Discovering IPv6 with Wireshark

June 14, 2011

Rolf Leutert
Network Consultant & Trainer | Leutert NetServices | Switzerland

SHARKFEST '11
Stanford University
June 13-16, 2011

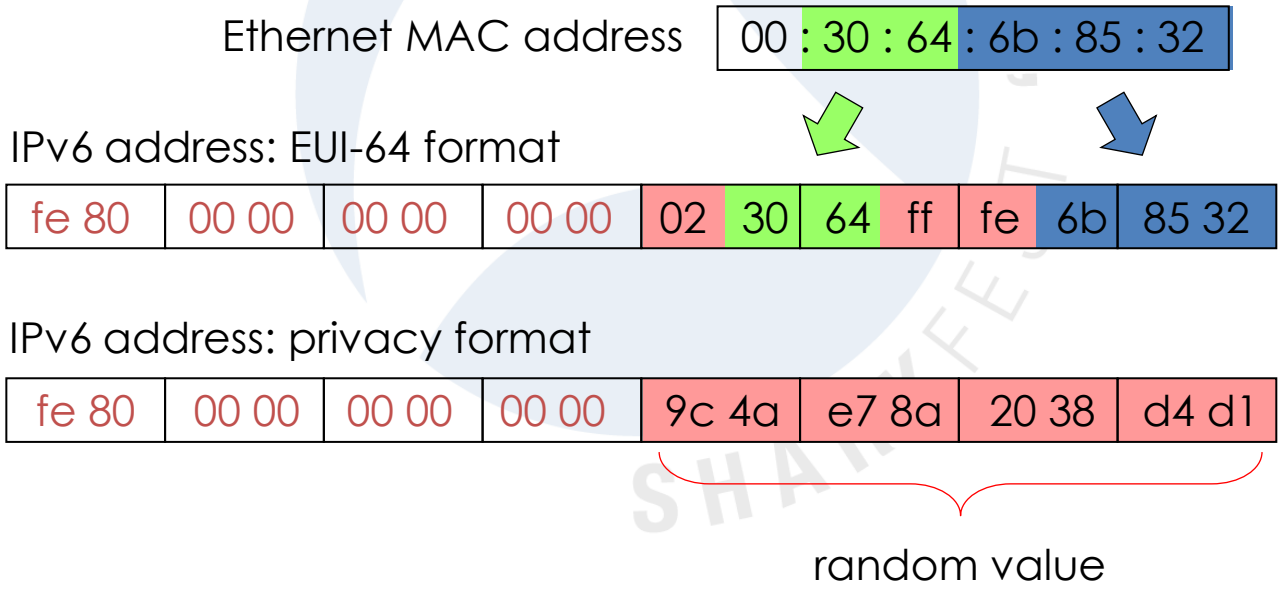
Agenda

- Address Autoconfiguration
- Neighbor discovery, Router discovery
- Host configuration with DHCPv6
- Transition technologies, ISATAP & Teredo Tunnel

Address Autoconfiguration

IPv6 Stateless Address Autoconfiguration (SLAAC)

- An IPv6 host will autoconfigure a link-local address for each interface
- Prefix for link-local address is fe80::/64
- Interface ID is either derived from MAC address or a random value

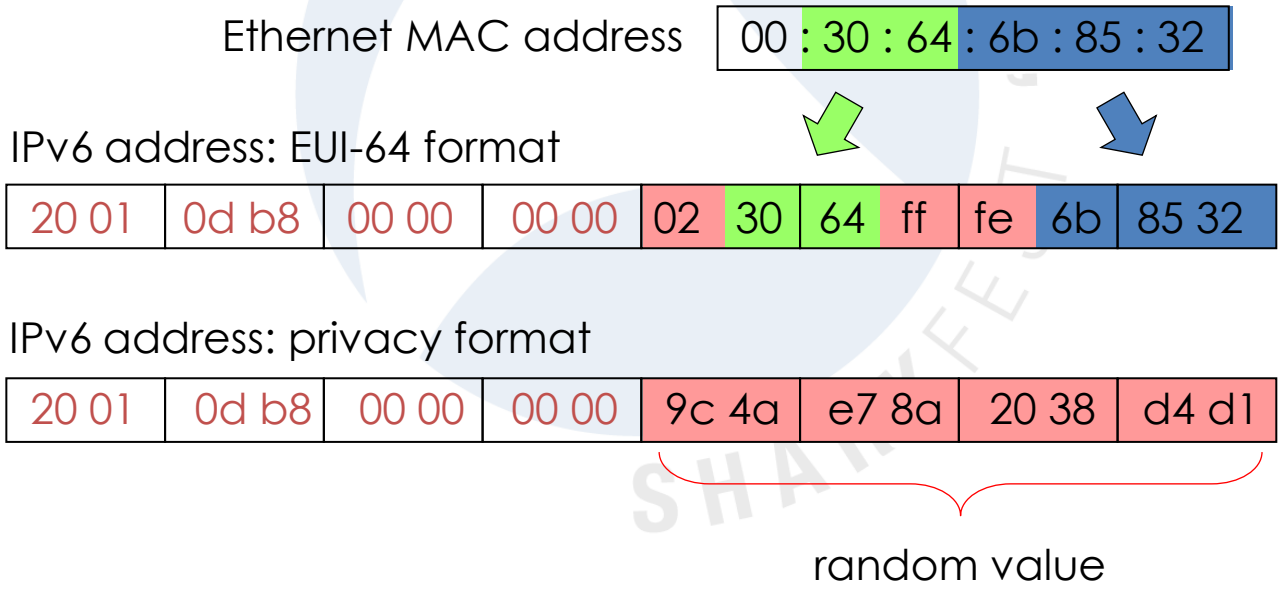


+

Address Autoconfiguration

IPv6 Stateless Address Autoconfiguration (SLAAC)

- If a router is present, host will also autoconfigure global address
- Prefix will be obtained from router, example 2001:db8::/64
- Interface ID is either derived from MAC address or a random value
- Router indicates in advertisement if stateful configuration may be used

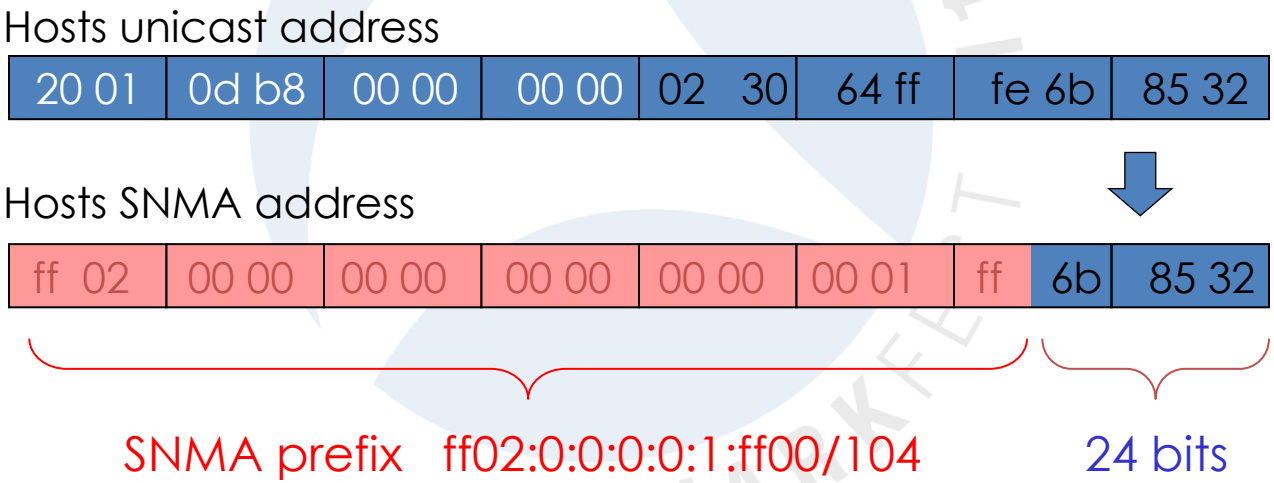


+

Address Autoconfiguration

Solicited Node Multicast Address (SNMA)

- Probably the most strange part of IPv6 addressing
- An IPv6 host forms a SNMA for each own unicast address in use
- The SNMA address is used for Neighbor Discovery (replacement of ARP)
- The SNMA address is derived from each unicast address in use

