

IPv6 und Microsoft Direct Access in einer SBS-Umgebung

Von der Vision zum Einsatz

Über mich

Thorsten Raucamp

- Jahrgang 1971
- verheiratet, eine Tochter
- staatlich geprüfter Betriebswirt *Schwerpunkt EDV / Organisation*
- Mediator (Univ.)
- Datenschutzbeauftragter (TÜV)

Tätigkeitsschwerpunkte

- IT-Projektleiter,
spez. Workflowanwendungen im Microsoft-Umfeld
- IT-Mediator
- Zertifizierter Datenschutzbeauftragter (TÜV)

- E-Mail: tr@raucamp-consulting.de

Web: www.raucamp-consulting.de



Warum DirectAccess?

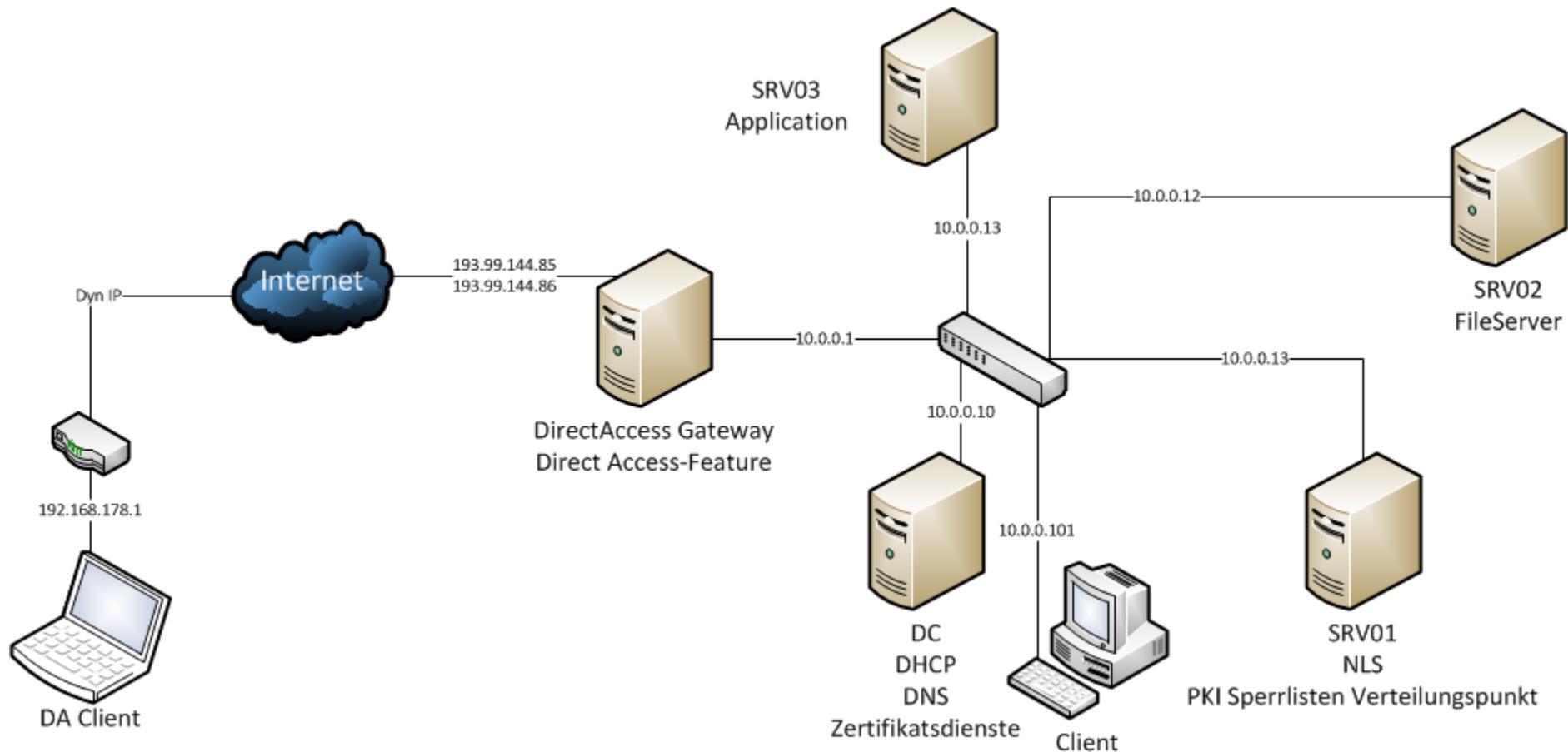
- Direkte Verbindung (kein VPN, TerminalServer, etc.)
- Funktioniert „überall“ (HTTPS)
- Remote Netzwerkadministration
- Versorgung mit Updates
- Sicher! (https , IPSec, IPv6 und Zertifikate)

