

LOKALE NETZE MIT IPv6

Erfahrungen aus der Implementierung

Autor: **Timo Baumgart**

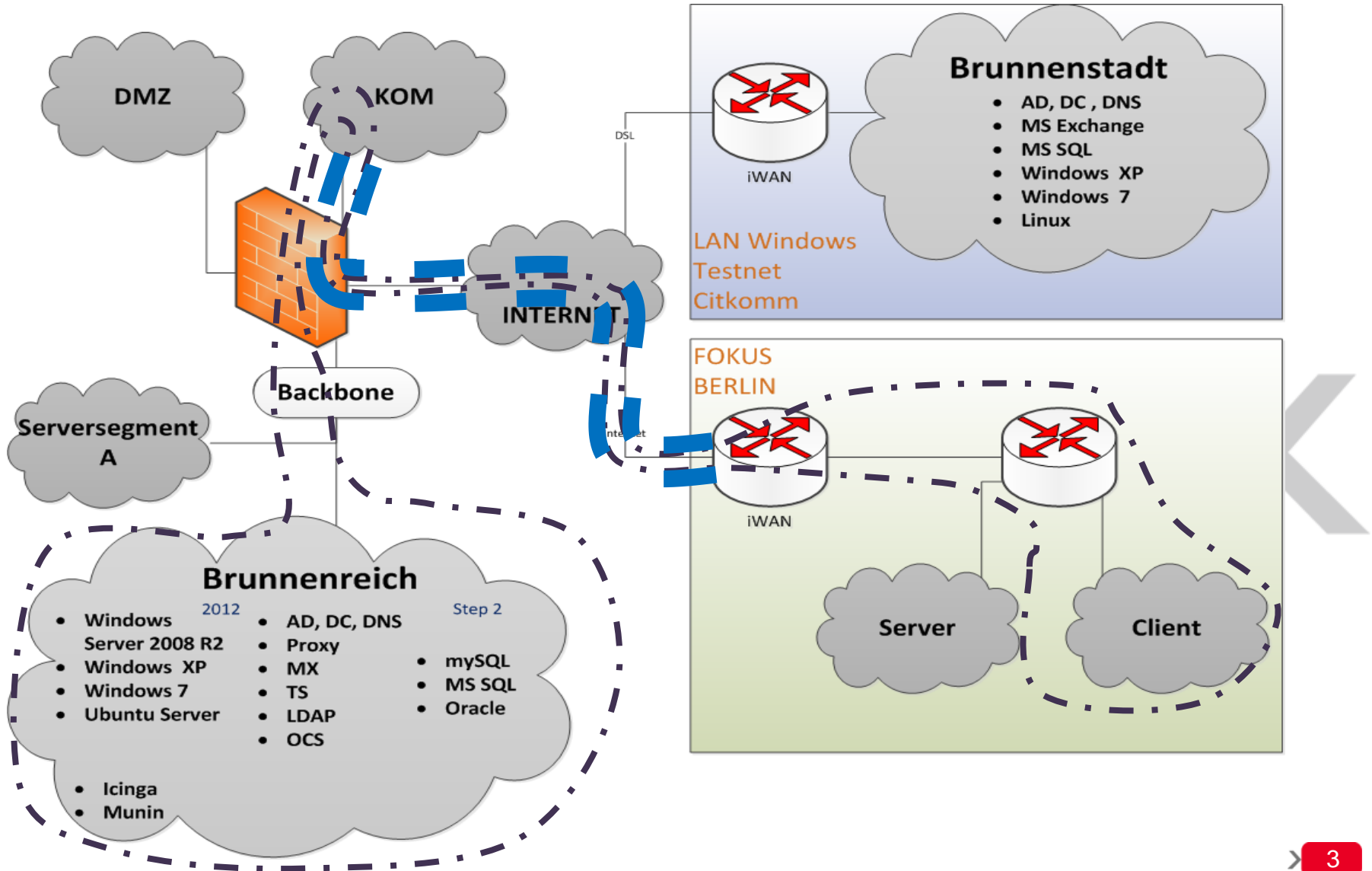
Version: 17.11.14
1.0

AGENDA

