

HAMNET

Zugangsdokumentation Bullet M2-HP

Datum: 16. Oktober 2011

I Versionsstände

Version	Datum	Kommentar	Bearbeiter
1.0	12.10.2011	Dokument erstellt	OE5HPM

Tabelle 1: Versionsstände

1 Inhaltsverzeichnis

1 Inhaltsverzeichnis.....	3
2 Userzugang Anwendungskonzepte.....	4
2.1 Bridged Mode.....	4
2.2 Networked Mode.....	5
3 Konfiguration Bullet.....	6
3.1 Verbindungsaufnahme zum HAMNET Zugang.....	6
3.2 Einbindung mittels 'Bridged-Mode'.....	11
3.3 Einbindung mittels 'Networked-Mode'.....	13
3.3.1 Einrichten des Gateways zum HAMNET.....	14
3.3.2 Einrichten des Namensservers vom HAMNET.....	16
4 offene Punkte, TODO.....	17

2 Userzugang Anwendungskonzepte

Es gibt grundsätzlich zwei verschiedene Möglichkeiten das Bullet und damit die eigene Station ins HAMNET einzubinden, dabei wird in „Bridged-Mode“ und „Networked-Mode“ unterschieden.

Beide haben Vor- und Nachteile, letztendlich bleibt es dem Anwender selbst überlassen für welche Konfiguration er sich entscheidet. Um sich entscheiden zu können, was für die eigene Station am besten passt, soll nachfolgend beschrieben werden wie sich die 2 Betriebsarten verhalten bzw. unterscheiden.

2.1 Bridged Mode

Im 'Bridged Mode' scheint das Bullet fast gar nicht im Netzwerk auf, sondern reicht lediglich alle Pakete aus dem HAMNET auf den Ethernetport durch und vice versa.

Scheint 'fast gar nicht auf' deswegen, weil das Bullet auch im 'Bridged Mode' eine IP-Adresse besitzt. Nämlich, sofern nicht vom Benutzer verändert, 192.168.1.20, die Standard IP-Adresse über welches es zur Konfiguration angesprochen wird.

Die IP-Adresse ist sowohl für den HF-Teil als auch für den Ethernet-Teil gültig, da ja diese 2 Interfaces als Bridge geschaltet sind.

Für diese Anwendung kann das Bullet nicht einfach in das lokale Netzwerk gesteckt werden, sondern muss an einer separaten Netzwerkkarte am PC angeschlossen werden.

Dieser PC erhält vom HAMNET-Userzugang eine offizielle IP-Adresse zugewiesen und sieht alle Pakete welche aus dem HAMNET kommen.

Der Bridged Mode bietet folgende Vorteile:

- beliebig viele IP-Adressen können an der eigenen Station existieren (PC, Webcam1, Webcam2, Wetterstation, ...)
- lokales Netzwerk und HAMNET sind physikalisch und damit sicher voneinander getrennt.
- jeder an das physikalisch angeschlossene Rechner ist ohne Schutz aus dem HAMNET erreichbar (kann auch ein Nachteil sein, darum weiter unten erneut angeführt)

Nachteile des Bridged Mode:

- das Bullet kann nicht direkt in das lokale Netzwerk angeschlossen werden
- jeder PC welcher das HAMNET nutzen möchte, muss über eine separate Netzwerkkarte verfügen und an das physikalische Netzwerk, an welchem auch das Bullet steckt, angeschlossen werden
- alle an das physikalische Netzwerk angeschlossene Rechner sind ohne Schutz aus dem HAMNET erreichbar (dies muss nicht unbedingt ein Nachteil sein).

2.2 Networked Mode

Im 'Networked Mode' sind HF-Teil und Ethernet-Teil voneinander entkoppelt, das Bullet agiert in diesem Fall als Firewall bzw. Router.

Pakete aus dem HAMNET gelangen bis zum Bullet und müssen von diesem dann in irgendeiner Form verarbeitet werden, wiederum Pakete aus dem Ethernet-Teil und damit aus dem lokalen Netzwerk gelangen ebenfalls bis zum Bullet und müssen dort ebenso in irgendeiner Form verarbeitet werden.

Die häufigste Form dieser Verarbeitung wird dabei das 'Masquering bzw. NAT' sein, Pakete werden vom Bullet 'maskiert', das heißt die Absenderadresse des Paketes wird ersetzt durch die 'offizielle' IP-Adresse vom HF-Teil (44.x.x.x), und ins HAMNET weitergereicht.

Nach außen (ins HAMNET) ist somit immer nur das Bullet sichtbar.

Auf dem Rückweg werden Pakete aus dem HAMNET, sofern diese zu einer bestehenden Verbindung gehören oder eine Konfiguration für selbige vorliegt (dazu an späterer Stelle), an die betroffene / zuständige IP-Adresse im lokalen Netzwerk geschickt.

Der 'Networked Mode' hat folgende Vorteile:

- das Bullet kann einfach in das lokale Netzwerk integriert werden und von jedem Rechner aus auf das HAMNET zugegriffen werden kann.
Natürlich kann der Zugriff mittels Konfiguration, falls gewünscht, auf bestimmte Rechner eingeschränkt werden.
- Nur Pakete welche zu einer aktiven Verbindung gehören, oder welche Explizit zugelassen wurden gelangen in das lokale Netzwerk bzw. auf den Rechner.

Nachteile des 'Networked Mode':

- Es ist nur eine IP-Adresse nach außen (ins HAMNET) sichtbar. Eventuell angebotene Services können unter Umständen nicht auf den Standardports angeboten werden weil ein laufender Webserver den Port 80 bereits einnimmt, muss das Webinterface der IP-Kamera (welches per default ebenfalls auf Port 80 läuft) auf einem anderen Port z.B. 8080 angeboten werden.

Der 'Networked Mode' ist wohl für die meisten Anwender, welche nur wenige bis keine Services anbieten, am praktikabelsten.

3 Konfiguration Bullet

3.1 Verbindungsaufnahme zum HAMNET Zugang

Nachfolgend wird beschrieben, wie die Verbindung zum lokalen HAMNET Knoten OE5XBL aufgebaut werden kann. Die Vorgehensweise ist für andere Zugangsknoten ähnlich bis gleich, lokale Unterschiede sind sicher von den ansässigen OMs bzw. am OV-Abend zu erfragen.

Netzwerk erfahrene und versierte Anwender können Punkt 1-2 überspringen und ab Punkt 3 fortfahren.

