JÜLICH
FORSCHUNGSZENTRUM

IPv6 – Daheim und Unterwegs

8. Oktober 2013 | Werner Anrath

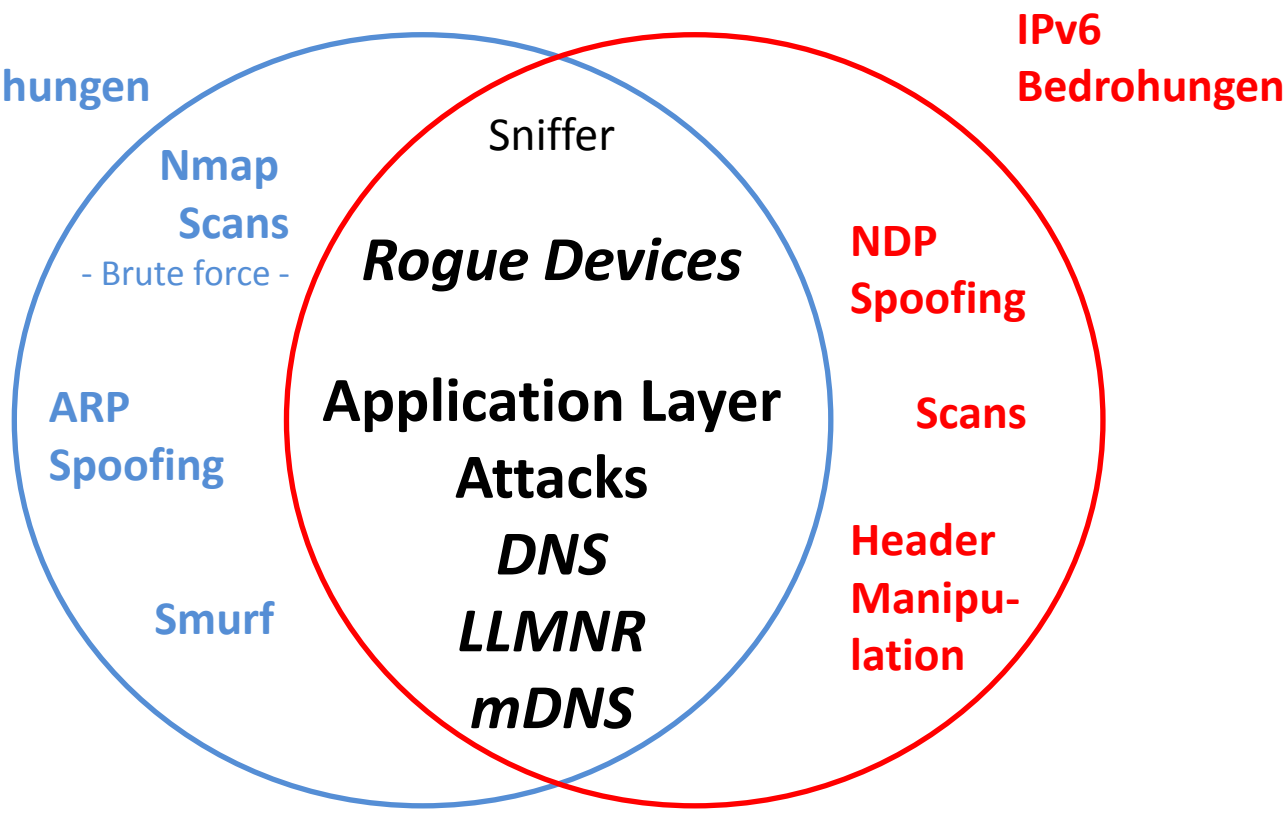
IPv6 - Merkmale

- Internet Protocol Version 6
  - früher auch Internet Protocol next Generation (IPnG) genannt
- IPv6 soll IPv4 ablösen
  - RFC 2460 ‚Internet Protocol, Version 6 (IPv6) Specification‘
- wesentliche Merkmale
  - Vergrößerung des Adressraums: 128 Bit Adressen
    - 2001:0db8:85a3:08d3:1319:8a2e:0370:7344
  - Vereinfachung des Protokollrahmens (Protocol Header)
    - feste Länge
    - Alignment
  - automatische Konfiguration von Host-Systemen
    - zustandslose Verfahren
      - Stateless Address Autoconfiguration
    - zustandsbehaftete Verfahren (z.B. DHCPv6)
  - Internet Protocol Security (IPsec)
  - Mobile IPv6

Inhalt

- **Motivation - Gefährdungen**
- **Grundlagen**
  - Implementierungen u. Adressen
- **IPv6 Interface Identifier**
- **Personal Firewall**
  - Trusted Networks vs. Untrusted Networks
  - ein Angriff
- **Transition Technologies (Problemfall automatische Tunnel)**
- **Netzwerkinfrastruktur – IPv6 First Hop Security**
  - Vorstellung
  - ein Angriff
- **Best Practice (Fazit)**

IPv6 - Gefährdungen



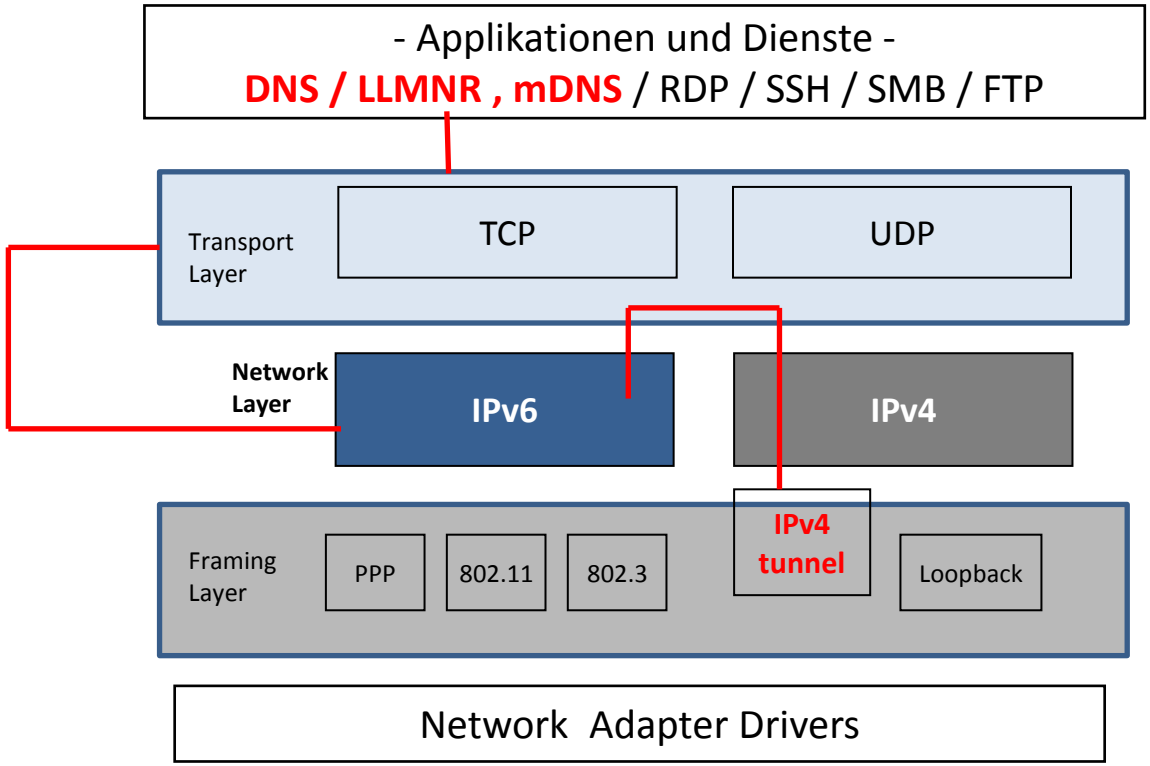
Nichts wirklich Neues – aber: auch reine IPv4-Netze sind zusätzlich gefährdet!

