

Linux Hotspot auf TEAC Vendotto

Peter Krausgrill
Folkert Saathoff

Hardware

TEAC Vendotto NS-40 LAN:

- 300 MHz NSC Geode CPU
- 64 MB SDRAM
- 2x 10/100 Realtek 8139 NIC
- Z-Com LANEscape/XI300 802.11b NIC



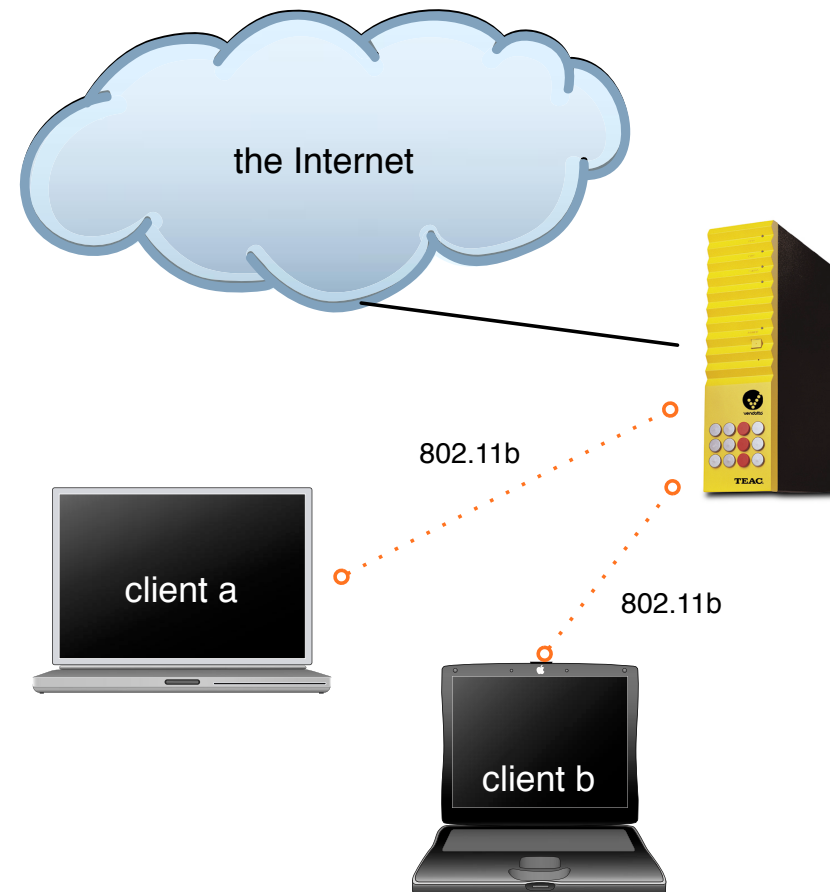
Software

- Linux 2.4.20
+ hostap 0.1
- Apache 2.0.48
- Mysql 4.0.16
- Php 4.3.3



WiFi Setup

- 802.11b
- kein WEP



Annahmen