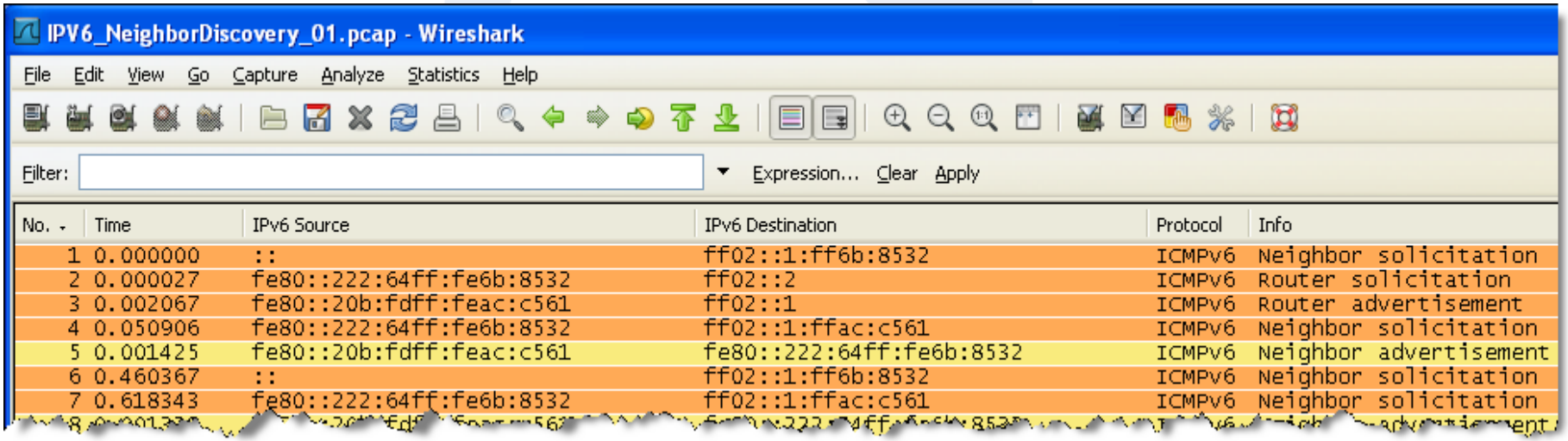


SNMA derived from unicast address: ff02::1:ff6b:8532

Duplicate Address Detection (DAD)

The initial client startup process includes the following steps:

Frame #	
1	Duplicate Address Detection after Link-Local autoconfiguration
2	Router Discovery
3	Router Advertisement and global address autoconfiguration
4	Neighbor Discovery (searching for Router MAC)
5	Neighbor Advertisement (reply from Router with MAC)
6	Duplicate Address Detection with acquired global address



No.	Time	IPv6 Source	IPv6 Destination	Protocol	Info
1	0.000000	::	ff02::1:ff6b:8532	ICMPv6	Neighbor solicitation
2	0.000027	fe80::222:64ff:fe6b:8532	ff02::2	ICMPv6	Router solicitation
3	0.002067	fe80::20b:fdff:feac:c561	ff02::1	ICMPv6	Router advertisement
4	0.050906	fe80::222:64ff:fe6b:8532	ff02::1:ffac:c561	ICMPv6	Neighbor solicitation
5	0.001425	fe80::20b:fdff:feac:c561	fe80::222:64ff:fe6b:8532	ICMPv6	Neighbor advertisement
6	0.460367	::	ff02::1:ff6b:8532	ICMPv6	Neighbor solicitation
7	0.618343	fe80::222:64ff:fe6b:8532	ff02::1:ffac:c561	ICMPv6	Neighbor solicitation

IPv6 Interfaces

- In Windows Vista/7, each IPv6 interface is numbered with unique 'Zone ID'

```
Administrator: Command Prompt
C:\windows\system32>route print -6
===========================================================================
Schnittstellenliste
 13 ...00 22 64 6b 85 32 ......  Marvell Yukon 88E8072 PCI-E Gigabit Ethernet Controller
 12 ...00 21 6b 17 a5 bc ......  Intel(R) WiFi Link 5100 AGN
 11 ...00 21 86 d1 3f 9b ......  Bluetooth-GerΣt (PAN)
  1 ........................... Software Loopback Interface 1
 16 ...00 00 00 00 00 00 00 e0  isatap.{0BF5943C-D67C-4195-9860-781CC293A689}
 17 ...00 00 00 00 00 00 00 e0  isatap.{BC043990-D4EC-4B5C-BDD2-8E9DD8697BF3}
 15 ...00 00 00 00 00 00 00 e0  6TO4 Adapter
 14 ...02 00 54 55 4e 01 ......  Teredo Tunneling Pseudo-Interface
===========================================================================
```

- A link-local address is automatically configured with the address prefix fe80::/64 for each physical or logical IPv6 interface
- If a router is available, a global address is configured on interface

IPv6 Interfaces

Administrator: Command Prompt

```
IPv6-Routentabelle
===========================================================================
Aktive Routen:
 If Metrik Netzwerkziel              Gateway
 13    286 ::/0                      fe80::20b:fdff:feac:c560
 16    281 ::/0                      fe80::5efe:192.168.20.1
  1    306 ::1/128                   Auf Verbindung
 14     18 2001::/32                 Auf Verbindung
 14    266 2001:0:d5c7:a2d6:281b:276f:3f57:ff32/128
                                     Auf Verbindung
 13     38 2001:cafe:0:20::/64       Auf Verbindung
 13    286 2001:cafe:0:20::113/128   Auf Verbindung
 13    286 2001:cafe:0:20:222:64ff:fe6b:8532/128
                                     Auf Verbindung
 13    286 2001:cafe:0:20:8d2d:33b4:5455:ad15/128
                                     Auf Verbindung
 16     33 2001:cafe:0:40::/64       Auf Verbindung
 16    281 2001:cafe:0:40:0:5efe:192.168.0.205/128
                                     Auf Verbindung
 13    286 fe80::/64                 Auf Verbindung
 14    266 fe80::/64                 Auf Verbindung
 16    281 fe80::5efe:192.168.0.205/128
                                     Auf Verbindung
 17    296 fe80::5efe:192.168.10.100/128
                                     Auf Verbindung
 13    286 fe80::222:64ff:fe6b:8532/128
                                     Auf Verbindung
 14    266 fe80::281b:276f:3f57:ff32/128
                                     Auf Verbindung
  1    306 ff00::/8                  Auf Verbindung
 14    266 ff00::/8                  Auf Verbindung
 13    286 ff00::/8                  Auf Verbindung
===========================================================================
```