1. Um lokale Fehler aus dem Netzwerk auszuschließen, wird zunächst das Bullet als einzigstes Gerät an die Netzwerkkarte angeschlossen (ältere Netzwerkkarten unterstützen kein 'AUTO-MDI', es muss evtl. ein gekreuztes Netzwerkkabel verwendet werden).
2. Es wird die IP-Adresse 192.168.1.10 an der Netzwerkkarte wie folgt eingestellt:

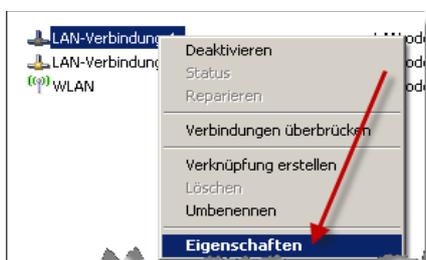
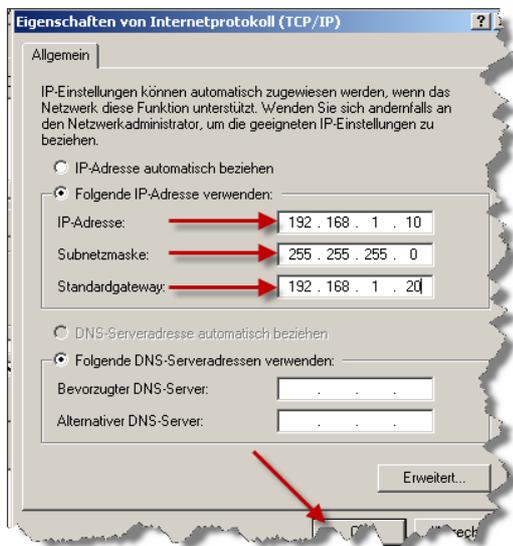


Abbildung 2: Kofiguration Netzwerkeinstellung 1/3



Abbildung 1: Kofiguration Netzwerkeinstellung 1/3



3. Als nächstes wird in einem beliebigen Browser die IP-Adresse des Bullet, 192.168.1.20 augerufen.

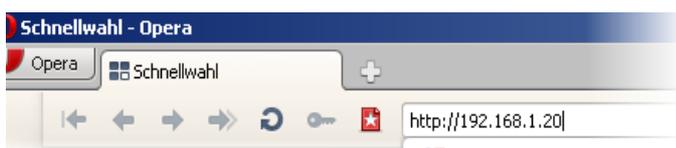


Abbildung 4: Browser Adresseingabe

4. Es öffnet sich die Startseite des Bullet, hier loggt man sich mit den Defaultwerten für Username und Password 'ubnt' / 'ubnt' ein.

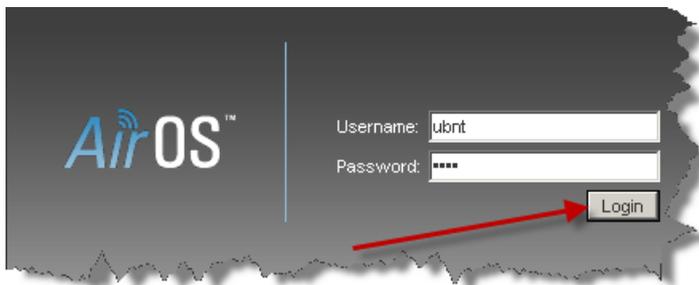


Abbildung 5: Bullet Login

5. Es sollte sich folgendes Bild nach dem Einloggen ergeben, in diesem Fall ist der Zugang bereits konfiguriert und mit dem Zugangsknoten OE5XBL verbunden.

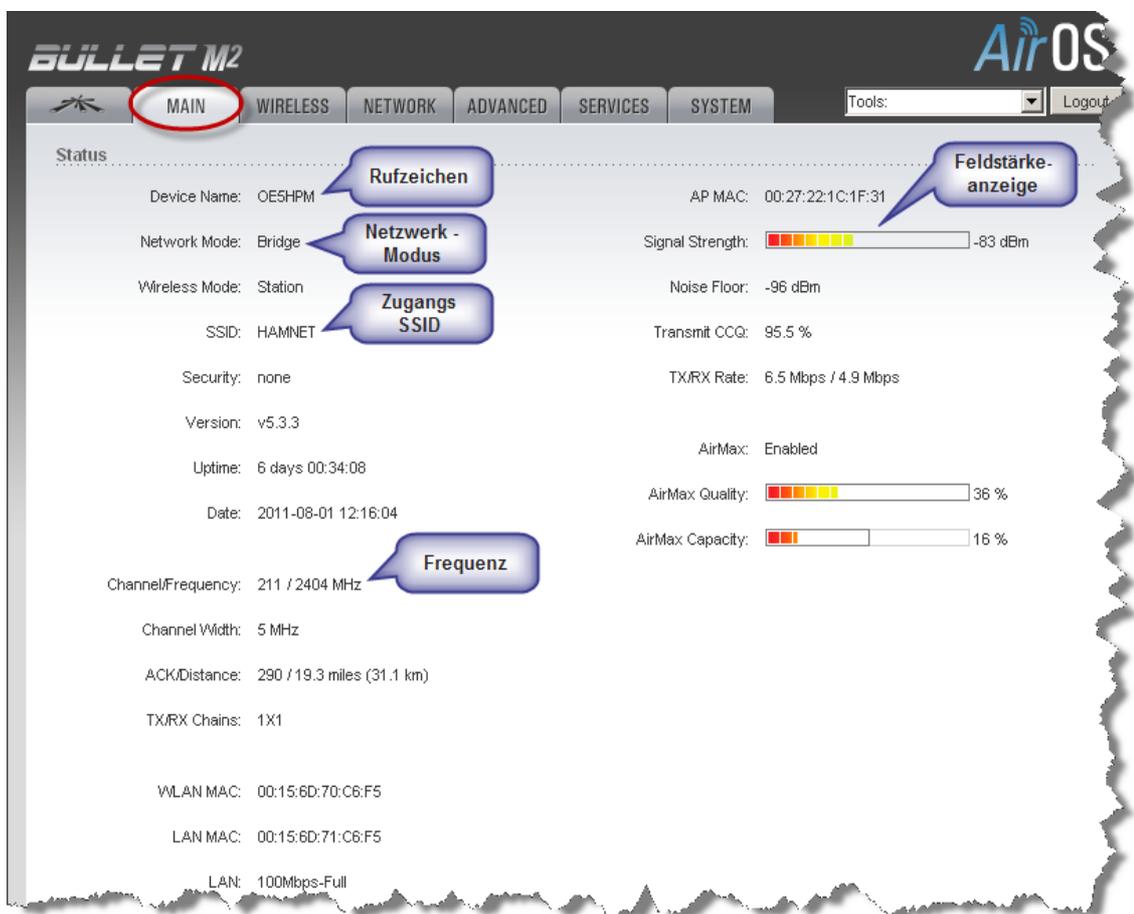


Abbildung 6: Bullet 'Reiter Main'

