

If you need more Information or details to the scripts feel free to contact me via Email: itsupport@tobiaskoenig.de

Solltet Ihr Fragen haben oder Details zu den Scripten benötigen schreibt mir einfach eine Email: itsupport@tobiaskoenig.de

Dieses Dokument beschreibt den Einsatz der Zeroshell Software auf einem WRAP Board in einer Hotelumgebung mit mehreren Repeatern und WLAN Gast Zugang welcher pro Kunde für je x Tage freigeschaltet wird !

Engines ALIX.2D3 (Embedded Hardware)

ALIX by PC Engines

Das PC Engines ALIX-System ist ein kostengünstiger x86-basierender Einplatinen-Computer für benutzerspezifische Anwendungen wie z.B. Router, Firewalls, VPN-Gateways uvm.

Technische Daten:

- 500 MHz AMD Geode LX800 CPU
- 256 MB SDRAM
- 1 CompactFlash(TM)-Slot (für Betriebssystem und Anwendungen)
- 44pol. IDE-Anschlußleiste
- 3 FastEthernet-Anschlüsse (VIA VT6105M)
- 1 MiniPCI-Slot
- 2 USB 2.0 Anschlüsse
- 1 serielle Konsole
- Leistungsaufnahme nur ca. 5 Watt (ohne Erweiterungen)
- Versorgungsspannung 7-20 Volt über Niederspannungsbuchse (5,5/2,1mm)
- in CPU integrierter Watchdog-Timer
- Automatische Systemabschaltung bei Überhitzung
- Abmessungen: ca. 15,2 cm x 15,2 cm
- Lieferung ohne Gehäuse, Netzteil oder sonstige Erweiterungen
- Increase USB current limit.
- USB headers as build option.
- USB ports 3 and 4 on header (not tested).
- Change optional serial header J12 to COM2.
- Add LED and switch pins to I2C header.
- Populate buzzer driver circuit, add pins for use as GPIO.
- Add option for power in header J18.
- Some enhancements to reduce EMI.
- Add second POSCAP to ruggedize 3.3V rail for high power radio cards.



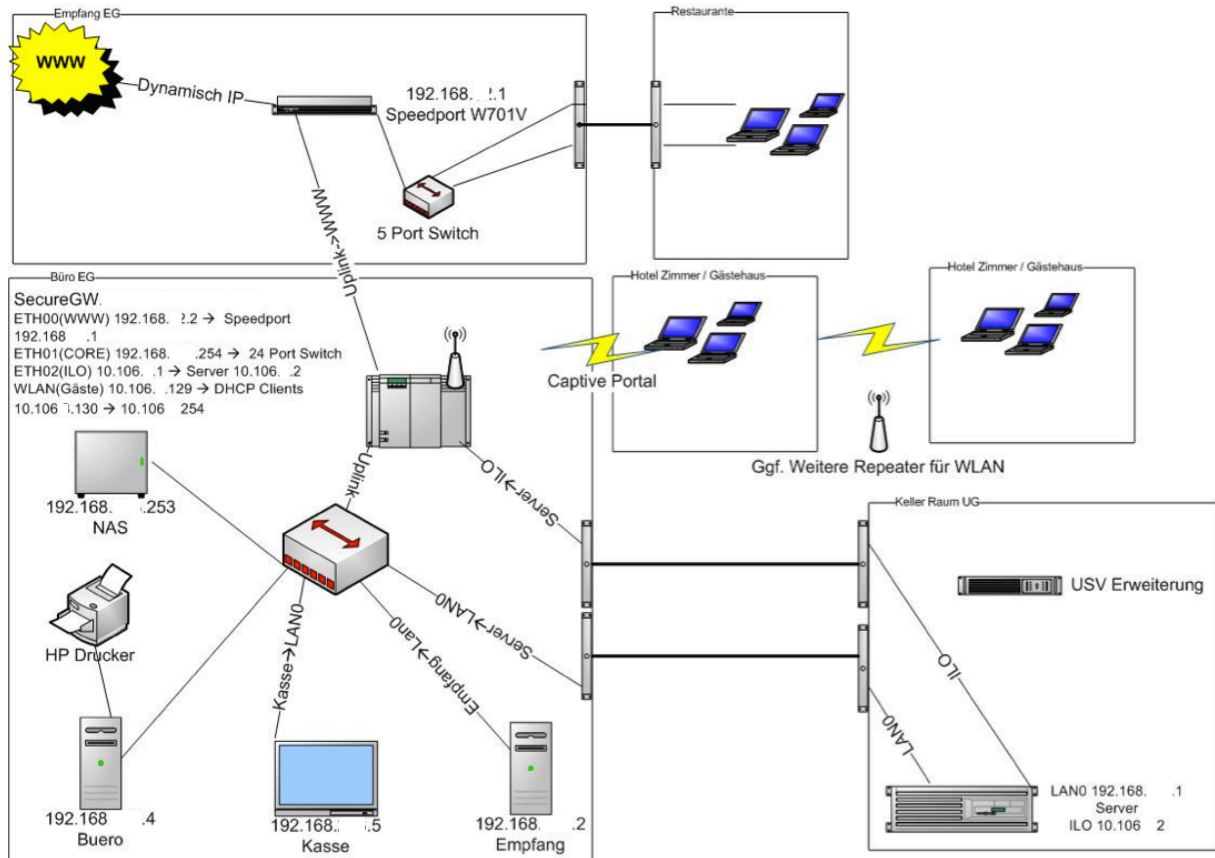
Als Add-On für die Integration der WLAN Access Points wurde noch eine MiniPCI Karte von Compex WLM54SAG23 integriert



