Discovering IPv6 with Wireshark

presented by
Rolf Leutert

LEUTERT NetServices

Instructor: Rolf Leutert, Network Expert & Trainer
Leutert NetServices
Troubleshooting & Trainings
Zürich-Airport, Switzerland

- Sniffer® certified Instructor since 1990
- Wireshark® Instructor since 2006
- Wireshark® Certified Network Analyst 2010

leutert@wireshark.ch
www.wireshark.ch

Sniffer Certified MASTER

Wireshark University
WIRESHARK® CERTIFIED NETWORK ANALYST

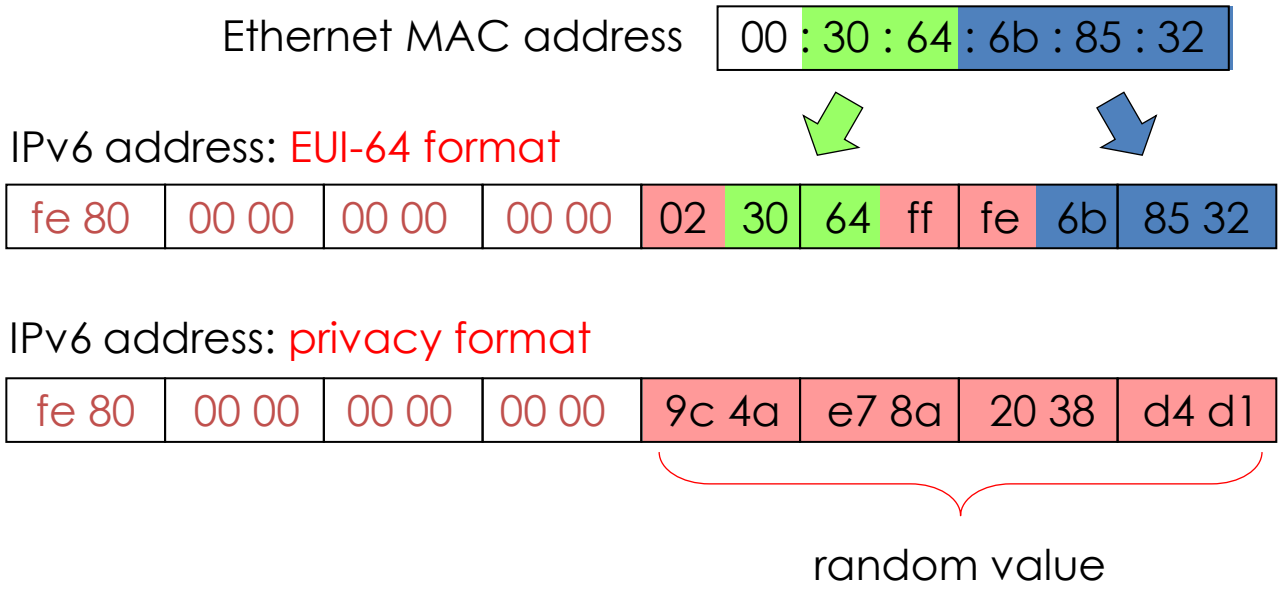
Agenda

- Address Autoconfiguration
- Neighbor discovery, Router discovery
- Host configuration with DHCPv6
- New DNS AAAA record
- Transition technologies, 6rd Tunnel

Address Autoconfiguration

IPv6 Stateless Address Autoconfiguration (SLAAC)

- An IPv6 host will auto configure 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