IPv6 – Dual Stack Hosts

IPv6 Features	Windows 7 Vista /2008 2008 R2 Windows 8 / 2012	Linux	Mac OS X
Installiert / Aktiv	ja / ja	ja / ja	ja / ja
GUI / CLI	ja / ja	ja / ja	ja / ja
Stateless Address Autoconfiguration	ja	ja	ja
Privacy Extensions	aktiv	optional	ab 10.7 aktiv
DNS	ja	ja	ja
RFC 3484	ja	ja	nein
DHCPv6 Client	ja	optional	ab 10.7
Link Local Multicast Name Resolution	LLMNR	mDNS	mDNS
Transition Technologies	aktiv	optional	optional
Stateful Inspection Firewall	aktiv	optional	optional

… mehr als 8000 Systeme

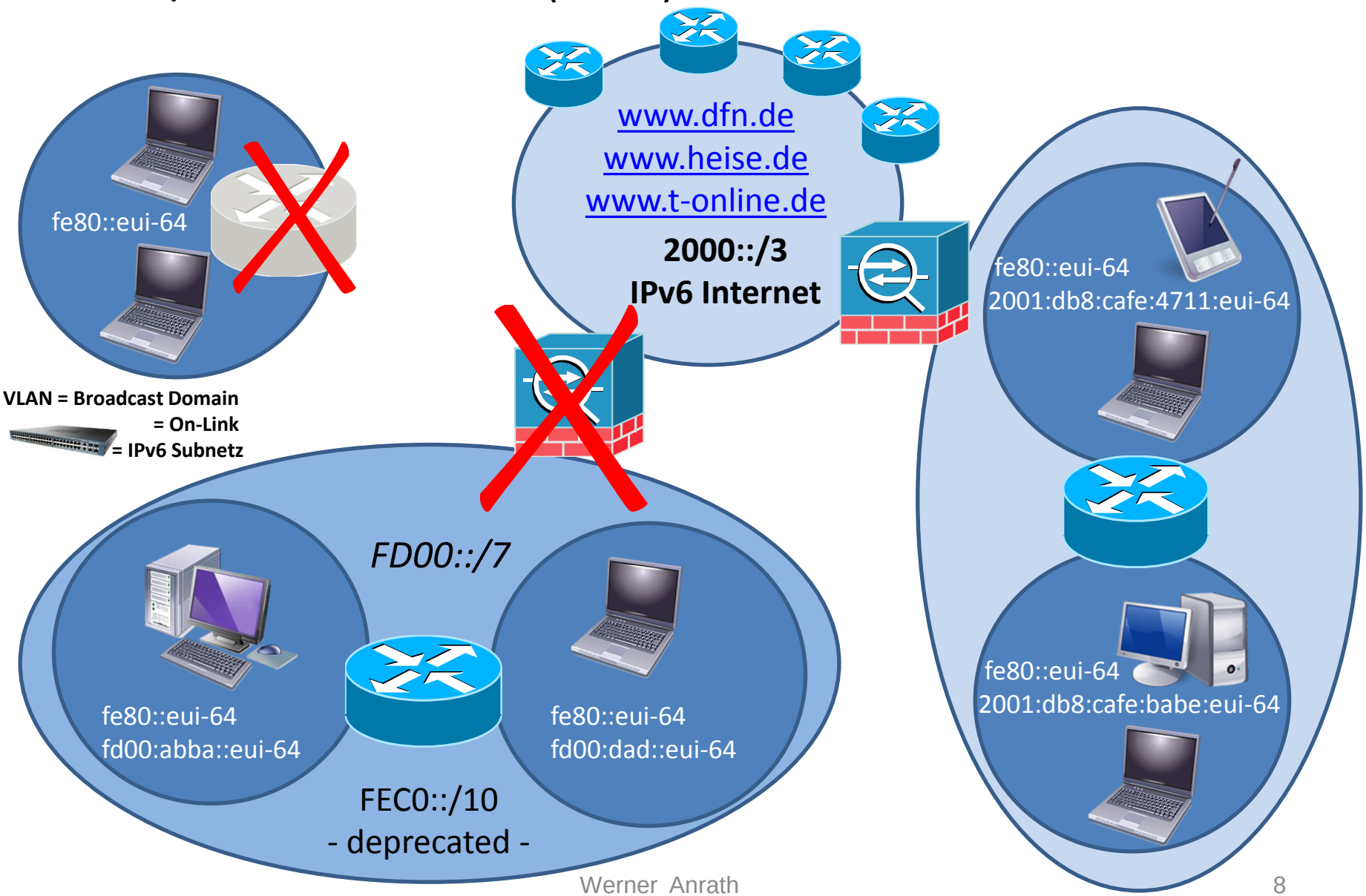
IPv6 - Dual Stack Hosts



Grundlagen – IPv6 Autokonfiguration (SLAAC)

- Link-Local Address (EUI-64 IID) generieren
- Neighbor Solicitation (NS) für Duplicate Address Detection (DAD) senden
- Autoconfiguration abbrechen, falls ein Neighbor Advertisement (NA) einen Adresskonflikt anzeigt
- Router Solicitation aussenden
- Falls kein Router Advertisement (RA) empfangen wird, starte DHCPv6
- Falls ein Router Advertisement (RA) empfangen wird:
  - generiere Adressen für die enthaltenen Prefixe; danach DAD
- M Flag == 1 im Router Advertisement (RA):
  - starte DHCPv6, um weitere Adressen und Parameter zu erhalten
- M Flag == 0 und O Flag == 1 im Router Advertisement (RA):
  - starte DHCPv6, um weitere Konfigurationsparameter zu erhalten (z.B DNS Parameter)

fe80::/10 Link Local Unicast Address
fd00::/7 Unique Local Address (Intranet)
2000::/3 Global Unicast Address (Internet)



Adressierung – EUI 64 Interface Identifier

Beispiel - IPv6 Address > 2001:0638:0404:a800:0215:77ff:fe76:74b9

Prefix Info > Global Unicast Address (RFC3587) - 2000::/3

Interface ID Info >
IEEE EUI-64 based Interface ID found (RFC4291)

Hardware Address (IEEE - 48 bit MAC)	00-15-77-76-74-b9
IPv6 Solicited-Node Multicast Address	ff02::1:ff76:74b9
Corresponding Ethernet Multicast Address	33-33-ff-76-74-b9

getaddrinfo Result > 2001:638:404:a800:215:77ff:fe76:74b9

Möglichen Muster – Modified EUI-64 IID:
::x**2**xx:xx**FF:FE**xx:xxxx
::x**6**xx:xx**FF:FE**xx:xxxx
::x**A**xx:xx**FF:FE**xx:xxxx
::x**E**xx:xx**FF:FE**xx:xxxx

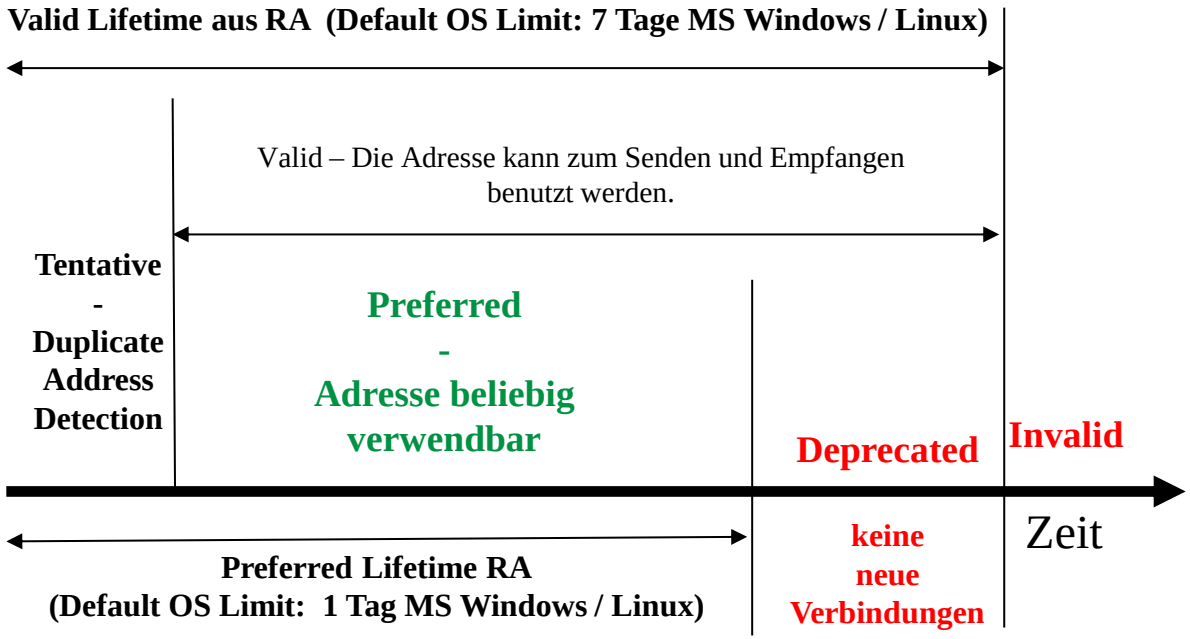
Adressierung – RFC 3041 Interface Identifier

