

WLAN/VPN Upgrade

Marc Seeger

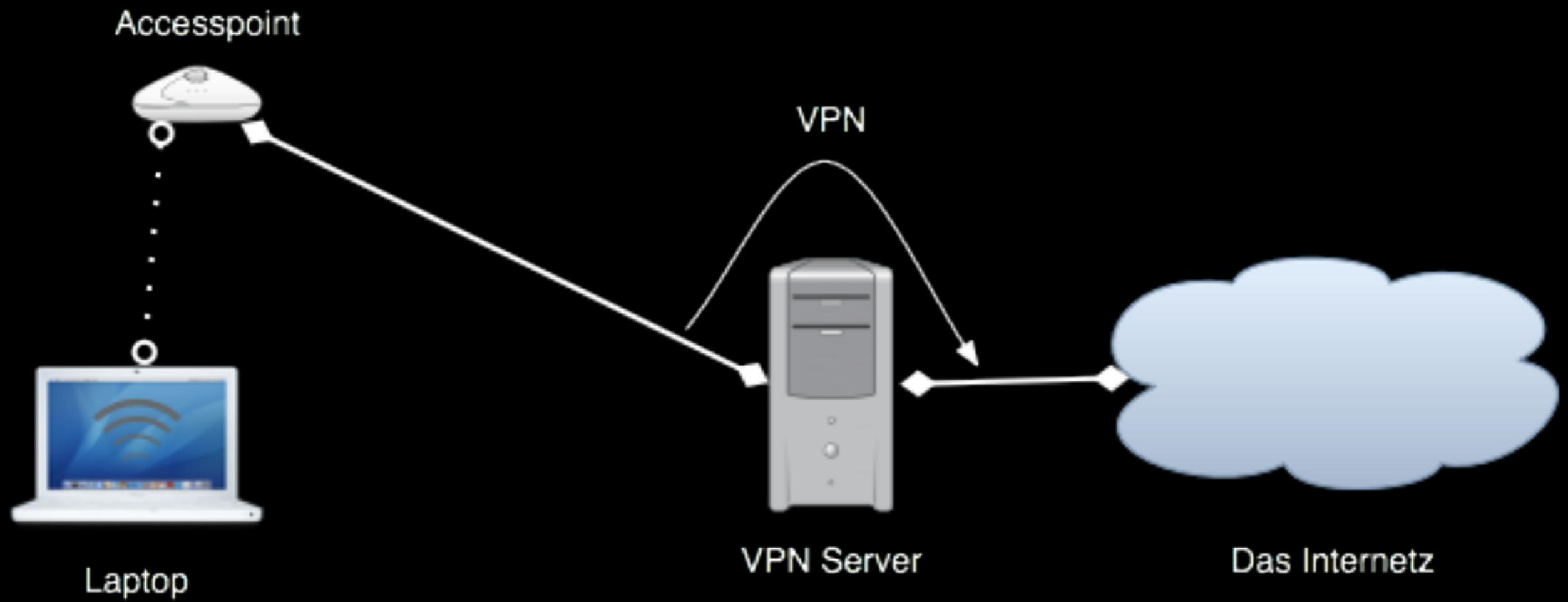
MIB6

Projekt Sommersemester 08

Was?

Aufbau einer PPTP Infrastruktur
mit Anbindung an das HdM LDAP
über einen Radiusserver

Infrastruktur



Warum?

Motivation #1

Say hello to iPhone.



Say bye to recep **T** · · · ion

Motivation #2

Terminal?

Zertifikat?

conf Datei?

OpenVPN?

Motivation #2

conf Datei?

Terminal?

OpenVPN?

Zertifikat?