Auf dieser Hardware wurde die Zeroshell Software integriert und getestet.

Netzwerk Infrastruktur:

Netzwerkübersicht



Das Netzwerk wurde komplett neu realisiert !

Den Knotenpunkt bildet die Zeroshell Applikation welche auf einer Alix Plattform realisiert ist. Die Verbindungen laufen über RJ45 CAT 5 Kabel auf einem 24 Port Switch zusammen. Die Verkabelung ist durch das gesamte Hotel verlegt. Die Verbindungen nutzen das TCP IP Protokoll und sind durch eine Firewall von einander getrennt. Es sind im Hotel XY 3 Netzwerkzonen realisiert worden (internes LAN (Hotelsoftware und Rechner)

IP-Adressen Übersicht

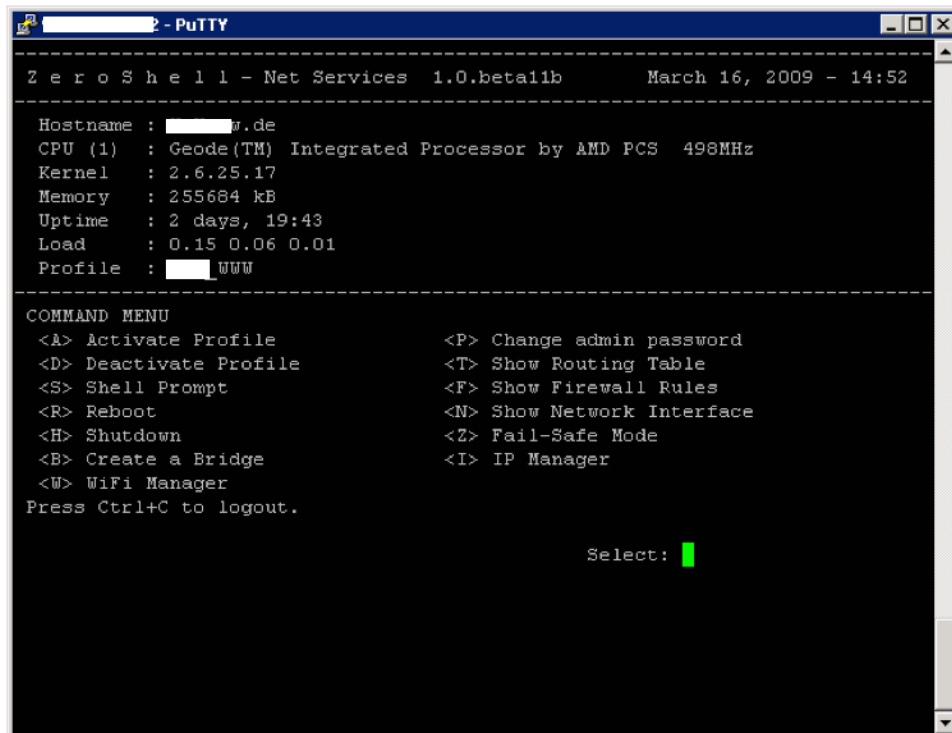
Servername	IP-Adresse	Subnetmask	Bemerkung
Server LAN0	192.168.y.1	255.255.255.0	Datenbestand Hotel // Administration über ILO oder Teamviewer
Server ILO	10.106.x.2	255.255.255.0	HTTPS Zugang
Buero	192.168.x.4	255.255.255.0	Zugang über Teamviewer nach Telefonisch Anfrage
Kasse	192.168.y.5	255.255.255.0	DOS Rechner (KEIN BACKUP)
Empfang	192.168.y.2	255.255.255.0	Rezeption Zugang über Server und VNC
SecureGW ETH0	192.168.y.254	255.255.255.0	AdminInterface Richtung INTERN LAN
SecureGW ETH1	10.106.x.1	255.255.255.0	Interface für ILO Server
SecureGW ETH2	192.168.a.2	255.255.255.0	Interface Richtung Speedport für WWW
Secure GW ETH3:0	10.106.b.1	255.255.255.128	IP Admin Bereich für Repeater Zugang
Secure GW ETH3:1	10.106.c.129	255.255.255.128	IP Bereich für WLAN Gäste des Hauses
Speedport W701V	192.168.a.1	255.255.255.0	Speeport W701V http Zugang → WWW
Repeater 2	10.106.b.2	255.255.255.128	http Port 80 Standort
Repeater 3	10.106.b.3	255.255.255.128	http Port 80 Standort
Repeater 4	10.106.b.4	255.255.255.128	http Port 80 Standort :
Repeater 5	10.106.b.5	255.255.255.128	http Port 80 Standort :
Repeater 6	10.106.b.6	255.255.255.128	http Port 80 Standort :
Repeater 7	10.106.b.7	255.255.255.128	http Port 80 Standort