Beispiel - IPv6 Address > 2001:0db8:4711:c800:08f1:343a:2610:b3b3

Prefix Info Global Unicast Address (RFC3587) - 2000::/3
Interface ID Info >
Locally administered Bit not set (U/L Bit)
Randomized Interface Identifier (RFC3041/RFC4941)

IPv6 Solicited-Node Multicast Address ff02::1:ff10:b3b3
Corresponding Ethernet Multicast Address 33-33-ff-10-b3-b3
getaddrinfo Result > 2001:db8:4711:c800:8f1:343a:2610:b3b3

Adressierung - Interface Identifier



RFC 4291 (ADDR-ARCH)
RFC 3041 / 4941 (Privacy Extensions)

Linux:
ip -6 addr show

Windows:
netsh interface show privacy
Netsh interface show address

Adressierung - Interface Identifier - BSI

Um diese globale Identifizierbarkeit zu vermeiden, unterstützen die meisten IPv6-Implementierungen sogenannte Privacy Extensions für die Adresskonfiguration. Dabei wird für das Interface in regelmäßigen Abständen eine neue Adresse aus dem jeweiligen Subnetz generiert und für neue Verbindungen verwendet. Auf diese Weise wird es einem Beobachter erschwert, ein Gerät weltweit allein anhand seiner IPv6-Adressen zu verfolgen. Der Nutzen der Privacy Extensions ist jedoch beschränkt, weil die Erstellung von Profilen anhand von Identifizierungsmerkmalen aus höheren Schichten (bspw. HTTP-Cookies) natürlich weiterhin möglich ist.

Im internen Netz erschwert die Nutzung von Privacy Extensions die Segmentierung des Netzes anhand von Paketfilterregeln, denn ein Whitelisting von zugelassenen IP-Adressen an Paketfiltern oder in Anwendungen ist auf diese Weise nicht möglich. Soll ein Teilnetz durch eine IP-Whitelist an einem Paketfilter geschützt werden, so müssen die Privacy Extensions deaktiviert werden oder es muss ein anderer Mechanismus für die Adresskonfiguration gewählt werden.

Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_lana_leitfaden_IPv6_pdf

Gefährdung durch Rogue Router Advertisements

Multicast Router Solicitation

Ethernet Header
- Destination MAC is 33-33-00-00-00-02

IPv6 Header
- Source Address is FE80::*Interface-Identifier*
- **Destination Address is FF02::2**
- Hop limit is 255