Evaluation

Plattform-Support



Einsatz auf Smartphones

 iPhone



Symbian



Windows Mobile



keine Zertifikate

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: SKS 1.0.10

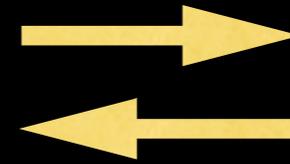
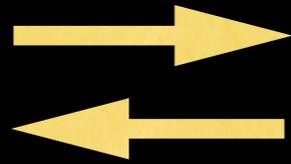
```
mQGIBEUa/PERBAC6pAcHyYLZX6ZGzbL3ANHawQLFTe9EetulZjaL6P4VrggaHH298lc6nDKa
uRz/mOG+1OiwkLFP2qsUnb5ozCTCgrAAHdLp5+3e7B+N8D7ytjFEi4waLVQxUMcpmy8GZ2fY
pLAP462VV7pQ8tNRqSlkZnZ73Yb7G/kBxGcHnnA91wCg+UyBd3vMV+bJIMx9zENLufWq/nEE
ALLe3OcTzkwbkGCjmM0VWJ7bMZx7jIINIUmX9yqtWgVwJ3AQscAtpiXtxwINotJYmBn6VNMU
3TferHIQHx6b3qqmxHcBmCOFucY/l9XYQs2gOsXKot2aY6F6A0MMe+EjdYjDoDqrE85ma2y7
yC1OhzLW1T1AqJdnXdC8i980Ag0qA/0XyAubHrvSjH7A+VQXoJamAJCeNOO4I777fZpMCHEI
R05lxaZOsm+ocLrqnKD/9AbUZUJr0TzBJQy7DQd8JQoOchDBi4tzDEM2AYakY7iHKBcWtAUi
w1kFVMgkZbW2zu+nRklX0JpssNUuvHDusOnD46r/fBISM3Z+Yzdg98xQ27QhTWfyYyBTZWVn
ZXlgPG1haWxAbWFyYy1zZWVnZXluZGU+iEYEEBECAAYFAkUbkBUACgkQa7NR0ZrY0dfpZACf
YsUh5LGLSbzqt7KFHtoQKa5iq2MAn06cyvCeylPLARbeH9vX+9dboe6KiEYEEBECAAYFAkcM
a8oACgkQjS31JhtlKH8e/ACcDwTuHjSsjB7wcd6KYi3wcFG4Gk8An0xOJq+xfTPiR9sTOq0W
tMdozedDiEYEEBECAAYFAkcuSNIACgkQt8QAD/33qWzjLgCfdTN9xp66ylwLbMlks0li5kfv
wyAAn3HJYH1I7GZGzn0GxUJ7JpAF2tpaiEYEEBECAAYFAkQhXyACgkQHcl4qC6MNVreSwCe
LLdoWD5TYrz7YLi00/f+A2sGPXwAnRrWbJxlVuLA/c48qqNNUcpC+T0KiGAEEExECACAFakUa
/PECGwMGCwklBwMCBBUCCAMEFgIDAQleAQIXgAAKCRAsGEIMfliDbO/eAJwMJOCpBbWswfQV
WtMcbvrs8dIEFwCbBh+Yh45G4TI18YnxMf5Pm23kwOyJAhwEEAECAAYFAkgGBrcACgkQOn9Q
r2eQ/3nJiA//TaTPHNTvpVmshLcYV7jLc9D1iKrxZElbbnK/PrexgGa3nllkpbOb0AmY0HQb
AhdGwel64zKvxvCTCltsXZaLA+xRgjTJY+K0w9QiXzf5wIU+xOYx+3mVu06UdY357AvfC+3M
7/6yj/a6QO02o7oC7eF9fSajS3BgazyQaCbGlvVsEurrcKRVyfoGqbfBzBSIIXalR1q+S0Hx
K/3Ng1oaXfS2110Jh7U46ZoQvM28U4utWJA4bt/5K9d2q4/FLB/wp4OfS57NUX4BVHwxnP/N
y8luMT6NC8G70TiAvJSOTodDTm/AulruuDBEKPj1Q2IGQnv7av25aCXllq6Fv01NUiDdDbmd
upphwt4zkOv1vlpI8N/9krvXnrAG6e65TDCPTQLYcmiW+lv/EWq1l/RrP/M5Jxn+mCX+s9qe
ANa8QLbAm14hmPOl1x/R29BsTisxvU1ofmxCiid1/Knd3iNiXyvaMalpdPXG29VC0T/OsNMf
DmmAWX32zSEd806AMZ3CHesadGnarhViccmmhVnreVkhpkv0JYFeA/JiKwnl8olywtqsd9p
PrymOETE5AR8lxhByAw/zVhWYGW81dnSEDleAeCndl9QLS3+vkUVEJGs3OUmaO+p789jVczx
Wdvh08ovD/5L1ZJGqjZ3zs0aeldLFUd+JzA7qb4vfNE91UaJAhwEEwECAAYFAkciSMIACgkQ
giuE4S+4WRAjGRAA3MNyC096Yo89TJ3xka8ZFxlqn3697ZG/jROxiFfrDOPhijux6sECBX+O
```

Resultate

	OpenVPN	IPSec	PPTP
OSX	X	X (nativ)	X (nativ)
Windows	X	X (nativ)	X (nativ)
Linux	X	X	X
iPhone		(X)	X
Symbian		naja...	
WM		(X)	X
User+Pass			X



Software-Setup



Probleme

Security

[...]