Zeroshell

- RADIUS server for providing secure authentication and automatic management of the encryption keys to the Wireless 802.11b, 802.11g and 802.11a networks supporting the 802.1x protocol in the EAP-TLS, EAP-TTLS and PEAP form or the less secure authentication of the client MAC Address; WPA with TKIP and WPA2 with CCMP (802.11i complaint) are supported too; the RADIUS server may also, depending on the username, group or MAC Address of the supplicant, allow the access on a preset 802.1Q VLAN;
- Captive Portal to support the web login on wireless and wired networks. Zeroshell acts as gateway for the networks on which the Captive Portal is active and on which the IP addresses (usually belonging to private subnets) are dynamically assigned by the DHCP. A client that accesses this private network must authenticate itself through a web browser using Kerberos 5 username and password before the Zeroshell's firewall allows it to access the public LAN. The Captive Portal gateways are often used to provide authenticated Internet access in the HotSpots in alternative to the 802.1X authentication protocol too complicated to configure for the users. Zeroshell implements the functionality of Captive Portal in native way, without using other specific software as NoCat or Chillispot;
- QoS (Quality of Service) management and traffic shaping to control traffic over a congested network. You will be able to guarantee the minimum bandwidth, limit the max bandwidth and assign a priority to a traffic class (useful in latency-sensitive network applications like VoIP). The previous tuning can be applied on Ethernet Interfaces, VPNs, bridges and VPN bondings. It is possible to classify the traffic by using the Layer 7 filters that allow the Deep Packet Inspection (DPI) which can be useful to shape VoIP and P2P applications;
- HTTP Proxy server which is able to block the web pages containing virus. This feature is implemented using the ClamAV antivirus and HAVP proxy server. The proxy server works in *transparent proxy* mode, in which, you don't need to configure the web browsers of the users to use it, but the http requests will be automatically redirected to the proxy;
- Wireless Access Point mode with Multiple SSID and VLAN support by using WiFi network cards based on the Atheros chipsets. In other words, a Zeroshell box with one of such WiFi cards could become a IEEE 802.11a/b/g Access Point providing reliable authentication and dynamic keys exchange by 802.1X and WPA protocols. Of course, the authentication takes place using EAP-TLS and PEAP over the integrated RADIUS server;
- Firewall Packet Filter and Stateful Packet Inspection (SPI) with filters applicable in both routing and bridging on all type of interfaces including VPN and VLAN;
- It is possible to reject or shape P2P File Sharing traffic by using IPP2P iptables module in the Firewall and QoS Classifier;
- Multi subnet DHCP server with the possibility to fix IP depending on client's MAC address;
- NTP (Network Time Protocol) client and server for keeping host clocks synchronized;
- Syslog server for receiving and cataloging the system logs produced by the remote hosts including Unix systems, routers, switches, WI-FI access points, network printers and others compatible with the syslog protocol;
- Kerberos 5 authentication using an integrated KDC and cross-authentication between realms;

