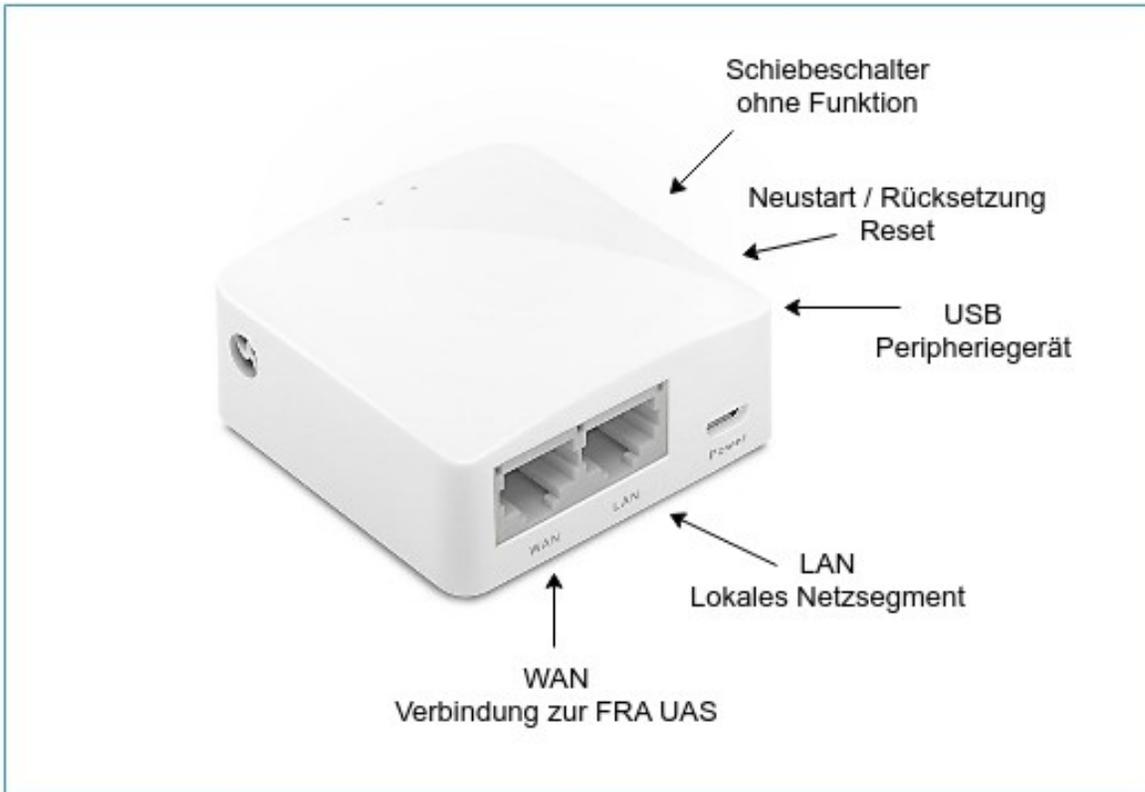


Inbetriebnahme eines GL-AR150 in den Wohnungen des Studierendenwohnheims Rat-Beil-Straße

Der GL-AR150 ist ein Mini-Router mit speziell angepasster Firmware auf der Basis von OpenWRT. Er verbessert die Internetanbindung in den Wohnungen des Studierendenwohnheims. Dafür baut er ein lokales, auf das Zimmer beschränktes Netzsegment auf und sorgt für den Aufbau des VPN-Tunnels für die Verbindung ins Internet. Das lokale Netzsegment kann kabelgebunden oder kabellos über eine spezielle WLAN-SSID genutzt werden.