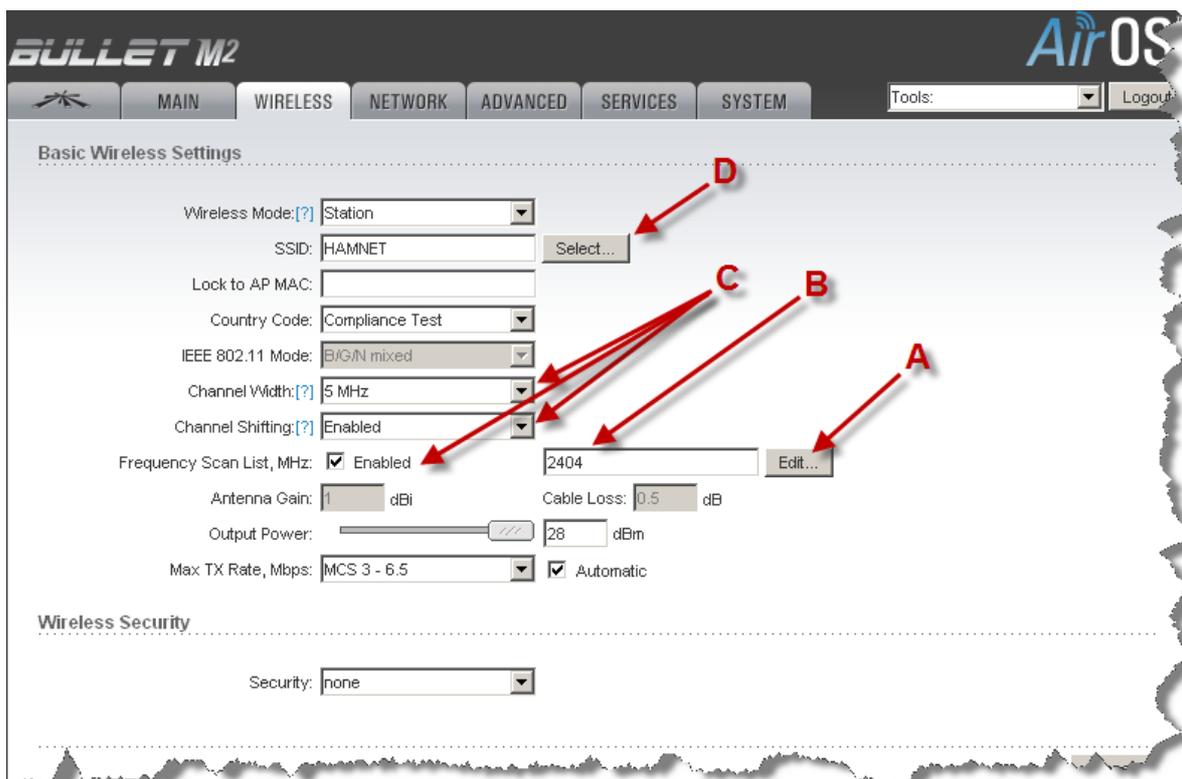


Abbildung 7: Bullet 'Reiter Wireless'

6. Zunächst ist es wichtig, die korrekten Suchfrequenzen für den Zugang zum HAMNET-Knoten einzustellen, im Falle von OE5XBL gibt es eine einzige Frequenz: 2404 MHz, welche wie folgt eingestellt wird:
- Der 'Country Code' wird auf 'Compliance Test' gestellt um alle Frequenzen welche nicht im ISM Bereich liegen auswählbar werden.
 - Nach dem Klick auf **A** öffnet sich ein Popup in welchem Frequenzen ausgewählt werden können, am besten wird hier nur eine ausgewählt – dann geht der spätere Suchvorgang schneller.

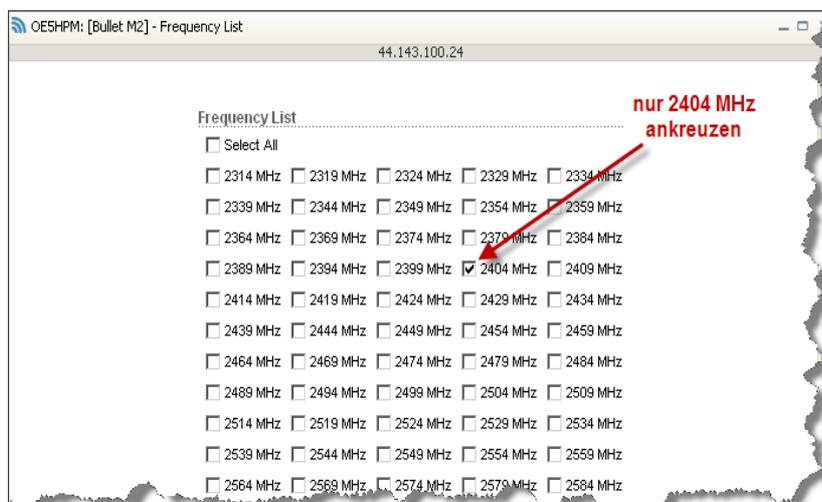


Abbildung 8: Bullet Frequenzpopup

1. Nun steht im Feld **B** nur noch eine Frequenz, die des Zugangs (in unserem Fall 2404 MHz), als nächstes ist es wichtig folgende Einstellungen zu tätigen, siehe **C**:
 1. Frequency Scan List → enabled
 2. Channel Shifting → enabled (notwendig um im Amateurband zu bleiben)
 3. Channel Width → 5MHz (so gut wie alle HAMNET Zugänge arbeiten mit 5 MHz Bandbreite)
2. Als nächstes folgt die Konfiguration des eigenen Rufzeichens im Reiter 'SYSTEM'