Die Funktionen können über ein WebInterface oder per SSH konfiguriert werden oder putty –load „SecureGW“)

Auch ein Zugang per SSH für Checks der Zeroshell steht über :
Securegateway.domain.de auf dem Port 9XXX bereit! Die Autorisierung erfolgt per
Username und Passwort:



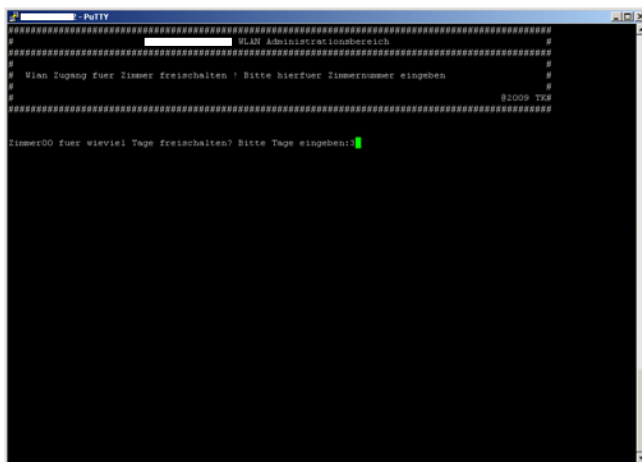
```
Z e r o S h e l l - Net Services 1.0.beta11b      March 16, 2009 - 14:52
-----
Hostname : ██████.de
CPU (1)  : Geode(TM) Integrated Processor by AMD PCS  498MHz
Kernel   : 2.6.25.17
Memory   : 255684 kB
Uptime   : 2 days, 19:43
Load     : 0.15 0.06 0.01
Profile  : ██████.WWW
-----
COMMAND MENU
<A> Activate Profile           <P> Change admin password
<D> Deactivate Profile        <T> Show Routing Table
<S> Shell Prompt              <F> Show Firewall Rules
<R> Reboot                    <N> Show Network Interface
<H> Shutdown                  <Z> Fail-Safe Mode
<B> Create a Bridge           <I> IP Manager
<W> WiFi Manager
Press Ctrl+C to logout.

                               Select: █
```

WLAN Zugang

Den Gästen im Hotel wird derzeit ein kostenloser Wlan Zugang zur Verfügung gestellt (WLAN Name XXX_WWW) Dieses WLAN hat keine Verschlüsselung aktiviert, damit alle Gäste mit ihren Laptop oder Peripheren Geräten dieses Netzwerk erreichen können! Die Überprüfung ob der Benutzer autorisiert ist oder nicht übernimmt das Captive Portal (siehe unten).

Damit den Gästen ein persönlicher zeitlich begrenzter Account zugeordnet ist , wurde ein Script programmiert welches per Batch Datei angestartet wird ! Das WLAN hat keine Verschlüsselung , damit sich alle Gäste ohne Probleme oder WPA Key Probleme anmelden können. Sie bekommen automatisch einen der nächsten Repeater zugeordnet und bekommen eine IP Adresse auf dem freien Bereich per DHCP Request. Alle Verbindungen über dieses WLAN werden in den unten genannten Logfiles gespeichert !