Voraussetzungen

Der Router wird Ihnen durch die Hochschule gestellt und verbleibt als Teil Ihrer Zimmerausstattung im Eigentum der Hochschule. Ihrerseits sind folgende Voraussetzungen zu erfüllen:

- **Reset-Knopf**: Wenn Sie neu in das Zimmer eingezogen sind und den Router das erste Mal in Betrieb nehmen, sollte zunächst der Reset-Knopf für ca. 10 Sekunden gedrückt werden, während das Gerät angeschlossen ist. Somit werden sämtliche Daten Ihres Vorgängers gelöscht und Sie erhalten Zugriff auf das Gerät.
- **DV-Benutzerkennung**: Die Anbindung an das Hochschulnetz erfolgt über eine VPN-Verbindung, an der Sie sich mit Ihrer DV-Benutzerkennung authentifizieren müssen. Eine DV-Benutzerkennung erhalten alle Mitglieder der Hochschule über den Servicedesk der Campus-IT. Die näheren Regularien sind im [Intranet](#) einzusehen.
- **Netzwerkkabel**: Sie benötigen mindestens ein, je nach Anforderung vielleicht aber auch mehrere Netzwerkkabel. Achten Sie hierbei bitte auf eine Mindestqualität gemäß Cat. 5e. Eine reichhaltige Auswahl erhalten Sie z.B. mit einer Suchanfrage nach rj45 cat5e slim. Slim-Kabel sind flache Netzwerkkabel mit flexiblen Biegeradien und damit ideal für den häuslichen Schreibtisch.
- **Mini-Switch (bei Bedarf)**: Der Router bietet nur einen kabelgebundenen Anschluss für ein Endgerät. Benötigen Sie mehr Anschlüsse, brauchen Sie noch einen kleinen Switch. Entsprechende Modelle gibt es mit 5, 8 oder noch mehr Ports zu Preisen ab ca. 10€.
- **Router-Firmware**: Jeder Mini-Router im Wohnheim besitzt eine durch die FRA-UAS speziell angepasste und individuelle Firmware für bestmögliche WLAN-Einstellungen, sowie einfache Bedienbarkeit. Damit die Funktionalität des Mini-Routers gewährleistet werden kann, dürfen Sie unter keinen Umständen eigenhändige Änderungen an der Firmware vornehmen, z.B. durch die Installation einer herstellereigenen Firmware.

Einrichtung

- **Verbindung mit dem FRA-UAS-Netz**: Stellen Sie sicher, dass der *GL-AR150* über das Netzwerkkabel an der mit *WAN* gekennzeichneten Buchse mit der Datendose des FRA-UAS-Netz verbunden ist. Dies sollte mit der Ersteinrichtung geschehen sein. Über diesen Anschluss wird der Router auch mit Betriebsstrom versorgt.
- **Konfiguration des GL-AR150**: Damit der Router seine Funktion erfüllen kann, müssen Sie mindestens zwei Schritte ausführen:
 - ein Administrationspasswort zum Schutz Ihrer Daten und der lokalen Netzumgebung setzen, und
 - Ihre DV-Benutzerkennung zum Aufbau des VPN-Tunnels eintragen.
- Dies erfolgt über die WEB-Oberfläche des Routers, die kabelgebunden oder per WLAN erreicht werden kann:

- **kabelgebunden:** Verbinden Sie einen PC oder Notebook per Netzwerkkabel mit der LAN-Buchse des Routers. Stellen Sie am PC /Notebook über die Adaptereinstellung den *automatischen Bezug der IP-Adresse* (DHCP) sicher. Starten Sie die Netzwerkschnittstelle des PC/Notebooks bei Bedarf neu. Sie sollten eine lokale IP-Adresse aus dem Bereich 192.168.8.x erhalten.
- **kabellos per WLAN:** Öffnen Sie die WLAN-Verbindungen an Ihrem PC/Notebook und verbinden Sie sich mit dem WLAN-Netz, das auf der Oberseite des Geräts angegeben ist (*SSID*). Beim Verbindungsaufbau wird ein Passwort abgefragt, geben Sie hier das ebenfalls auf der Oberseite aufgebrauchte *PW*: ... an.