Conclusions

Microsoft has improved PPTP to correct the major security weaknesses described in [SM98]. However, the fundamental weakness of the authentication and encryption protocol is that it is **only as secure as the password chosen by the user.**

Quelle:

Bruce Schneier: Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)

<http://www.schneier.com/paper-pptpv2.html>

Hashes

Edit - [uid=ms155, ou=people,ou=POOL,ou=domainlist,dc=hdm-stuttgart,dc=de]

File Edit

objectClass:	inetOrgPerson
objectClass:	posixAccount
objectClass:	shadowAccount
objectClass:	sambaSamAccount
objectClass:	hdmAccount
sambaLMPassword:	[REDACTED]
sambaPrimaryGroupSID:	S-1-5-21-2281445993-2658238127-836942063-513
sambaLogonScript:	logon.bat
sambaLogonTime:	0
sambaHomeDrive:	logonDrive
uid:	ms155
uidNumber:	37689
cn:	Marc Seeger
sambaLogoffTime:	2147483647
sambaPwdLastSet:	1091537214
sambaAcctFlags:	[U]
loginShell:	/bin/sh
sambaProfilePath:	\\fs-POOL\profiles\stud\ms155
hdmCategory:	1
gidNumber:	31111
sambaSID:	S-1-5-21-2281445993-2658238127-836942063-37689
sambaPwdCanChange:	1091537199
sambaNTPassword:	[REDACTED]
homeDirectory:	/stud/ms155
sambaKickoffTime:	2147483647
sn:	Seeger
sambaHomePath:	logonhome

Apply Cancel

Umleitung

		 <p>HOCHSCHULE DER MEDIEN</p>
<p>Samstag 21. Juni 2008</p>		
<p>Gastzugang</p> <p>News</p> <p>FAQ</p> <p>Login</p>	<p>Bitte melden Sie sich mit Ihrem HdM-Benutzernamen und Passwort an:</p> <p>Login:</p> <p>Benutzername: <input type="text"/></p> <p>Passwort: <input type="password"/></p> <p><input type="button" value="Anmelden"/></p> <p>++++ Latest News +++++</p> <hr/> <p>23.8.2007 Autor: WLAN-Admin</p> <hr/> <p>Umstellung auf OpenVPN</p> <p>In den nächsten Tagen kann es auf Grund der Umstellung des WLAN-VPN von IPsec auf OpenVPN zu Ausfällen kommen. Wir bitten Sie dies zu entschuldigen.</p>	<p>Sie sind nicht angemeldet</p>
<p>Powered by  Velocity Tools</p>		

