

Schnurlos auf Draht

Jens-Uwe Winks | Computer- und Medienservice, Systemsoftware und Kommunikation | winks@cms.hu-berlin.de

Chronologie

Seit dem Jahr 2001 wird an der HU ein zentral verwaltetes WLAN betrieben. Angefangen wurde der WLAN-Betrieb mit WEP-Verschlüsselung und MAC-Authentifizierung der Clients. Dieses Verfahren war sehr simpel, sehr unsicher, dafür aber durch fast alle Clients benutzbar.

Um die Sicherheit im Netz und für die Clients zu erhöhen, mussten neue Verfahren geplant und eingesetzt werden. Ziel war es, bei jeder Anmeldung am WLAN die Benutzerdaten zu prüfen, also eine persönliche Anmeldung sicherzustellen. Weiterhin sollten die Sicherheitsstandards bei der Verschlüsselung angepasst werden. Es zeigte sich, dass die vorhandenen Accesspoints den Anforderungen, die die neuen Technologien stellen, technisch nicht genügten und es seitens des Herstellers für diese Accesspoints keine Weiterentwicklung geben würde. Das Problem: Es waren schon rund 300 Accesspoints campusweit verbaut. Es blieb also nur ein Weg: Der Austausch aller Geräte.

Im Rahmen eines Trade-in-Programms der Firma Enterasys konnten die alten Accesspoints günstig ersetzt werden. Der Austauschprozess zog sich mehr als ein Jahr hin. Als etwa die Hälfte der Accesspoints getauscht waren, bekamen wir Unterstützung von 2 netten Studenten, die den restlichen Austausch in etwa 8 Wochen durchzogen. Außerdem gab es auch oft von Administratoren in den Instituten Unterstützung und Zuarbeit. Bereits während der Austauschphase, ab etwa Februar 2007, folgte die erste Stufe der Umstellung. In Gebäuden, die komplett auf neue WLAN-Accesspoints um-

gestellt waren, gab es nun die Möglichkeit, verschiedene WLAN-SSIDs, also mehrere WLANs pro Accesspoints, anzubieten. So wurde an diesen Orten ein weiteres WLAN eröffnet. Es hat heute campusweit die SSID HU-VPN. Der Zugang zu diesem WLAN ist für alle Clients ohne Voranmeldung offen, nur die Benutzung eines VPN-Clients ist eine zwingende Voraussetzung, um eine Verbindung zum Internet aufzubauen.

Nach dem Austausch der Accesspoints, der im Sommer 2007 abgeschlossen war, unterstützten alle Accesspoints die höheren Geschwindigkeiten der Standards IEEE 802.11a und IEEE 802.11g mit Bruttoübertragungsraten von bis zu 54 Mbit/s. Dies war eine weitere positive Nebenwirkung des Austauschprogramms.

Dann folgte die nächste Phase der Umstellung. Das bisher am CMS angebotene VPN-Verfahren unterstützt nur Notebooks mit einem proprietären VPN-Client von Cisco. Eine schöne Ergänzung dazu stellt SSL-VPN dar (siehe vorhergehender Artikel „SSL-VPN-Zugang mit SA 4000“). Ab September 2007 wurde das SSL-VPN-Gateway offiziell in Betrieb genommen. Bei der nächsten Stufe der Umstellung, Ende Oktober 2007, wurde die Anmeldung von MAC-Adressen für das alte Wireless Campus Network eingestellt, die Nutzung dieses WLANs war aber weiterhin möglich.

Am 16.03.2008 erfolgte der Abschluss der Umbauarbeiten im WLAN: Das alte, unsichere WLAN wurde abgeschaltet und ein neues WLAN wurde in Betrieb genommen: HU-802.1X. In diesem WLAN ist die Verwendung eines Clients erforderlich, der IEEE 802.1X mit EAP

Der folgende Artikel gibt eine Übersicht über den Einsatz neuer Technologien im WLAN an der HU. Dabei liegt der Schwerpunkt der Betrachtungen auf der Sicherheit, der Entwicklung und Chronologie und den Ausblicken. Auf technische Standards und Definitionen wird weniger eingegangen.

(Extensible Authentication Protocol) nach der Methode EAP-TTLS und PAP unterstützt. EAP ist ein Standardverfahren, welches das Anmelden eines Nutzers an einer Netzwerkkomponente ermöglicht. Des Weiteren wird im WLAN HU-802.1X eine Verschlüsselung nach WPA und WPA2 zwischen WLAN-Client und Accesspoint angeboten. Diese gilt als sehr sicher.