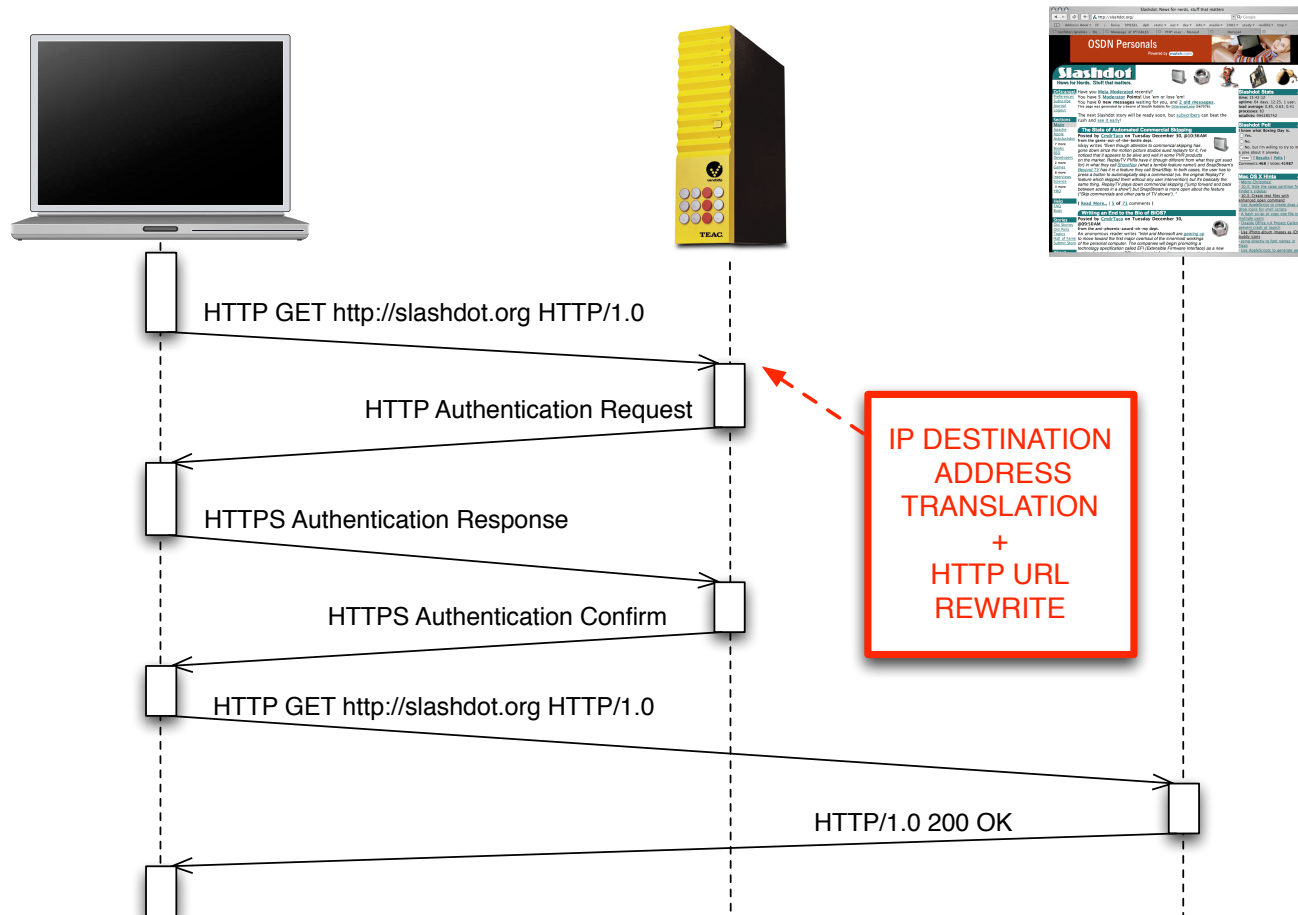
- User haben einen Browser installiert
- User benutzen DHCP, um ihre Netzwerk-Parameter zu bekommen
- User wollen / können keinen WEP Schlüssel eingeben
- User können ihre MAC Adresse nicht ändern

Authentifikation Verfahren

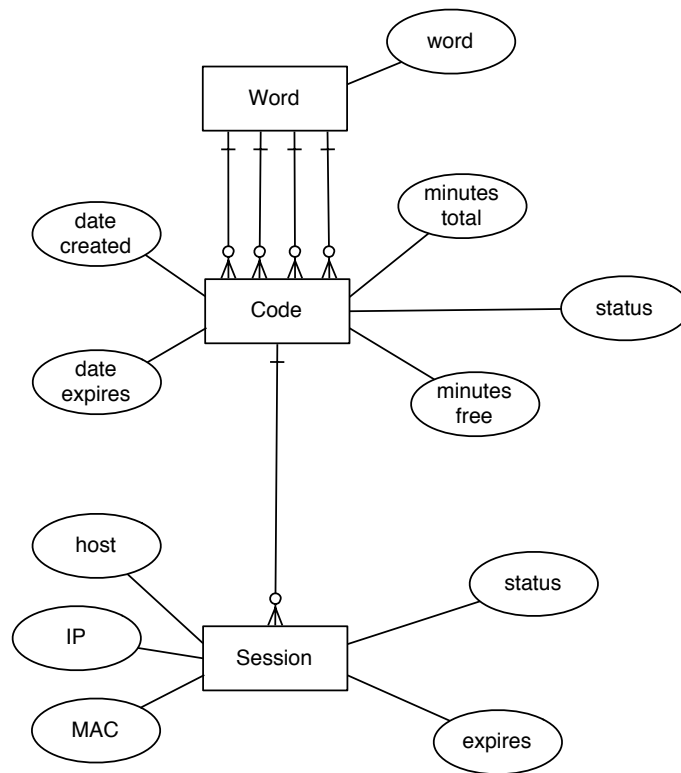
- Betreiber erstellt einen Schlüssel
- User erwirbt einen Einmal-Schlüssel für ein Zeitkontingent
- Beispiel:



Authentifikation Ablauf



Accounting



- Authentifikation
 - 4 Wörter Code
 - Aktiv
 - Abgelaufen
 - Guthaben
- Session
 - IP/Host/MAC
 - Aktiv
 - Abgelaufen

Betreiber [admin.php]

- Zugangsdaten für DB generieren
- Zugangsdaten als PDF rendern
- Verwaltung erlaubter Websites

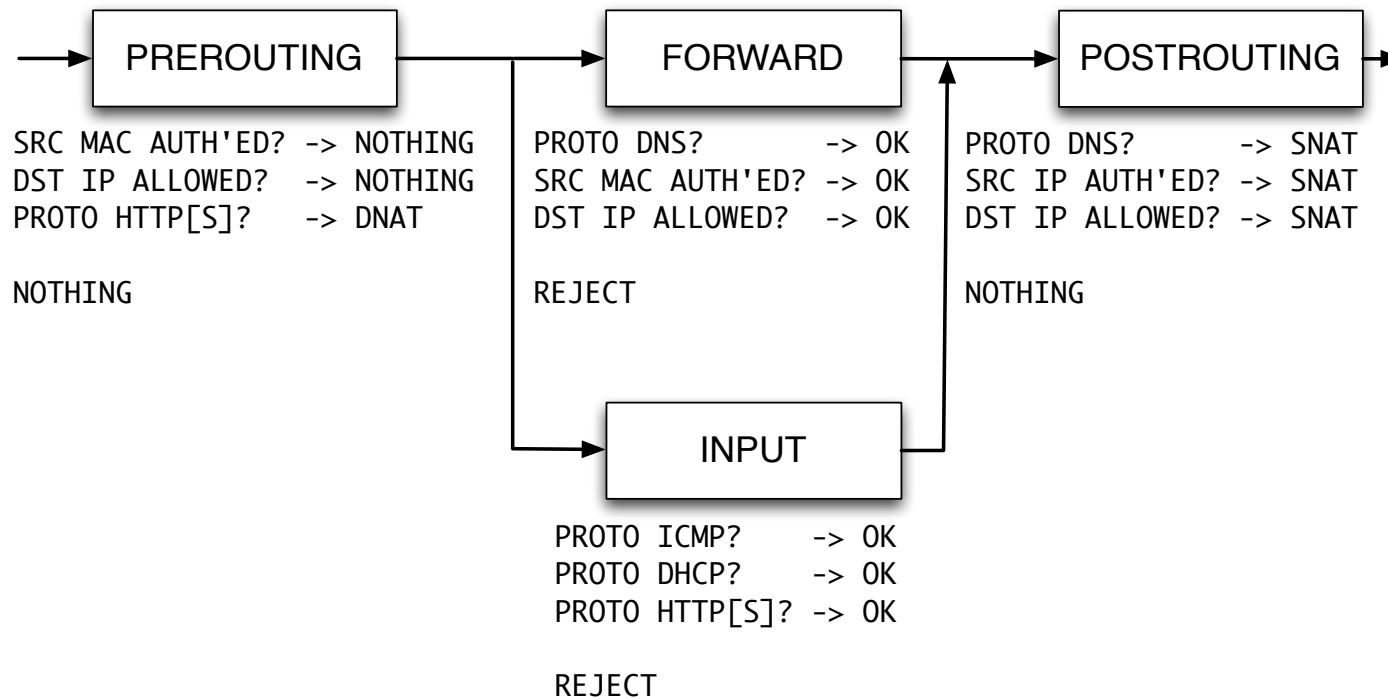
User [index.php]