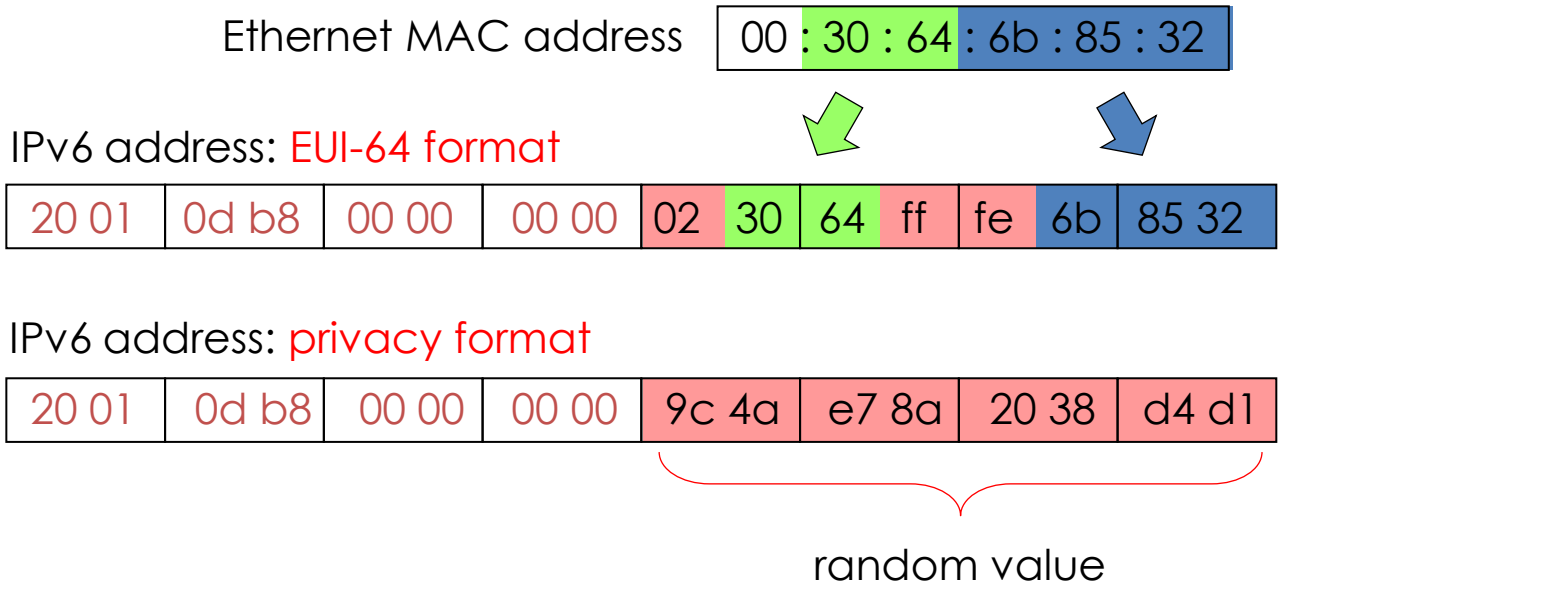


+

Address Autoconfiguration

IPv6 Stateless Address Autoconfiguration (SLAAC)

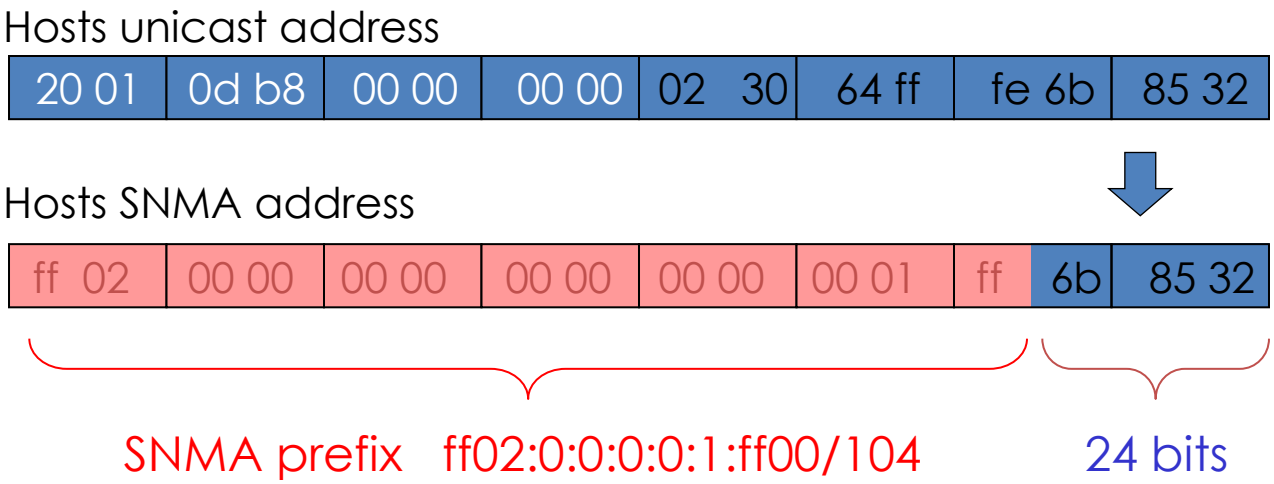
- If a router is present, host will also autoconfigure global address
- Prefix will be obtained from router, example 2001:db8::/64
- Interface ID is either derived from MAC address or a random value
- Router indicates in advertisement if stateful configuration may be used