Global Addresses

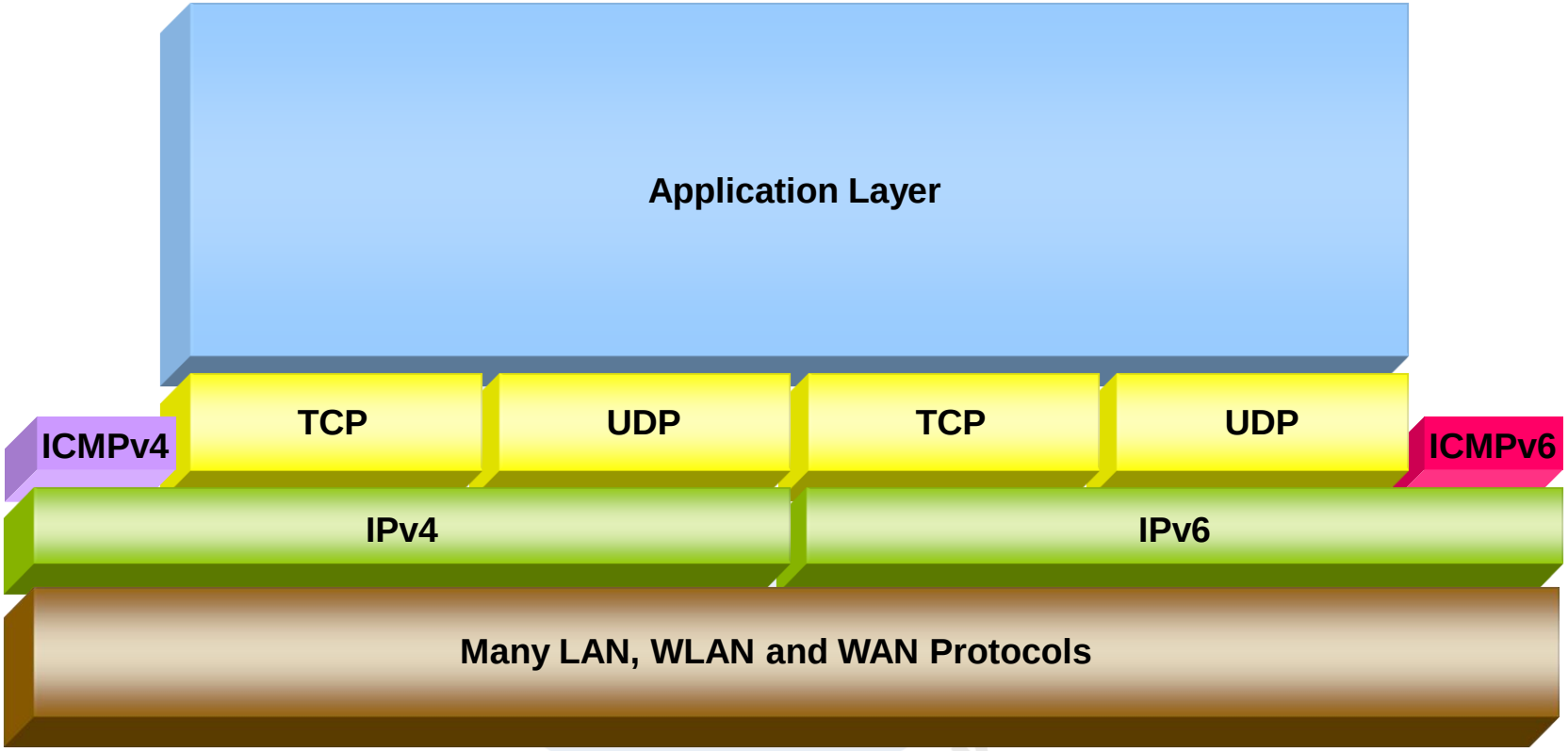
Link Local Addresses

Agenda

- Address Autoconfiguration
- Neighbor discovery, Router discovery
- Host configuration with DHCPv6
- Transition technologies, ISATAP & Teredo Tunnel

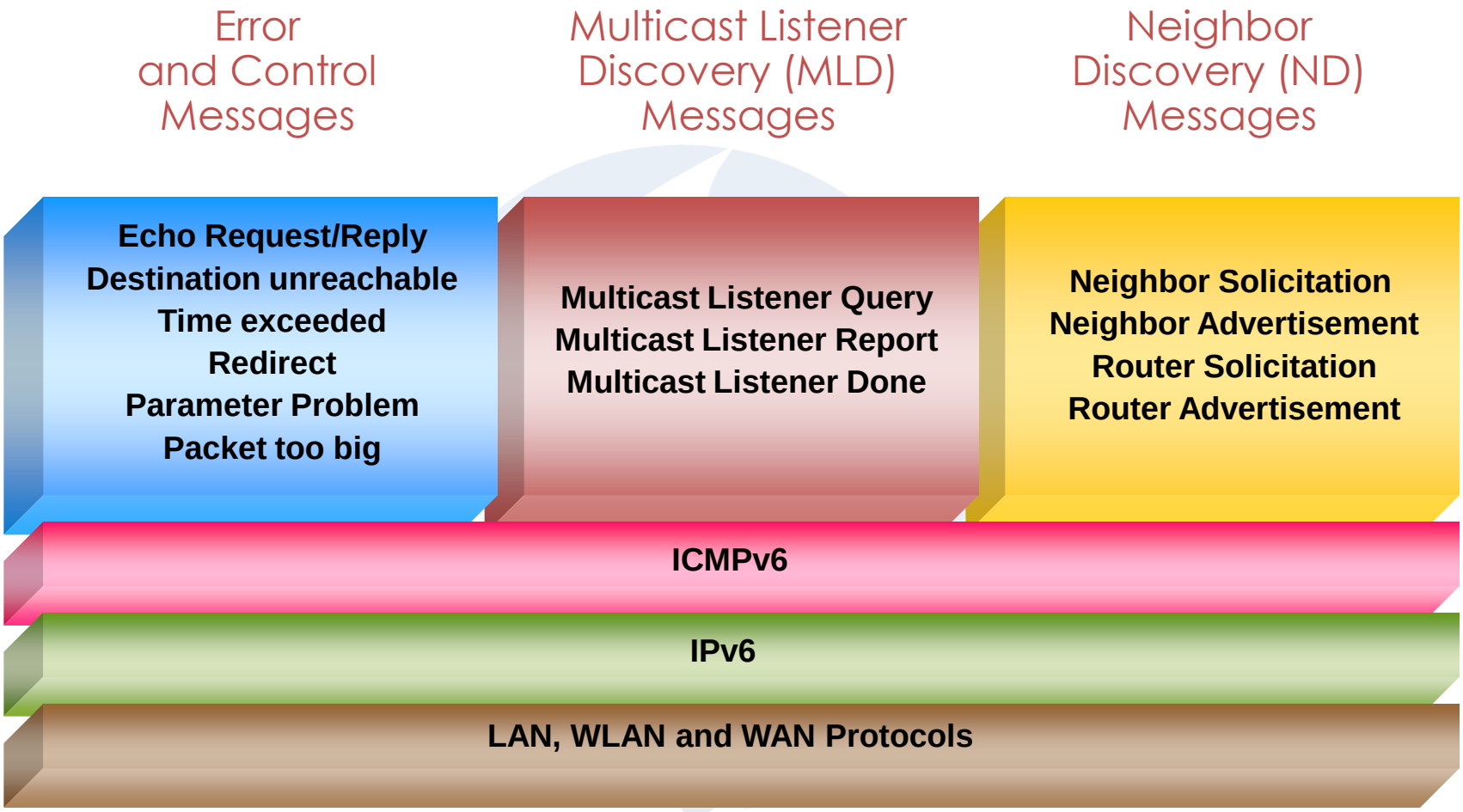
TCP/IP Protocol Family

Dual stack implementation



- Internet Control Message Protocol v6 (ICMPv6) plays an important role
- Many new ICMPv6 messages have been defined

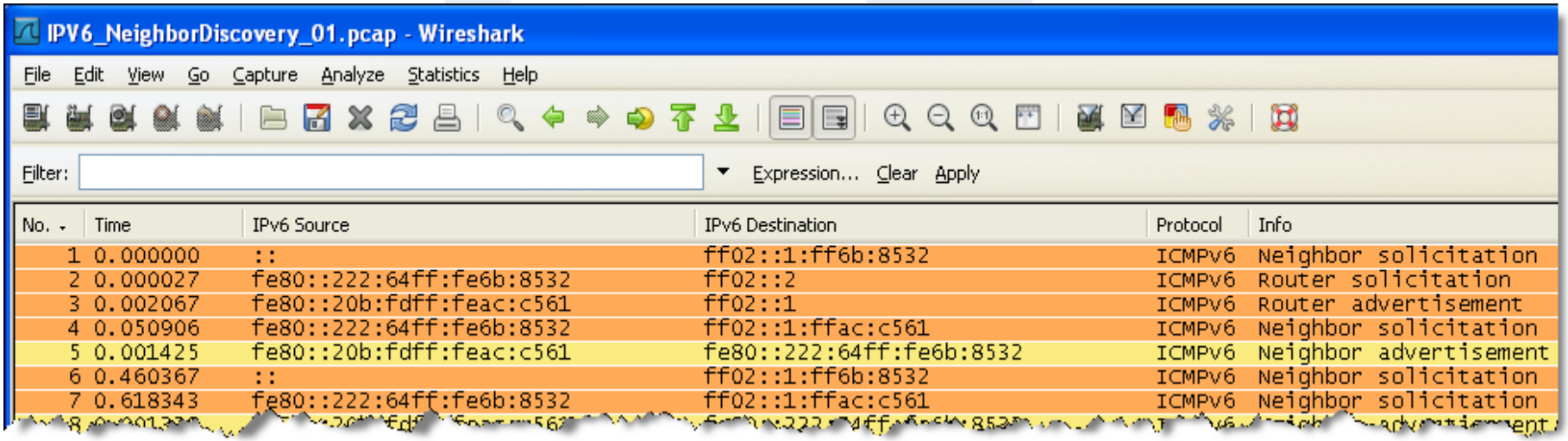
ICMPv6 Messages



Neighbor Discovery (ND)

The initial client startup process includes the following steps:

Frame #	
1	Duplicate Address Detection after Link-Local autoconfiguration
2	Router Discovery
3	Router Advertisement and global address autoconfiguration
4	Neighbor Discovery (searching for Router MAC)
5	Neighbor Advertisement (reply from Router with MAC)
6	Duplicate Address Detection with acquired global address



No.	Time	IPv6 Source	IPv6 Destination	Protocol	Info
1	0.000000	::	ff02::1:ff6b:8532	ICMPv6	Neighbor solicitation
2	0.000027	fe80::222:64ff:fe6b:8532	ff02::2	ICMPv6	Router solicitation
3	0.002067	fe80::20b:fdff:feac:c561	ff02::1	ICMPv6	Router advertisement
4	0.050906	fe80::222:64ff:fe6b:8532	ff02::1:ffac:c561	ICMPv6	Neighbor solicitation
5	0.001425	fe80::20b:fdff:feac:c561	fe80::222:64ff:fe6b:8532	ICMPv6	Neighbor advertisement
6	0.460367	::	ff02::1:ff6b:8532	ICMPv6	Neighbor solicitation
7	0.618343	fe80::222:64ff:fe6b:8532	ff02::1:ffac:c561	ICMPv6	Neighbor solicitation

Agenda

- Address Autoconfiguration
- Neighbor discovery, Router discovery
- Host configuration with DHCPv6
- Transition technologies, ISATAP & Teredo Tunnel

Host configuration with DHCPv6

Despite Address Autoconfiguration, DHCP plays an important role in IPv6 environment. It is required to provide clients with additional parameters like DNS server address and many other options.

DHCPv6 offers different level of control over the workstations:

Client parameters	Stateless Auto Address Config. RFC2462	Stateless DHCP Service for IPv6 RFC3736	Stateful DHCPv6 RFC3315
Subnet Prefix & Mask	From Router Advertisements (O-Flag=0 M-Flag=0)	From Router Advertisements (O-Flag=1 / M-Flag=0)	From Router Advertisements (O-Flag=1 / M-Flag=1)
Interface Identifier	Auto Configuration	Auto Configuration	From DHCPv6 Server
DNS, NTP address etc.	Manual Configuration	From DHCPv6 Server	From DHCPv6 Server

O = Other Flag / M = Managed Flag

Host configuration with DHCPv6

During this phase, the client is supplied with additional parameters:

Frame #

- 2 Router Discovery
- 3 Router Advertisement with 'Other Flag' set
- 6 Client contacts DHCP server
- 7 DHCP server delivers additional parameter like DNS, suffixes etc.

IPV6_DHCP_01.pcap - Wireshark

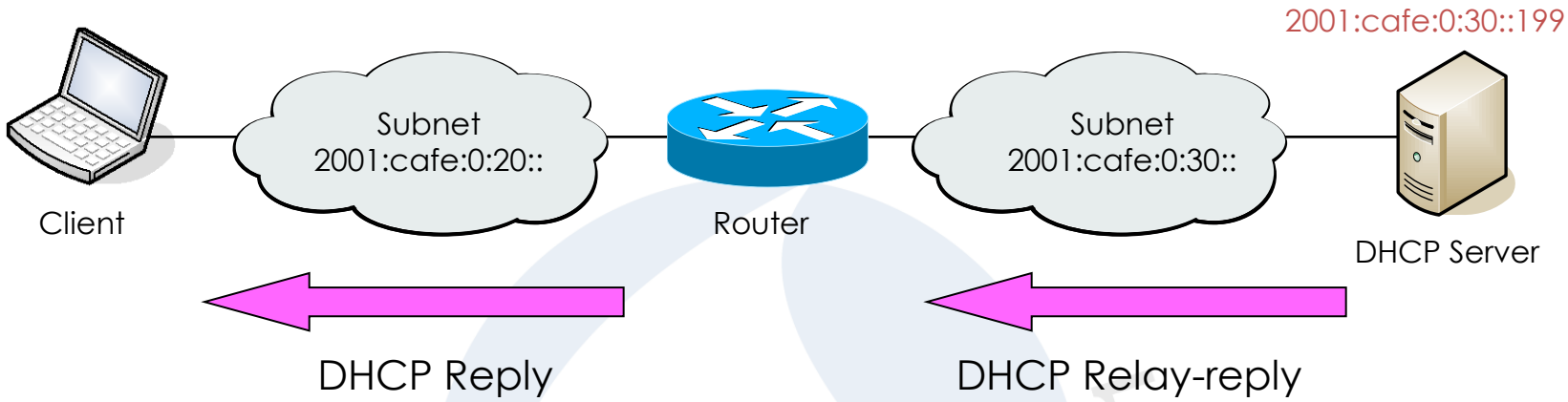
File Edit View Go Capture Analyze Statistics Help

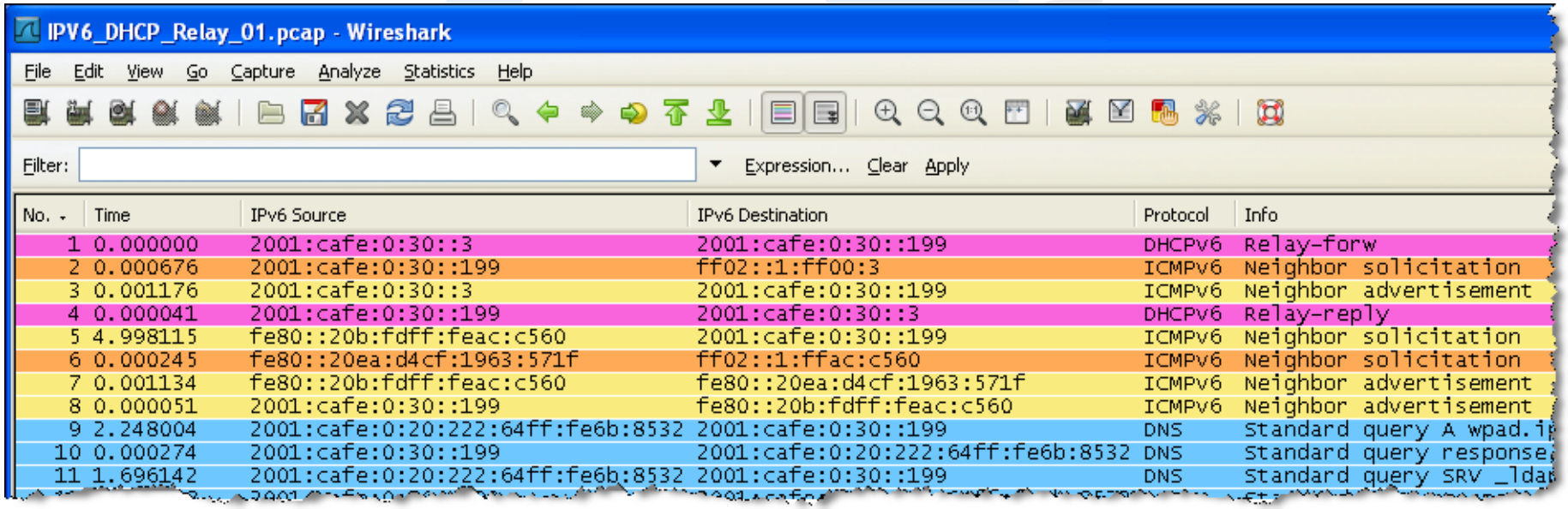
Filter: Expression... Clear Apply

No.	Time	IPv6 Source	IPv6 Destination	Protocol	Info
1	0.000000	::	ff02::1:ff6b:8532	ICMPv6	Neighbor solicitation
2	0.000025	fe80::222:64ff:fe6b:8532	ff02::2	ICMPv6	Router solicitation
3	0.001949	fe80::20b:fdff:feac:c561	ff02::1	ICMPv6	Router advertisement
4	0.028447	fe80::222:64ff:fe6b:8532	ff02::1:ffac:c561	ICMPv6	Neighbor solicitation
5	0.001672	fe80::20b:fdff:feac:c561	fe80::222:64ff:fe6b:8532	ICMPv6	Neighbor advertisement
6	0.031346	fe80::222:64ff:fe6b:8532	ff02::1:2	DHCPv6	Information-request
7	0.005862	fe80::20b:fdff:feac:c561	fe80::222:64ff:fe6b:8532	DHCPv6	Reply
8	0.445466	::	ff02::1:ff6b:8532	ICMPv6	Neighbor solicitation
9	0.539325	fe80::20b:fdff:feac:c561	ff02::d	PIMv2	Hello
10	0.044362	fe80::222:64ff:fe6b:8532	ff02::1:ffac:c561	ICMPv6	Neighbor solicitation
11	0.001273	fe80::20b:fdff:feac:c561	fe80::222:64ff:fe6b:8532	ICMPv6	Neighbor advertisement
12	3.930072	fe80::20b:fdff:feac:c561	fe80::222:64ff:fe6b:8532	ICMPv6	Neighbor solicitation
13	0.000104	fe80::222:64ff:fe6b:8532	fe80::20b:fdff:feac:c561	ICMPv6	Neighbor advertisement
14	2.284340	2001:cafe:0:20:222:64ff:fe6b:8532	2001:cafe:0:30::199	DNS	Standard query A wpad.ip
15	0.002288	2001:cafe:0:30::199	2001:cafe:0:20:222:64ff:fe6b:8532	DNS	Standard query response,