Zugang zum HU-WLAN

Voraussetzungen

- Account
- WLAN-Karte
- Software
- Zugangsdaten

Account

Voraussetzung für den Zugang zum HU-WLAN ist ein Account (Benutzerkennzeichen + Passwort). Dieser Account muss an einer der folgenden Einrichtungen registriert und gültig sein:

- CMS (Computer- und Medienservice)
- Institut für Informatik
- Institut für Mathematik
- Institut für Physik
- Universitätsverwaltung

Eine Zugangsmöglichkeit für Gäste wird weiter unten beschrieben.

WLAN-Karte

Eine weitere Voraussetzung für den WLAN-Zugang ist eine WLAN-Karte. Im HU-WLAN werden die Standards IEEE 802.11b/g (11 und 54 MBit/s auf 2,4 GHz) und IEEE 802.11a (54 MBit auf 5 GHz) unterstützt.

Software

Auf dem Rechner, der mit dem WLAN verbunden werden soll, muss sich eine Software zur Anmeldung am WLAN befinden. Dabei gibt es 3 grundsätzliche Möglichkeiten:

- Cisco VPN Clientsoftware
- WWW-Browser (Internet Explorer, Mozilla Firefox, Safari)
- 802.1X Clientsoftware

Die einzelnen Möglichkeiten werden nachfolgend kurz beschrieben. Welche der drei Möglichkeiten genutzt werden sollte, hängt von den individuellen Voraussetzungen ab. Dabei spielt es eine Rolle, welche Art von mobilem Gerät eingesetzt und welche Software darauf betrieben wird.

Am Ende dieses Abschnitts gibt es einen kurzen Überblick mit empfehlenden Überlegungen.

VPN-Clientsoftware

Zur Anmeldung im VPN-WLAN ist ein VPN-Client Voraussetzung. VPN steht für „Virtual Private Networking“ und erlaubt die authentifizierte und verschlüsselte Übertragung von Daten zwischen einem PC oder Laptop und einem VPN-Gateway. Es werden am CMS zwei Arten angeboten:

Cisco-VPN

Cisco-VPN erfordert die einmalige Installation eines VPN-Clients. Das ist die Software, die die Tunnel aufbaut, die Anmeldung ausführt und die Verschlüsselung realisiert. Diese Software gibt es für Linux, Windows und MacOS. Installations- und Konfigurationsanleitungen sowie die Software selbst gibt es unter <http://www.cms.hu-berlin.de/dl/netze/vpn/>.

Anmeldung mit Web-Browser

Dies ist eine sehr einfache Variante, die ohne vorherige Softwareinstallation genutzt werden kann. Das SSL-Gateway kann zunächst in seiner einfachsten Form durch den Browser als Proxy benutzt werden und gestattet so jedem Client mit einem javafähigen-Web-Browser die Benutzung des WLANs.

Weiterhin erlaubt SSL-VPN den Aufbau eines VPN-Tunnels (Network Connect). Dadurch steht über das SSL-Gateway eine vollwertige Internetverbindung zur Verfügung. Weitere Informationen dazu gibt es unter <http://www.cms.hu-berlin.de/dl/netze/vpn/SSL-VPN/>.

802.1X-Clientsoftware

802.1X ist ein standardisiertes Verfahren, welches die Anmeldung eines Clients an einer Netzwerkkomponente (z. B. einem WLAN-Accesspoint) ermöglicht. Im WLAN muss der Client (z. B. ein Laptop) dafür mit einer Software ausgestattet sein. Einige Betriebssysteme verfügen bereits über diese Software, für andere Systeme gibt es freie Clientsoftware. Ebenso gibt es 802.1X-Unterstützung, die in den Treibern einiger Hersteller von WLAN-Karten integriert ist. Weitere Details und Hinweise gibt es auf der Übersichtsseite zu 802.1X unter der URL: <http://www.cms.hu-berlin.de/dl/netze/wlan/config/802.1x/>.

Welche Zugangssoftware?

Es gibt keine pauschalen Aussagen, welche Art des Zugangs favorisiert werden sollte. Deshalb an dieser Stelle der Versuch, die einzelnen Verfahren zu klassifizieren.