In beiden Fällen können Sie anschließend den Web-Browser Ihres PC/Notebooks öffnen (z.B. Chrome, Firefox, Safari, etc...) und sich mit der Administrationsoberfläche des Routers verbinden. Tippen Sie hierzu die folgende Zeile in die Adressleiste Ihres Browsers:

Es dauert in der Regel einen kurzen Moment, bis die Konfigurationsseite geladen wird. Es erscheint dann eine Anmeldemaske mit dem Hinweis, dass noch kein 'root'-Passwort gesetzt wurde:

No password set!

There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.
[Go to password configuration...](#)

Authorization Required

Please enter your username and password.

Username

Password

Powered by [LuCI Master \(git-18.015.48508-co01dd0\)](#) / [OpenWrt 15.05.1 r5833-030176e0e7](#)

Klicken Sie dafür zunächst auf **Login** ohne ein Passwort anzugeben und folgen Sie dann dem Link in dem farblich unterlegten Hinweiskasten; alternativ erreichen Sie die Seite für die Eingabe der Passwörter auch über die Tabs "System => Administration"

No password set!

There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.
[Go to password configuration...](#)

Router Password

Changes the administrator password for accessing the device

Password

Confirmation

OpenVPN Password

Eingabe der Benutzerdaten zum Aufbau der VPN-Verbindung

Username (IT-Benutzerkennung)

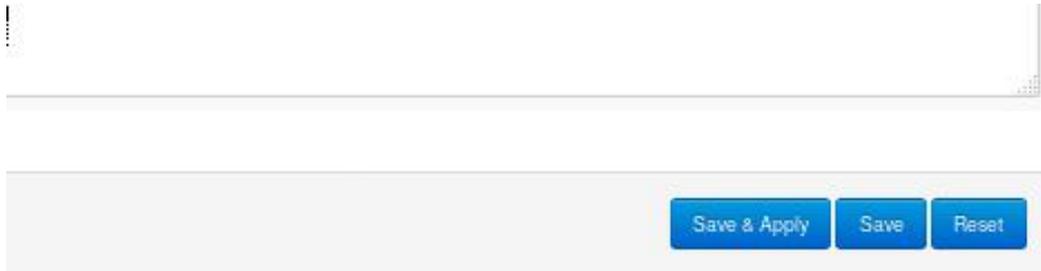
Password

Confirmation

Tragen Sie hier unter *Router Password* ein hinreichend komplexes Passwort ein, es schützt den Zugang zum Router und muss bei der nächsten Anmeldung zur Authentifizierung angegeben werden. Bewahren Sie es daher gut und geschützt auf.

Unter *OpenVPN Password* tragen Sie bitte die Informationen zu Ihrer *DV-Benutzerkennung* ein, diese Informationen werden für den Aufbau des VPN-Tunnels benötigt. Auch hier muss das Passwort zweimal eingegeben werden, um mögliche Tippfehler abzufangen.

ACHTUNG: Gehen Sie jetzt unbedingt ans Ende der Seite und bestätigen Ihre Angaben mit Klick auf "Save & Apply" - andernfalls gehen Ihre Eingaben verloren und Sie müssen noch mal von vorne beginnen ...



The image shows a portion of a web interface. At the bottom, there are three blue buttons with white text: "Save & Apply", "Save", and "Reset". Above the buttons is a large, empty rectangular area, likely a form for entering a password or other configuration details.

Die Seite baut sich jetzt neu auf und sollte Ihnen die folgende Bestätigung liefern; ansonsten folgen Sie dem Hinweis und wiederholen Sie die vorgehende Prozedur:



The image shows two yellow rectangular boxes with black text. The first box contains the text "Password successfully changed!". The second box contains the text "OpenVPN Benutzerdaten erfolgreich angelegt!".