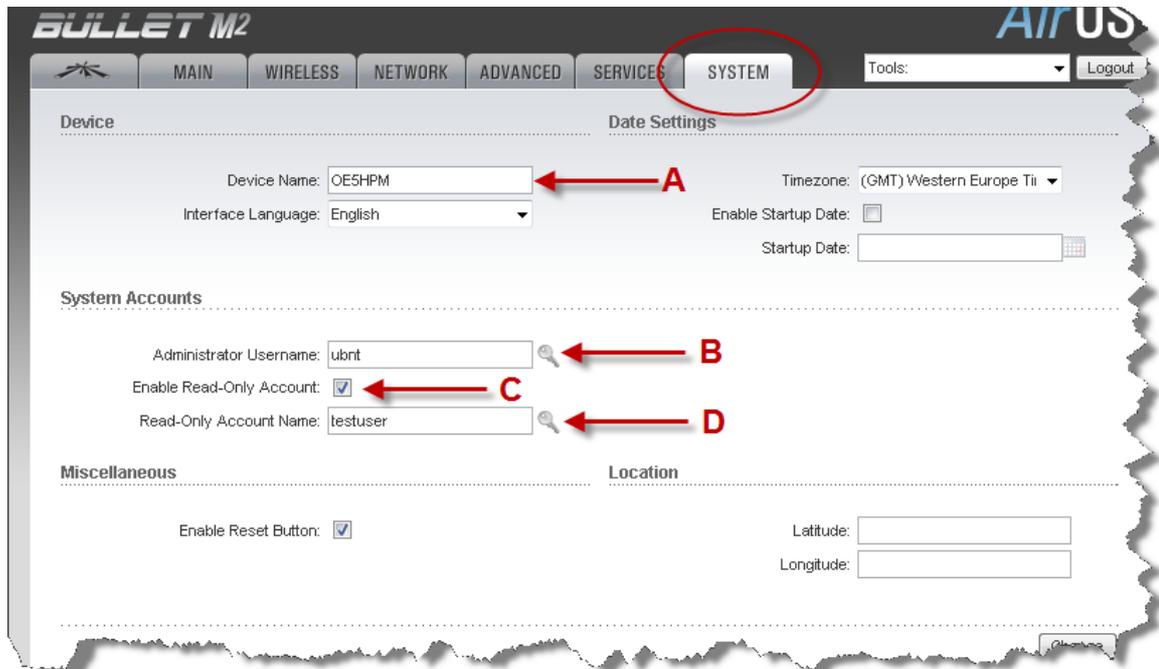


Abbildung 9: Bullet 'Reiter System'

Der Devicename **A** wird mit eigenen Rufzeichen belegt.

Bei dieser Gelegenheit wird auch gleich, falls gewünscht, der 'Read-Only' Account **C** mit dem Accountnamen 'testuser' **D** aktiviert. Damit ist es anderen, nicht Sysops, möglich zumindest die Startseite des Bullet aufzurufen um evtl. die Feldstärke zu beobachten.

Weiters sollte auch für den Administrator ein Passwort vergeben werden, dies geschieht mit einem Klick auf die kleine Lupe **B** neben 'Administrator Username'.

3. Nun wird wieder auf den Reiter 'WIRELESS' zurück gewechselt und zu guter letzt mit **D** nach dem HAMNET Knoten gesucht ...

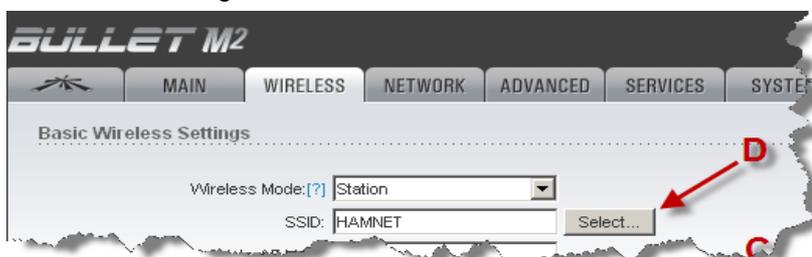


Abbildung 10: Bullet 'Reiter WIRELESS'

dabei sollte nachfolgend abgebildetes Popup erscheinen:

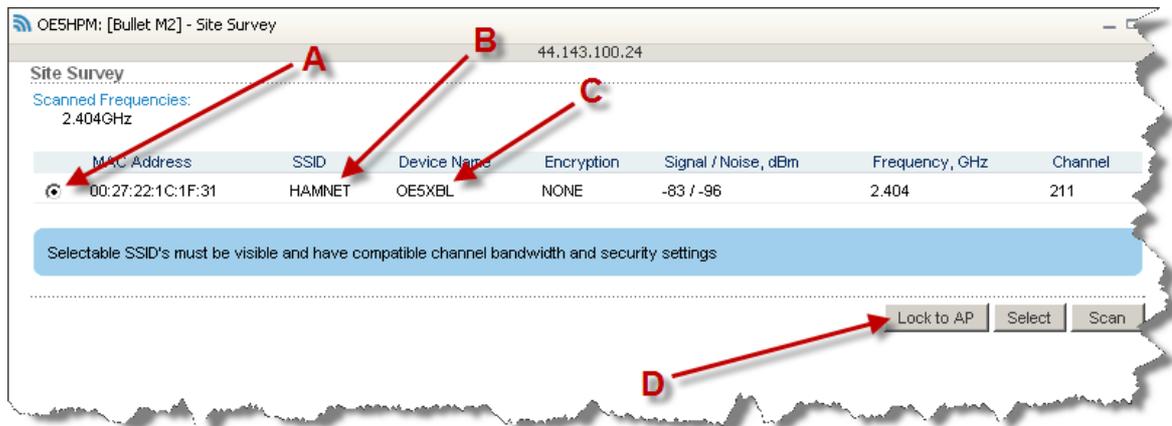


Abbildung 11: Bullet Site Survey

Es sollte zumindest eine Station gefunden werden, welche die Netzwerkennung (SSID) HAMNET trägt **B**, in **C** ist ersichtlich um welches Rufzeichen es sich beim Zugang handelt, mit **A** wird der Knoten angewählt und schlussendlich mit einem Klick auf 'Lock to AP' **D** verbunden.

Somit sollte die erste Hürde geschafft sein und die Verbindung zum HAMNET Knoten aufgebaut worden sein und es müsste sich ein Bild wie in Abbildung 6 ergeben.