Router Solicitation Header

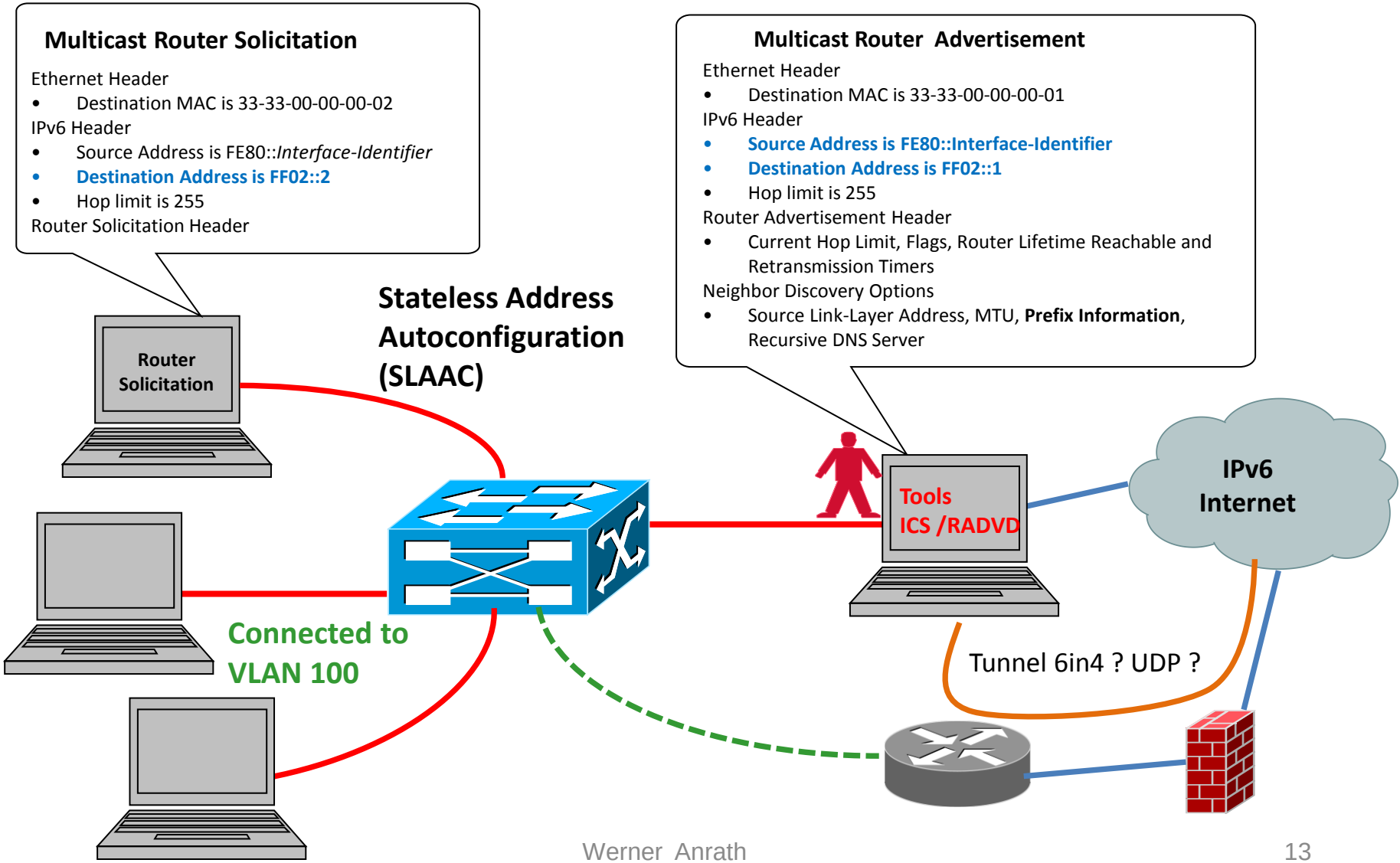
Multicast Router Advertisement

Ethernet Header
- Destination MAC is 33-33-00-00-00-01

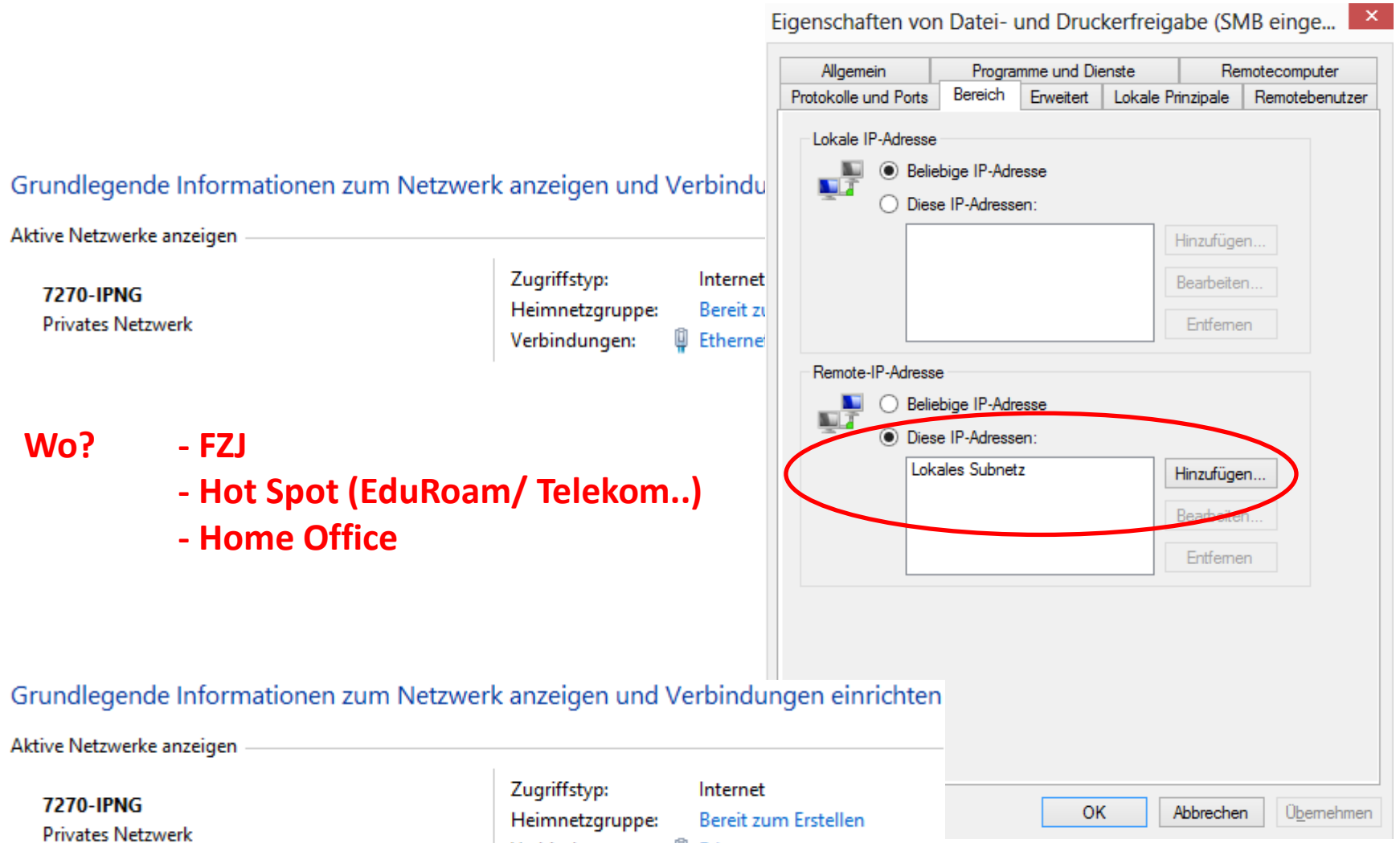
IPv6 Header
- **Source Address is FE80::Interface-Identifier**
- **Destination Address is FF02::1**
- Hop limit is 255

Router Advertisement Header
- Current Hop Limit, Flags, Router Lifetime Reachable and Retransmission Timers

Neighbor Discovery Options
- Source Link-Layer Address, MTU, **Prefix Information**, Recursive DNS Server

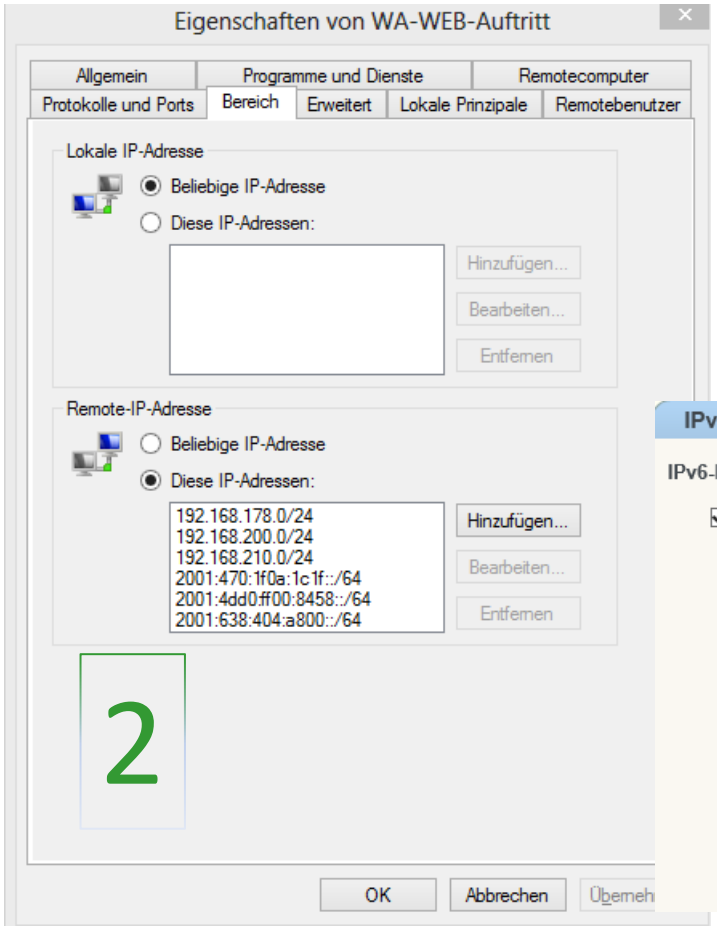


Personal Firewall – MS Windows



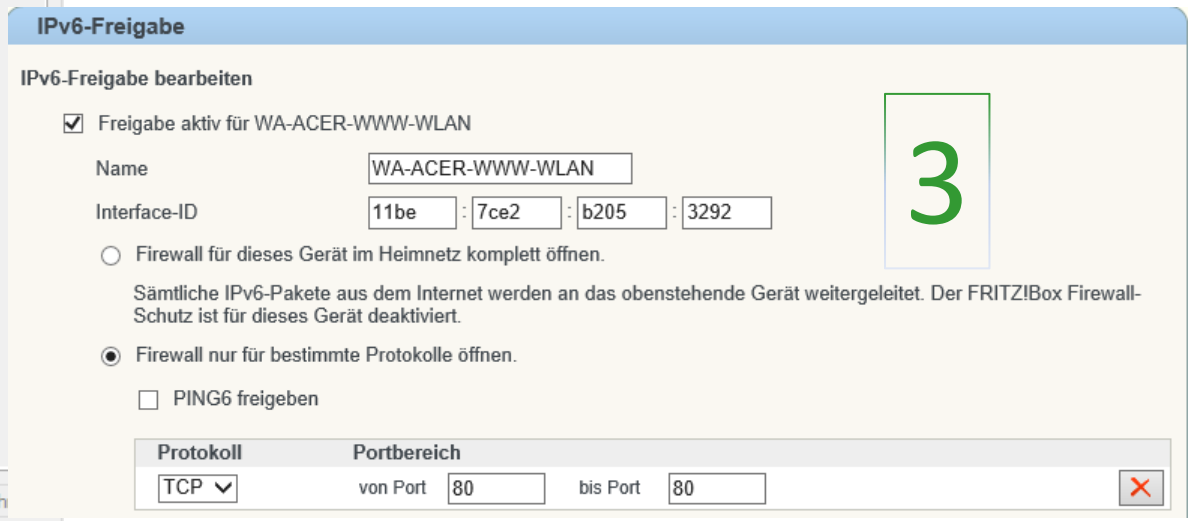
Wo? **- FZJ**
- Hot Spot (EduRoam/ Telekom..)
- Home Office