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



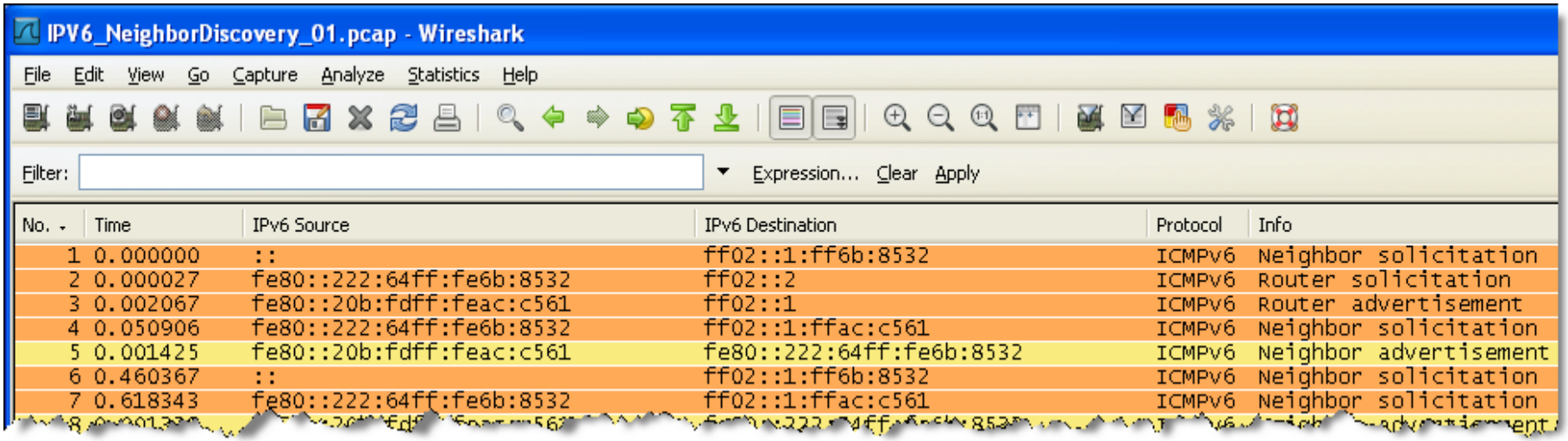
SNMA derived from unicast address: ff02::1:ff6b:8532

Duplicate Address Detection (DAD)

The initial client startup process includes the following steps:

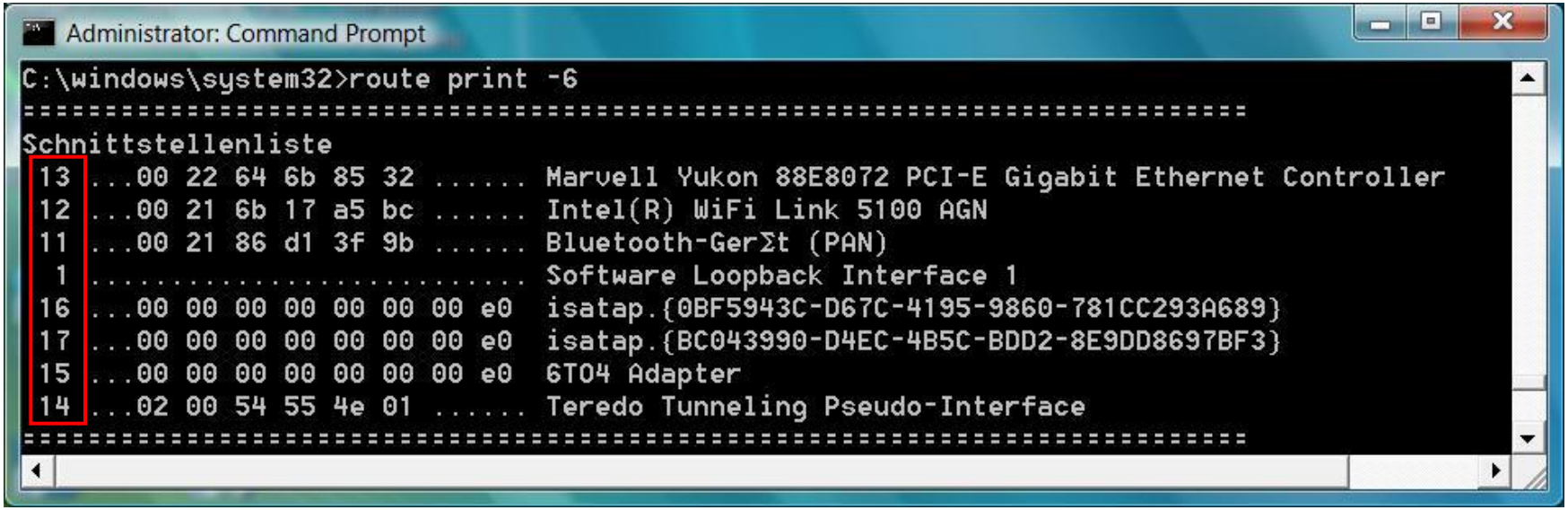
Frame #

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



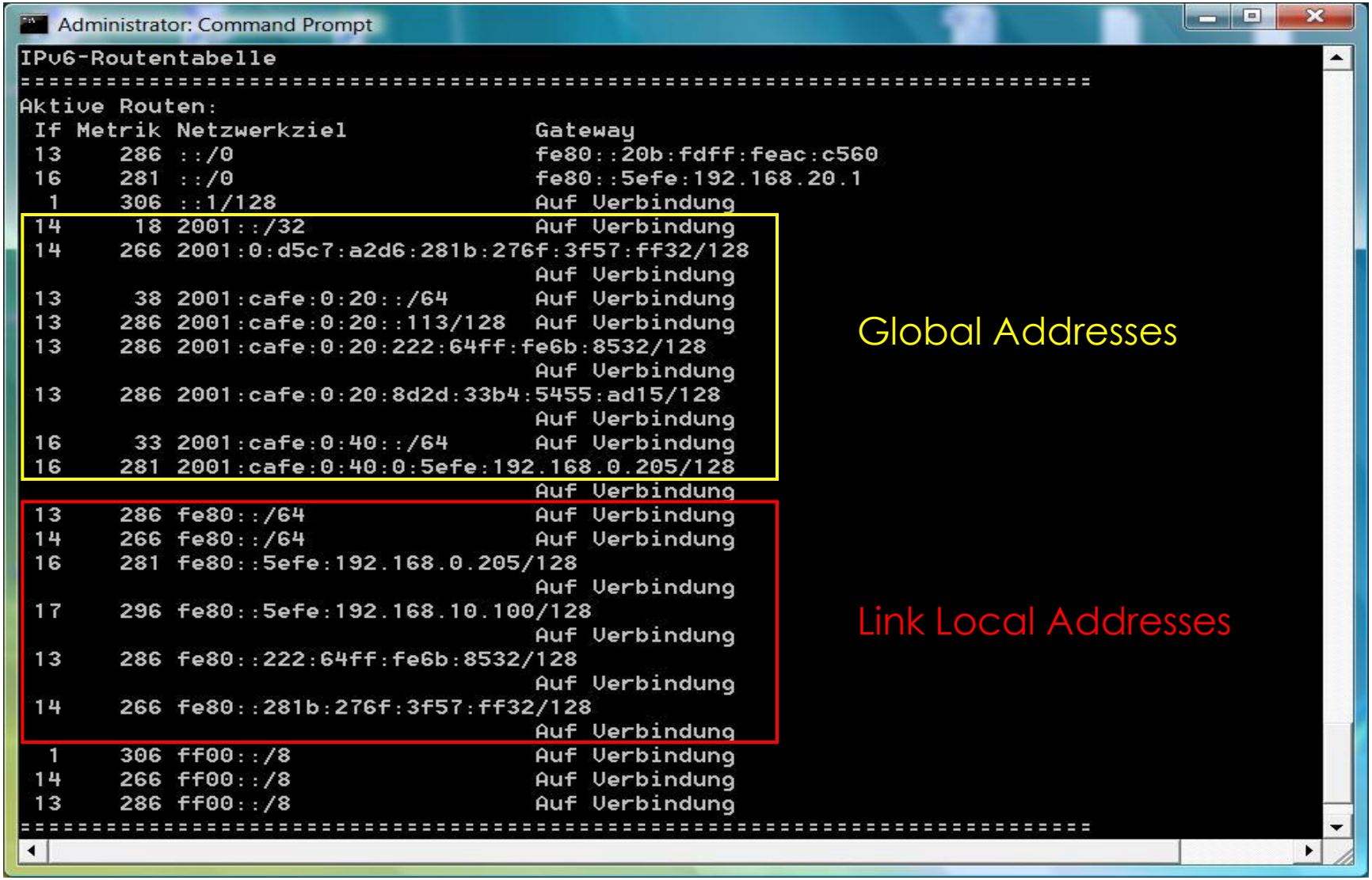
IPv6 Interfaces

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



