dann wieder zum Hotspot begeben und sich neu authentisieren.

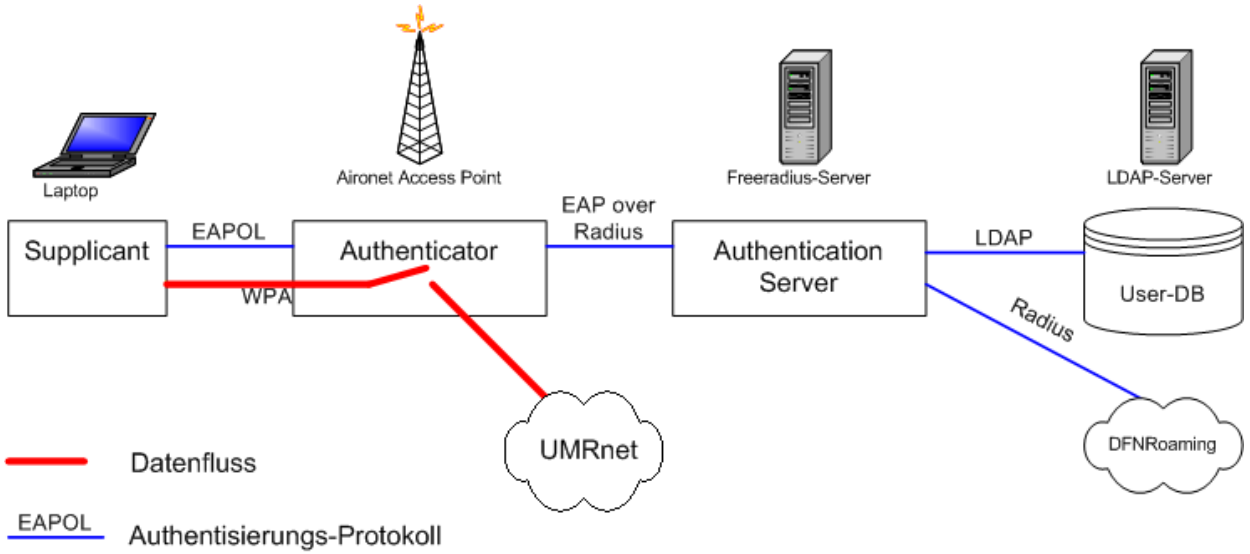
Beispielhaft finden Sie im Folgenden **Schritt für Schritt Anleitungen** zur Installation und Konfiguration der notwendigen Software:

- Windows XP Service Pack 2
- Windows XP Service Pack 1
- Windows 2000
- MacOS X
- Linux

▲ Zugang, Voraussetzungen, Nutzung, Infrastruktur, Hotspots

WLAN-Infrastruktur

Der Aufbau einer sicheren WLAN-Infrastruktur bedarf besonderer Vorkehrungen, da Funkverkehr grundsätzlich abgehört werden kann. Das ausgewählte Betriebskonzept soll diese **Sicherheit**
gewährleisten: Nur berechtigte Nutzer sollen Zugang erhalten, der Datenverkehr darf nicht abgehört werden können und insb. dürfen Username/Passwort nicht im Klartext übertragen werden. Die erforderlichen Komponenten sind im folgenden Bild dargestellt und werden anschließend näher erläutert.



Die **Authentisierung** für einen Netzzugang gemäß IEEE Standard 802.1x basiert auf einem allgemeinen, dreigeteilten Modell:

- der sogenannte Supplicant (*Supplikant, lat. für Bittsteller*), der den Zugang verlangt,
- der Authenticator, der den Zugang gewährt und
- der Authentication Server, der die Berechtigung überprüft.

Die Kommunikation zwischen dem Supplikanten, d.h. dem Betriebssystem bzw. der Client-Software, und dem Authentisierungs-Server, einem Radius-Server, basiert auf dem Authentisierungs-Protokoll EAP-TTLS; dabei werden Username und Passwort verschlüsselt übertragen. Hierfür muss der Nutzer einmal das Wurzelzertifikat der DFN-Zertifizierungsinstanz in das Betriebssystem seines Laptops laden. Je nach Medium kommen unterschiedliche Transportprotokolle zum Einsatz (EAPOL: Extensible Authentication Protocol over LAN; EAP over RADIUS: Remote Authentication Dial-In User Service). Da der Radius-Server selbst keine Benutzerinformationen vorhält, wird je nach Anfrage die User-Datenbank des HRZ (LDAP-Server) oder ein anderer Radius-Server, der am DFN-Roaming teilnimmt, befragt. Nach erfolgreicher Authentisierung gewährt der Access Point den uneingeschränkten Zugang zum UMRnet.