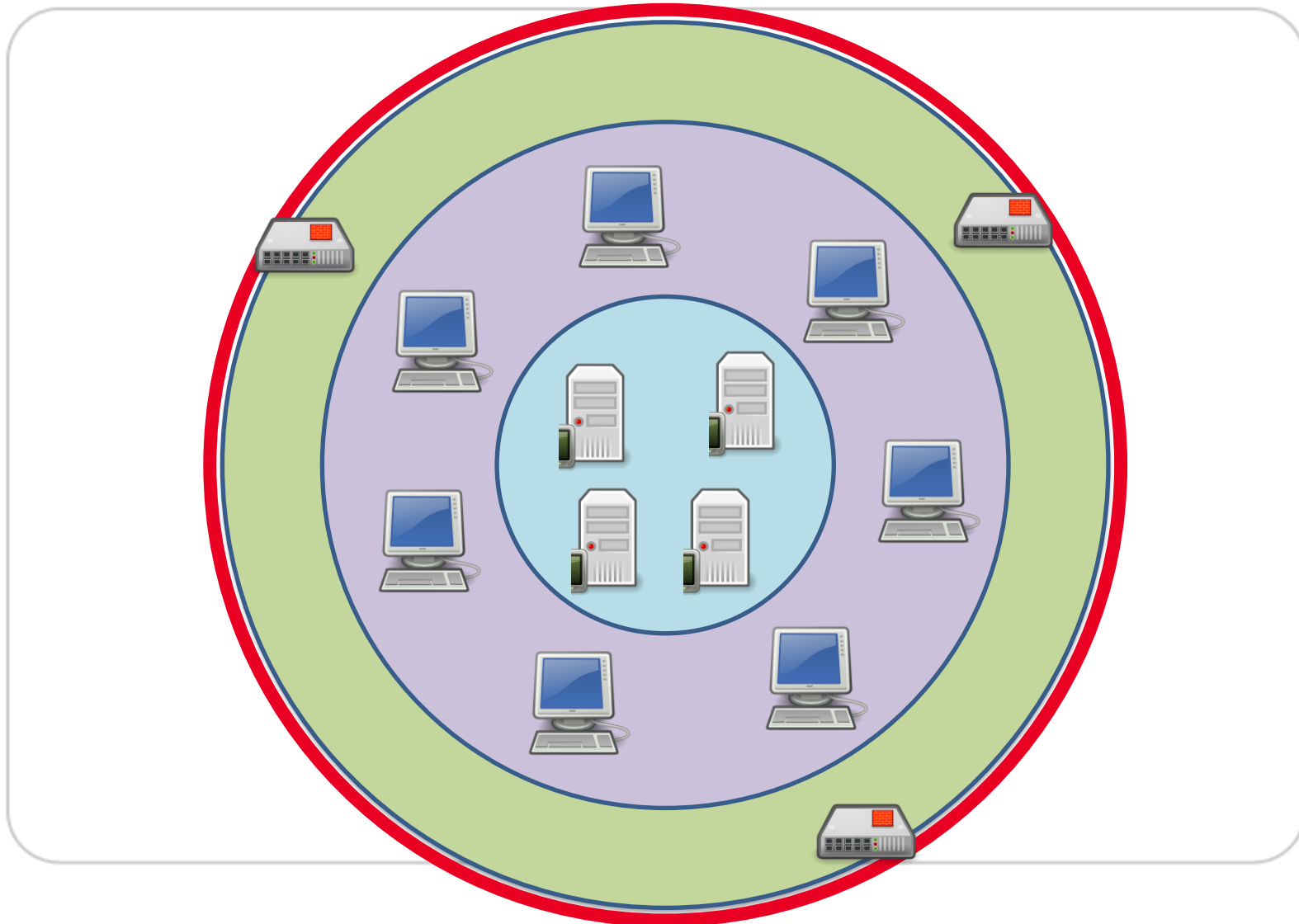
- Überblick
- Vorgehensmodell
- IPv6 Adresskonzept
- Router Advertisement Daemon
- Server
- Rollen
- Clients
- Testen
- Zusammenfassung