Direct Access in Windows 2008 R2

Anforderungen:

- Domäne mit Active Directory Struktur (2008+)
- DirectAccess Server (Server 2008 R2) mit 2 Netzwerkkarten
- Clients: Windows 7 (Ultimate / Enterprise)
- Public-Key Infrastruktur
- Firewall muss Teredo-Pakete durchlassen
- ISATAP-Infrastruktur
- NAT64 für IPv4 Ressourcen
- **2 öffentliche IPv4-Adressen**

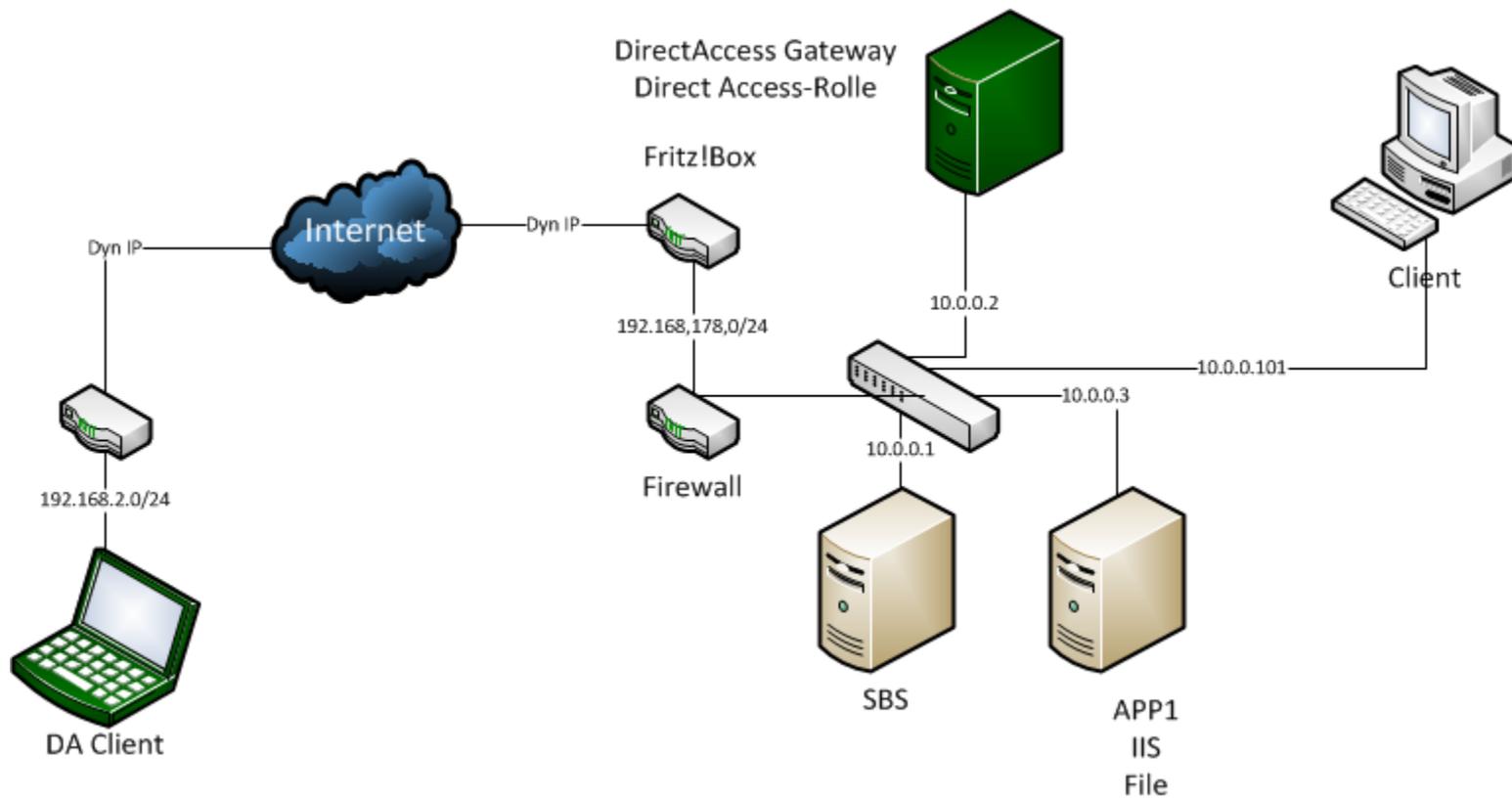
Direct Access in Windows 2008 R2



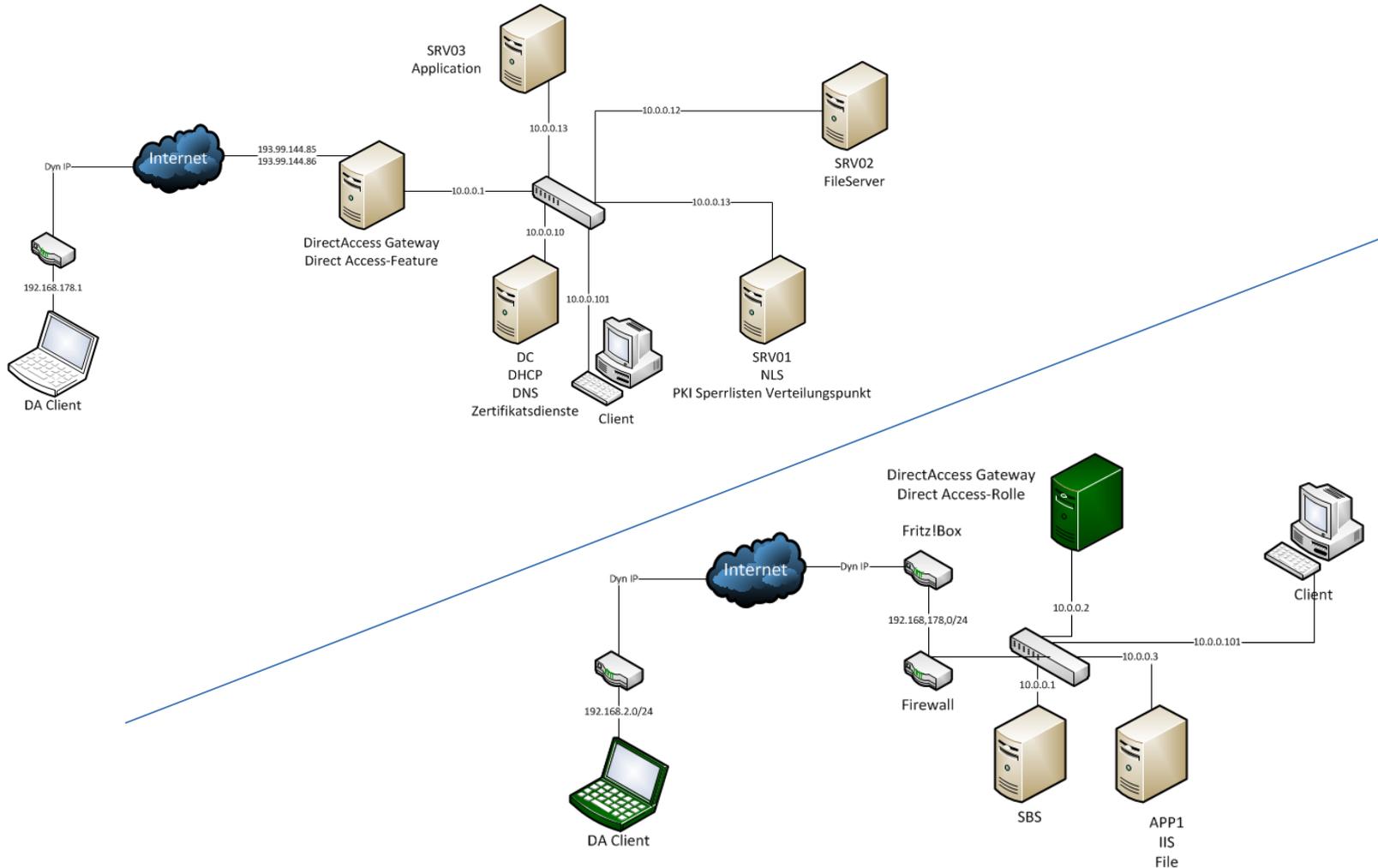
Bestehende Infrastruktur

- ADSL-Anschluss, dynamische IP, DynDNS
- FritzBox
- Endian Firewall
- SBS2011 Essentials
- Server „8“ CP (Server 2012)
- Windows 7 Ultimate Clients
- Notebook Windows 8 CP

Aktuelle Infrastruktur



Infrastruktur-Vergleich



Erste Überlegungen

- 2 Feste IP-Adressen: Eine neue Leitung muss her
 - 2Mbit CompanyConnect ca. 299 EUR/Monat
- Öffentliche IPv6 über sixXS
 - funktioniert nur, wenn das Quell-Netz auch IPv6 hat
- Eigene Tunnellösung
 - Stabil? Viel Bastelarbeit
- Endpunkt „in der Cloud“
 - Wie dann wieder zurück ins eigene Netz?
- Feste IP über VPN-Tunnel
 - Wird von Microsoft für Produktiven Einsatz nicht empfohlen
- Aber...