Zur Sicherung der **Funkstrecke**
zwischen Laptop und Access-Point kommt eine Weiterentwicklung der WEP-Verschlüsselung gemäß WPA zum Einsatz. Unterschiedliche Nutzer erhalten auf diese Weise unterschiedliche Schlüssel, die von Zeit zu Zeit neu ausgehandelt werden; statische Schlüssel brauchen nicht konfiguriert zu werden.

Eine Funkzelle, die von einem Access Point gebildet wird, kann mehrere Clients gleichzeitig bedienen; dabei teilen sich die Clients die zur Verfügung stehende Bandbreite (shared medium, ähnlich einem Ethernet-Koaxial-Kabelstrang). Verlässt ein Client eine Funkzelle, kann er von einer eventuell vorhandenen Nachbarfunkzelle unterbrechungsfrei übernommen werden (Roaming).

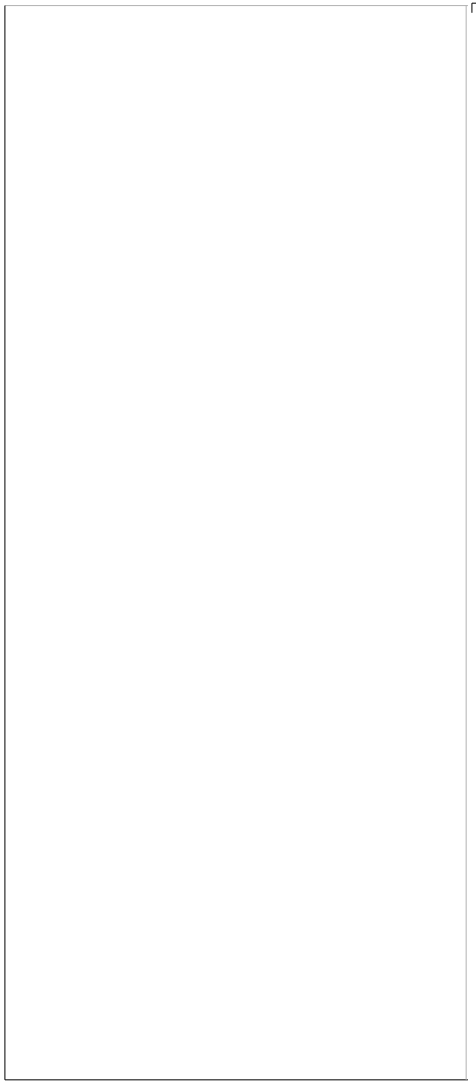
▲ Zugang, Voraussetzungen, Nutzung, Infrastruktur, Hotspots

Hotspots in Betrieb

Folgende Orte innerhalb der Gebäude der Philipps-Universität sind zurzeit mit WLAN-Hotspots versorgt:

in Betrieb					
Gebäude (Geb.-Nr.) Strasse, Haus-Nr.	**Versorgungsbereich**	**Access Point**	**Typ Funkstandart Frequenz**	**Position**	**Inbetriebnahme**
Alte Jägerkaserne (2010), Gutenbergstr.18	Bibliothek des FB 04	warz028	Cisco AIR-AP1230, 802.11a/b/g 2412 MHz (1), 5580 MHz (116), DFS	Bibliothek FB 04, 09/016	25.11.05
Alte Universität (2070), Lahntor 3	Foyer und Aufenthaltsbereich der Bibliothek des FB 05	warz036	Cisco AIR-AP1230, 802.11a/b/g 2437 MHz (6), 5220 MHz (44), DFS	Lichthof im Foyer	09.02.06
Alte Staatsbibliothek (2080), Universitätsstr. 25	Bibliothek des FB 02 im 1.OG	warz017	Cisco AIR-AP1230, 802.11a/b/g 2412 MHz (1), 5640 MHz (128), DFS	gr. Lesesaal, 04/012	13.10.05
	Dekanat des FB 02 im EG	warz018	Cisco AIR-AP1230, 802.11a/b/g 2437 MHz (6), 5700 MHz (140), DFS	Sitzungszimmer R10, 01/042	13.10.05
Savigny-Haus (2110), Universitätsstr. 6	Juristisches Seminar und Foyer im EG	warz019	Cisco AIR-AP1230, 802.11a/b/g 2412 MHz (1), 5260 MHz (52), DFS	Raum 16, 02/002	25.11.05
Physik, Mainzer Gasse 33 (2250)	Bibliothek des FB 13	warz032	Cisco AIR-AP1230, 802.11a/b/g 2412 MHz (1), 5180 MHz (36), DFS	Raum 60, 2/007	12.12.05
Fachbereich Pharmazie, Gebäude B (2311)	EG, Foyer	warz034	Cisco AIR-AP1230, 802.11a/b/g 2412 MHz (1), 5280 MHz (56), DFS	Foyer, 07/010	07.02.06
Hörsaalgebäude (2370), Biegenstr.14	Erdgeschoss			warz006	Cisc 802.1

		2462 MHz (11), 5320 MHz (64), DFS		
	warz007	Cisco AIR-AP1230, 802.11a/b/g 2412 MHz (1), 5540 MHz (108), DFS	vor HS 6, 03/012	05.10.05
	warz008	Cisco AIR-AP1230, 802.11a/b/g 2437 MHz (6), 5180 MHz (36), DFS	vor WC, 03/022	05.10.05
	warz015	Cisco AIR-AP1230, 802.11a/b/g 2437 MHz (6), 5620 MHz (124), DFS	Cafe Leonardo, 05/015	19.10.05
1. Obergeschoss	warz009	Cisco AIR-AP1230, 802.11a/b/g 2437 MHz (6), 5180 MHz (36), DFS	vor HS 116, 02/016	05.10.05
	warz010	Cisco AIR-AP1230, 802.11a/b/g 2462 MHz (11), 5660 MHz (132), DFS	vor HS 115, 02/002	05.10.05
	warz011	Cisco AIR-AP1230, 802.11a/b/g 2412 MHz (1), 5280 MHz (56), DFS	vor WC, 02/012	05.10.05
	warz016	Cisco AIR-AP1230, 802.11a/b/g 2462 MHz (12), 5560 MHz (112), DFS	HS 114, 02/014	19.10.05
2. Obergeschoss		Cisco AIR-AP1230, 802.11a/b/g		


Cisco AIR-AP1230,

		warz002	Cisco AIR-AP1210, 802.11a/b/g 2462 MHz Channel 11, 5320 MHz Channel 64	Raum A6704, 29/014	27.04.05
	Ebene A5	warz003	Cisco AIR-AP1210, 802.11b/g 2412 MHz Channel 1	Flur vor A5612, 03/003	07.09.05
		warz004	Cisco AIR-AP1210, 802.11b/g 2437 MHz Channel 6	Flur vor A5623b, 02/036	07.09.05
	Foyer A3	warz005	Cisco AIR-AP1210, 802.11b/g 2462 MHz Channel 11	Wand zum Innenhof A3, 43/001	07.09.05
	Ebene D5	warz025	Cisco AIR-AP1230, 802.11a/b/g 2462 MHz (11), 5260 MHz (52), DFS	Flur vor D5437, 19/029	11.11.05
	Ebene D4	warz026	Cisco AIR-AP1230, 802.11a/b/g 2437 MHz (6), 5700 MHz (140), DFS	Bibliothek des FB 12, Raum D4417, 11/035	14.11.05
	Ebene C4	warz027	Cisco AIR-AP1230, 802.11a/b/g 2412 MHz (1), 5560 MHz (112), DFS	Raum C4352, 14/015	14.11.05
Chemie (3070), Hans-Meerwein-Str.	Foyer zwischen C3 und D3	warz020	Cisco AIR-AP1230, 802.11a/b/g 2412 MHz (1), 5540 MHz (105), DFS	Foyer D3, 36/002	04.11.05
ZMB (3105), Conradistr.	Zentrale Medizinische Bibliothek	warz030	Cisco AIR-AP1230, 802.11a/b/g 2412 MHz (1), 5180 MHz (36), DFS	Aufzugsrückwand im ZG, 05/012	05.12.05