Überlastung verhindern

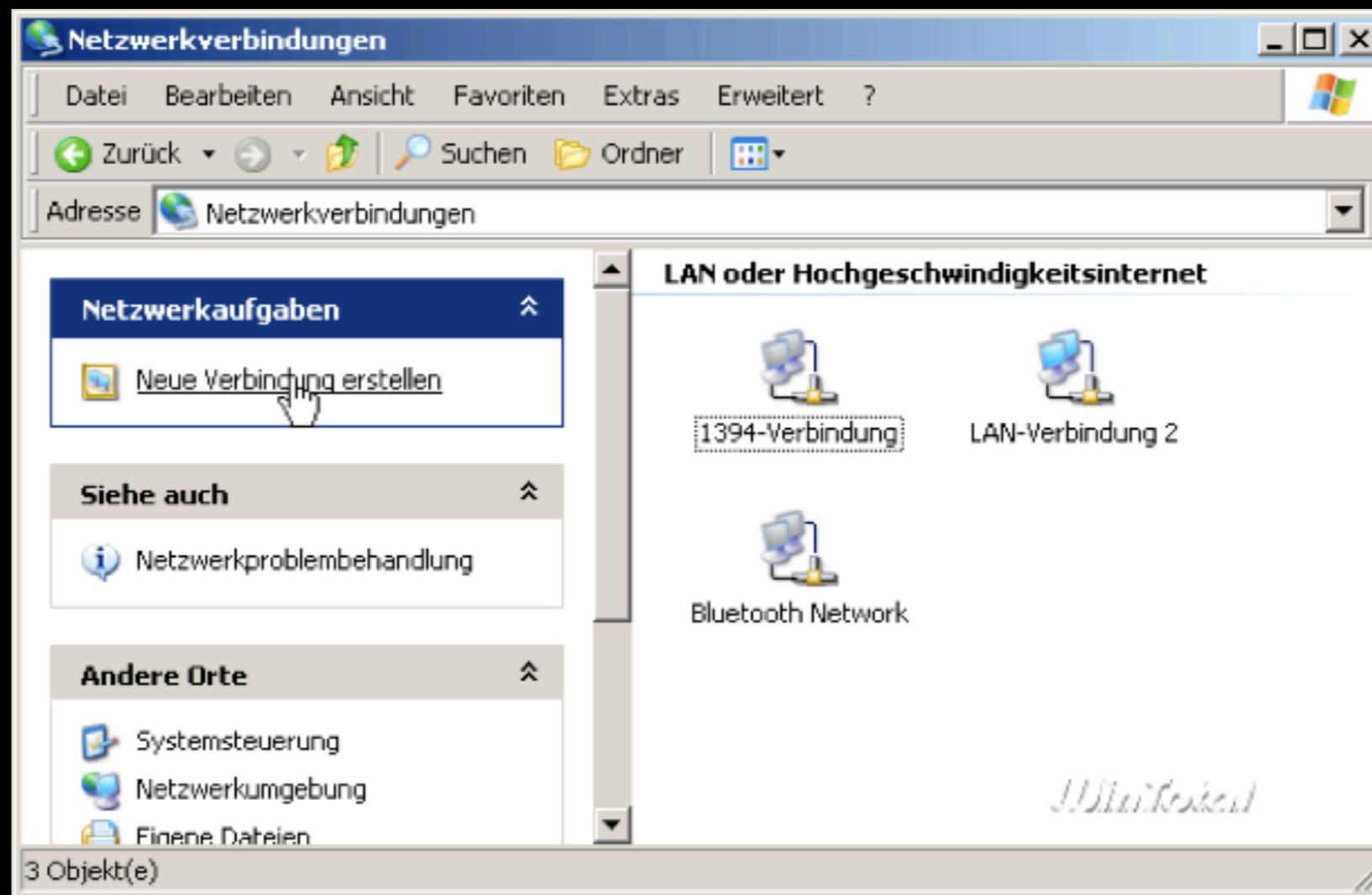


Usability

Daten

- IP: 141.62.39.253
- User: Euer HdM Kürzel
- Passwort: Euer HdM Passwort

Windows



Windows

Assistent für neue Verbindungen

Netzwerkverbindungstyp
Wie möchten Sie vorgehen?



- Verbindung mit dem Internet herstellen**
Stellt eine Verbindung mit dem Internet her, so dass Sie den Browser verwenden und E-Mail lesen können.
- Verbindung mit dem Netzwerk am Arbeitsplatz herstellen**
Stellt eine Verbindung mit einem Firmennetzwerk (über eine DFÜ- oder VPN-Verbindung) her, so dass Sie von zu Hause oder unterwegs arbeiten können.
- Ein Heim- oder ein kleines Firmennetzwerk einrichten**
Stellt eine Verbindung mit einem bestehenden Heim- oder kleinem Firmennetzwerk her oder richtet eine neue Verbindung ein.
- Eine erweiterte Verbindung einrichten**
Stellt eine direkte Verbindung mit einem anderen Computer über einen seriellen, parallelen oder Infrarotanschluss her oder richtet diesen Computer so ein, dass andere Computer darauf zugreifen können.

< Zurück Weiter > Abbrechen

Windows

Assistent für neue Verbindungen

Netzwerkverbindung
Wie soll die Netzwerkverbindung am Arbeitsplatz hergestellt werden?



Folgende Verbindung erstellen:

- DFÜ-Verbindung**
Stellt eine Verbindung über ein Modem und eine reguläre Telefonleitung oder über eine ISDN-Telefonleitung her.
- VPN-Verbindung**
Stellt eine Netzwerkverbindung mit einer VPN-Verbindung (Virtual Private Network) über eine Internetverbindung her.

< Zurück Weiter > Abbrechen

Windows

Assistent für neue Verbindungen

Verbindungsname
Geben einen Namen für die Verbindung mit Ihrem Arbeitsplatz an.



Geben einen Namen für die Verbindung im folgenden Feld ein.

Firmenname

Sie können zum Beispiel den Namen Ihres Arbeitsplatzes oder den Namen des Servers, mit dem eine Verbindung hergestellt werden soll, eingeben.

< Zurück Weiter > Abbrechen

Windows

Assistent für neue Verbindungen

VPN-Serverauswahl
Wie lautet der Name bzw. die Adresse des VPN-Servers?