Zugriff mit Web-Browser

Grundsätzlich sollte diese einfachste Art des Zugangs, das Surfen über das SSL-Gateway, mit jedem Client möglich sein. Dieser Zugang ist aber relativ unkomfortabel und gestattet es nur, WWW-Verbindungen aufzubauen. Daher ist diese Art des WLAN-Zugangs nur für PDAs und ähnliche Geräte empfehlenswert, die keine der anderen Methoden unterstützen.

Network Connect

Dies ist eine einfache, schnelle, sichere und meist auch recht stabile Möglichkeit des Zugangs. Nach dem Login wird ein Java-Applet geladen und ausgeführt (Network Connect). Dazu sind als Voraussetzungen nur ein WWW-Browser und aktuelle Java-Software notwendig. Nach erfolgreicher Ausführung besteht eine vollwertig benutzbare Internetverbindung. Gegenüber dem oben beschriebenen Verfahren (einfacher Zugriff mit einem Web-Browser) ist dies ein großer Vorteil. Allerdings eignet sich diese Art des Zugangs nur für Benutzer, die einen Computer oder Laptop mit einem gängigen Betriebssystem benutzen. PDAs werden von diesem Verfahren nicht unterstützt.

Grundsätzlich funktioniert dieser Zugang unter Linux, Windows und MacOS mit einem modernen Browser (Internet Explorer, Mozilla Firefox, Safari) und aktueller Java-Software. Aufgrund der einfachen Handhabung wird dieses Zugangsverfahren durch den CMS empfohlen.

Cisco-VPN

Diese meist auch stabile und zuverlässige Art des Zugangs ist vor allem für Benutzer älterer Windows-Systeme gedacht. Für Windows VISTA ist dieses Verfahren ungeeignet, da die Verbindungen in der Regel nicht stabil laufen.

Des Weiteren kann der Cisco-VPN-Client auch unter Linux und Systemen mit MacOS laufen.

802.1X

Der WLAN-Zugang mit Authentifizierung nach 802.1X sollte vor allem von erfahrenen Benutzer angewandt werden, die Wert auf hohe Sicherheitsstandards legen. Weiterhin ist diese Art des Zugang für Nutzer von Interesse, die häufig an anderen am DFN angeschlossenen Einrichtungen unterwegs sind, die am DFN-Roaming teilnehmen. Dabei wird eine Authentifizierung an der Heimateinrichtung durchgeführt, die anschließend die Benutzung des WLANs der Gasteinrichtung ermöglicht.

Außerdem ist dieses Anmeldeverfahren für Benutzer interessant, die einen PDA haben, der 802.1X nach TTLS und PAP unterstützt - wobei es hier keine Garantie gibt, dass eine Funktionalität wirklich gegeben ist.

Für Nutzer mit Windows-Mobile gibt es einen freien Client, der zumindest in einem Test erfolgreich eine 802.1X-Anmeldung durchgeführt hat.

VPN-Software anderer Anbieter

Es gibt weitere VPN-Clients basierend auf freier oder proprietärer Software, die auf PDAs, auf iPods, unter Linux usw. laufen. Diese alle werden seitens des CMS nicht unterstützt.

Zugangsdaten

An der HU werden 2 WLANs mit verschiedenen SSIDs betrieben. Die Abdeckung ist aber gleich, da jeder Accesspoint beide WLANs anbietet.

HU-VPN

Das erste WLAN der HU wird mit der SSID „HU-VPN“ betrieben. Dieses WLAN-Netz ist offen und kann von allen WLAN-fähigen Geräten gefunden werden. Nach dem Einbuchen in das WLAN „HU-VPN“ erhält man eine IP-Adresse aus dem Bereich 172.24.x.y. Verbindungen aus diesem WLAN sind nur mit einem VPN-Client möglich.

HU-802.1X

Das zweite WLAN, das an der HU angeboten wird, arbeitet mit der SSID HU-802.1X. Ein 1X-Client, der EAP mit TTLS und PAP unterstützt, ist Voraussetzung (siehe oben). Das Zuweisen der IP-Parameter erfolgt erst nach erfolgreicher Anmeldung.

Gastzugänge

DFN-Roaming nach 802.1X

Die HU beteiligt sich am Roamingverfahren nach 802.1X des DFN-Vereins. Ziel dieses Verfahrens ist es, Mitarbeitern und Gästen aus fremden Einrichtungen über das lokale WLAN einen Zugang zum Internet zu ermöglichen, wenn sie sich zuvor über ihre Heimateinrichtung authentifizieren. Natürlich funktioniert diese Roaming-Methode sowohl für Gäste aus DFN-Roaming-Einrichtungen an der HU als auch für HU-Angehörige, die zu Gast sind an einer Einrichtung, die auch am DFN-Roaming teilnimmt. Als Basis dient 802.1X, so dass eine Anmeldung am WLAN mit einem 802.1X-Client eine Voraussetzung für die Teilnahme am DFN-Roaming ist.