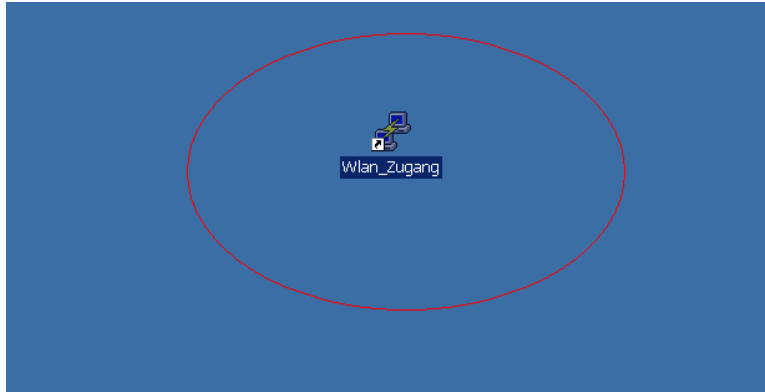


Nach starten des WLAN_Gäste_Zugangs wird nach der Zimmernr und die Gültigkeit erfragt! Es wird danach im System erstellt und ein Dokument zum Druck vorbereitet:

WLAN Gäste einrichten:

Wenn ein Zimmer Zugang zum kostenlosen WLAN möchte bitte wie folgt vorgehen :

1.) WLAN Icon auf dem Desktop drücken



Danach öffnet sich ein neues Fenster wo nur noch die Zimmernummer sowie die Anzahl der Tage eingeben werden muss (z.b für Zimmer 10 bitte nur 10 eingeben , Zimmer 1 bitte 01 eingeben.) Die Anzahl der Tage ab heute z.b 2 für 2 Tage oder 3 für 3 Tage usw.)

Danach wird die Zimmer Nummer sowie das Passwort für den Gast generiert!

Der Benutzername ist seine Zimmernummer (Zimmer10 , Zimmer50 usw.)

Das Z muss grossgeschrieben werden. Das Passwort besteht nur aus Zahlen und ist immer 8 Zeichen lang.

Danach startet automatisch das WORD Programm mit den Kennungen Hier wird ein Macro eingesetzt welches sich die Informationen per smb vom NAS holt

(Kennung/Passwort/Gültigkeit)! Sie werden direkt zum Drucken aufgefordert ! Alle Details sind auf dem Blatt für den Kunden. (Siehe oben)

Hierzu wurde ein Script gebaut:

Beispiel:

```
User=$1 // User muss übergeben werden...
```

```
PW=`date +%j%N` // Erstellt eine Zahlenfolge als Kennwort
```

```
/usr/local/sbin/kadmin.local <<EOF 1>/dev/null 2>/dev/null
```

```
change_password -pw $PW $user /// Ändert das Kennwort für den User
```

```
/usr/local/sbin/kadmin.local <<EOF 1>/dev/null 2>/dev/null
```

```
modprinc -pwexpire +"$tage"day $user //Gültigkeit in Tagen für User
```

Captive Portal

Das Captive Portal ist eine Website welche Automatisch gestartet wird nachdem ein Gast versucht sich ins Internet einzuwählen:



Hier müssen die erstellten Zugangsdaten eingeben werden! Danach erfolgt eine Überprüfung über LDAP und Kerberos Tickets. Sobald die Autorisierung und die Gültigkeit bestätigt wurden, erhält der Gast die gewünschte Seite über den Proxy angezeigt!

Logfile :

```
Mar 16 10:49:39 Zeroshell CaptivePortal: AS: https session (Client: 10.106.x.135) captured for authentication (AS: 10.106.x.1)
Mar 16 10:50:13 Zeroshell CaptivePortal: AS: http session (Client: 10.106.x.135) captured for authentication (AS: 10.106.x.1)
Mar 16 10:50:42 Zeroshell CaptivePortal: AS: trying Kerberos 5 (Local KDC) authentication for Zimmer00@ZEROSHELL.DE (Client: 10.106.x.135)
Mar 16 10:50:42 Zeroshell CaptivePortal: AS: Success: user Zimmer00@ZEROSHELL.DE (Client: 10.106.x.135) successfully authenticated (Username,Password)
Mar 16 10:50:43 Zeroshell CaptivePortal: GW: Success: user Zimmer00@ZEROSHELL.DE (IP: 10.106.x.135 MAC: 00:xx:62:xx:xx:78) connected
Mar 16 11:00:41 Zeroshell CaptivePortal: GW: warning: authenticator expired for Zimmer00@ZEROSHELL.DE (Client: 10.106.x.135)
Mar 16 11:xx:41 Zeroshell CaptivePortal: GW: Success: user Zimmer00@ZEROSHELL.DE (IP: 10.106.x.135 MAC: 00:xx:xx:xx:xx:78) disconnected
```

Proxy

Alle Verbindungen werden über den Proxy Prozess nach Viren oder gesperrten Webseiten durchsucht! Derzeit sind alle internen Webseiten (Administration NAS, Repeater oder Speedport) gesperrt. Somit wird verhindert, dass der Gast ggf. Angriffe oder Änderungen im System durchführen kann.