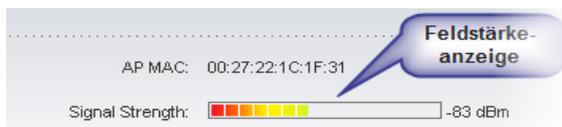


Abbildung 12: Feldstärkeanzeige

Es steht nun die Entscheidung an, wie das Bullet bzw. die eigene Station ins HAMNET eingebunden werden soll, die Möglichkeiten dazu wurden bereits in 'Userzugang Anwendungskonzepte' beschrieben.

3.2 Einbindung mittels 'Bridged-Mode'

Im Bridged-Mode gibt es im wesentlichen 2 relevante Dinge zu beachten:

- dynamische IP-Adresse (wird vom Zugangsknoten verteilt)
- statische IP-Adresse (wird vom Sysop des Zugangsknoten individuell ausgegeben)

Ansonsten ist lediglich noch die Einstellung 'Network Settings' zu beachten, hier wird festgelegt unter welcher IP-Adresse das Bullet im Netzwerk erreichbar ist.

Denkbar wäre hier, sich beim Sysop 2 IP-Adressen zuteilen zu lassen und eine davon dem Bullet selbst und die andere dem angeschlossenen PC zuzuweisen.

In nachfolgendem Bild wird die Konfiguration für dynamische Adresszuweisung dargestellt:

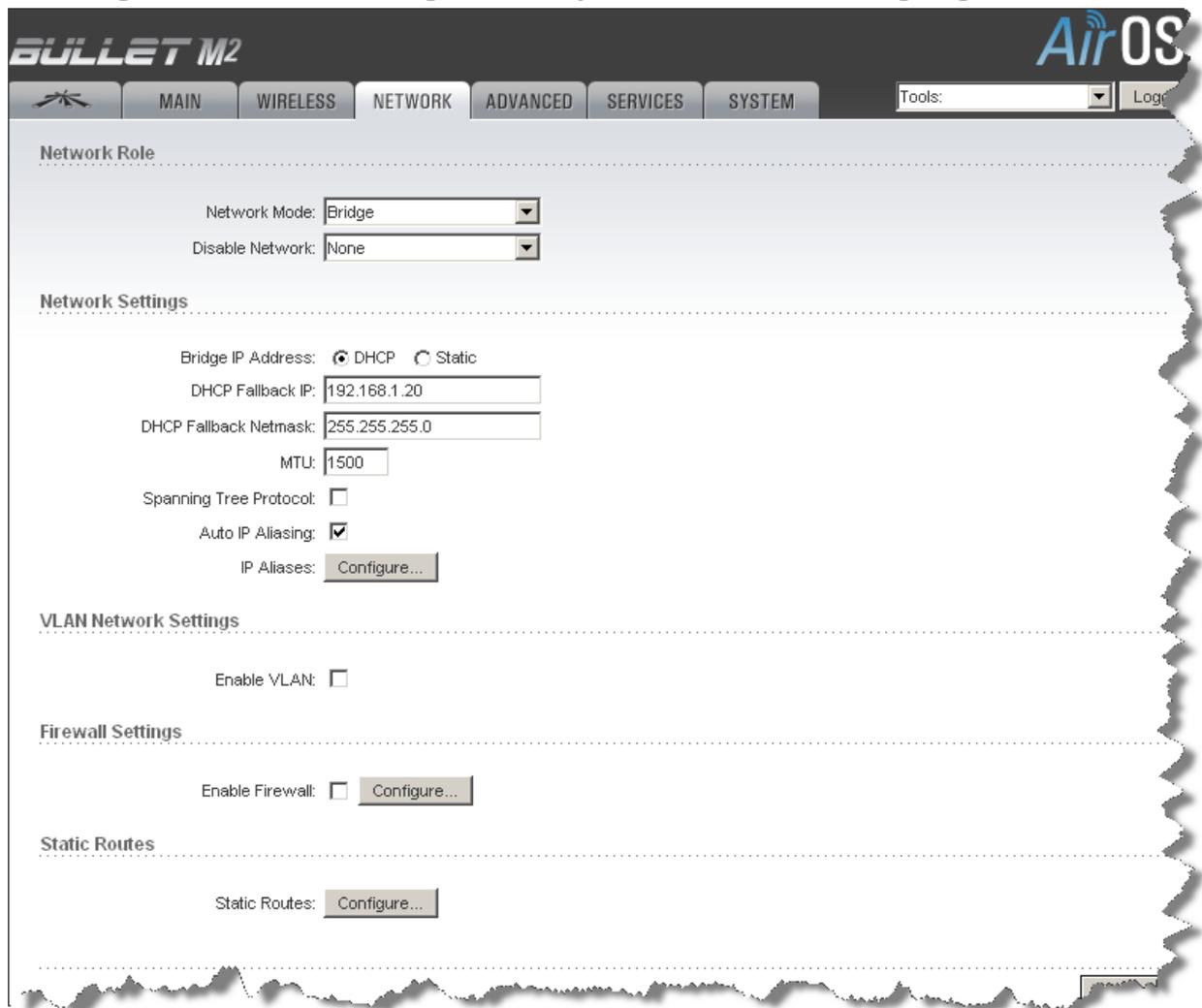


Abbildung 13: Bullet Network - bridged dynamisch

Wie vorhin angedeutet wäre auch eine statische Konfiguration möglich, wie nachfolgendes Bild verdeutlicht:

The screenshot shows the web interface of a Bullet M2 device running AirOS. The navigation menu includes MAIN, WIRELESS, NETWORK, ADVANCED, SERVICES, and SYSTEM. The 'NETWORK' tab is selected. The interface is divided into several sections:

- Network Role:** Network Mode is set to 'Bridge' and Disable Network is set to 'None'.
- Network Settings:** Bridge IP Address is set to 'Static'. The IP Address is 44.143.100.24, Netmask is 255.255.255.0, Gateway IP is 44.143.100.1, and Primary DNS IP is 44.143.100.1. MTU is 1500. Spanning Tree Protocol is disabled, and Auto IP Aliasing is enabled.
- VLAN Network Settings:** Enable VLAN is disabled.
- Firewall Settings:** Enable Firewall is disabled.
- Static Routes:** A 'Configure...' button is present.

Abbildung 14: Bullet Network - bridged statisch

In diesem Fall hätte das Bullet im Netzwerk die statische IP-Adresse 44.143.100.24 (zugewiesen für OE5HPM).