Personal Firewall – IIS Server Beispiel




```
C:\Windows\system32>netsh int  ipv6 15 show address
Der folgende Befehl wurde nicht gefunden: int ipv6 15 show address.

C:\Windows\system32>netsh int  ipv6  show address

Schnittstelle 1: Loopback Pseudo-Interface 1

Adresstyp  DAD-Status  Gültigkeit Bevorzugt Adresse
---------  ----------  ---------- ---------- ------------------------
Andere     Bevorzugt     infinite   infinite ::1

Schnittstelle 15: WiFi

Adresstyp  DAD-Status  Gültigkeit Bevorzugt Adresse
---------  ----------  ---------- ---------- ------------------------
öffentlich Bevorzugt      1h58m5s      58m5s 2001:470:1f0a:1c1f:11be:7ce2:b205:3292
Temporär   Bevorzugt      1h58m5s      58m5s 2001:470:1f0a:1c1f:780d:515:31c3:9fa6
Andere     Bevorzugt     infinite   infinite fe80::11be:7ce2:b205:3292%15
```

1




```
C:\>
C:\>netstat -an | findstr :80 | findstr ABH
  TCP    0.0.0.0:80             0.0.0.0:0              ABHöREN
  TCP    [::]:80                [::]:0                 ABHöREN
```

4

```
C:\Windows\system32>nslookup www.wa-ontour.de
Server:  fritz.box
Address:  192.168.178.1

Nicht autorisierende Antwort:
Name:    wa-ontour.de
Address:  2001:470:1f0a:1c1f:11be:7ce2:b205:3292
Aliases:  www.wa-ontour.de
```

5

Personal Firewall – SSH und Link-Local-Addrs

LINUX SYSLOG Einträge

Nov 6 12:43:31 linux-hsrk sshd[9811]: Accepted keyboard-interactive/pam for root from fe80::9c6b:6db2:331a:133c%eth0 port 50699 ssh2

Nov 6 12:45:57 linux-hsrk sshd[9972]: Accepted keyboard-interactive/pam for root from fe80::9c6b:6db2:331a:133c%eth0 port 50700 ssh2

Nov 9 16:29:29 linux-hsrk sshd[12866]: Accepted keyboard-interactive/pam for root from fe80::221:6aff:fe0d:8cbe%eth0 port 49260 ssh2

Personal Firewall – Dokumentation

Jülich Supercomputing Centre
52425 Jülich, ☎ (02461) 61-6402

Beratung und Betrieb, ☎ (02461) 61-6400

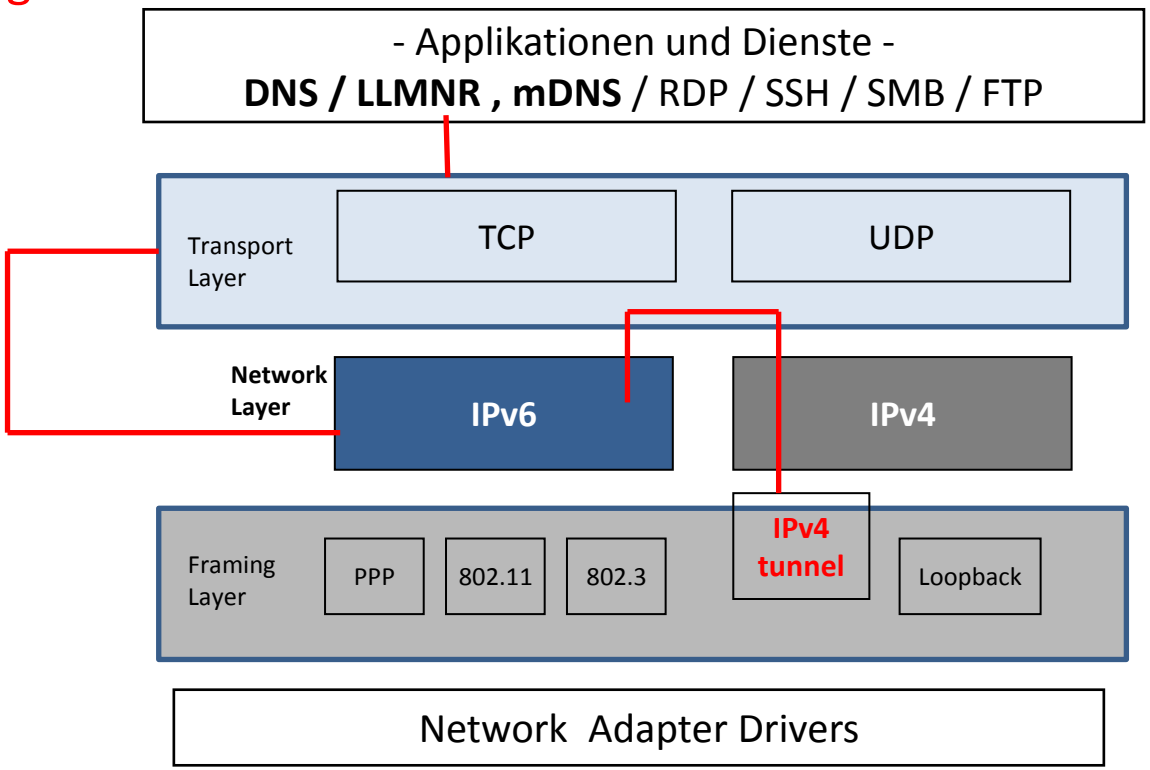
Technische Kurzinformation

FZJ-JSC-TKI-0402
E. Grünter, W. Anrath, S. Werner
04/09/2013

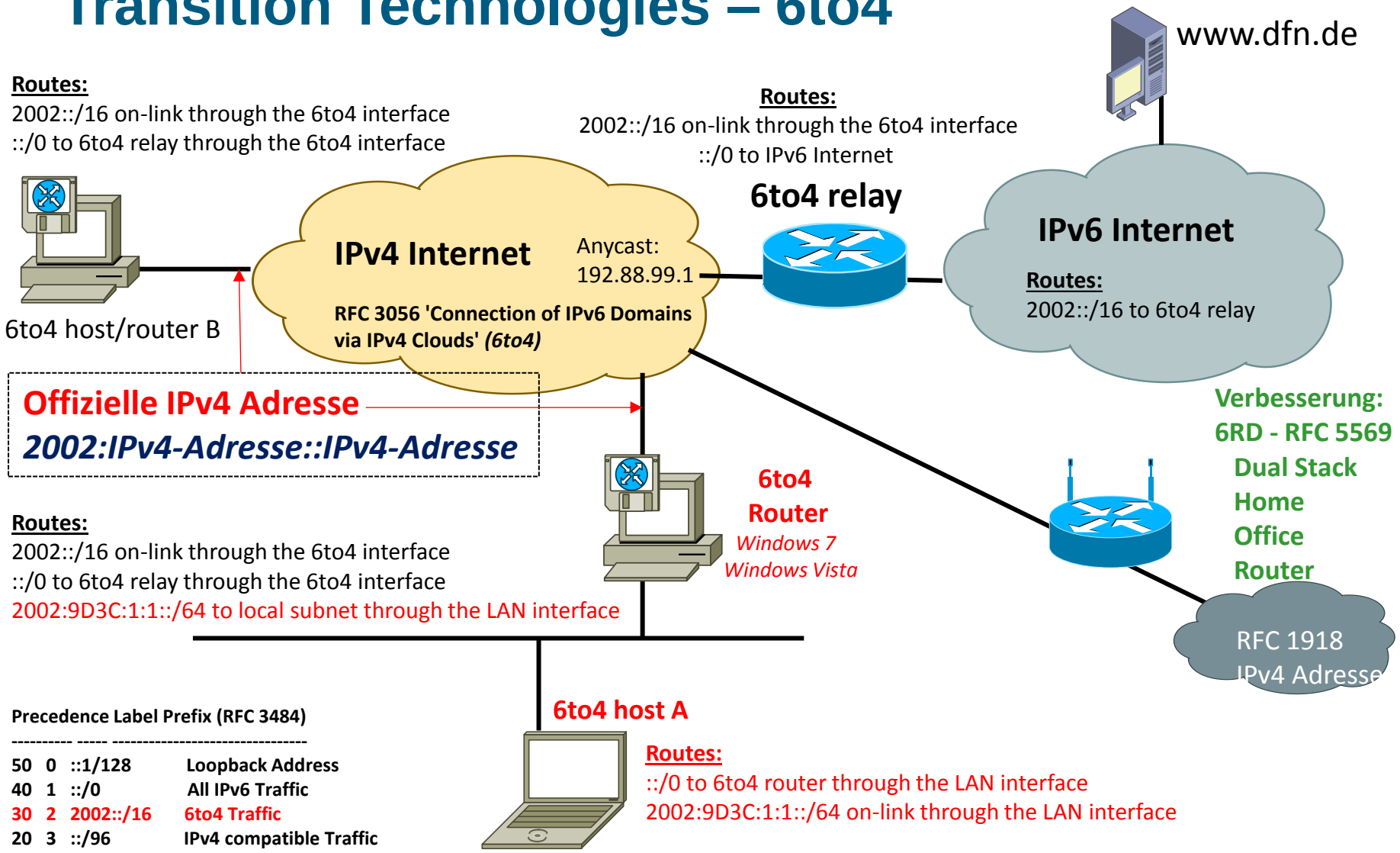
Linux Personal Firewall mit iptables und ip6tables