Eine Übersicht über die Einrichtungen, die sich am DFN-Roaming beteiligen, ist auf den WWW-Seiten des DFN-Vereins unter <http://www.dfn.de/de/dienstleistungen/dfnroaming/roamingstandorte/> zu finden.

Des Weiteren gibt es eine internationale Variante des Roamings: Eduroam. Der DFN-Verein beteiligt sich daran,

so dass für die Teilnehmer des DFN-Roamings auch ein WLAN-Roaming in anderen Ländern möglich ist. Mehr Informationen unter <http://www.eduroam.org/>.

Nutzer der HU, die Funknetze anderer am Roaming teilnehmenden Einrichtungen nutzen wollen, müssen beachten, dass bei der Authentifizierung der Account um einen Realm zu erweitern ist. Das ist eine Zeichenkette, die den Account einer Einrichtung zuordnet und so die Identifizierung ermöglicht. Zum Beispiel: Der Nutzer mit dem am CMS registrierten Account „mueller“ muss bei der Anmeldung an einem WLAN des DFN-Roamings die Zeichenkette @cms.hu-berlin.de an seinen Account anhängen. Aus dem Account „mueller“ wird also „mueller@cms.hu-berlin.de“. Je nach HU-Einrichtung variiert dieser Realm. Folgende Realms sind möglich:

- Account registriert bei: Realm
- CMS: @cms.hu-berlin.de
- Institut für Informatik: @informatik.hu-berlin.de
- Institut für Mathematik: @mathematik.hu-berlin.de
- Institut für Physik: @physik.hu-berlin.de
- Universitätsverwaltung: @uv.hu-berlin.de

DFN-Roaming nach CASG

Die HU beteiligt sich am CASG des DFN-Vereins. CASG steht für Controlled Address Space for Gateways. Das Verfahren vereinfacht beschrieben: Es gibt einen gemeinsamen Adressraum, der auf den Firewalls der teilnehmenden Einrichtungen freigeschaltet wird. Nutzer, die sich bei uns im „HU-VPN“-WLAN befinden, können sich per VPN-Tunnel (IPsec, HTTPS) zu ihrer Heimateinrichtung verbinden, wenn diese am CASG des DFN-Vereins teilnimmt. In Berlin sind u. a. FU und TU im CASG-Verbund. Damit können z. B. Angehörige und Studierende dieser Unis aus unserem „HU-VPN“-WLAN eine VPN-Verbindung zu ihrer eigenen Universität herstellen.

Umgekehrt geht das auch: Inhaber eines Accounts an der HU (CMS, Informatik, Mathematik, Physik, UV) können aus dem WLAN einer CASG-Einrichtung einen Tunnel zu den VPN-Gateways des

CMS aufbauen. Einrichtungen, die am CASG-Roaming teilnehmen, sind auf der Seite <http://www.dfn.de/de/dienstleistungen/dfnroaming/roamingstandorte/> vermerkt.

Ausblicke und Entwicklung

Gegenwärtig werden an der HU etwa 460 Accesspoints betrieben. Diese verteilen sich sehr unterschiedlich auf die einzelnen Standorte. Eine Übersicht

über die Abdeckung ist online auf den WLAN-Seiten des CMS zu finden.

Die Entwicklung im WLAN-Bereich geht weiter. Neue Standards mit höheren Reichweiten und Transferraten, wie zum Beispiel IEEE 802.11N, werden in den nächsten Jahren Einzug halten, so auch an der HU. Im Bibliotheksneubau in Mitte (Jacob und Wilhelm Grimm-Zentrum) ist geplant, eine Accesspoint-Switch-Lösung einzusetzen. Diese soll die 802.11N-Accesspoints zentral steuern, überwachen und verwalten. Die Abwicklung des

Datenverkehrs erfolgt dezentral. Die Inbetriebnahme wird im ersten Halbjahr 2009 erwartet.

Weiterhin ist die Einführung von neuen Verfahren für die Authentifizierung im WLAN angedacht. Es wird derzeit geprüft, ob ein OpenVPN-Server als weitere alternative VPN-Lösung in Frage kommt. Außerdem ist die Unterstützung von zertifikatsbasierter Authentifizierung (EAP-TLS) geplant. Damit sollten vor allem Clients bedient werden, die EAP-TTLS nicht unterstützen.