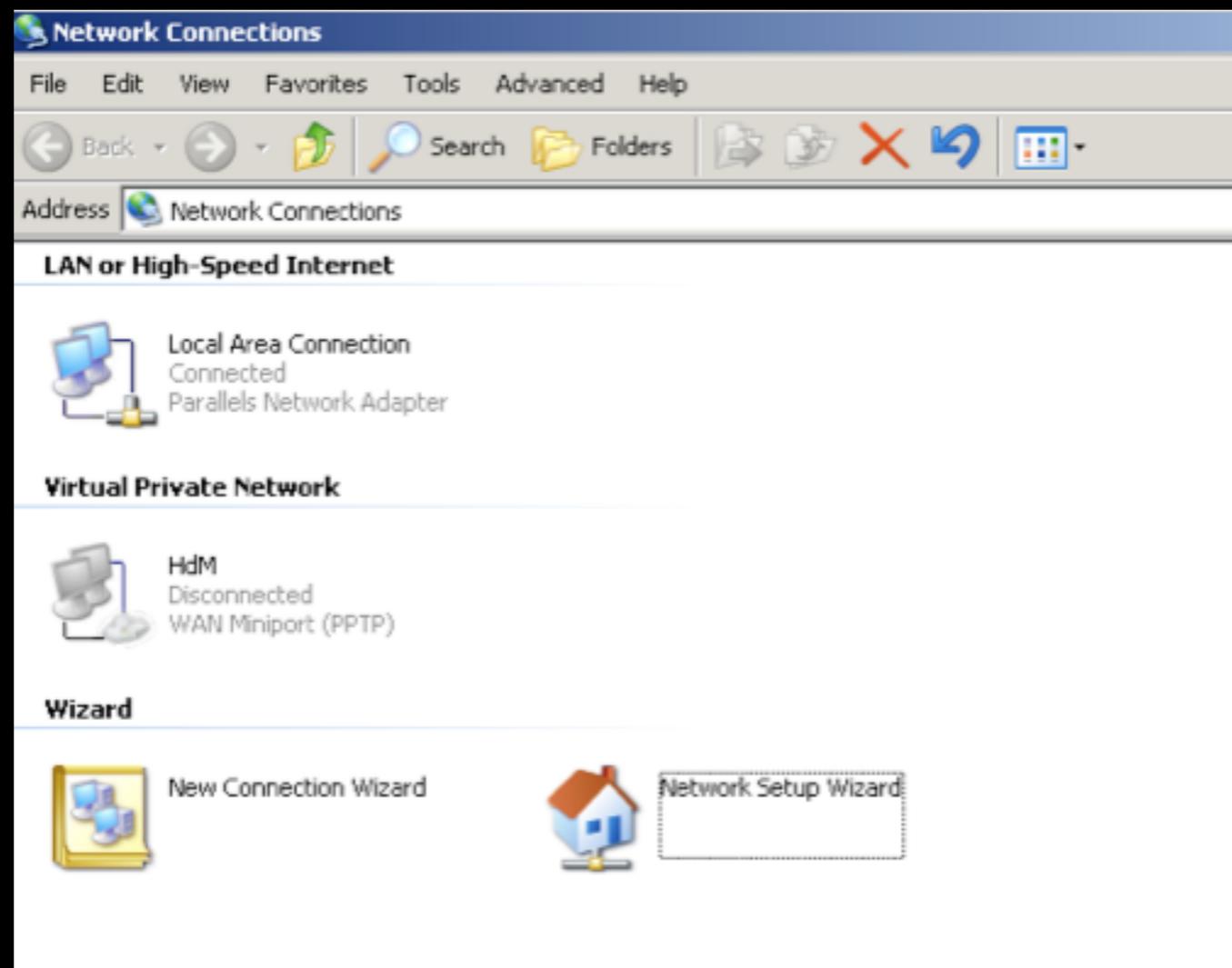


Geben Sie den Hostnamen oder die IP-Adresse des Computers ein, zu dem eine Verbindung hergestellt werden soll.

Hostname oder IP-Adresse (z.B. microsoft.com oder 157.54.0.1):