... da gibt's doch was Neues von...

... **Microsoft !!!**

DirectAccess im Server 2012

DISCLAIMER: These are the features and functions available in the [Windows Server 8 "Beta"](#) Preview. All items are subject to change or removal by Microsoft and are not considered to be final until release of Windows 8.

Die neue Option

Configure Remote Access

Remote Access Server Setup

Konfigurieren Sie die Einstellungen für DirectAccess und VPN.

Select the network topology of the server.

Edge

H_{inter} einem Edgegerät (mit zwei Netzwerkadaptern)

B_{ehind} an edge device (with a s_{ingle} network adapter)

In this topology, the Remote Access server is deployed with a single network adapter that is connected to the internal network.

Type the public name or IPv4 address used by clients to connect to the Remote Access

DirectAccess.dyndns.org

< Zurück Weiter > Fertig stellen Abbrechen

- DirectAccess Server hinter einer Firewall !!!

In 3 Schritten zu Direct Access



Willkommen
Die Optionen auf dieser Seite dienen zum Konfigurieren von DirectAccess und VPN.

→ **DirectAccess und VPN bereitstellen (empfohlen)**
Configure DirectAccess and VPN on the server, and enable DirectAccess to allow remote client computers not supported for DirectAccess to connect.

→ **Nur DirectAccess bereitstellen**
Configure DirectAccess on the server, and enable DirectAccess to allow remote client computers not supported for DirectAccess to connect.

→ **Nur VPN bereitstellen**
Configure VPN using the Routing and Remote Access console. Remote client computers connect over VPN, and multiple sites can be connected using VPN. Remote client computers can be used by clients not supported for DirectAccess.



Select the network topology of the server.

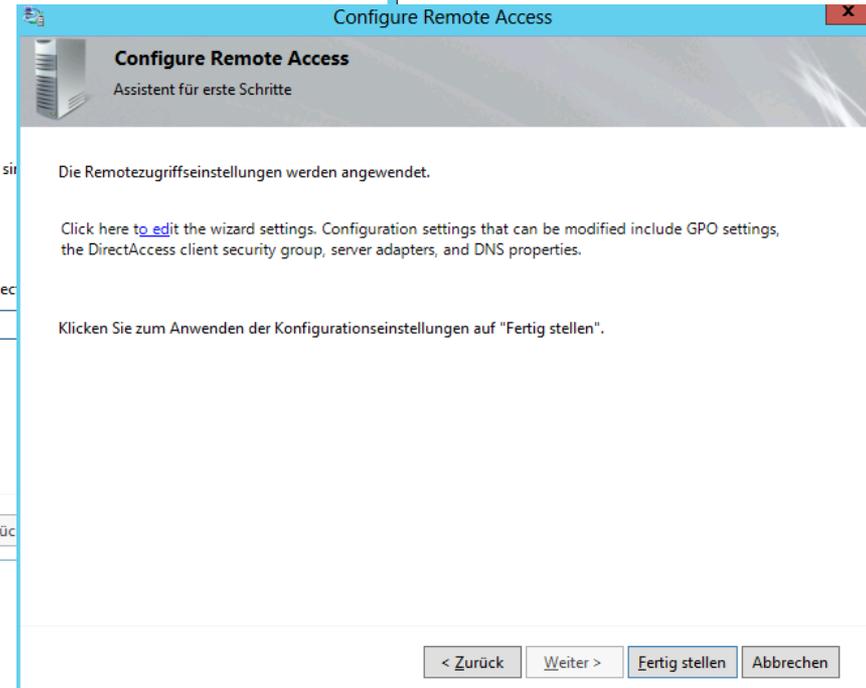
- Edge
- Hinter einem Edgegerät (mit zwei Netzwerkadaptern)
- Behind an edge device (with a single network adapter)

In this topology, the Remote Access server is deployed with a single network adapter connected to the internal network.

Type the public name or IPv4 address used by clients to connect to the server.

DirectAccess.dyndns.org

< Zurück



Die Remotezugriffseinstellungen werden angewendet.

Click here [to edit](#) the wizard settings. Configuration settings that can be modified include GPO settings, the DirectAccess client security group, server adapters, and DNS properties.