NETZWERK - ÜBERBLICK



VORGEHENSMODELL



VORGEHENSMODELL – DIESE SCHRITTE SIND EIN MUSS

- Mithilfe des Migrationsleitfaden den derzeitigen Sachstand des Netzes dokumentieren
 - Welche Voraussetzungen muss mein Netzwerk haben
- Erstellen eines Adresskonzeptes
- Router Advertisement Daemon
 - Was ist das und wofür benötige ich diesen?
- Zuerst kommen die Server
- Rollen nachinstallieren und/oder bearbeiten
 - DHCP(v6), ADDS (Active Directory Domain Services – beinhaltet AD [LDAP], DNS, GPO)
- Clients migrieren
- Applikationstest



SACHSTAND DES NETZWERKS

- Separates Netzwerk-Segment im Dual-Stack Betrieb
- 2 Windows Server 2008 R2 für die Kerndienste AD, DC & DNS für die Versorgung der anderen Server und Clients im Netz
- 1 Windows Server 2012 R2 für DHCP
- Statische Adressvergabe an die Clients per DHCP
 - Kein SLAAC (**S**tateless **A**ddress **A**uto**c**onfiguration)
- Exchange und MS SQL Server
- Proxy für den Internet-Zugriff aus dem LAN
- verschiedene Clients (Windows 7, Windows 8/8.1, Ubuntu 14.04 Desktop)

IPv6 ADRESSKONZEPT

PRÄFIXGRÖßE FÜR SUBNETZE

Beispiel Präfix: 2001:db8:ffff::/48

Subnetzbildung in dem 4. Wort des Präfixes

interface identifier

Basis Konzept (2 Nibbles f. Typ + 2 Nibbles f. Anzahl = 16 bits)