Host configuration with DHCPv6

DHCP server reply





No.	Time	IPv6 Source	IPv6 Destination	Protocol	Info
1	0.000000	2001:cafe:0:30::3	2001:cafe:0:30::199	DHCPv6	Relay-forw
2	0.000676	2001:cafe:0:30::199	ff02::1:ff00:3	ICMPv6	Neighbor solicitation
3	0.001176	2001:cafe:0:30::3	2001:cafe:0:30::199	ICMPv6	Neighbor advertisement
4	0.000041	2001:cafe:0:30::199	2001:cafe:0:30::3	DHCPv6	Relay-reply
5	4.998115	fe80::20b:fdff:feac:c560	2001:cafe:0:30::199	ICMPv6	Neighbor solicitation
6	0.000245	fe80::20ea:d4cf:1963:571f	ff02::1:ffac:c560	ICMPv6	Neighbor solicitation
7	0.001134	fe80::20b:fdff:feac:c560	fe80::20ea:d4cf:1963:571f	ICMPv6	Neighbor advertisement
8	0.000051	2001:cafe:0:30::199	fe80::20b:fdff:feac:c560	ICMPv6	Neighbor advertisement
9	2.248004	2001:cafe:0:20:222:64ff:fe6b:8532	2001:cafe:0:30::199	DNS	Standard query A wpad.i
10	0.000274	2001:cafe:0:30::199	2001:cafe:0:20:222:64ff:fe6b:8532	DNS	Standard query response
11	1.696142	2001:cafe:0:20:222:64ff:fe6b:8532	2001:cafe:0:30::199	DNS	Standard query SRV _lda

Host configuration with DHCPv6

At this state, the client is configured with all required parameters:

```
C:\windows\system32>ipconfig /all

Ethernet-Adapter LAN-Verbindung:

   Verbindungsspezifisches DNS-Suffix: ipv6.ch
   Beschreibung. . . . . . . . . . . : Marvell Yukon 88E8072 PCI-E Gigabit Ethernet
   Physikalische Adresse . . . . . . : 00-22-64-6B-85-32
   DHCP aktiviert. . . . . . . . . . : Ja
   Autokonfiguration aktiviert . . . : Ja
   IPv6-Adresse. . . . . . . . . . . : 2001:cafe:0:20:222:64ff:fe6b:8532(Bevorzugt)
   Verbindungslokale IPv6-Adresse  . : fe80::222:64ff:fe6b:8532%13(Bevorzugt)
   Lease erhalten. . . . . . . . . . : Samstag, 21. Februar 2009 11:46:04
   Lease läuft ab. . . . . . . . . . : Sonntag, 1. März 2009 11:46:03
   Standardgateway . . . . . . . . . : fe80::20b:fdff:feac:c561%13
   DHCPv6-IAID . . . . . . . . . . . : 251667044
   DHCPv6-Client-DUID. . . . . . . . : 00-01-00-01-10-D2-B9-65-00-22-64-6B-85-32
   DNS-Server  . . . . . . . . . . . : 2001:cafe:0:30::199
   Suchliste für verbindungsspezifische DNS-Suffixe:
                                       yourdomain.ch
                                       ipv6.ch
                                       dummy.ch
```

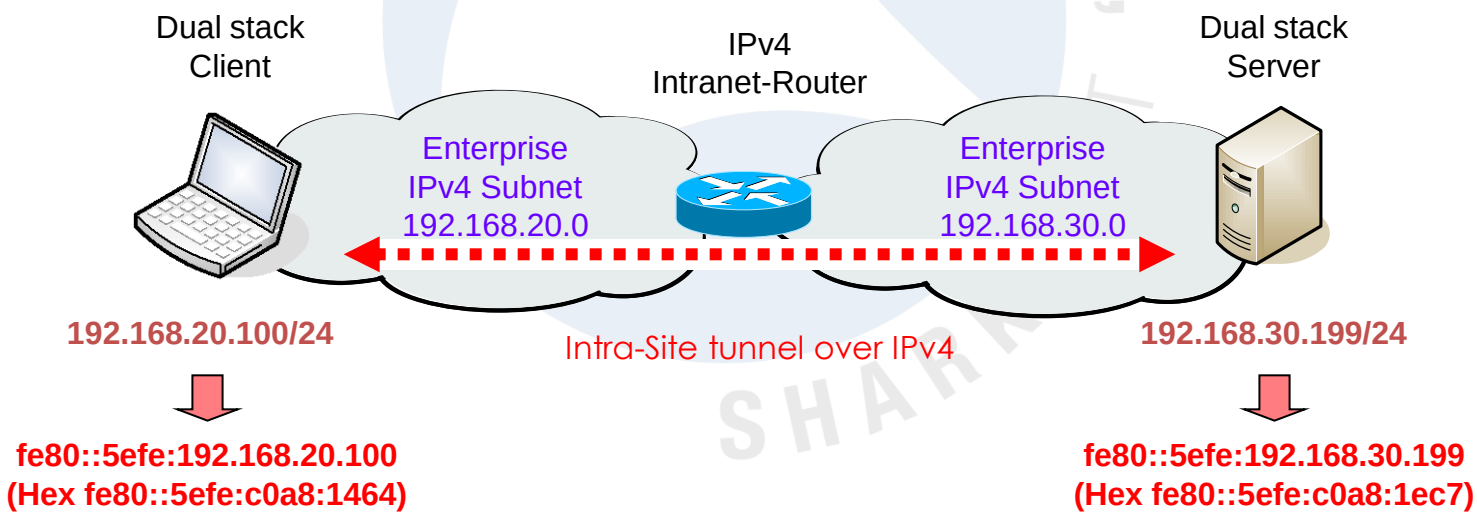
Agenda

- Address Autoconfiguration
- Neighbor discovery, Router discovery
- Host configuration with DHCPv6
- Transition technologies, ISATAP & Teredo Tunnel

IPv6 Transition Technologies

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

- ISATAP enables easy deployment of IPv6 in existing IPv4 infrastructure
- ISATAP hosts do not require any manual configuration
- IPv6 address contains an embedded IPv4 source or destination address
- ISATAP clients uses locally assigned IPv4 address (public or private) to create the 64-bit interface identifier



IPv6 Transition Technologies

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

- ISATAP interface is created at the same time the IPv6 stack is installed

```
Administrator: Command Prompt

Tunneladapter LAN-Verbindung* 2:

   Verbindungsspezifisches DNS-Suffix: yourdomain.ch
   Beschreibung. . . . . . . . . . . : isatap.{BC043990-D4EC-4B5C-BDD2-8E9DD8697BF3}
   Physikalische Adresse . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP aktiviert. . . . . . . . . . : Nein
   Autokonfiguration aktiviert . . . : Ja
   Verbindungslokale IPv6-Adresse  . : fe80::5efe:192.168.20.100%17(Bevorzugt)
   Standardgateway . . . . . . . . . :
   DNS-Server  . . . . . . . . . . . : 2001:cafe:0:30::199
   NetBIOS über TCP/IP . . . . . . . : Deaktiviert
```

- Local interface ID # (%17) must be appended to destination address

Ping fe80::5efe:192.168.30.199%17

IPv6 Transition Technologies

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

IPV6_Ping_through_ISATAP_tunnel.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: vlan.id == 20 Expression... Clear Apply