3.3 Einbindung mittels 'Networked-Mode'

Diese Methode ist, wie bereits Eingangs erwähnt, wohl die praktikabelste für die meisten Benutzer. Daher wird auf die Konfiguration etwas detaillierter eingegangen:

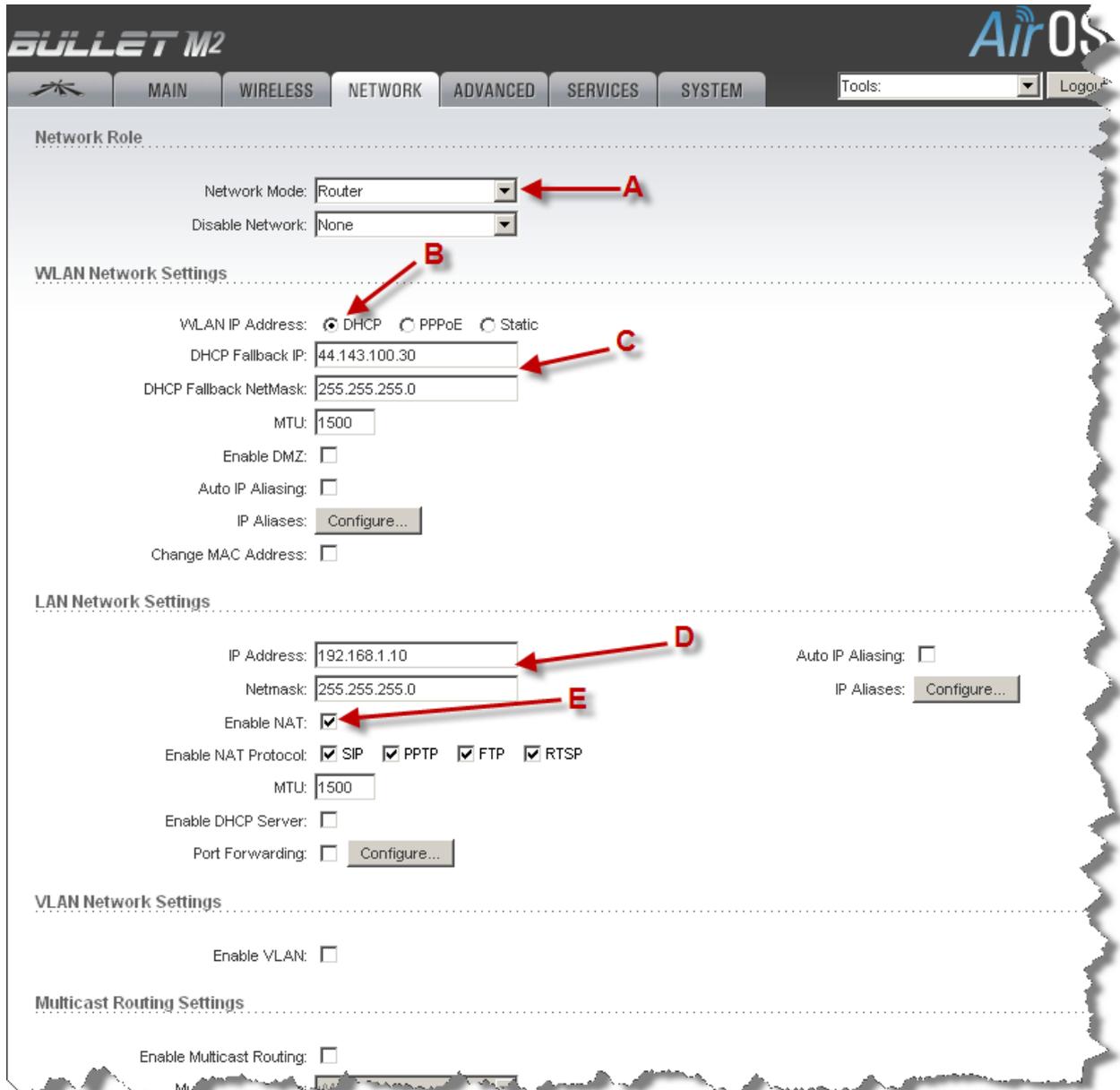


Illustration 15: Bullet Network - networked

Zuerst wird der Network Mode **A** auf 'Router' umgestellt, als nächstes gibt es wieder die Entscheidung ob die IP-Adresse im HAMNET statisch oder dynamisch zur Verfügung steht, im Beispiel ist diese auf DHCP **B** – also dynamisch – eingestellt, weil dies in den meisten Anwendungen der Fall ist.

Weiters kann man auch optional eine 'Fallback' Adresse **C** eingeben, diese wird dann gezogen wenn vom Zugangsknoten keine Zuteilung erfolgt.

Dieses Feld sollte am besten leer bleiben, denn wenn man keine Adresse vom Knoten zugeteilt bekommt, ist dieser wahrscheinlich auch nicht erreichbar und die Einstellung bringt nichts.

Nächster wichtiger Schritt ist, die IP-Adresse des Bullet für das lokale Netzwerk festzulegen **D**, im Beispiel ist dies 192.168.1.10. Danach muss noch das Häkchen für 'enable NAT' **E** gesetzt werden, damit die Pakete auch ins HAMNET „geroutet“ werden.

Somit wäre die Konfiguration am Bullet abgeschlossen und es muss noch der oder die PCs entsprechend eingerichtet werden, hier sind im wesentlichen 2 Sachen zu beachten:

- einrichten des Gateways zum HAMNET (damit die für das HAMNET gedachten Pakete zum Bullet geschickt werden)
- einrichten des Nameservers vom HAMNET (damit die Namensauflösung, z.B. web.oe5xbl.ampr.at, funktioniert).