Personalia

Herr Thomas Gleißner ist seit dem 1.6.07 für die Administration von Windows-Servern zuständig. Hauptverantwortlich betreut er die Windows-Server der Universitätsverwaltung. Ab 26.5.08 besetzt er eine volle Stelle und ist zusätzlich im Netzmanagement tätig.

Herr Manuel Selling wurde im Anschluss an eine zweijährige Projektstelle am 28.6.07 fest eingestellt und bearbeitet Aufgaben des Windows-Servernetzes.

Herr Sandy Pleißner wurde am 1.7.07 vorerst befristet für 2 Jahre als technischer

Projektleiter zur Einführung des elektronischen Lehrveranstaltungssystems auf Basis von HISLSF eingestellt.

Herr Daniel Rohde hat seit dem 1.1.08 ein erweitertes Aufgabenprofil. Er ist verantwortlich für die Arbeitsgruppe Internet- und Datenbankdienste.

Herr Matthias Schulz ist nach seiner Tätigkeit als studentischer Mitarbeiter seit dem 1.2.08 fest eingestellt und für Aufgaben des Speichernetzes, des Datenbankservice und der Webserveradministration zuständig.

Herr Daniel Koschmieder wurde am 3.3.08 als Vertreter für Frau Frohmut Seckinger eingestellt.

Herr Boris Masinovsky beendete seine Tätigkeit am 31.3.08. Er war seit dem 1.6.05 im Rahmen des Projekts zur Ablösung des Netzwerkbetriebssystems Banyan VINES in der Universitätsverwaltung erfolgreich als Projektleiter tätig. Wir danken ihm für seine sehr gute Arbeit.

Wir wünschen allen Kollegen viel Freude und Erfolg bei ihrer neuen Tätigkeit.

Verabschiedung von Herrn Dr. Hans-Joachim Spitzer

Herr Dr. Spitzer hat im April 2007 die Humboldt-Universität nach 47 Jahren Zugehörigkeit verlassen, um in den wohlverdienten Ruhestand zu gehen.

Nach seinem Abitur absolvierte er zunächst im Auftrag der Humboldt-Universität ein praktisches Jahr im Werk für Fernsehelektronik. Im Anschluss studierte er von 1961 bis 1966 Mathematik an der Humboldt-Universität und fertigte seine Diplomarbeit im Rechenzentrum an. Von 1966 bis 1978 arbeitete er zunächst als wissenschaftlicher Assistent am Institut für physikalische Chemie und bot dort Mathematikvorlesungen und Übungen für Chemiker an. Daneben übernahm er die mathematische Betreuung der Mitarbeiter des Instituts. Dabei promovierte er

mit der „Berechnung quantenchemisch relevanter Integrale mit gebrochenen Kernladungszahlen“. 1978 wechselte Herr Dr. Spitzer zur Mathematik in die Arbeitsgruppe Geometrie von Prof. Sulanke. Danach wurde er Mitarbeiter in der Arbeitsgruppe Berechnungstheorie von Prof. Franken. Hier beschäftigte er sich mit der Programmierung eines „ableitungsfreien Extrapolationsverfahrens zur Berechnung gewöhnlicher Differentialgleichungssysteme mit Bifurkationspunkten“ innerhalb der Zusammenarbeit der Humboldt-Universität mit Mikroelektronik Dresden, die den Megachip produzieren sollte (heute AMD). Schließlich erfolgte der Wechsel ins Rechenzentrum. Hier leitete Herr Dr. Spitzer die Arbeits-

gruppe Numerik und führte verschiedene Programmierdienstleistungen, anfangs in Fortran, dann ab 1992 mit Mathematica, für verschiedene Institute der Universität durch. Diese Arbeit führte zur Mitautorschaft von einigen Publikationen. Eines seiner bis heute wirksamen Verdienste war die breite Einführung von Mathematica in der Universität, einschließlich der Betreuung der Campuslizenz. Zwischenzeitlich hatte Herr Dr. Spitzer auch die Weiterführung der Fortranusbildung der Azubis nach dem Ausscheiden von Herrn Wagner übernommen.

Wir danken Herrn Dr. Spitzer sehr für die langjährige gute Zusammenarbeit und wünschen ihm alles Gute für den Ruhestand.