Klicken Sie zum Anwenden der Konfigurationseinstellungen auf "Fertig stellen".

< Zurück Weiter > Fertig stellen Abbrechen

... Na ja, nicht ganz:

- Die restliche Infrastruktur muss richtig eingerichtet sein:
 - Firewall
 - Active Directory
 - Zertifikatsdienste SBS2011e
 - DNS installieren
 - DHCP

Was sonst noch aufhielt:

- DirectAccess-Konfigurationsdatei äußerst sensibel
- Windows 8 Client Standardtreiber-Probleme
- Windows 8 Client stürzt in einem bestimmten Netz regelmäßig ab
- Tunnel wird aufgebaut, aber es funktioniert trotzdem nicht
- Kaum Hinweise im Netz auf die gewünschte Konfiguration

Erfolgreiche Verbindung!

```
Administrator: Windows PowerShell
PS C:\Windows\system32> ipconfig

Windows-IP-Konfiguration

Ethernet-Adapter Bluetooth-Netzwerkverbindung:
    Medienstatus . . . . . : Medium getrennt
    Verbindungsspezifisches DNS-Suffix:
Drahtlos-LAN-Adapter WiFi:
    Verbindungsspezifisches DNS-Suffix: t-mobile.de
    Verbindungslokale IPv6-Adresse . . : fe80::8912:e19c:83d2:3c8%22
    IPv4-Adresse . . . . . : 10.130.98.187
    Subnetzmaske . . . . . : 255.255.255.224
    Standardgateway . . . . . : 10.130.98.190

Ethernet-Adapter Verkabelte Ethernet-Verbindung:
    Medienstatus . . . . . : Medium getrennt
    Verbindungsspezifisches DNS-Suffix: rc.lan
Tunneladapter isatap.t-mobile.de:
    Medienstatus . . . . . : Medium getrennt
    Verbindungsspezifisches DNS-Suffix: t-mobile.de
Tunneladapter Teredo Tunneling Pseudo-Interface:
    Verbindungsspezifisches DNS-Suffix:
    IPv6-Adresse . . . . . : 2001:0:5ef5:79fb:2476:faaa:af44:36a7
    Verbindungslokale IPv6-Adresse . . : fe80::2476:faaa:af44:36a7%15
    Standardgateway . . . . . :
Tunneladapter iphttpsinterface:
    Verbindungsspezifisches DNS-Suffix:
    IPv6-Adresse . . . . . : fd34:6fb3:9b3e:1000:9473:bce5:be2c:b8a5
    Temporäre IPv6-Adresse . . . . . : fd34:6fb3:9b3e:1000:e845:c794:7d1a:921
    Verbindungslokale IPv6-Adresse . . : fe00::9473:bce5:be2c:b8a5%19
    Standardgateway . . . . . :
PS C:\Windows\system32> ping sbs

Ping wird ausgeführt für sbs.TR.lan [fd34:6fb3:9b3e:7777::a6f:6f01] mit 32 Bytes Daten:
Antwort von fd34:6fb3:9b3e:7777::a6f:6f01: Zeit=115ms
Antwort von fd34:6fb3:9b3e:7777::a6f:6f01: Zeit=227ms
Antwort von fd34:6fb3:9b3e:7777::a6f:6f01: Zeit=341ms
Antwort von fd34:6fb3:9b3e:7777::a6f:6f01: Zeit=510ms

Ping-Statistik für fd34:6fb3:9b3e:7777::a6f:6f01:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 115ms, Maximum = 510ms, Mittelwert = 298ms
PS C:\Windows\system32>
```

Netzwerke

Flugzeugmodus
Aus

Verbindungen

- Arbeitsbereichver... **Verbunden**
- ALDI TALK Verbindungsassistent
- MEDIONConnection

WiFi

- Telekom **Verbunden**
- 2IP-AP
- Cathrins GÄ#stenetzwerk
- EasyBox-B5FE66
- EpicFail
- Erde
- Klaerchen74
- Klaerchen74US
- PaedWuF.net
- Puderbach

Fazit:

- Server muss sauber konfiguriert sein, besonders DNS und DHCP!
- IPv6 wird intern nicht (zwingend) benötigt!
- Für Microsoft gibt's noch ein paar Baustellen
- Die How-To und Troubleshooting-Tipps müssen noch angepasst werden
- Lizenzpolitik von Microsoft ist zu beachten
- Basis für weitere Konfigurationen (z.B. PKI)

Vielen Dank für Ihre Aufmerksamkeit!