- 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

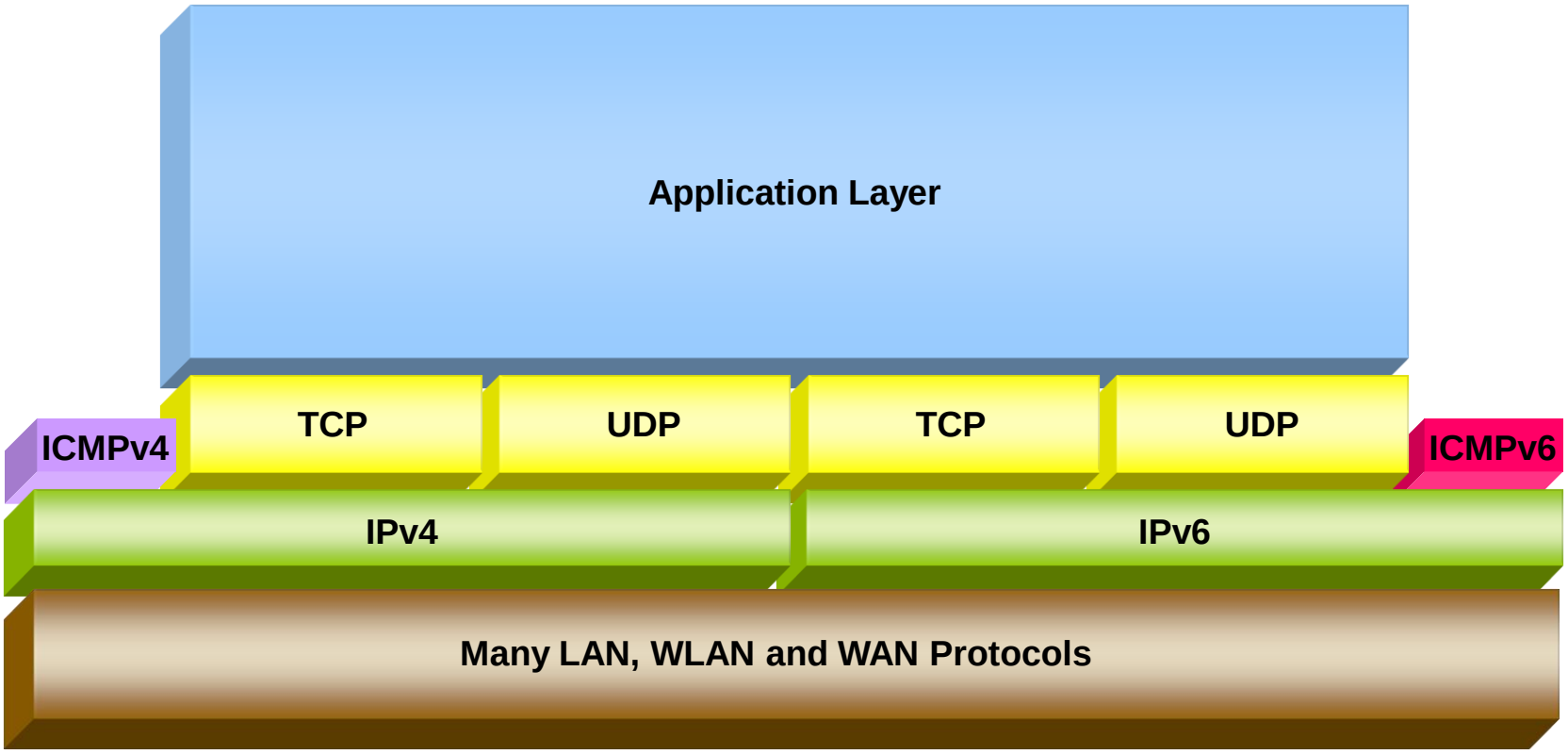


Agenda

- Address Autoconfiguration
- Neighbor discovery, Router discovery
- Host configuration with DHCPv6
- New DNS AAAA record
- Transition technologies, 6rd Tunnel