Alle Verbindungen auf Webseiten werden aus Sicherheitsgründen mitgeloggt und in einem Logfile gespeichert. Dieses wird 1x täglich auf das Sicherungstorage (NAS) kopiert! Hierfür wurde ein Script in der Crontab erstellt! Dieses packt die Daten als Tar Archive und kopiert dieses automatisch auf der NAS System per LAN. Hier liegen die Daten bis zur derzeitigen manuellen Löschung vor.

Das Logfile sieht wie folgt aus:

Mar 16 10:50:48 Zeroshell proxy[7244]: 10.106.x.135 GET 200 http://dict.leo.org/ 210+8935 OK

Proxy Blacklist:

<i>192.168.xx.1/*</i>	<i>10.106.x.5/*</i>
<i>192.168.xx.2/*</i>	<i>10.106.x.6/*</i>
<i>192.168.xx.3/*</i>	<i>10.106.x.7/*</i>
<i>192.168.xx.4/*</i>	<i>10.106.x.8/*</i>
<i>192.168.xx.5/*</i>	<i>192.168.x.1/*</i>
<i>192.168.xx/*</i>	<i>192.168.x.2/*</i>
<i>192.168.xx.254/*</i>	<i>10.106.x.2/*</i>
<i>10.106.xx.1/*</i>	<i>10.106.x.1/*</i>
<i>10.106.xx.2/*</i>	
<i>10.106.x.3/*</i>	
<i>10.106.x.4/*</i>	

Der Proxy Virenschanner aktualisiert sich 12x täglich auf die neuesten Virensignaturen!

Mar 16 11:11:11 Zeroshell freshclam[5290]: Received signal: wake up

Mar 16 11:11:11 Zeroshell freshclam[5290]: ClamAV update process started at Mon Mar 16 11:11:11 2009

Mar 16 11:11:11 Zeroshell freshclam[5290]: Your ClamAV installation is OUTDATED!

Mar 16 11:11:11 Zeroshell freshclam[5290]: Local version: 0.94 Recommended version: 0.94.2

Mar 16 11:11:11 Zeroshell freshclam[5290]: DON'T PANIC! Read <http://www.clamav.net/support/faq>

Mar 16 11:11:11 Zeroshell freshclam[5290]: main.cvd is up to date (version: 50, sigs: 500667, f-level: 38, builder: sven)

Mar 16 11:11:11 Zeroshell freshclam[5290]: Downloading daily-9112.cdiff [100%]

Mar 16 11:11:11 Zeroshell freshclam[5290]: daily.cld updated (version: 9112, sigs: 20136, f-level: 38, builder: ccordes)

Mar 16 11:11:11 Zeroshell freshclam[5290]: Your ClamAV installation is OUTDATED!

Mar 16 11:11:11 Zeroshell freshclam[5290]: Current functionality level = 35, recommended = 38

Mar 16 11:11:11 Zeroshell freshclam[5290]: DON'T PANIC! Read <http://www.clamav.net/support/faq>

Mar 16 11:11:11 Zeroshell freshclam[5290]: Database updated (520803 signatures) from db.DE.clamav.net (IP: 212.1.60.18)

Mar 16 11:11:11 Zeroshell freshclam[5290]: -----

Automatische Jobs Zeroshell (Crontab)

Es werden täglich automatische Jobs gestartet Übersicht:

```
root@Zeroshell scripte> crontab -l
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab installed on Sun Mar 15 11:49:19 2009)
# (Cron version V5.0 -- $Id: crontab.c,v 1.12 2004/01/23 18:56:42 vixie Exp $)
59 23 * * * /root/kerbynet.cgi/scripts/runscript Cron_SaveLogs-Cron
0 19 * * * /root/kerbynet.cgi/scripts/runscript Repeater_Check-Cron
root@Zeroshell scripte>
```