3.3.1 Einrichten des Gateways zum HAMNET

Das einrichten der Standardroute für Pakete ins HAMNET funktioniert in allen Windows-Versionen (NT, XP, Win7) gleich. Bei Windows 7 ist darauf zu achten, dass die 'DOS-Box' als Administrator ausgeführt wird, den nur er kann Netzwerkeinstellungen verändern. Dazu am besten eine Verknüpfung am Desktop anlegen:

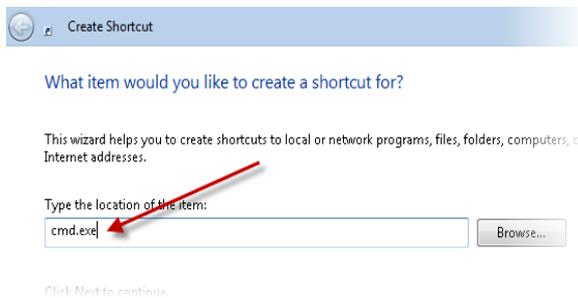


Abbildung 16: Win7 Verknüpfung DOS-Box

und angeben, dass diese als Administrator ausgeführt werden soll:

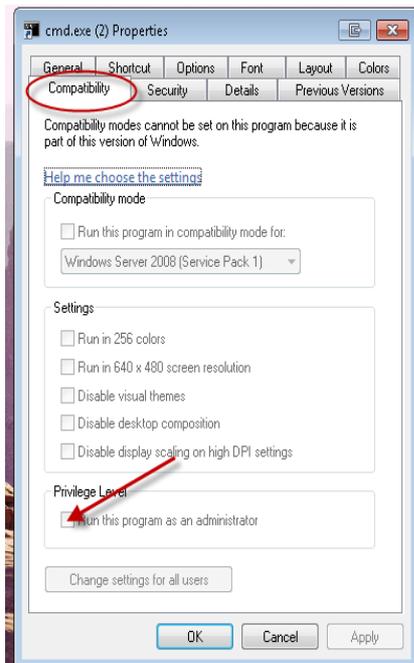


Abbildung 17: Win7 Verknüpfung DOS-Box Administrator

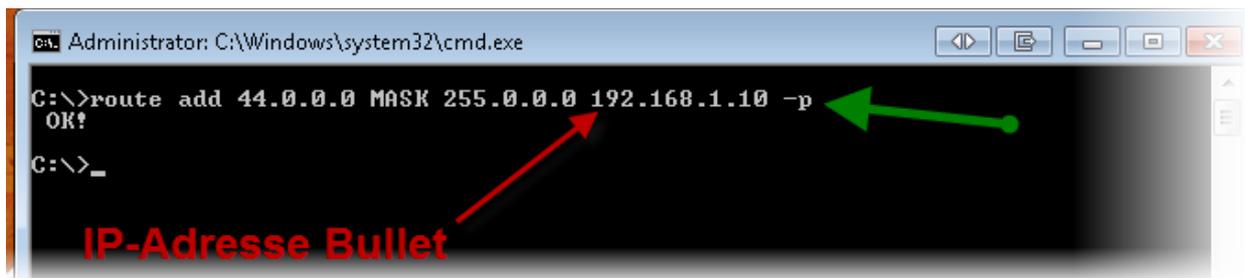
Unter Windows XP und Vorgängern, kann die DOS-Box einfach mit START → AUSFÜHREN → cmd.exe aufgerufen werden.

Nun das Kommando:

```
route add 44.0.0.0 MASK 255.0.0.0 192.168.1.10 -p
```

eingeben.

192.168.1.10 entspricht der IP-Adresse des Bullet, hier ist selbstverständlich die eingestellte Adresse einzutragen :-)



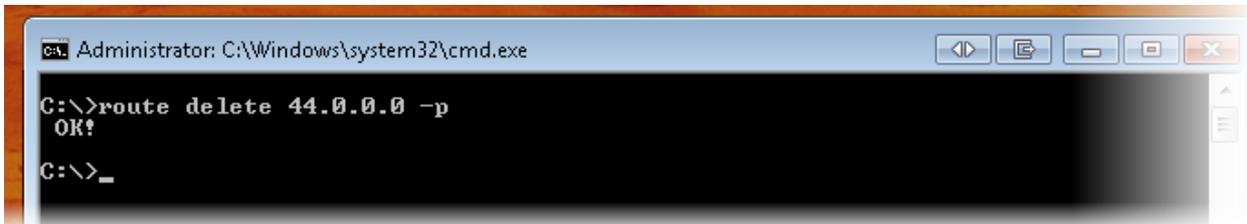
```
Administrator: C:\Windows\system32\cmd.exe
C:\>route add 44.0.0.0 MASK 255.0.0.0 192.168.1.10 -p
OK!
C:\>_
```

Abbildung 18: DOS-Box route add Kommando

Das Anhängsel '-p' sorgt dafür, dass das Kommando nur einmalig eingeben werden muss, lässt man dieses weg, ist die Einstellung der Route nur bis zum nächsten Neustart gültig.

Soll die Einstellung rückgängig gemacht werden, gibt man ein:

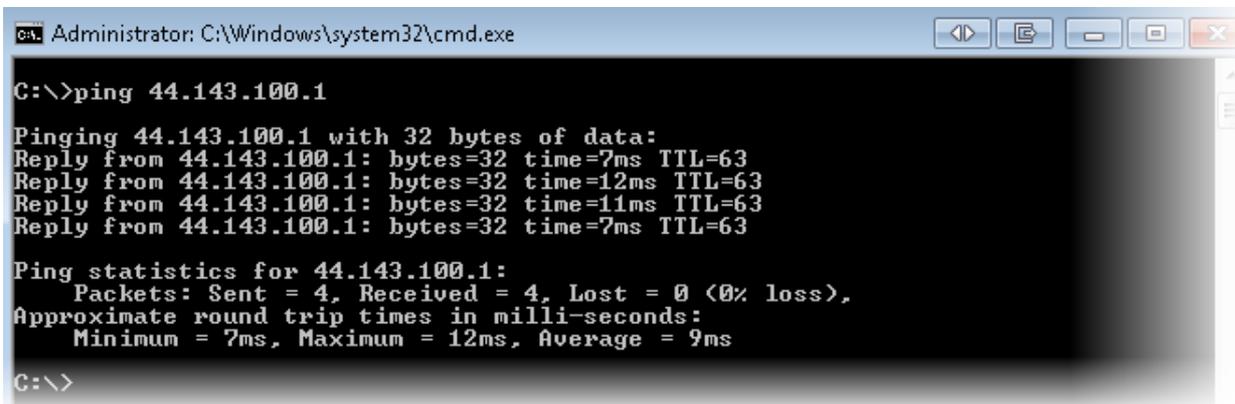
```
route delete 44.0.0.0 -p
```



```
Administrator: C:\Windows\system32\cmd.exe
C:\>route delete 44.0.0.0 -p
OK!
C:\>_
```