1. Wort

2. Wort

3. Wort

4. Wort

1. Nibble

2. Nibble

3. Nibble

4. Nibble

Geräteklasse

3. Byte IPv4

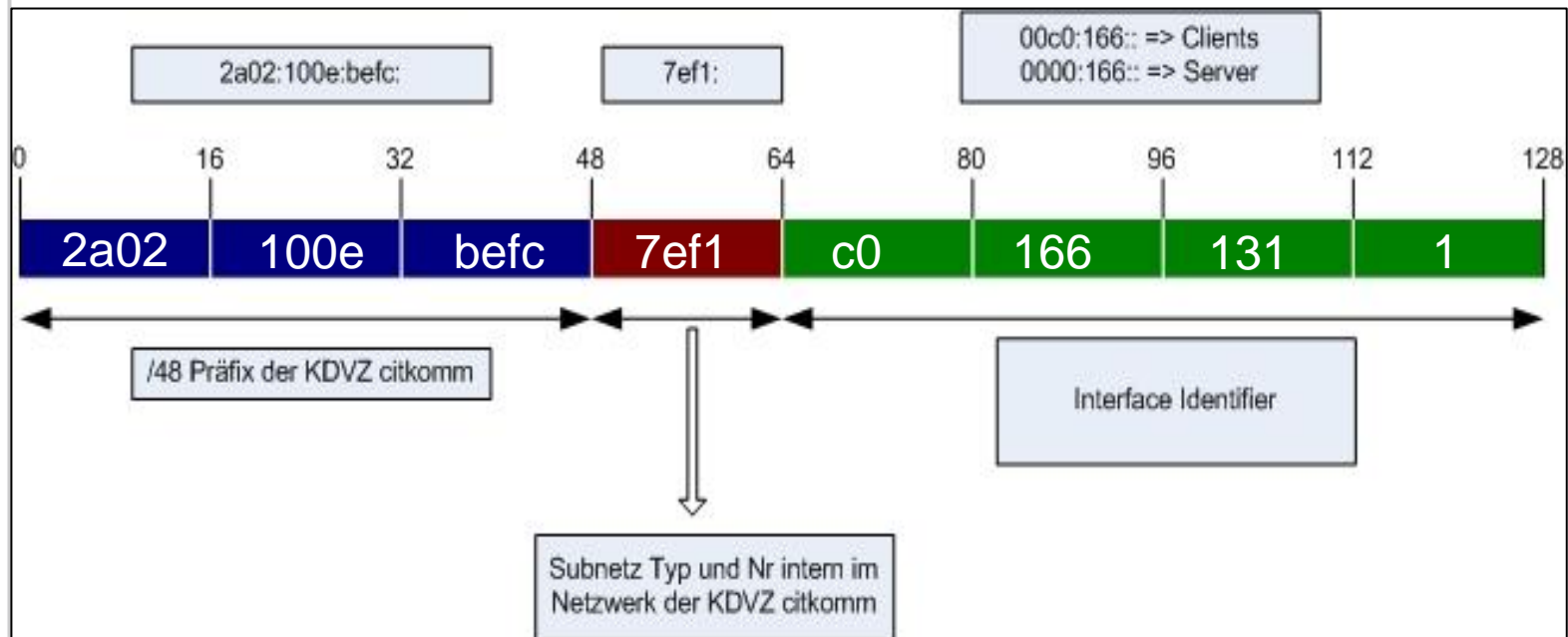
4. Byte IPv4

0	Data Centre 1	0	Infrastruktur/Transfer	Server	0000		Privater
1		1			0010		Address
2		2		Storage	0020		Bereich
3		3			0030		
4	Data Centre 2	4		Router	0040		
5		5			0050		
6		6			0060		
7		7			0070		
8	Shared	8	Backbone	Switches	0080		
9		9			0090		
a		a	Management		00a0		
b		b			00b0		
c	LAN Site 1	c	DMZ	Clients	00c0		
d		d		Printer	00d0		
e	KOM WAN	e	LAN	Phones	00e0		
f		f			00f0		

IPv6 ADRESSKONZEPT

> 10.192.166.131 /24

> 2a02:100e:befc:7ef1:c0:166:131:1 /64



- Ziel
 - Verteilung des IPv6-Präfixes in das Subnetz
 - Automatische Konfiguration der Clients
 - Bekanntgabe des default-IPv6-Gateway

- Funktion
 - Server und Clients senden Router Solicitations (RS)
 - radvd antwortet mit Router Advertisements (RA)
 - link-local-Adresse des Routers wird als Default-Gateway in Routing-Table eingetragen



- Damit die Windows Clients ihre reservierten IPv6-Adressen und die Nameserver-Adressen vom DHCP-Server bekommen, muss über das RA das Managedaddress-Flag und das Otherstateful-Flag aktiviert werden (Windows- wie Linux-Clients)
- Clients sollen keine IPv6-Adresse durch Stateless Address Autoconfiguration [SLAAC] beziehen
- Übersicht über alle Einstellungen, auch Standard-Werte, des radvd mit Hilfe von `radvddump` (Befehl wird mit dem Paket radvd ausgeliefert)
- Kann an dieser Stelle eingeschaltet werden, muss er aber nicht



- IPv6 auf den Servern kann eingeschaltet werden
- Grundsätzlichste Art eine Verbindung auf ihre IPv6-Tauglichkeit zu testen: ping6 an link-local-Adresse
- Server erhalten eine statische IPv6-Adresse
- Um sicher zu gehen, dass Windows Server (ab 2008) eine statische IPv6-Adresse besitzen, kann man über netsh-Befehle das IPv6-Interface beeinflussen



> netsh int ipv6 set int "LAN-Verbindung" ...