- Zugangsdaten überprüfen
- Verbindungsparameter ermitteln
 - Client MAC/IP aus dhcpd.leases
- Session anlegen
- Zugang freischalten
 - MAC/IP in ACLs aufnehmen

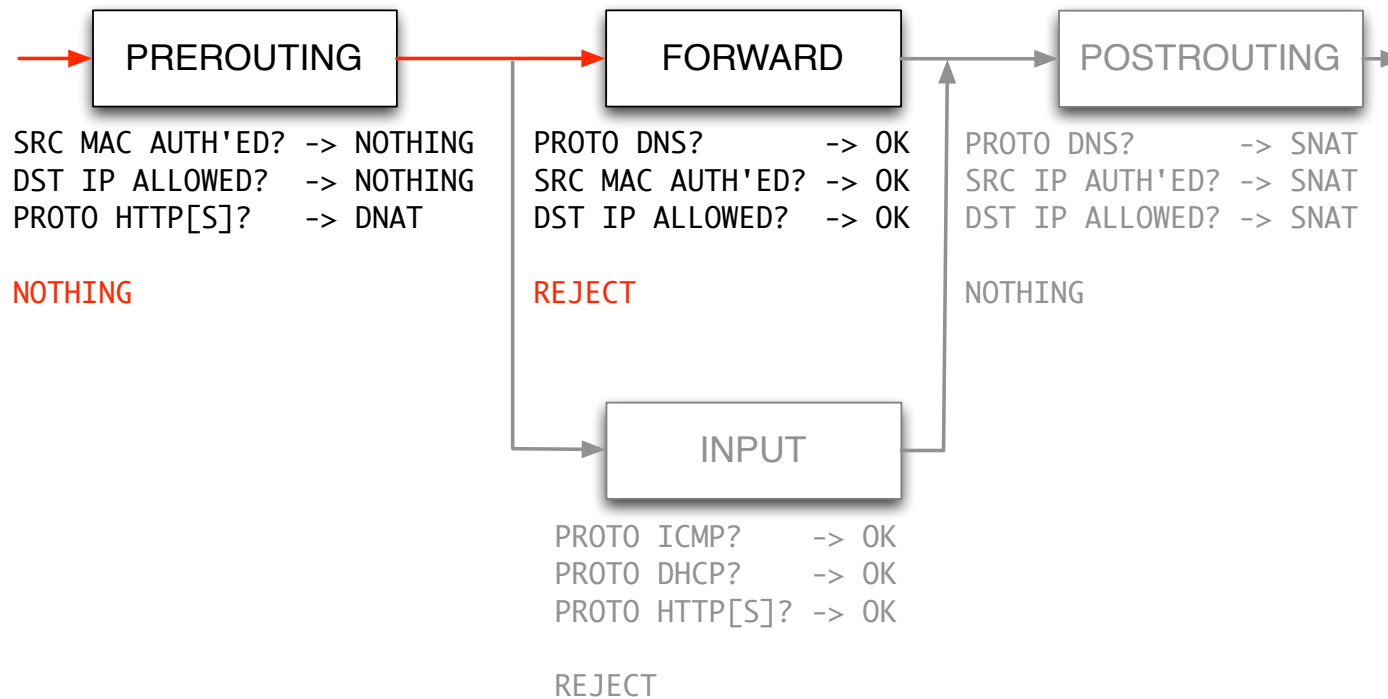
System [expire.php]