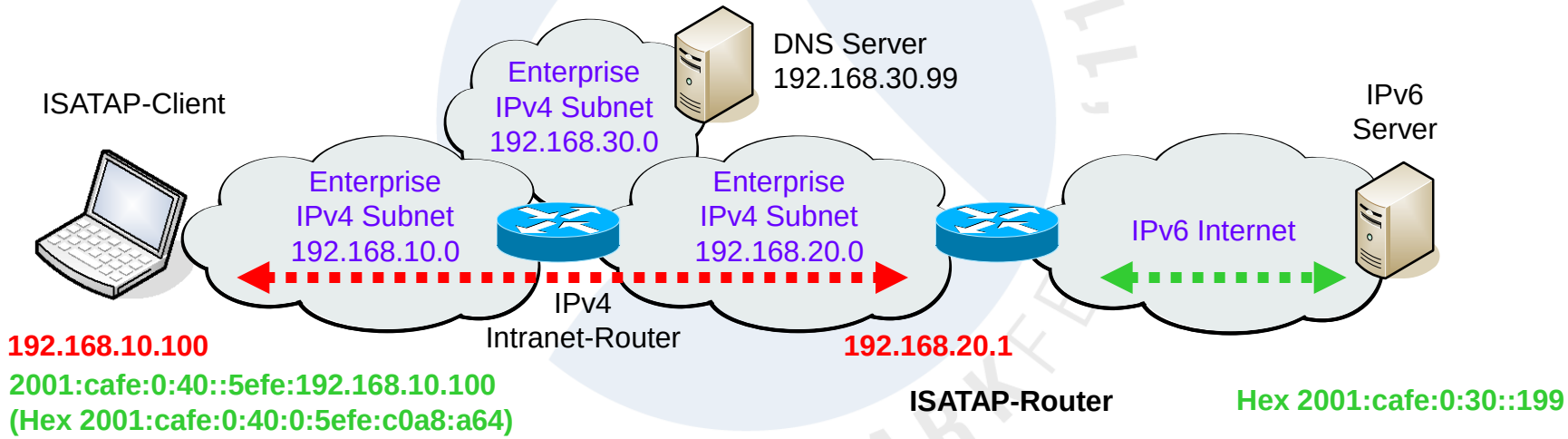
No.	Time	IPv6 Source	IPv6 Destination	IPv4 Source	IPv4 Destination	Protocol	Info
1	0.000000	fe80::5efe:c0a8:1464	fe80::5efe:c0a8:1ec7	192.168.20.100	192.168.30.199	ICMPv6	Echo request
4	0.000819	fe80::5efe:c0a8:1ec7	fe80::5efe:c0a8:1464	192.168.30.199	192.168.20.100	ICMPv6	Echo reply
5	1.002117	fe80::5efe:c0a8:1464	fe80::5efe:c0a8:1ec7	192.168.20.100	192.168.30.199	ICMPv6	Echo request
8	0.000794	fe80::5efe:c0a8:1ec7	fe80::5efe:c0a8:1464	192.168.30.199	192.168.20.100	ICMPv6	Echo reply
9	1.013203	fe80::5efe:c0a8:1464	fe80::5efe:c0a8:1ec7	192.168.20.100	192.168.30.199	ICMPv6	Echo request
12	0.000811	fe80::5efe:c0a8:1ec7	fe80::5efe:c0a8:1464	192.168.30.199	192.168.20.100	ICMPv6	Echo reply
13	1.013145	fe80::5efe:c0a8:1464	fe80::5efe:c0a8:1ec7	192.168.20.100	192.168.30.199	ICMPv6	Echo request
16	0.000854	fe80::5efe:c0a8:1ec7	fe80::5efe:c0a8:1464	192.168.30.199	192.168.20.100	ICMPv6	Echo reply

```
⊞ Frame 1 (118 bytes on wire, 118 bytes captured)
⊞ Ethernet II, Src: HewlettP_6b:85:32 (00:22:64:6b:85:32), Dst: Cisco_ac:c5:60 (00:0b:fd:ac:c5:60)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 20
⊞ Internet Protocol, Src: 192.168.20.100 (192.168.20.100), Dst: 192.168.30.199 (192.168.30.199)
⊟ Internet Protocol Version 6
  ⊞ 0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 40
    Next header: ICMPv6 (0x3a)
    Hop limit: 128
    Source: fe80::5efe:c0a8:1464 (fe80::5efe:c0a8:1464)
    Destination: fe80::5efe:c0a8:1ec7 (fe80::5efe:c0a8:1ec7)
⊞ Internet Control Message Protocol v6
```

IPv6 Transition Technologies

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

- ISATAP can also be used to access native IPv6 destinations
- Client resolves ISATAP router IPv4 address through internal DNS
- Client request IPv6 global unicast prefix from ISATAP router
- Client sends IPv6 in IPv4 embedded packets to ISATAP router



- ISATAP router unpacks embedded packets and forwards them

+

IPv6 Transition Technologies

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

IPV6_Ping_through_ISATAP_router.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	IPv6 Source	IPv6 Destination	IPv4 Source	IPv4 Destination	Protocol	Info
3	0.610461	2001:cafe:0:40:0:5efe:c0a8:a64	2001:cafe:0:30::199	192.168.10.100	192.168.20.1	ICMPv6	Echo requ
4	0.001282	2001:cafe:0:40:0:5efe:c0a8:a64	2001:cafe:0:30::199			ICMPv6	Echo requ
5	0.000339	2001:cafe:0:30::199	2001:cafe:0:40:0:5efe:c0a8:a64			ICMPv6	Echo repl
6	0.001015	2001:cafe:0:30::199	2001:cafe:0:40:0:5efe:c0a8:a64	192.168.20.1	192.168.10.100	ICMPv6	Echo repl
7	0.996878	2001:cafe:0:40:0:5efe:c0a8:a64	2001:cafe:0:30::199	192.168.10.100	192.168.20.1	ICMPv6	Echo requ
8	0.001323	2001:cafe:0:40:0:5efe:c0a8:a64	2001:cafe:0:30::199			ICMPv6	Echo requ
9	0.000266	2001:cafe:0:30::199	2001:cafe:0:40:0:5efe:c0a8:a64			ICMPv6	Echo repl
10	0.000992	2001:cafe:0:30::199	2001:cafe:0:40:0:5efe:c0a8:a64	192.168.20.1	192.168.10.100	ICMPv6	Echo repl
11	0.995744	2001:cafe:0:40:0:5efe:c0a8:a64	2001:cafe:0:30::199	192.168.10.100	192.168.20.1	ICMPv6	Echo requ
12	0.001326	2001:cafe:0:40:0:5efe:c0a8:a64	2001:cafe:0:30::199			ICMPv6	Echo requ
13	0.000317	2001:cafe:0:30::199	2001:cafe:0:40:0:5efe:c0a8:a64			ICMPv6	Echo repl
14	0.000933	2001:cafe:0:30::199	2001:cafe:0:40:0:5efe:c0a8:a64	192.168.20.1	192.168.10.100	ICMPv6	Echo repl
15	0.995771	2001:cafe:0:40:0:5efe:c0a8:a64	2001:cafe:0:30::199	192.168.10.100	192.168.20.1	ICMPv6	Echo requ
16	0.001304	2001:cafe:0:40:0:5efe:c0a8:a64	2001:cafe:0:30::199			ICMPv6	Echo requ
17	0.000288	2001:cafe:0:30::199	2001:cafe:0:40:0:5efe:c0a8:a64			ICMPv6	Echo repl

```
⊞ Frame 3 (118 bytes on wire, 118 bytes captured)
⊞ Ethernet II, Src: HewlettP_6b:85:32 (00:22:64:6b:85:32), Dst: Cisco_ac:c5:60 (00:0b:fd:ac:c5:60)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 10
⊞ Internet Protocol, Src: 192.168.10.100 (192.168.10.100), Dst: 192.168.20.1 (192.168.20.1)
⊞ Internet Protocol Version 6
⊞ Internet Control Message Protocol v6
```

IPv6 Transition Technologies

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

- Client received prefix 2001:cafe:0:40:: from ISATAP router

```
Command Prompt
Tunneladapter LAN-Verbindung* 2:

   Verbindungsspezifisches DNS-Suffix:
   Beschreibung. . . . . . . . . . . : isatap.{BC043990-D4EC-4B5C-BDD2-8E9DD8697BF3}
   Physikalische Adresse . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP aktiviert. . . . . . . . . . : Nein
   Autokonfiguration aktiviert . . . : Ja
   IPv6-Adresse. . . . . . . . . . . : 2001:cafe:0:40:0:5efe:192.168.10.100(Bevorzugt)
   Verbindungslokale IPv6-Adresse  . : fe80::5efe:192.168.10.100%17(Bevorzugt)
   Standardgateway . . . . . . . . . : fe80::5efe:192.168.20.1%17
   DNS-Server  . . . . . . . . . . . : 192.168.30.199
   NetBIOS über TCP/IP . . . . . . . : Deaktiviert
```