Check Repeater

Es werden um 19Uhr alle Repeater abgefragt ob die Erreichbarkeit gewährleistet ist:

```
root@Zeroshell scripte> ./repv4.sh
Status vom Mon Mar 16 14:42:57 CET 2009 :
Hole Daten fuer 10.106.x.2... Daten gesandt : 6 Empfangen : 6
Hole Daten fuer 10.106.x.3... Daten gesandt : 6 Empfangen : 6
Hole Daten fuer 10.106.x.4... Daten gesandt : 6 Empfangen : 6
Hole Daten fuer 10.106.x.5... Daten gesandt : 6 Empfangen : 6
ACHTUNG!!! 10.106.x.6 nicht erreichbar (Repeater )
*****
ACHTUNG!!! 10.106.x.7 nicht erreichbar (Repeater)
*****
#####
Repeater 2 (10.106.x.2) Vorraum SAAL
Wlanadresse : '00:4f:62:xxx:0c:7e'
BasisWLAN : '00:4f:xxx:21:xxx:78'
Clients auf dem Repeater
Uptime:
2day:20h:5m:43s
#####
Repeater 3 (10.106.x.3) Theke
Wlanadresse : '00:4f:xxx:xxx:xxx:78'
BasisWLAN : '00:xx:21:xx:00:06'
Clients auf dem Repeater
00:xx:62:xx:0c:xx Rate 29
Uptime:
2day:20h:5m:45s
#####
Repeater 4 (10.106.x.4) Gaestehaus Links
Wlanadresse : '00:xx:62:xx:0b:xx'
BasisWLAN : '00:xx:23:xx:xx:06'
Clients auf dem Repeater
00:xx:xx:21:xx:30 Rate 30
Uptime:
2day:19h:1m:31s
#####
Repeater 5 (10.106.x.5) Gaestehaus Rechts
Wlanadresse : '00:xx:62:xx:03:xx'
BasisWLAN : '00:4f:xx:21:xx:74'
Clients auf dem Repeater
Uptime:
2day:19h:0m:37s
```

Sicherung der Logfiles auf NAS

Es werden um 23.59 automatische alle Logfiles per Tar gepackt und per FTP auf das NAS in den Ordner [\\nas\store\Logfiles](#) kopiert! Hier liegen die Daten bis zur manuellen Löschung bereit.

```
# Bash script: Cron_SaveLogs-Cron
tar -cyf/DB/logs`date +%G%d%b`.tar /Database/LOG/`date +%G`/`date +%b`/`date +%d`/Zeroshell/*
gzip /DB/logs`date +%G%d%b`.tar
ftp -i -n 192.168.xxx.253 <<EOF
user securegw *****
cd Store
cd Logs
bin
put /DB/logs`date +%G%d%b`.tar.gz logs`date +%G%d%b`.tar.gz
bye
EOF
rm -f/DB/logs`date +%G%d%b`.tar.gz
```

Post Boot Script

Nach dem Reboot oder start werden automatische wichtige Variablen und SSH Keys für die Remote Einwahl gesetzt!

```
# Startup Script
echo "adminwww:x:0:0:root:/root:/bin/bash">>/etc/passwd
mkdir -p /root/.ssh/
echo "ssh-rsa
*****+GA8VUILxxxxxxxx47bVK98NdLYyTLKx/bSZ50uvzxSonSvdM8n7yYwvJMmA6FD
r2r0f2+6H8wPX03Gi7HJ6hw7GdIVhMzERweMZft0zM2hrKwo1FoqEw== rsa-key-20090223"
>>/root/.ssh/authorized_keys
echo "ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIEAIFL+*****+vH/vN2SDM4IUw6ydxmZxm6hvzQrGTfcBUuF9
q4Ue5aMyua1bfo+Ixxxxxxxxxxxxxxxxx14TrIVKagKBKrUoXj43Dcy4CnxRcmkq0tCMhD6eC+ZxNdd9Oq3bF1n
ODvrhRs= rsa-key-20090216" >>/root/.ssh/authorized_keys
rm -f/etc/ssh/sshd_config
cp -f/DB/scripte/sshd_config /etc/ssh/sshd_config
/etc/init.d/sshd restart
ln -s /DB/scripte/ /root/scripte
cp /DB/scripte/.profile /root/.profile
```