Router Password

Changes the administrator password for accessing the device

Mit Eingabe der DV-Benutzerkennung wird auch der OpenVPN-Tunnel neu gestartet. Erst jetzt ist eine Internet-Verbindung möglich. Ob der Aufbau erfolgreich war, können Sie leicht unter "*Status => OpenVPN Log*" prüfen:

OpenVPN Log

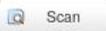
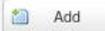
```
Mon Jan 15 13:53:10 2018 OpenVPN 2.4.4 mips-openwrt-linux-gnu [SSL (OpenSSL)][LZO][LZ4][EPOLL][AEAD]
Mon Jan 15 13:53:10 2018 library versions: OpenSSL 1.0.2n 7 Dec 2017, LZO 2.10
Mon Jan 15 13:53:10 2018 WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.
Mon Jan 15 13:53:11 2018 TCP/UDP: Preserving recently used remote address: [AF_INET]194.94.82.4:1194
Mon Jan 15 13:53:11 2018 UDP link local: (not bound)
Mon Jan 15 13:53:11 2018 UDP link remote: [AF_INET]194.94.82.4:1194
Mon Jan 15 13:53:12 2018 [ovpn-srv-01] Peer Connection Initiated with [AF_INET]194.94.82.4:1194
Mon Jan 15 13:53:13 2018 TUN/TAP device tap0 opened
Mon Jan 15 13:53:13 2018 do_ifconfig, if->did_ifconfig_ipv6_setup=0
Mon Jan 15 13:53:13 2018 /sbin/ifconfig tap0 10.15.170.34 netmask 255.255.0.0 mtu 1500 broadcast 10.15.255.255
Mon Jan 15 13:53:13 2018 Initialization Sequence Completed
```

Wesentlich ist die letzte Zeile - sie signalisiert den erfolgreichen Aufbau des Tunnels. Damit ist die Weiterleitung des lokalen Datenverkehrs ins Internet möglich und die Konfiguration abgeschlossen - Herzlichen Glückwunsch!

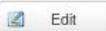
Zum Abschluss sollten Sie unbedingt das WLAN-Passwort - eigentlich den sogenannten PreShared-Key - zum Schutz ihrer lokalen Infrastruktur ändern. Das Default-Passwort ist am Gehäuse ablesbar, um Ihnen die Erst-Konfiguration über WLAN zu ermöglichen, damit aber auch leicht für Dritte ermittelbar. Sie ändern den Schlüssel in der Weboberfläche unter *Network / Wireless*:

Wireless Overview

 **Generic MAC80211 802.11bgn (radio0)**
Channel: 1 (2.412 GHz) | Bitrate: ? Mbit/s

 Scan  Add

 0% **SSID:** rbs-49 | **Mode:** Master
BSSID: E4:95:6E:43:1A:A4 | **Encryption:** WPA2 PSK (CCMP)

 Disable  Edit  Remove

Associated Stations

SSID	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
------	-------------	------	----------------	-------------------

No information available

Powered by LuCI Master (git-18.015.48508-cc01dd0) / OpenWrt 15.05.1 r5833-030176e0e7

Hier sehen Sie das WLAN-Netz, welches ihr Router ausstrahlt - die SSID weicht daher geringfügig von der Darstellung ab. Klicken Sie nun bitte auf **Edit** und dort zum Abschnitt **Interface Configuration**:

Interface Configuration

General Setup

Wireless Security

MAC-Filter

Advanced Settings

Mode

ESSID

Jetzt noch nach **Wireless Security**:

Interface Configuration

General Setup

Wireless Security

MAC-Filter

Advanced Settings

Encryption

Cipher

Key 

Tragen Sie dort im Feld **Key** ihr neues WLAN-Passwort / ihren neuen WLAN-Schlüssel ein. Richten Sie sich dabei nach den gängigen Empfehlungen für die Vergabe von Passwörtern (wenigstens 8 Zeichen, möglichst Gross- und Kleinbuchstaben sowie Zahlen und Sonderzeichen) und speichern Sie ihre Änderungen mit dem Button "Save & Apply". Ändern Sie an dieser Stelle bitte keine weiteren Einstellungen, die Vorgaben sind optimiert für die Situation in ihrer besonderen Umgebung.