- Client installs address of Default Gateway

IPv6 Transition Technologies

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

- Command ‘route print -6’ displays clients routing table

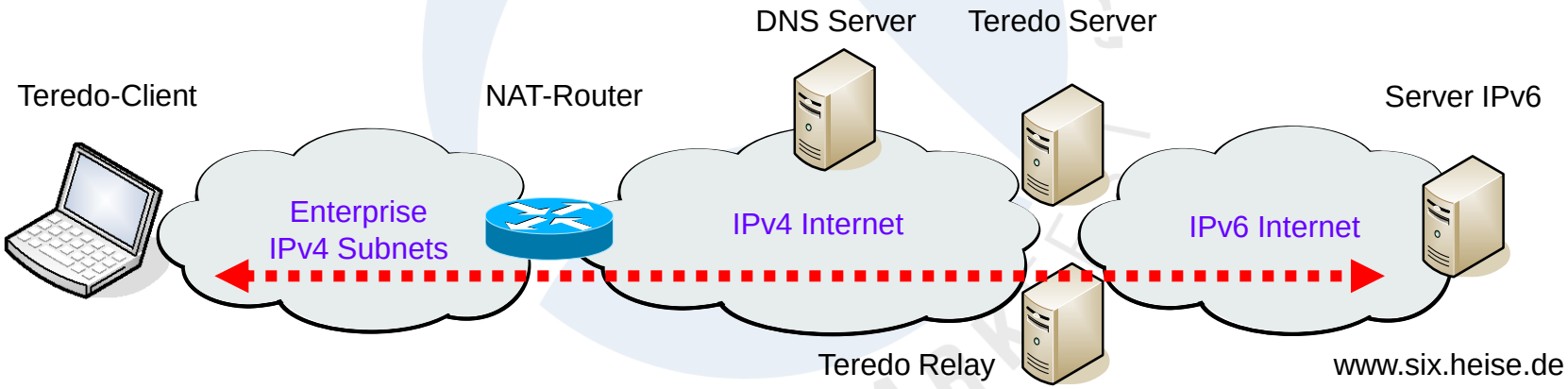
```
Command Prompt
C:\Users\Rolf>route print -6
===========================================================================
Schnittstellenliste
 13 ...00 22 64 6b 85 32 ......  Marvell Yukon 88E8072 PCI-E Gigabit Ethernet Controller
 12 ...00 21 6b 17 a5 bc ......  Intel(R) WiFi Link 5100 AGN
  1 ........................... Software Loopback Interface 1
 16 ...00 00 00 00 00 00 00 e0  isatap.{0BF5943C-D67C-4195-9860-781CC293A689}
 17 ...00 00 00 00 00 00 00 e0  isatap.{BC043990-D4EC-4B5C-BDD2-8E9DD8697BF3}
 15 ...00 00 00 00 00 00 00 e0  6TO4 Adapter
 14 ...02 00 54 55 4e 01 ......  Teredo Tunneling Pseudo-Interface
===========================================================================

IPv6-Routentabelle
===========================================================================
Aktive Routen:
 If Metrik Netzwerkziel              Gateway
 17    296 ::/0                      fe80::5efe:192.168.20.1
  1    306 ::1/128                   Auf Verbindung
 14     18 2001::/32                 Auf Verbindung
 14    266 2001:0:d5c7:a2d6:24d9:1e15:3f57:f59b/128
                                     Auf Verbindung
 14    266 2001:8a8:20::23/128       Auf Verbindung
 17     48 2001:cafe:0:40::/64       Auf Verbindung
 17    296 2001:cafe:0:40:0:5efe:192.168.10.100/128
                                     Auf Verbindung
 13    286 fe80::/64                 Auf Verbindung
```

IPv6 Transition Technologies

Teredo Tunnel

- Tunneling method named after Teredo Navalis (shipworm)
- Teredo encapsulates IPv6 packets within UDP/IPv4 datagram
- Most NAT Routers can forward these packets properly
- Teredo allows a client to communicate with a native IPv6 server
- Teredo Server and Teredo Relay in the Internet care for transitions



- Teredo tunnels are set up automatically, no configuration is needed.

+

IPv6 Transition Technologies

Teredo Tunnel interface

- In WIN Vista clients, the Teredo Tunneling I/F is created automatically
- The IPv6 prefix of all Teredo clients is 2001:0::/32

```
Administrator: Eingabeaufforderung

Tunneladapter Teredo Tunneling Pseudo-Interface:

   Verbindungsspezifisches DNS-Suffix:
   Beschreibung. . . . . . . . . . . : Teredo Tunneling Pseudo-Interface
   Physikalische Adresse . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP aktiviert. . . . . . . . . . : Nein
   Autokonfiguration aktiviert . . . : Ja
   IPv6-Adresse. . . . . . . . . . . : 2001:0:5ef5:79fd:3c37:1e2b:acb2:7e97(Bevorzugt)
   Verbindungslokale IPv6-Adresse  . : fe80::3c37:1e2b:acb2:7e97%21(Bevorzugt)
   Standardgateway . . . . . . . . . : ::
   NetBIOS über TCP/IP . . . . . . . : Deaktiviert
```

- The client resolves teredo.ipv6.microsoft.com to build the /64 prefix
- The value 5ef5:79fd is the IPv4 Teredo server address: 94.245.121.253
- Miredo is the open-source Teredo tunneling software for Linux, BSD etc.

IPv6 Transition Technologies

Teredo Tunnel initialization (File IPV6_Teredo_www_six_heise_de)

IPV6_Teredo_www_six_heise_de.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source Address	Destination Address	Protocol	Info
1	0.000000	192.168.0.201	192.168.0.1	DNS	Standard query A teredo.ipv6.microsoft.com
2	0.020750	192.168.0.1	192.168.0.201	DNS	Standard query response CNAME teredo.ipv6.microsoft.com.nsatc.net A 94.245.121.253
3	70.867437	192.168.0.201	192.168.0.1	DNS	Standard query A www.six.heise.de
4	0.023322	192.168.0.1	192.168.0.201	DNS	Standard query response
5	0.001338	192.168.0.201	192.168.0.1	DNS	Standard query AAAA www.six.heise.de
6	0.004647	192.168.0.1	192.168.0.201	DNS	Standard query response AAAA 2a02:2e0:3fe:100::6
7	0.015022	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	2a02:2e0:3fe:100::6	Teredo	Direct IPv6 Connectivity Test id=0x65d6, seq=36125
8	0.076991	fe80::24ac:fa35:f9ed:545c	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	IPv6	IPv6 no next header
9	59.981557	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	fe80::24ac:fa35:f9ed:545c	IPv6	IPv6 no next header
10	0.020733	2a02:2e0:3fe:100::6	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	ICMPv6	Echo (ping) reply id=0x7dfe, seq=56827
11	3.917426	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	2a02:2e0:3fe:100::6	TCP	50592 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1220 SACK_PERM=1
12	0.022013	2a02:2e0:3fe:100::6	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	TCP	http > 50592 [SYN, ACK] Seq=0 Ack=1 Win=5760 Len=0 MSS=1440 SACK_PERM=1
13	0.000368	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	2a02:2e0:3fe:100::6	TCP	50592 > http [ACK] Seq=1 Ack=1 Win=17080 Len=0
14	0.002041	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	2a02:2e0:3fe:100::6	HTTP	GET / HTTP/1.1
15	0.027842	2a02:2e0:3fe:100::6	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	TCP	http > 50592 [ACK] Seq=1 Ack=391 Win=6432 Len=0
16	0.148421	2a02:2e0:3fe:100::6	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	TCP	[TCP segment of a reassembled PDU]
17	0.002209	2a02:2e0:3fe:100::6	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	TCP	[TCP segment of a reassembled PDU]
18	0.000233	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	2a02:2e0:3fe:100::6	TCP	50592 > http [ACK] Seq=391 Ack=2441 Win=15860 Len=0
19	0.003756	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	2a02:2e0:3fe:100::6	TCP	[TCP Window Update] 50592 > http [ACK] Seq=391 Ack=2441 Win=17080 Len=0
20	0.018471	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	2a02:2e0:3fe:100::6	TCP	50593 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1220 SACK_PERM=1
21	0.005230	2a02:2e0:3fe:100::6	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	TCP	[TCP segment of a reassembled PDU]
22	0.001451	2a02:2e0:3fe:100::6	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	TCP	[TCP segment of a reassembled PDU]
23	0.000174	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	2a02:2e0:3fe:100::6	TCP	50592 > http [ACK] Seq=391 Ack=4881 Win=15860 Len=0
24	0.002851	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	2a02:2e0:3fe:100::6	TCP	[TCP Window Update] 50592 > http [ACK] Seq=391 Ack=4881 Win=17080 Len=0
25	0.000820	2a02:2e0:3fe:100::6	2001:0:5ef5:79fd:2801:1e2b:acb2:6c85	TCP	[TCP segment of a reassembled PDU]

```
⊞ Frame 14: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits)
⊞ Ethernet II, Src: QuantaCo_6d:6c:e0 (00:23:8b:6d:6c:e0), Dst: Avm_bb:c1:0b (00:1a:4f:bb:c1:0b)
⊞ Internet Protocol, Src: 192.168.0.201 (192.168.0.201), Dst: 216.66.80.238 (216.66.80.238)
⊞ User Datagram Protocol, Src Port: 57812 (57812), Dst Port: 37070 (37070)
  Teredo IPv6 over UDP tunneling
⊞ Internet Protocol Version 6, Src: 2001:0:5ef5:79fd:2801:1e2b:acb2:6c85 (2001:0:5ef5:79fd:2801:1e2b:acb2:6c85), Dst: 2a02:2e0:3fe:100::6 (2a02:2e0:3fe:100::6)
⊞ Transmission Control Protocol, Src Port: 50592 (50592), Dst Port: http (80), Seq: 1, Ack: 1, Len: 390
⊞ Hypertext Transfer Protocol

0020  50 ee e1 d4 90 ce 01 ca  ec 7d 60 00 00 00 00 01 9a   P....... .}`.....
0030  06 80 20 01 00 00 5e f5  79 fd 28 01 1e 2b ac b2   .. ...^. y.(..+..
0040  6c 85 2a 02 02 e0 03 fe  01 00 00 00 00 00 00 00   l.*..... ........
0050  00 06 c5 a0 00 50 87 23  05 81 69 8a 0f c2 50 18   .....P.# ..i...P.
0060  42 b8 ad 8b 00 00 47 45  54 20 2f 20 48 54 54 50   B.....GE T / HTTP
```