Abbildung 19: DOS-Box route delete Kommando

Damit wäre nun das Gateway gesetzt und man kann nun mittels Ping schon den ersten Test fahren:



```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping 44.143.100.1

Pinging 44.143.100.1 with 32 bytes of data:
Reply from 44.143.100.1: bytes=32 time=7ms TTL=63
Reply from 44.143.100.1: bytes=32 time=12ms TTL=63
Reply from 44.143.100.1: bytes=32 time=11ms TTL=63
Reply from 44.143.100.1: bytes=32 time=7ms TTL=63

Ping statistics for 44.143.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 12ms, Average = 9ms
C:\>
```

Abbildung 20: DOS-Box ping

Schlägt der Ping fehl, besteht wahrscheinlich keine Verbindung zum HAMNET Knoten oder Bullet. Die Verbindung zum Bullet kann mit einem einfachen ping 192.168.1.10 getestet werden, auch hier ist die 192.168.1.10 durch die korrekte Adresse des Bullet zu ersetzen. Schlägt auch dieser Ping Versuch fehl, sollte man die Konfiguration vom Bullet im Reiter 'Network' nochmal überprüfen.

3.3.2 Einrichten des Namensservers vom HAMNET

Um Namen wie web.oe5xbl.ampr.at auflösen zu können, muss ein Nameserver im System konfiguriert werden, dies geschieht wie folgt – die Vorgehensweise ist in allen Windows-Versionen ähnlich und fast ident.

Im folgenden Beispiel wird dies unter Win7 demonstriert:

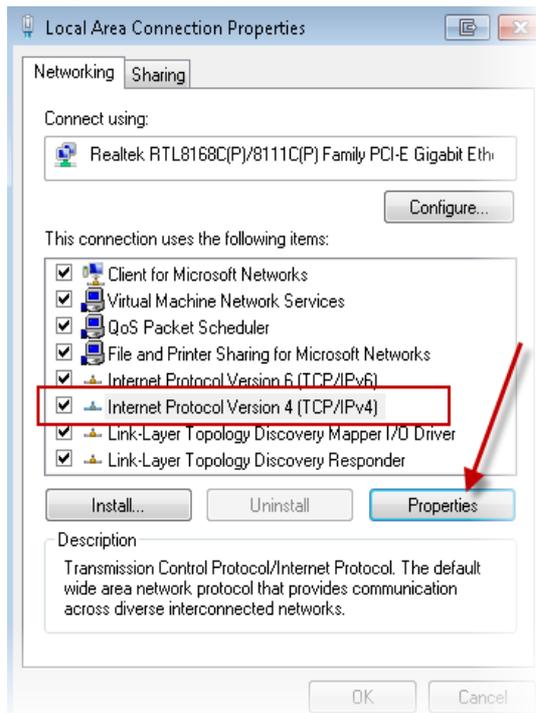


Abbildung 21: DNS Netzwerkeinstellungen

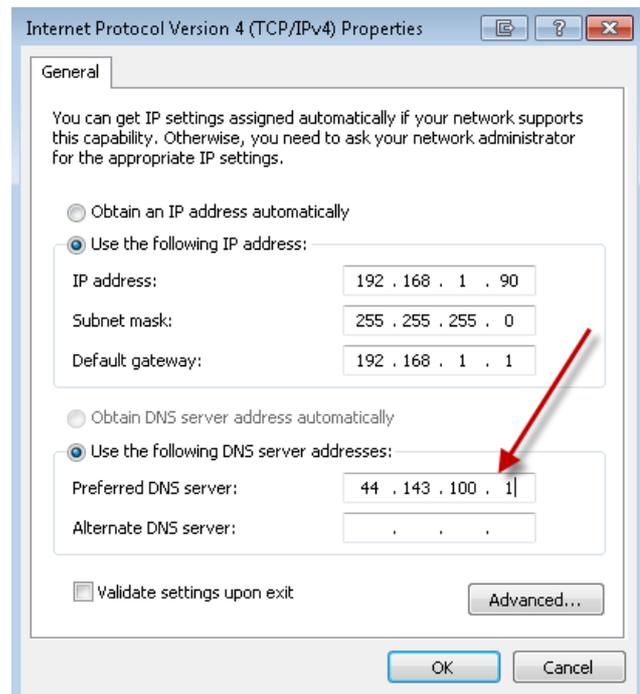


Illustration 22: DNS Netzwerkeinstellungen 1

Hier wird nun der Nameserver eingetragen, im Falle für den Zugangsknoten OE5XBL ist dies 44.143.100.1.

Danach kann man mittels Ping die getätigten Einstellungen testen:

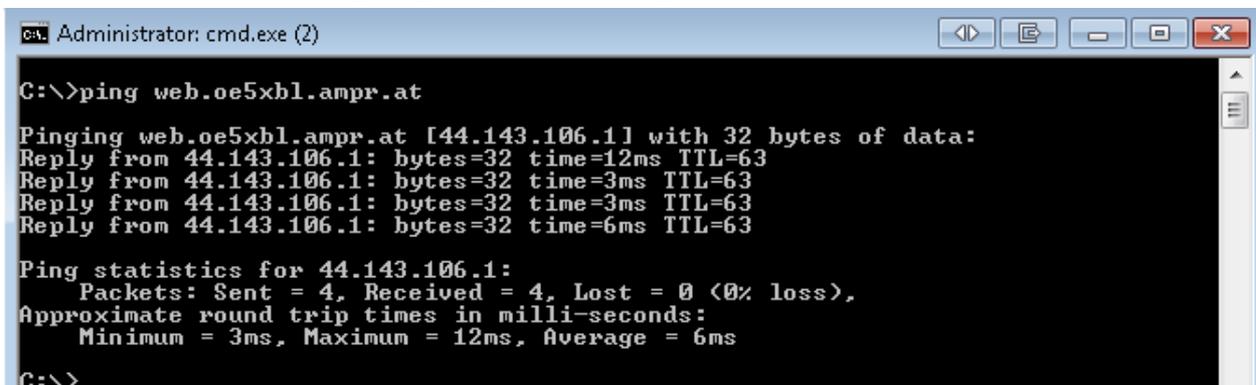


Abbildung 23: DOS-Box ping ...

4 offene Punkte, TODO

Folgende Sachen fehlen in dieser Beschreibung noch und werden in einer der nächsten Versionen ergänzt:

- Anbieten eigener Services / Konfiguration
- Firewall Konfiguration