Transition Technologies

- nutzen die etablierte IPv4-Infrastruktur
- Domain Name System (DNS) Infrastruktur wird genutzt
- IPv6 over IPv4 tunneling
- Protocol 41



Transition Technologies – 6to4

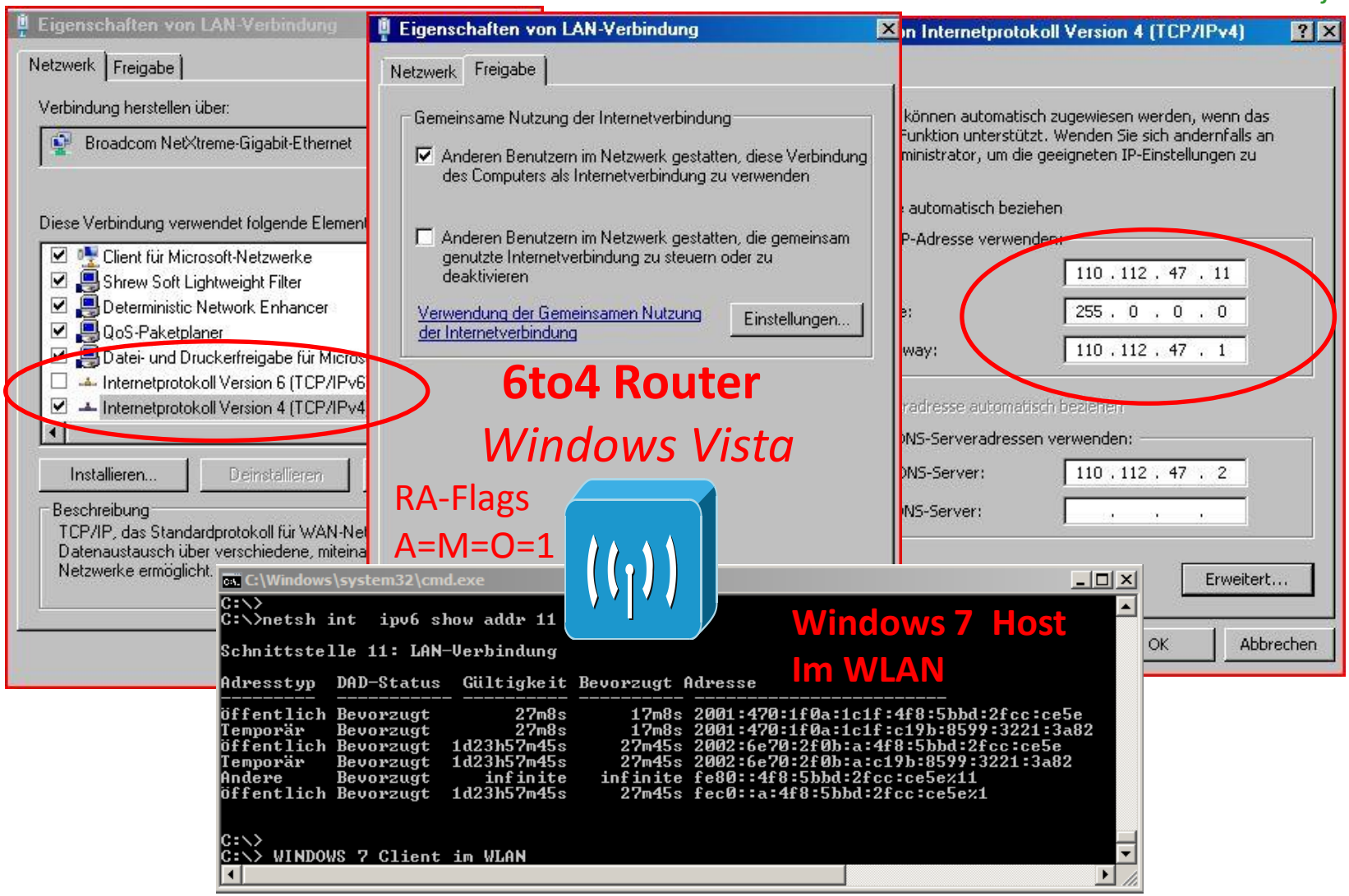


Precedence Label Prefix (RFC 3484)

50	0	::1/128	Loopback Address
40	1	::/0	All IPv6 Traffic
30	2	2002::/16	6to4 Traffic
20	3	::/96	IPv4 compatible Traffic
10	4	::ffff:0:0/96	IPv4 mapped Traffic
5	5	2001::/32	Teredo