Wlan Repeater WL5460 AP v2

Hardwarebeschreibung:

Besonderheiten

- 54Mbps Wireless AP, 20 dBm Sendeleistung
- Bridge-, Client-, Repeater-, WDS-Funktionen, Sendeleistungsregulierung, Watchdog
- WPA, WPA2 in allen Modi
- Abnehmbare Antenne, 2 LAN-Ports
- 2 MB Flash und 16 MB SDRAM
- Notfall Upload Möglichkeit der Firmware

Übersicht

Der AirLive WL-5460APv2 ist das aktuelle Modell des Wireless-Access-Point von Ovislink. Er bietet eine herausragende Funktionen zu einem sehr konkurrenzfähigen Preis. Voll übereinstimmend mit den Standards 802.11g und 802.11b ist er kompatibel mit den meisten derzeit genutzten Wireless-Geräten. Über seine beiden LAN-Ports kann ein Router sowie ein LAN eingebunden werden. Und durch seinen extragroßen 2MB-Flashspeicher und 16MB SDRAM laufen sogar die für den WL-1120AP entwickelten Applikationen auf ihm.

Web-Management

Da dieser AP über einen Webbrowser konfiguriert wird geht die Konfiguration schnell und einfach von der Hand. Die zulässigen Ports für das Web-Management können durch den Benutzer frei definiert werden, wodurch in einer NAT-Umgebung problemlos auf mehrere APs zugegriffen werden kann. Die neue Firmware beinhaltet sogar eine TX-Leistungsregulierung in 4 Stufen. Und wenn der PING zu einer benutzerdefinierbaren IP-Adresse fehlschlägt wird der AP durch die integrierte Watchdog-Funktion automatisch neu gestartet.

Universal Repeater-Modus

Durch eine Änderung in der Software-Einstellung kann dieser Access-Point die Reichweite ihres Wireless-Netzwerk vergrößern, dadurch das der WLAN Access Point mit einer Repeater-Funktion ausgestattet ist, können die Signale eines anderen APs verstärkt werden. Erweiterte Sicherheitsfunktionen

Für die Wireless-Sicherheit ist OvisLink noch einen Schritt weiter gegangen. Durch die versteckte SSID werden fremde Benutzer davon abgehalten, ins Netzwerk einzudringen ohne dass sie die ID des Wireless-Netzwerks kennen. Um unerwünschte Eindringlinge fernzuhalten wird zudem WPA- und 64/128-Bit-WEP-Verschlüsselung sowie eine Zugriffskontrolle für die Ports zur Verfügung gestellt.

Gleich ob Privat- oder Büroumgebung - die AirLive-802.11g-Familie von OvisLink gibt Ihnen maximale Performanz und Sicherheit für die Hochgeschwindigkeits-Wireless-Netzwerke der heutigen Zeit.



NAS Storage

Hardwarebeschreibung

- NAS System für Heim- und Büronetzwerke
- Aluminium Gehäuse für optimale Wärmeableitung ohne Lüfter
- Einfache Konfiguration über Webbrowser
- Keine Softwareinstallation auf Client PC erforderlich
- Standby für HDD bei Nichtgebrauch frei einstellbar
- Unterstützt 3,5“ SATA (bis 1TB) & PATA (IDE bis 750GB) Festplatten
- Verwendung von FAT32 als Dateisystem
- Betrieb an Ethernet oder USB möglich
- 10/100Mbit Ethernet Schnittstelle
- USB 2.0 Schnittstelle (bis 480 Mbit/s)
- 3 Server in einem
 - Samba (für Windows Netzlaufwerke, Mac OS)
 - FTP Server (Fernzugriff über Internet)
 - DHCP (Automatische IP Konfiguration für Netzwerk-Clients)
- IP Konfiguration statisch oder von vorhandenen DHCP Server
- Niedriger Stromverbrauch, Spin Down (Sleep Mode) für HDD einstellbar
- Externe Datenkabel inklusive
- Externe Stromversorgung AC: 100~240V 34W

ICY BOX