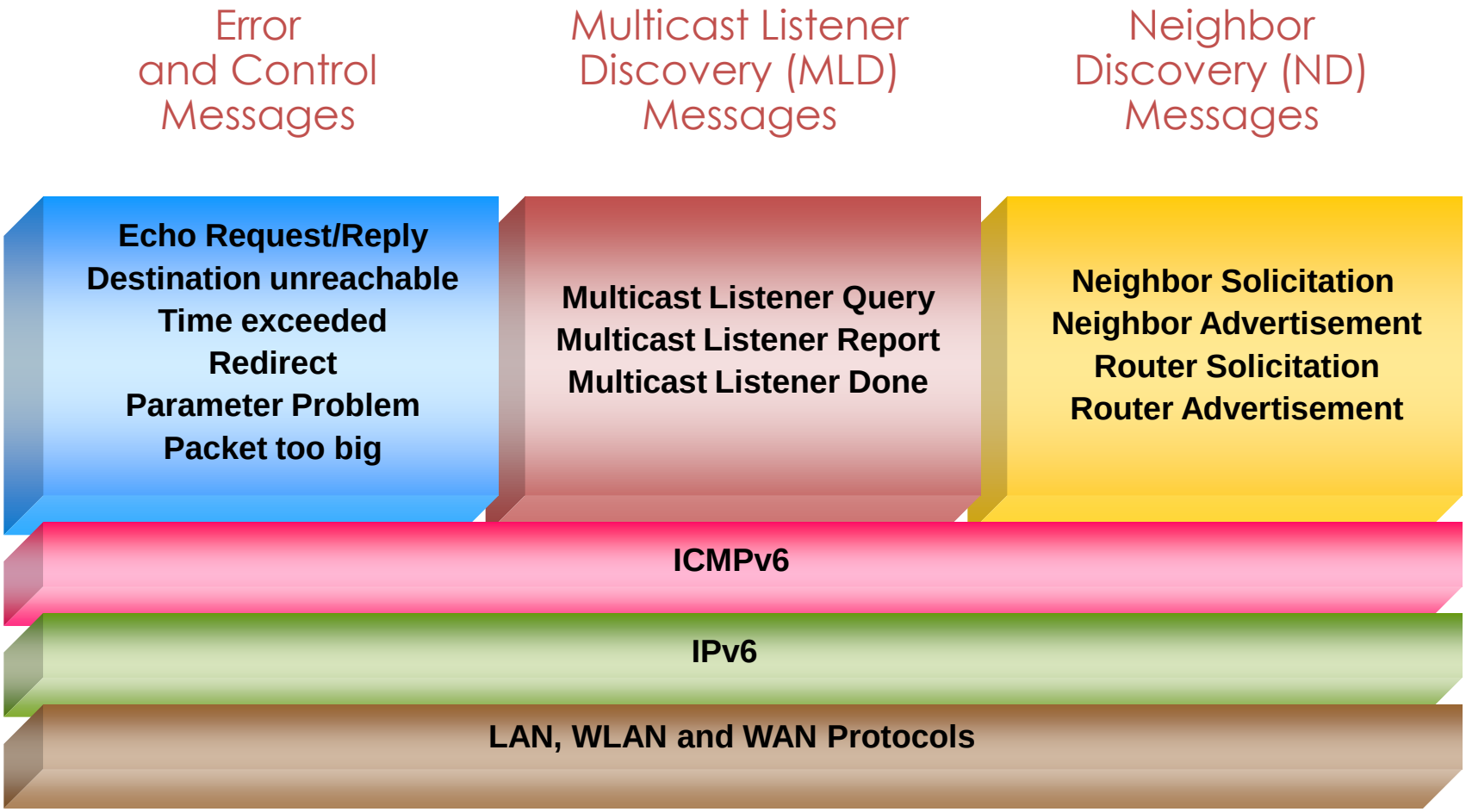
TCP/IP Protocol Family

Dual stack implementation



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

ICMPv6 Messages

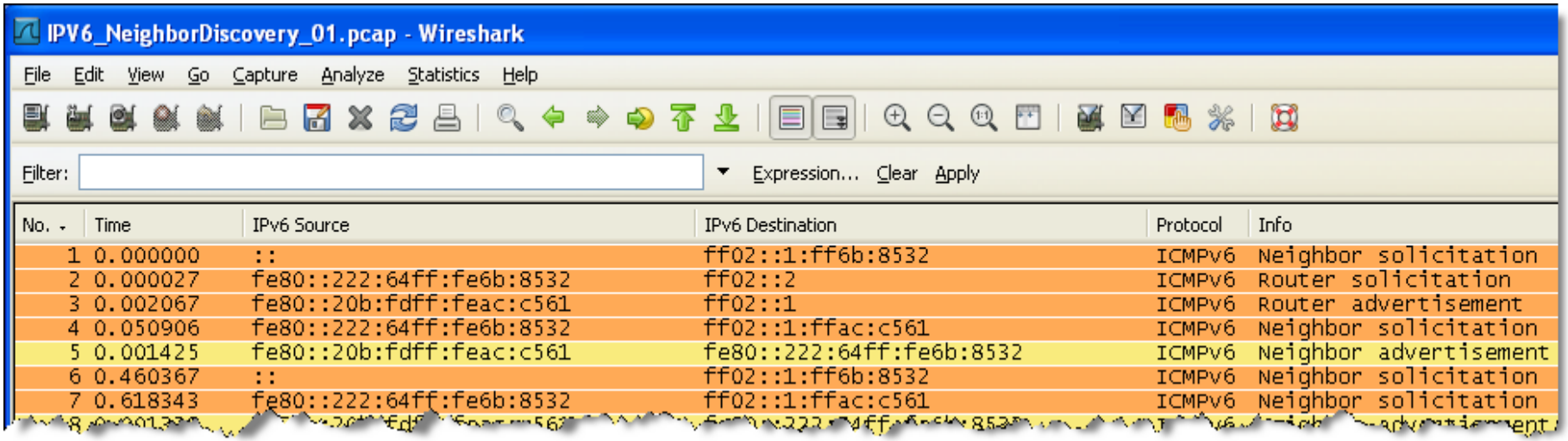


Neighbor Discovery (ND)

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



Agenda