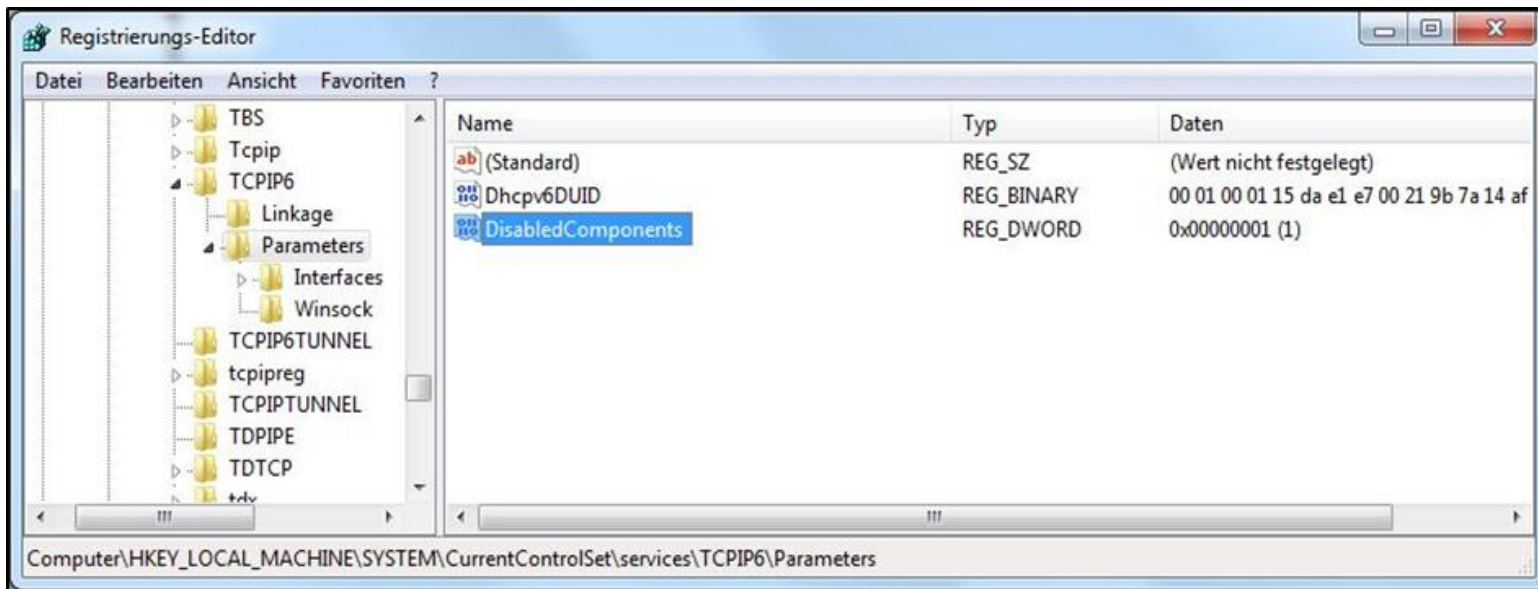
```
Administrator: cmd.exe
C:\Windows\system32>netsh int ipv6 sh int LAN-Verbindung

Parameter für die Schnittstelle LAN-Verbindung
...
Schnittstellen-LUID : ethernet_0
Schnittstellenindex : 10
Status : connected
metrik : 0
Verbindungs-MTU : 1500 Bytes
Erreichbare Zeit : 38500 ms
Erreichbare Basiszeit : 30000 ms
Intervall für die erneute Übertragung : 1000 ms
off-iles-prüfung : 1
Standortpräfixlänge : 64
Standort-ID : 1
Weiterleitung : disabled
Ankündigung : disabled
Nachbarermittlung : enabled
Nachbar-Nichterreichbarkeitserkennung : enabled
Routersuche : disabled
Verwaltete Adresskonfiguration : disabled
Andere statusbehaftete Konfiguration : disabled
Schwacher Host sendet : disabled
Schwacher Host empfängt : disabled
Automatische Metrik verwenden : enabled
Standardrouten ignorieren : disabled
Angekündigte Router gültigkeitsdauer : 1800 Sekunden
Standardroute ankündigen : disabled
Aktuelles Hoplimit : 0
AFFIX-Übertragungszwangsnetzwerk : disabled
Gerichtetes MAC-Reaktivierungsmuster : disabled
C:\Windows\system32>
```

> ... `routerdiscovery=disabled`
> ... werden keine Router Solicitations mehr vom Server gesendet, um einen Router zu finden. Die IPv6-Gateway-Adresse wird statisch eingegeben.
> ... `neighboraddress=disabled`
> ... kein DHCP-Server für die IPv6-Adressvergabe benutzt.
> ... `neighbordiscoverycapable=disabled`
> ... Anfragen an den DHCP-Server gesendet werden, um Metrijnformationen wie z.B. RDNSS (Recursive DNS Server) zu erhalten. Diese werden wenn bei Servern auch statisch eingegeben.