< Zurück Weiter > Abbrechen

Windows



Windows

Connect HdM



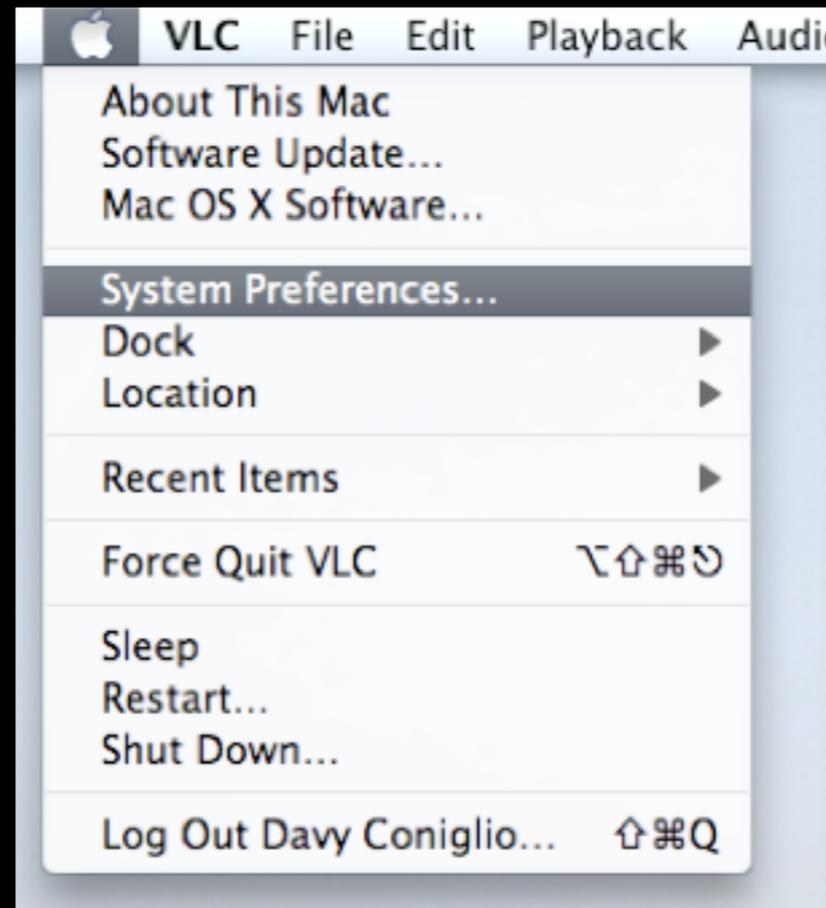
User name:

Password:

Save this user name and password for the following users:

- Me only
- Anyone who uses this computer

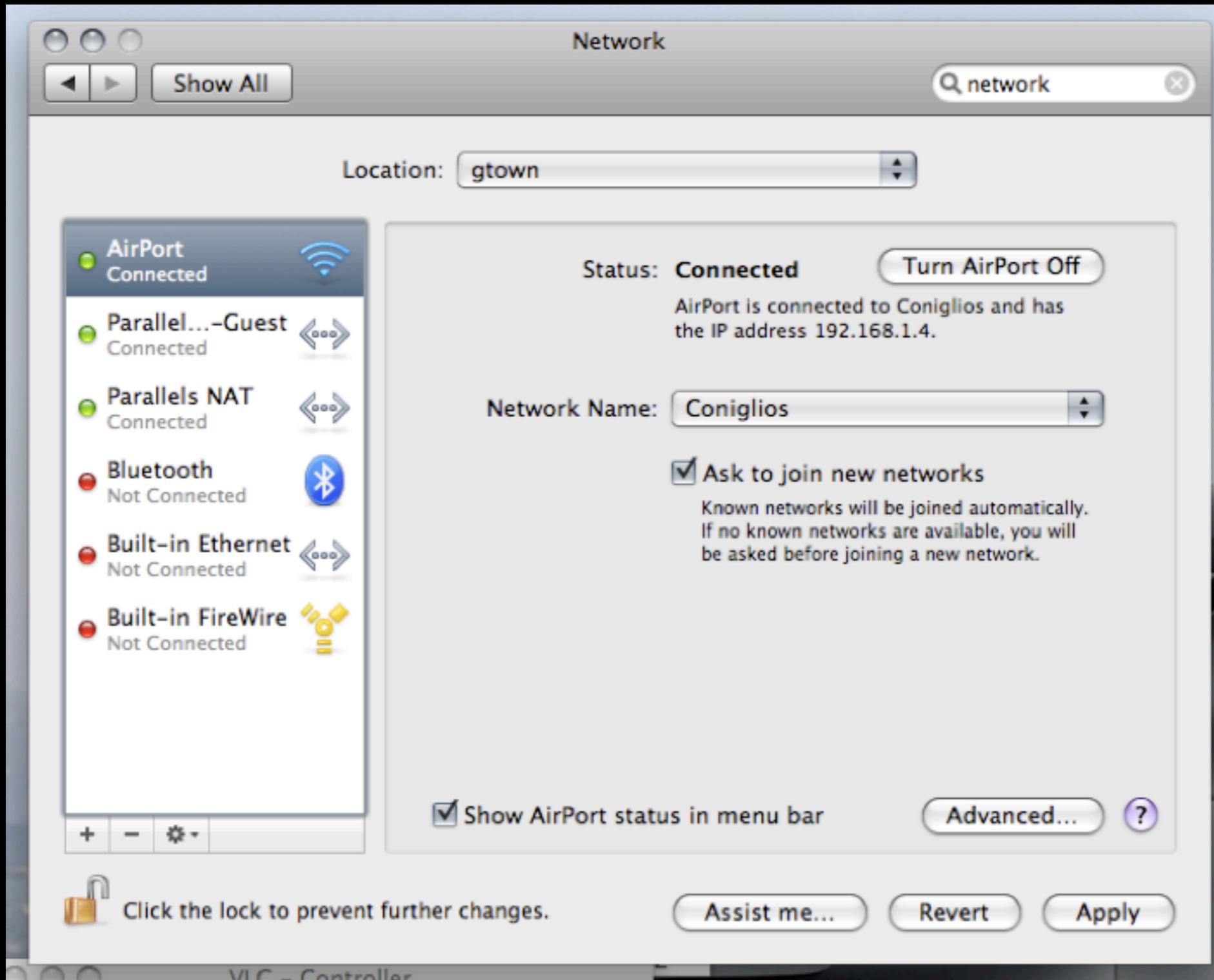
OSX



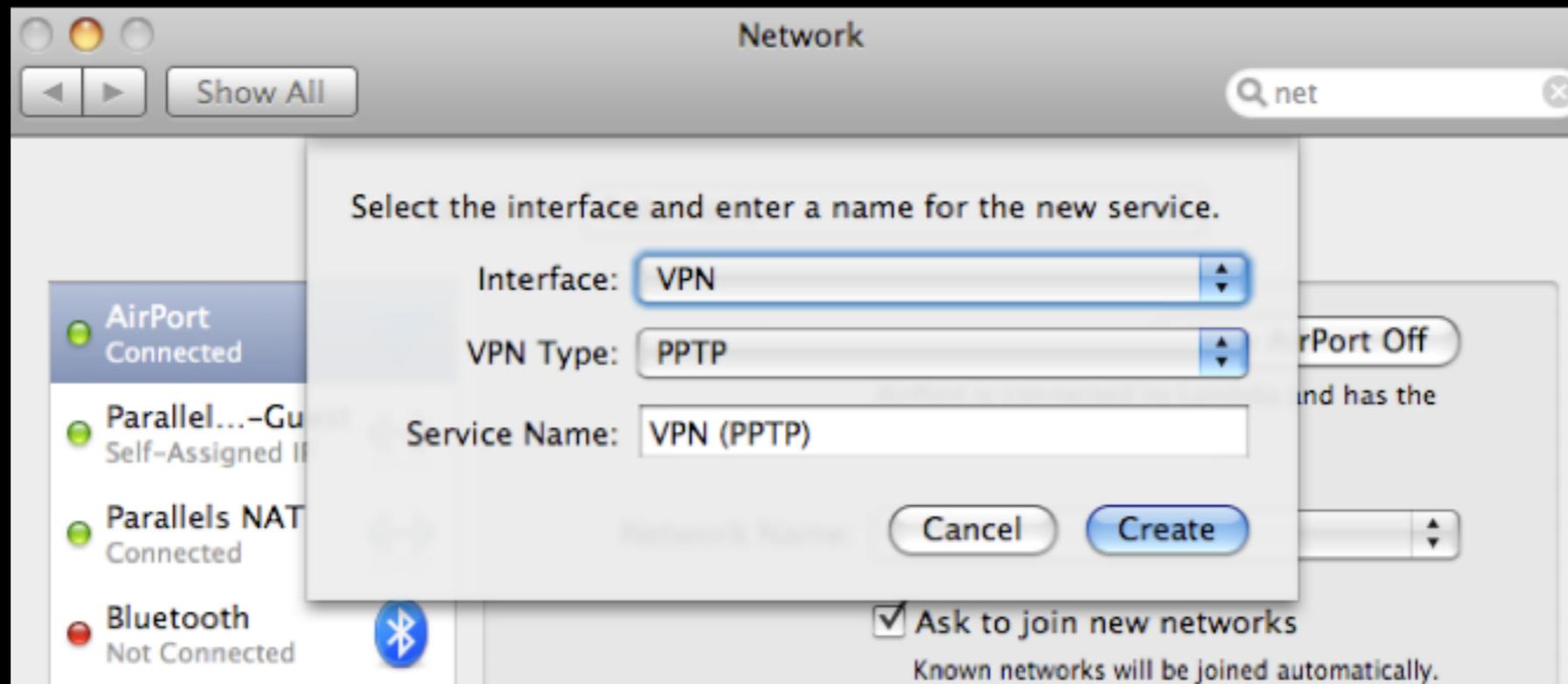