Geplante Hotspots

Folgende Orte innerhalb der Gebäude der Philipps-Universität sind zurzeit für WLAN-Hotspots vorgesehen:

in Arbeit

Gebäude	Ort	Stand der Arbeiten	zzt. zuständig	angemeldet	Fertigstellung		Anzahl Access Points
					geplant	realisierbar	
Alte Universität (2070), Lahntor 3	Aufenthaltsbereiche im 1.OG und Seminarräume im 2.OG	Konfiguration und Montage des AccessPoints	HRZ (Borsdorf)	Jan. 06	Mrz. 06	Mrz. 06	1
Gebäude Biegenstr. 12 (2361), EG	Senats-Sitzungssaal	vorhandene Verkabelung kann genutzt werden, Austausch des Access-Swtches notwendig	HRZ (Borsdorf)	Jan. 06	Mrz. 06	Mrz. 06	1
BMFZ (3075), Hans-Meerwein-Str.	Aufenthaltsbereich in Ebene 0	Konfiguration und Montage des AccessPoints	HRZ (Borsdorf)	Jan. 06	Mrz. 06	Mrz. 06	1
Fachbereich Biologie	Aufenthaltsbereich um D1 und gr. Hörsaal	Verkabelung ist beauftragt	HRZ (Kesper) / Fa. Heinrich	Nov. 05	2.Q 2006	Mrz. 06	1
Fachbereich Chemie	Bibliothek in A7	Verkabelung ist beauftragt	HRZ (Kesper) / Fa. Heinrich	Feb. 05	2.Q 2006	Mrz. 06	1
Gesamt							**5**

in Planung							
Gebäude	Ort	Stand der Arbeiten	zzt. zuständig	angemeldet	Fertigstellung		Anzahl Access Points
					geplant	realisierbar	
Physik, Laborbau 2 (2263)	Bereiche um die Switchstandorte im Gebäude	vermutlich keine Verkabelungsarbeiten notwendig	FB13 (Schrimpf) / HRZ (Borsdorf)	Apr. 05	3.Q 2005	1.Q 2006	2
Mensa Erlenring, Erlenring 5	Cafè Journal	Vorbereitung zur Montage, Fragen zum Brandschutz sind noch zu klären	Moog (StW)	Okt. 05	Dez. 05	unbestimmt	1
Mensa Lahnberge	Cafeteria	Zustimmung des Studentenwerks fehlt noch	Moog (StW) / HRZ (Borsdorf)	Okt. 05	Dez. 05	unbestimmt	1
Gesamt							**4**

Bedarf angemeldet							
Gebäude	Ort	Stand der Arbeiten	zzt. zuständig	angemeldet	Fertigstellung		Anzahl Access Points
					geplant	realisierbar	
GWS, Block A (2390)	Bibliothek im 3. und/oder 4.OG	TP-Verkabelung für Block A und PC-Saal FB09 ist noch in der Planung	FB09 (Künzel) / HRZ (Borsdorf/Kesper)	Mrz. 05	unbestimmt	unbestimmt	1

BMFZ (3075), Hans-Meerwein-Str.	Seminarräume in Ebene 0	Klärung der Notwendigkeit	FB20 / HRZ (Kreile)	Jan. 06	unbestimmt	unbestimmt	1
Mehrzweckgebäude (3060)	Buffet Lahnberge	Verkabelung im Rahmen anderer Projekte Zustimmung des Studentenwerks fehlt noch	HBM (Bipp) / HRZ (Borsdorf)	Okt. 05	Jun. 06	unbestimmt	1
Mehrzweckgebäude (3060)	weitere Seminarräume und Hörsäle des FB 12	weiterer Ausbau zurückgestellt wg. dringender Projekte	FB12 (Sommer) / HRZ (Borsdorf)	Apr. 05	1.Q 2006	unbestimmt	4
Gesamt							**7**

Uni Marburg / HRZ / UMRnet / WLAN-Zugang für Laptops ▲

Christian Borsdorf (erste Fassung: *28.02.2005*, voriger Stand: *15.02.2006*)