- Tunnelinterfaces deaktivieren
 - *reg add „HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters“ /v DisabledComponents /t REG_DWORD /d 0x01*
- Unterschiede zwischen Windows Server 2008 und 2012
 - für Windows Server 2012 sollten die Befehle über die Powershell eingegeben werden
 - zusätzliche, vom DHCP Server bezogene IPv6 Adresse auf Server 2012, obwohl eine statische IPv6-Adresse vergeben wurde und das M-Flag deaktiviert war
 - Mit Hilfe eines Powershell-Befehls die DHCPv6-Anfragen deaktivieren (Multicast)



- DHCP-Dienst
 - Stateful Address Autoconfiguration
 - Keine Gateway-Option mehr
 - Der DHCP-IPv6-Bereich wird allokiert durch Ausschließen anderer Bereiche
 - Client sendet v6-Anfrage an die Multicast-Adresse ff02::1:2
- IPv6-Reservierungen erfolgen über die für jeden Client eindeutigen Kennungen DUID und IAID
 - DUID: **D**HCP **U**nique **I**dentifier
 - IAID: **I**ntity **A**ssociation **I**dentifier
- Powershell-Skript zur Vereinfachung von DHCPv6-Reservierungen

- Anwendungsbeispiel
- Ausschluss der Bereiche
 - von `2a02:100e:befc:7ef1:0:0:0:1`
 - bis `2a02:100e:befc:7ef1:bfff:ffff:ffff:ffff`
 - und von `2a02:100e:befc:7ef1:c1:0:0:0`
bis `2a02:100e:befc:7ef1:ffff:ffff:ffff:ffff`
- Somit ist folgender IPv6-Bereich für die DHCP-Clients reserviert
 - von `2a02:100e:befc:7ef1:c0:0:0:0`
 - bis `2a02:100e:befc:7ef1:c0:ffff:ffff:ffff`



- Gruppenrichtlinien
 - GPO zum deaktivieren der Tunnelinterfaces
 - muss nachinstalliert werden
 - Powershell Remote Execution Policy ändern
 - Mindestens auf „RemoteSigned“



- Bei allen Windows Versionen (außer Server-Editionen) sind standardgemäß Privacy Extensions aktiviert, welche abgeschaltet wurden
- Unser Konzept der IPv6-Adressvergabe: stateful address autoconfiguration
- *netsh int ipv6 set privacy state=disabled*
- Jetzt darf auch auf den Clients das v6-Protokoll aktiviert werden
- Windows Systeme können ab der Installation, ohne einen zusätzlichen Dienst, RA's verteilen



- Abschalten Tunneladaptern wie Teredo, isatap oder 6to4 verhindert unerwünschten parasitären IPv6-Datenverkehr
 - Wird über die Gruppenrichtlinie gesteuert
- Internet mit Hilfe eines Reverse-Proxys
- Ganz am Ende:
 - RADVD einschalten
 - IPv6-Routing-Table wird mit /64-Präfix und dem default-gateway



- Als erstes ping6 zwischen den Servern und Clients
- Nach der Migration auf IPv6 ist einer der einfachsten und schnellsten Tests die Verbindung zum Mailserver
 - Zur Kontrolle wie sich der Client mit dem Mailserver verbindet einfach nur eine netstat-Ausgabe kontrollieren
- Verbindungen zu DB-Servern



- Vorgehen mit Hilfe des vom BVA veröffentlichten Migrationsleitfadens für die ÖV sehr stringent
- Einführung von IPv6 im LAN ist soweit schmerzfrei
- Grenze ist dabei der Gateway-Router
- Einfache Einführung von IPv6
- Läuft der IPv6-Traffic im LAN stabil, kann man den nächsten Schritt planen
 - IPv6-Uplink einrichten
 - forwarding aktivieren





FRAGEN?

Ihr Ansprechpartner:

Timo Baumgart

Citkomm

Abteilung ISysP

Baumgart@citkomm.de

www.citkomm.de