Transition Technologies – 6to4

Status: Netzwerkkabel wurde entfernt

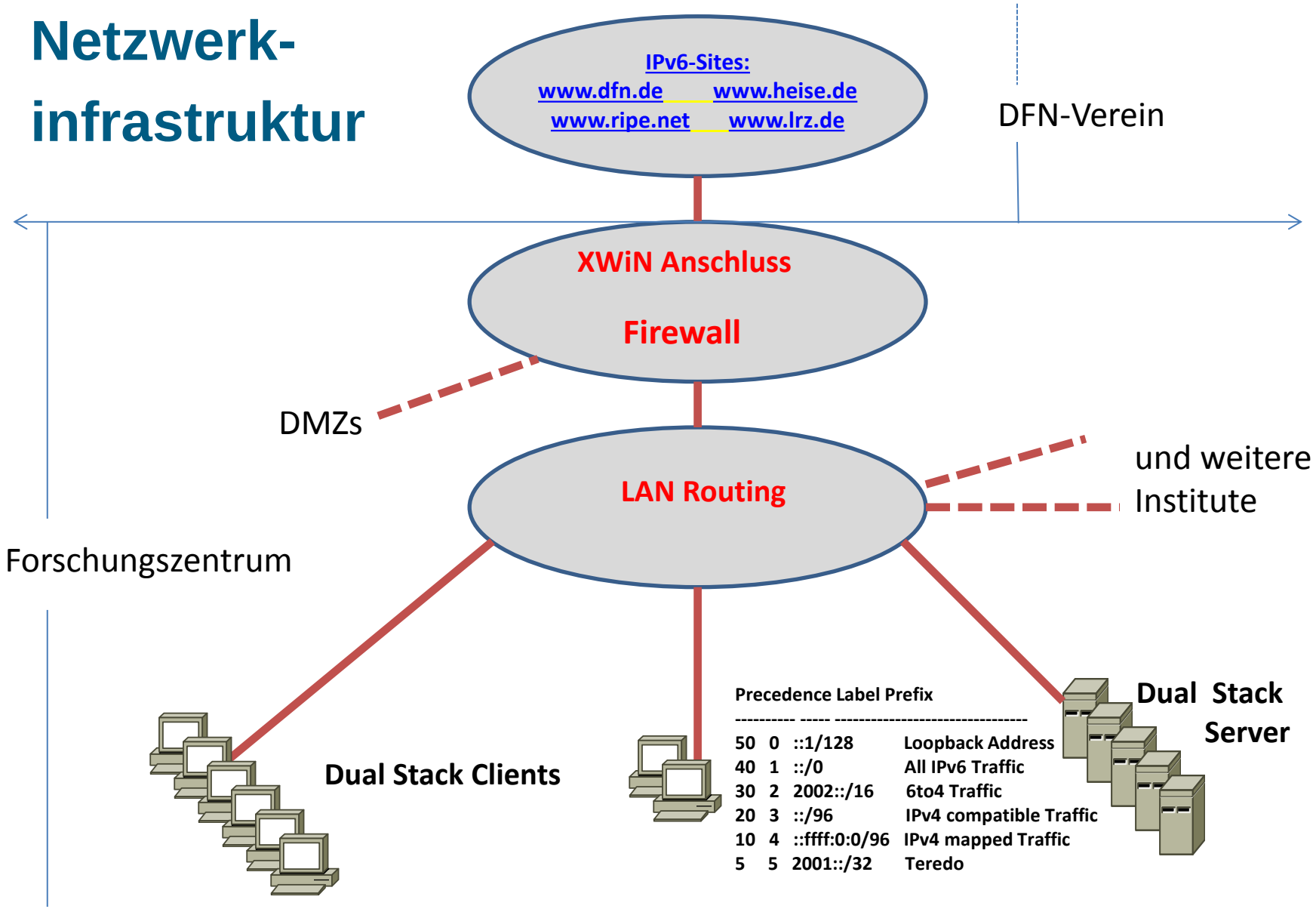


Transition Technologies - BSI

Neben „festen“ Tunneln zu Netzbetreibern, mit denen eine entsprechende Vertragsbeziehung etabliert wird, gibt es verschiedene automatische Techniken wie 6to4, Teredo oder ISATAP. Diese automatischen Tunneltechniken sind aus Sicherheitssicht allesamt kritisch und für den produktiven Einsatz nicht geeignet. Insbesondere in Netzwerken mit Windows-Clients ist es wichtig, darauf zu achten, dass Clients nicht von sich aus Tunnel aufbauen und auf diese Weise möglicherweise das Sicherheits-Gateway umgehen.

Quelle: isi_lana_leitfaden_IPv6_pdf

Netzwerk-infrastruktur



Netzwerkinfrastruktur – First Hop Security

- IPv6 Snooping
  - NDP Inspection / DHCP Guard – Rolle Client / Ra-Guard – Rolle HOST
- RA-Guard
- DHCP-Guard
- NDP Inspection
  - subset of IPv6 Snooping
- IPv6 Destination Guard
  - prevent the build up of outstanding neighbor discovery resolutions
- IPv6 Source/Prefix Guard
  - drop data packets where the IPv6 SA is not in the binding table
  - prefix guard – block IPv6 SA outside any known prefix
- RA Throttler (WIFI) / ND Multicast Suppress

Netzwerkinfrastruktur – First Hop Security

Attack: send malicous Neighbor Advertisement with illegal mapping –> poison Neighbor Cache

Attacker blocked!

00:0c:29:6f:d6:41

Default Router Addr fe80:: be05:43ff:fe34:35da
Victim Link Local Addr fe80::226:2dff:fe50:380b
Malicious HW Address: 00:0c:29:6f:d6:41

1.) send malicious NA

SAVI Protection Perimeter

5.) Trusted-Port:
NA recv
delete BT Entry

2.) create new BT Entry
3.) Situation?
DAD-NS Target IP Addr > fe80::be05:43ff:fe34:35da

Trusted Ports /
device-role switch

Non-SAVI-capable Switch

fe80::be05:43ff:fe34:35da

4.) Response:
send NA -> ff02::1

fe80::226:2dff:fe50:380b

Validating Ports on SAVI Devices

SAVI Protection Perimeter

JÜLICH
FORSCHUNGSZENTRUM

Netzwerkinfrastruktur – First Hop Security

Attack: send malicous Neighbor Advertisement with illegal mapping –> poison Neighbor Cache

fe80::be05:43ff:fe34:35da	fe80::226:2dff:fe50:380b	ICMPv6	86 Neighbor Advertisement fe80::be05:43ff:fe34:35da (none) is at 00:0c:29:6f:d6:41
fe80::be05:43ff:fe34:35da	ff02::1	ICMPv6	86 Neighbor Advertisement fe80::be05:43ff:fe34:35da (rtr, ovr) is at bc:05:43:34:35:da
fe80::be05:43ff:fe34:35da	fe80::226:2dff:fe50:380b	ICMPv6	86 Neighbor Advertisement fe80::be05:43ff:fe34:35da (ovr) is at 00:0c:29:6f:d6:41
fe80::be05:43ff:fe34:35da	fe80::226:2dff:fe50:380b	ICMPv6	86 Neighbor Advertisement fe80::be05:43ff:fe34:35da (none) is at 00:0c:29:6f:d6:41
fe80::be05:43ff:fe34:35da	ff02::1	ICMPv6	86 Neighbor Advertisement fe80::be05:43ff:fe34:35da (rtr, ovr) is at bc:05:43:34:35:da
fe80::be05:43ff:fe34:35da	fe80::226:2dff:fe50:380b	ICMPv6	86 Neighbor Advertisement fe80::be05:43ff:fe34:35da (ovr) is at 00:0c:29:6f:d6:41
fe80::be05:43ff:fe34:35da	fe80::226:2dff:fe50:380b	ICMPv6	86 Neighbor Advertisement fe80::be05:43ff:fe34:35da (none) is at 00:0c:29:6f:d6:41
fe80::be05:43ff:fe34:35da	ff02::1	ICMPv6	86 Neighbor Advertisement fe80::be05:43ff:fe34:35da (rtr, ovr) is at bc:05:43:34:35:da

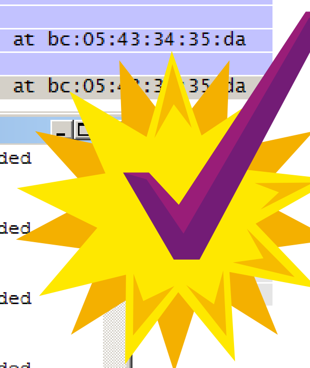
Untrusted Zone - SAVI Switch - Traffic send to Validating Port