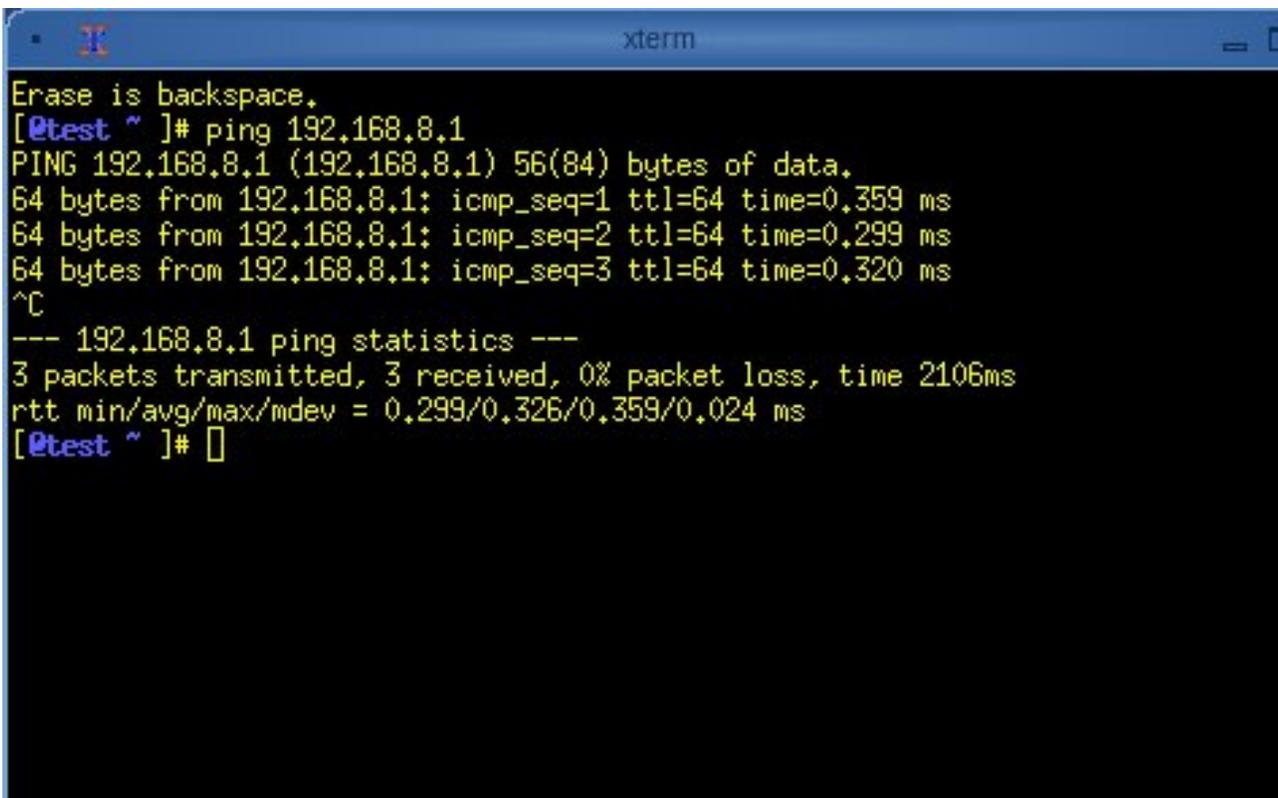
Zum Schluss: Beim Auszug aus dem Wohnheim verbleibt der Router im Zimmer und steht ihrem/r Nachmieter/in zur Verfügung. Für diese Situation bitten wir Sie, als letzte Aktion beim Router einen *Factory Reset* durchzuführen, der alle individuell von Ihnen geänderten Werte wieder zurücksetzt. Dazu drücken Sie den `Reset`-Taster ca. 8 Sekunden und lassen dann los. Kurz danach blinken die kleinen LED's und der Router startet neu. Sie können den Erfolg der Aktion überprüfen, wenn Sie sich letztmalig mit dem Router verbinden - auf der Weboberfläche sollte der Hinweis auf das nicht gesetzte `root`-Passwort (siehe oben) erscheinen.