- über crontab, 1/60 Hz
- Sessions überprüfen
- gegebenenfalls Zugang sperren

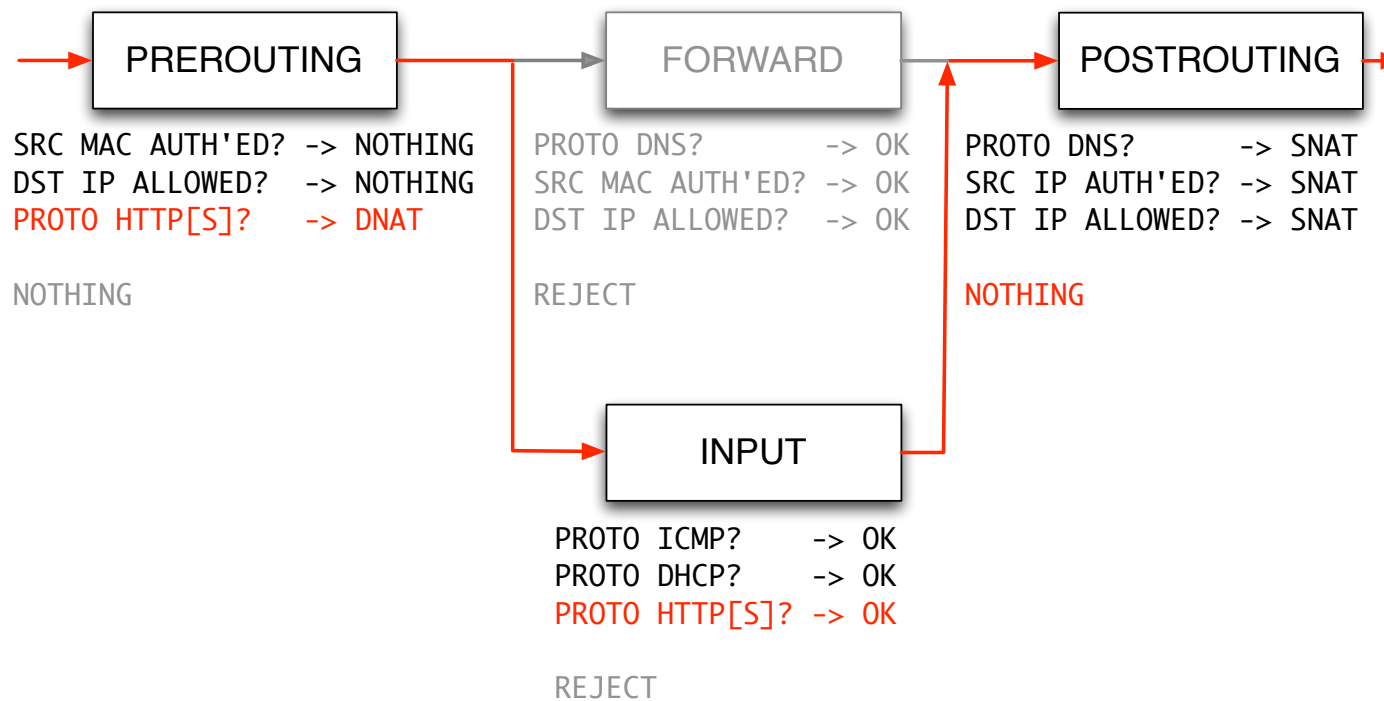
Netfilter: Architektur



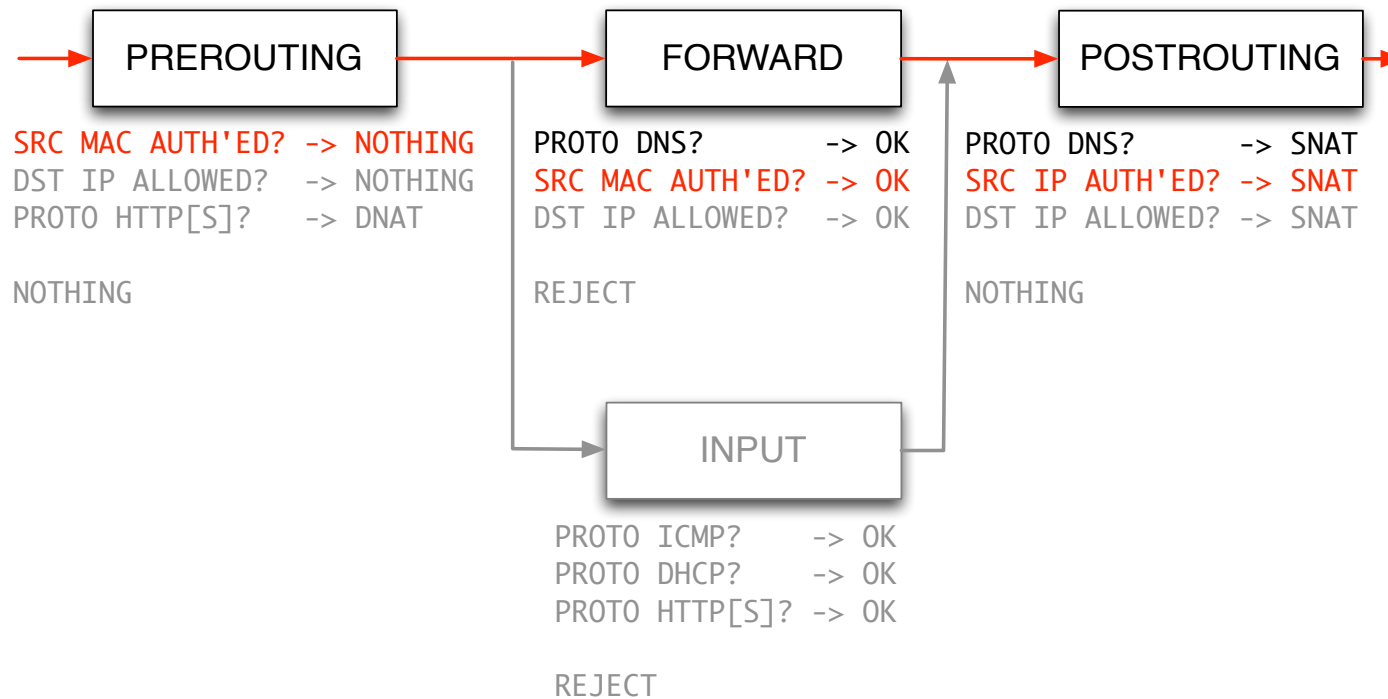
Unauthentifizierter Netzzugriff



Unauthentifzierter Webzugriff

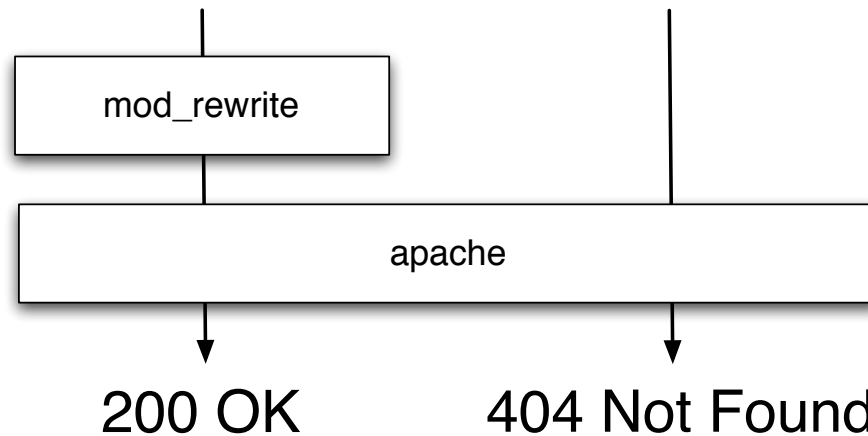


Authentifizierter Client



mod_rewrite

<http://www.google.com/search?q=hello&num=2>



<http://10.11.12.13/index.php>

[?url=www.google.com/search&q=hello&num=2](http://10.11.12.13/index.php?url=www.google.com/search&q=hello&num=2)

Attack Vectors

- MAC Spoofing
 - benötigt spezielle Treiber
 - DNS Tunneling
 - benötigt präparierten DNS Server
 - DHCP Server Spoofing
- ⇒ Man-In-The-Middle Attack