OSX



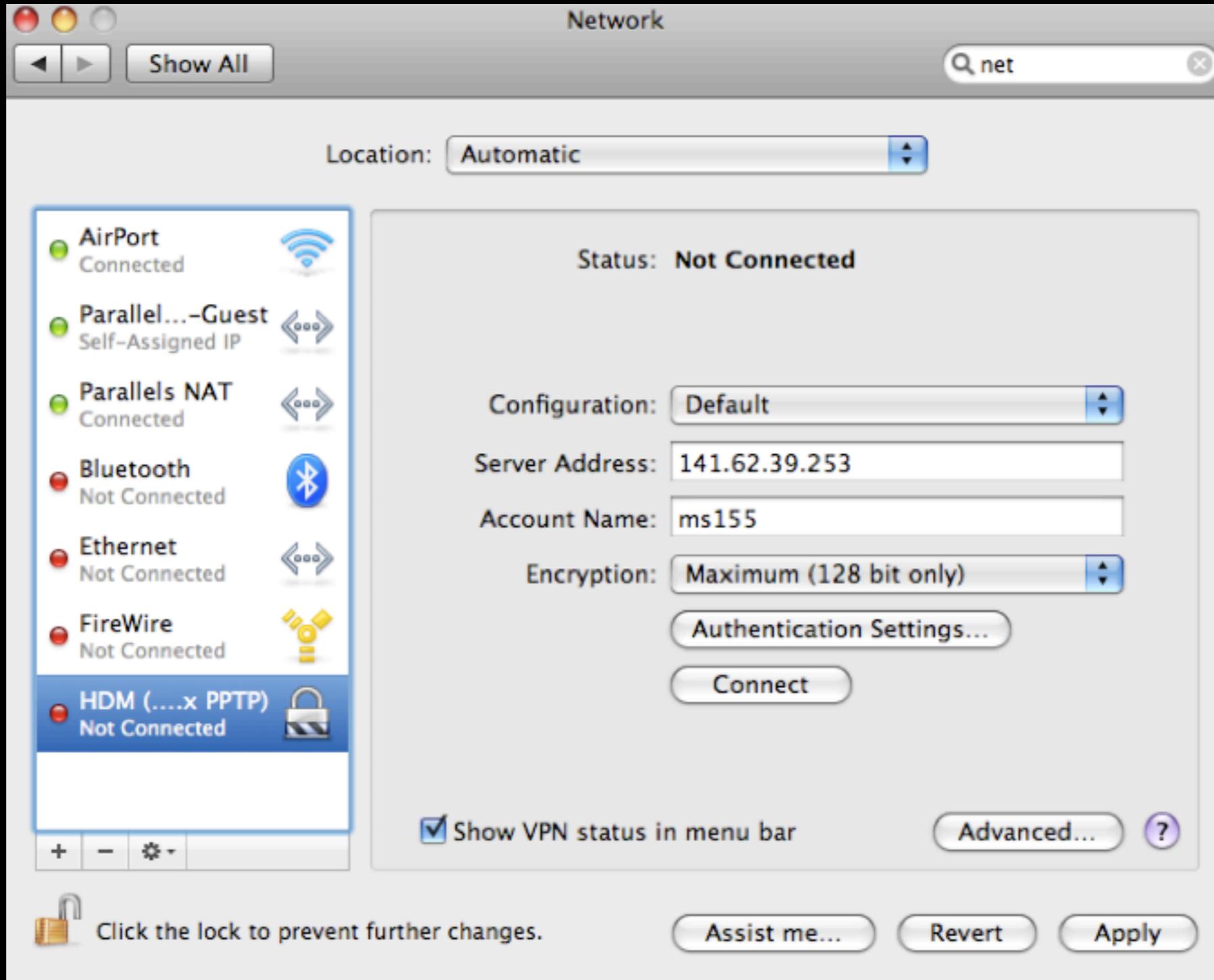
OSX



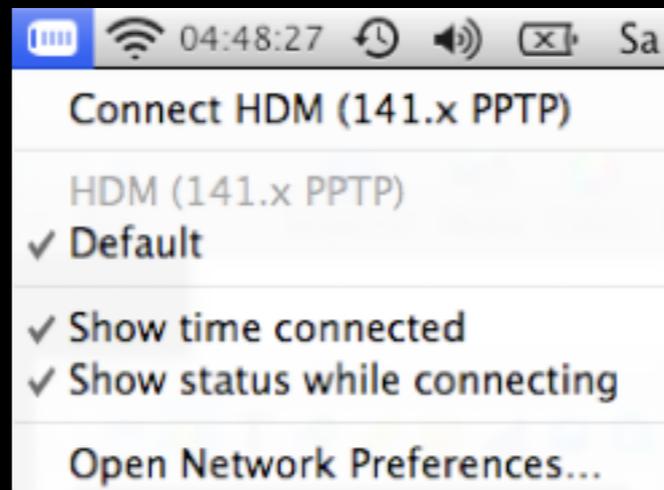
OSX



OSX



OSX



KTIXBYE