Trusted Zone - SAVI Switch - Traffic recv from Trusted Port

No.	Time	Source	Destination	Info
1	17:59:31.396111	::	ff02::1:ff34:35da	Neighbor Solicitation for fe80::be05:43ff:fe34:35da
2	17:59:31.396480	fe80::be05:43ff:fe34:35da	ff02::1	Neighbor Advertisement fe80::be05:43ff:fe34:35da (rtr, ovr) is at bc:05:43:34:35:da
3	17:59:36.410942	::	ff02::1:ff34:35da	Neighbor Solicitation for fe80::be05:43ff:fe34:35da
4	17:59:36.411419	fe80::be05:43ff:fe34:35da	ff02::1	Neighbor Advertisement fe80::be05:43ff:fe34:35da (rtr, ovr) is at bc:05:43:34:35:da
5	17:59:41.426152	::	ff02::1:ff34:35da	Neighbor Solicitation for fe80::be05:43ff:fe34:35da
6	17:59:41.426499	fe80::be05:43ff:fe34:35da	ff02::1	Neighbor Advertisement fe80::be05:43ff:fe34:35da (rtr, ovr) is at bc:05:43:34:35:da
7	17:59:46.448188	::	ff02::1:ff34:35da	Neighbor Solicitation for fe80::be05:43ff:fe34:35da
8	17:59:46.448508	fe80::be05:43ff:fe34:35da	ff02::1	Neighbor Advertisement fe80::be05:43ff:fe34:35da (rtr, ovr) is at bc:05:43:34:35:da
9	17:59:51.459045	::	ff02::1:ff34:35da	Neighbor Solicitation for fe80::be05:43ff:fe34:35da
10	17:59:51.459361	fe80::be05:43ff:fe34:35da	ff02::1	Neighbor Advertisement fe80::be05:43ff:fe34:35da (rtr, ovr) is at bc:05:4[illegible]da

```
%SISF-4-PAK_DROP: Message dropped A=FE80::BE05:43FF:FE34:35DA G=- V=100 I=Gi1/0/13 P=NDP::NA Reason=Packet accepted but not forwarded
%SISF-6-ENTRY_CREATED: Entry created A=FE80::BE05:43FF:FE34:35DA V=100 I=Gi1/0/13 P=0005 M=000C.296F.D641
%SISF-6-ENTRY_DELETED: Entry deleted A=FE80::BE05:43FF:FE34:35DA V=100 I=Gi1/0/13 P=0005 M=000C.296F.D641
%SISF-4-PAK_DROP: Message dropped A=FE80::BE05:43FF:FE34:35DA G=- V=100 I=Gi1/0/13 P=NDP::NA Reason=Packet accepted but not forwarded
%SISF-6-ENTRY_CREATED: Entry created A=FE80::BE05:43FF:FE34:35DA V=100 I=Gi1/0/13 P=0005 M=000C.296F.D641
%SISF-6-ENTRY_DELETED: Entry deleted A=FE80::BE05:43FF:FE34:35DA V=100 I=Gi1/0/13 P=0005 M=000C.296F.D641
%SISF-4-PAK_DROP: Message dropped A=FE80::BE05:43FF:FE34:35DA G=- V=100 I=Gi1/0/13 P=NDP::NA Reason=Packet accepted but not forwarded
%SISF-6-ENTRY_CREATED: Entry created A=FE80::BE05:43FF:FE34:35DA V=100 I=Gi1/0/13 P=0005 M=000C.296F.D641
%SISF-6-ENTRY_DELETED: Entry deleted A=FE80::BE05:43FF:FE34:35DA V=100 I=Gi1/0/13 P=0005 M=000C.296F.D641
%SISF-4-PAK_DROP: Message dropped A=FE80::BE05:43FF:FE34:35DA G=- V=100 I=Gi1/0/13 P=NDP::NA Reason=Packet accepted but not forwarded
%SISF-6-ENTRY_CREATED: Entry created A=FE80::BE05:43FF:FE34:35DA V=100 I=Gi1/0/13 P=0005 M=000C.296F.D641
%SISF-6-ENTRY_DELETED: Entry deleted A=FE80::BE05:43FF:FE34:35DA V=100 I=Gi1/0/13 P=0005 M=000C.296F.D641
```

BT Logging Events



Netzwerkinfrastruktur – First Hop Security

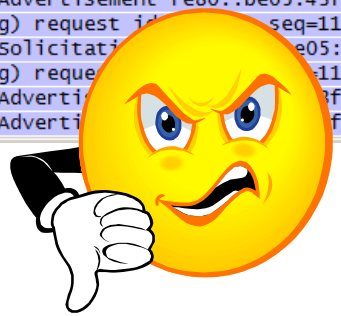
Victim Link Local Addr

Default Router Link Local Addr

Attack: send malicous Neighbor Advertisement with illegal mapping –> poison Neighbor Cache

Attacker‘s HW-Address is …:d6:41

31	fe80::226:2dff:fe50:380b	fe80::be05:43ff:fe34:35da	Echo (ping) request id=0x0001, seq=1190
32	fe80::be05:43ff:fe34:35da	fe80::226:2dff:fe50:380b	Echo (ping) reply id=0x0001, seq=1190
33	fe80::226:2dff:fe50:380b	fe80::be05:43ff:fe34:35da	Echo (ping) request id=0x0001, seq=1191
34	fe80::be05:43ff:fe34:35da	fe80::226:2dff:fe50:380b	Echo (ping) reply id=0x0001, seq=1191
35	fe80::20c:29ff:fe6f:d641	ff02::1:ff50:380b	Neighbor Solicitation for fe80::226:2dff:fe50:380b from 00:0c:29:6f:d6:41
36	fe80::226:2dff:fe50:380b	ff02::1:ff6f:d641	Neighbor Solicitation for fe80::20c:29ff:fe6f:d641 from 00:26:2d:50:38:0b
37	fe80::20c:29ff:fe6f:d641	fe80::226:2dff:fe50:380b	Neighbor Advertisement fe80::20c:29ff:fe6f:d641 (sol, ovr) is at 00:0c:29:6f:d6:41
38	fe80::226:2dff:fe50:380b	fe80::20c:29ff:fe6f:d641	Neighbor Advertisement fe80::226:2dff:fe50:380b (sol, ovr) is at 00:26:2d:50:38:0b
39	fe80::be05:43ff:fe34:35da	fe80::226:2dff:fe50:380b	Neighbor Advertisement fe80::be05:43ff:fe34:35da (ovr) is at 00:0c:29:6f:d6:41
40	fe80::be05:43ff:fe34:35da	fe80::226:2dff:fe50:380b	Neighbor Advertisement fe80::be05:43ff:fe34:35da (none) is at 00:0c:29:6f:d6:41
41	fe80::226:2dff:fe50:380b	fe80::be05:43ff:fe34:35da	Echo (ping) request id=0x0001, seq=1192
42	fe80::226:2dff:fe50:380b	fe80::be05:43ff:fe34:35da	Neighbor Solicitation for fe80::be05:43ff:fe34:35da from 00:26:2d:50:38:0b
43	fe80::226:2dff:fe50:380b	fe80::be05:43ff:fe34:35da	Echo (ping) request id=0x0001, seq=1193
44	fe80::be05:43ff:fe34:35da	fe80::226:2dff:fe50:380b	Neighbor Advertisement fe80::be05:43ff:fe34:35da (ovr) is at 00:0c:29:6f:d6:41
45	fe80::be05:43ff:fe34:35da	fe80::226:2dff:fe50:380b	Neighbor Advertisement fe80::be05:43ff:fe34:35da (none) is at 00:0c:29:6f:d6:41



```
Antwort von fe80::be05:43ff:fe34:35da: Zeit<1ms
Antwort von fe80::be05:43ff:fe34:35da: Zeit<1ms
Antwort von fe80::be05:43ff:fe34:35da: Zeit<1ms
Antwort von fe80::be05:43ff:fe34:35da: Zeit<1ms
Antwort von fe80::be05:43ff:fe34:35da: Zeit<1ms
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

Ping-Statistik für fe80::be05:43ff:fe34:35da:
    Pakete: Gesendet = 320, Empfangen = 317, Verloren = 3
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 9ms, Mittelwert = 0ms
STRG-C
^C
```

Unprotected Network
NO IPv6 SNOOPING Policy -

Victim‘s Neighbor Cache -> illegal mapping (Attacker‘s HW-Address) -> ping failures!
(Race Condition: Malicious NA, NUD / …:35:da is the default router)

JuNet – Best Pratice

- VLAN Konsolidierung – in einem VLAN nur ein IP-Subnetz
  - sehr wichtig für alle OEs (Altlast VLAN-11) – nicht nur wegen IPv6
  - **konsolidiert: JSC , ITS, IBG, INM-6, ICS-6, PTJ, INM, IEK-8, IEK-4, *IBG-2, IBG-3, S, ZEA-2***
- Tunnel deaktivieren, Privacy Extensions deaktivieren (JuNet)
- Personal Firewall prüfen
  - Profile für LAN / WLAN auf Einsatzzweck abstimmen
  - Linux: iptables / ip6tables (JSC TKI-0402)
- voll qualifizierte Hostnamen verwenden (FQDNs) / offizielle Adressen
- IPv6 kann am lokalen **Ethernet** aktiv bleiben
  - IPv6 Ready für künftige Anforderungen
  - Ausnahme: VLAN-11 – IPv6 LAN Konnektivität abschalten (Server!)
- JSC ‚IPv6 Schulung für SysAdmins' besuchen / JSC TKIs 412 u. 413 beachten