Troubleshooting - Was tun, wenn's nicht auf Anhieb klappt

Hinweis: Die folgenden Vorschläge zur Problemlösung setzen zum Teil weitergehende Kenntnisse im Umgang mit den Netzwerkeinstellungen der beteiligten Geräte voraus. Sollten Sie mit den Hinweisen nicht weiterkommen, hilft - vielleicht - ein*e freundliche*r Nachbar*in oder - in jedem Fall - der Servicedesk der FRA UAS.

Problem: keine Verbindung zum Router

- Prüfen Sie, ob das Netzkabel zwischen Administrationsrechner und Router richtig steckt, beim Router auf die Bezeichnung *LAN* achten!
- Prüfen Sie, ob die lokale Firewall die Verbindungen blockt
- Prüfen Sie die Netzwerk-Einstellungen des Administrationsrechners: entweder muss hier die dynamische Adressvergabe aktiviert sein (empfohlen!) oder eine statische Adresse aus dem Netzbereich `192.168.8.0/24`, z.B. `192.168.8.10` gesetzt werden.
- Prüfen Sie die Verbindung zum Router: Öffnen Sie dazu auf dem Administrationsrechner eine Konsole und starten Sie den Befehl `ping` mit dem Router als Ziel (`ping 192.168.8.1`). Es sollte ein Echo zurückkommen ...
- In seltenen Fällen aktiviert der Router nach einem Neustart/Reset seinen integrierten DHCP-Server nicht. Wenn Sie mit dem Router verbunden sind und eine IP-Adresse erhalten haben, die mit "169.254" beginnt könnte dieser Fall eingetreten sein.
- Hierzu müssen Sie Ihrem Administrationsrechner vorübergehend eine statische IP-Adresse, z.B. `192.168.8.10` zuweisen. Versuchen Sie erneut über die Konsole den Router anzupingen (`ping 192.168.8.1`).
- Wenn diesmal der Ping funktioniert hat, können Sie ihre fest eingestellte IP-Adresse entfernen und wieder die dynamische Adressvergabe (DHCP) aktivieren. Sobald der Router einen Ping erhalten hat, aktiviert er seinen DHCP-Server wieder.



```
xterm
Erase is backspace.
[!test ~ ]# ping 192.168.8.1
PING 192.168.8.1 (192.168.8.1) 56(84) bytes of data.
64 bytes from 192.168.8.1: icmp_seq=1 ttl=64 time=0.359 ms
64 bytes from 192.168.8.1: icmp_seq=2 ttl=64 time=0.299 ms
64 bytes from 192.168.8.1: icmp_seq=3 ttl=64 time=0.320 ms
^C
--- 192.168.8.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2106ms
rtt min/avg/max/mdev = 0.299/0.326/0.359/0.024 ms
[!test ~ ]#
```

Problem: VPN-Tunnel wird nicht aufgebaut

- Schauen Sie sich zunächst die Ausgabe unter *Status/OpenVPN Log* (vgl. das vorletzte Bild) an - eventuell gibt es hier Hinweise auf:
 - keine Netzverbindung? Prüfen Sie auf der *Status/Übersicht*-Seite, ob der WAN-Anschluss eine IP erhalten hat. Hier sollte unter *Network* eine IP angezeigt werden, die mit `10.16` beginnt. Ist dies nicht der Fall, prüfen Sie, ob das Kabel am WAN-Anschluss richtig steckt und mit der korrekten Wanddose verbunden ist.
 - keine Authentifizierung wg. falschem Passwort? Prüfen Sie Ihre Angaben bei der DV-Benutzererkennung und setzen das Passwort neu - der Restart der OpenVPN-Verbindung erfolgt dann selbständig.

Problem: Passwort vergessen - kein Zugriff mehr auf den Router

- **Lösung:** Drücken Sie den *Reset*-Taster auf dem Router und halten ihn etwa 8 Sek. gedrückt, lassen Sie dann los; die LEDs fangen an zu blinken und gehen anschließend kurz aus. Damit führen Sie einen *Factory-Reset* durch, der alle Benutzereingaben löscht, also auch das durch Sie gesetzte root-Passwort. Gehen Sie anschließend die Einrichtungsprozedur erneut durch.