Teredo IPv6 over UDP tunneling (teredo), 450 bytes | Packets: 325 Displayed: 325 Marked: 0 Load time: 0:00.022 | Profile: LNS_IPv6

IPv6 Transition Technologies

Teredo Tunnel initialization (File IPV6_Teredo_www_six_heise_de)

SA	DA	SA	DA	
Data	TC-v6	SRV-v6	TC-v4	TS-v4

(Frame# 7) — Step 1 →

SA	DA	SA	DA	
Data	TC-v6	SRV-v6	NR-v4	TS-v4

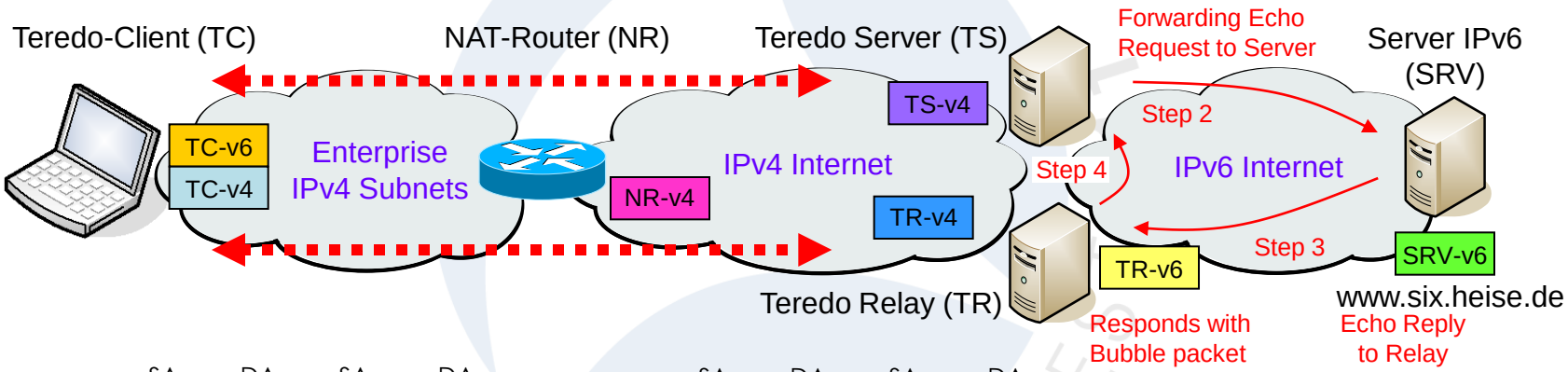
ICMP Echo Request

DA	SA	DA	SA	Teredo
TC-v4	TS-v4	TC-v6	TR-v6	TR-v4

← (Frame# 8) — Step 5

DA	SA	DA	SA	Teredo
NR-v4	TS-v4	TC-v6	TR-v6	TR-v4

Bubble Packet (with IP and UDP Port of Teredo Relay)



SA	DA	SA	DA	
TC-v6	TR-v6	TC-v4	TR-v4	

(Frame# 9) — Step6 →

SA	DA	SA	DA	
TC-v6	TR-v6	NR-v4	TR-v4	

Bubble Packet (Tunnel init.)

DA	SA	DA	SA	
TC-v4	TR-v4	TC-v6	SRV-v6	Data

← (Frame# 10) — Step 7

DA	SA	DA	SA	
NR-v4	TR-v4	TC-v6	SRV-v6	Data

ICMP Echo Reply

SA	DA	SA	DA	
Data	TC-v6	SRV-v6	TC-v4	TR-v4

(Frame# 11) — Step 8 →

SA	DA	SA	DA	
Data	TC-v6	SRV-v6	NR-v4	TR-v4

SA	DA	
Data	TC-v6	SRV-v6

Step 9 →

TCP SYN +

IPv6 Transition Technologies

Teredo Tunnel

- When starting, a Windows-based computer using Teredo resolves the IPv4 address of the Teredo server teredo.ipv6.microsoft.com
- By the Router solicitation/advertisement dialog through Teredo, the client receives a valid IPv6 prefix
- When activated, the Teredo client contacts Teredo server to obtain information such as the type of NAT that the client is behind
- If the client has only link-local or Teredo IPV6 addresses assigned, then the DNS Client will send only queries for A records
- The client needs at least one valid IPv6 address configured (may be manually) in order to query for AAAA records
- Windows Vista Client computers will always use IPV6 over IPV4
- A default route may have to be configured on Teredo interface:

netsh interface ipv6 add route ::/0 14 ← Teredo Interface ID

IPv6 Transition Technologies

Teredo commands & settings

- netsh interface teredo show state
- netsh interface teredo set state disabled
- netsh interface teredo set state client
- netsh interface teredo set state enterpriseclient
- netsh int ipv6 set teredo client teredo.remlab.net
- netsh int ipv6 set teredo client teredo.ipv6.microsoft.com
- netsh interface ipv6 show address
- netsh interface ipv6 add address "Local Area Connection 2" fd00:0:0:1::1
- netsh interface ipv6 add route ::/0 14
- Windows firewall must be activated to enable Teredo!

IPv6 Session Summary

How to get

- Verify IPv6 readiness of your suppliers
- Verify IPv6 readiness of your applications
- IPv6 can perfectly coexist with IPv4
- Start experimenting using ISATAP and Teredo
- Network migration can be done smoothly
- Train yourself and your people
- Wireshark is the perfect tool to learn and train
- Interesting IPv6 references:

www.sixxs.net IPv6 Deployment and IPv6 Tunnel Broker, helping to deploy IPv6 around the world, IPv6 monitoring, IPv6 routing monitoring, IPv6 coordination.

www.ipv6forum.com World-wide consortium of Internet vendors aiming to promote IPv6. Includes mailing lists, event listings, technical information, and links

www.ipv6tf.org The IPv6 Portal. IPv6 Deployment and Support, IPv6 trainings, IPv6 workshops, IPv6 labs.

Thanks for visiting

Rolf Leutert, Leutert NetServices, www.wireshark.ch