- Address Autoconfiguration
- Neighbor discovery, Router discovery
- Host configuration with DHCPv6
- New DNS AAAA record
- Transition technologies, 6rd 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.

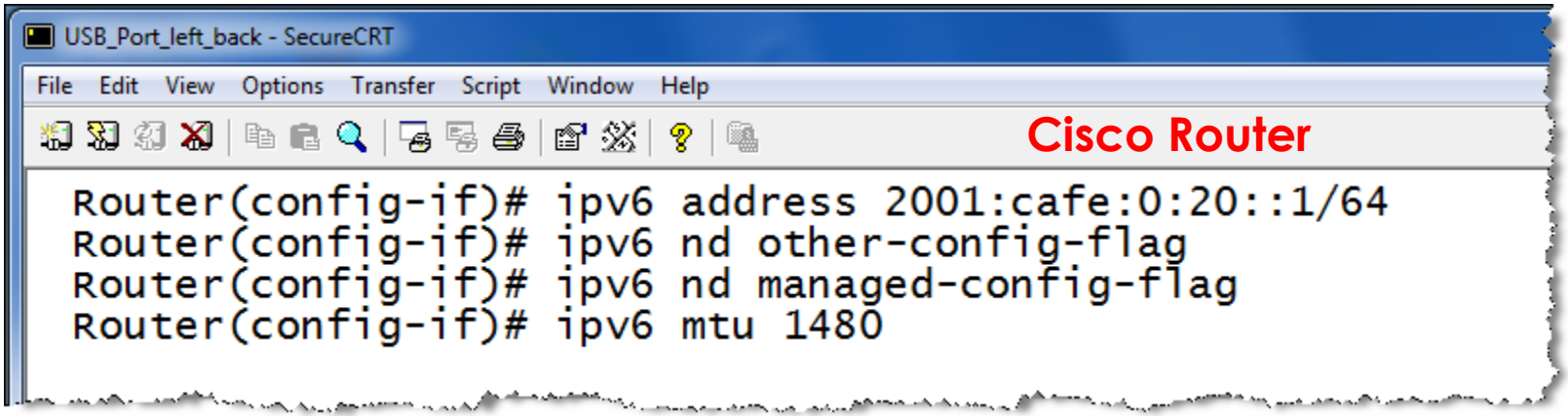
DHCPv6 offers different level of control over the workstations:

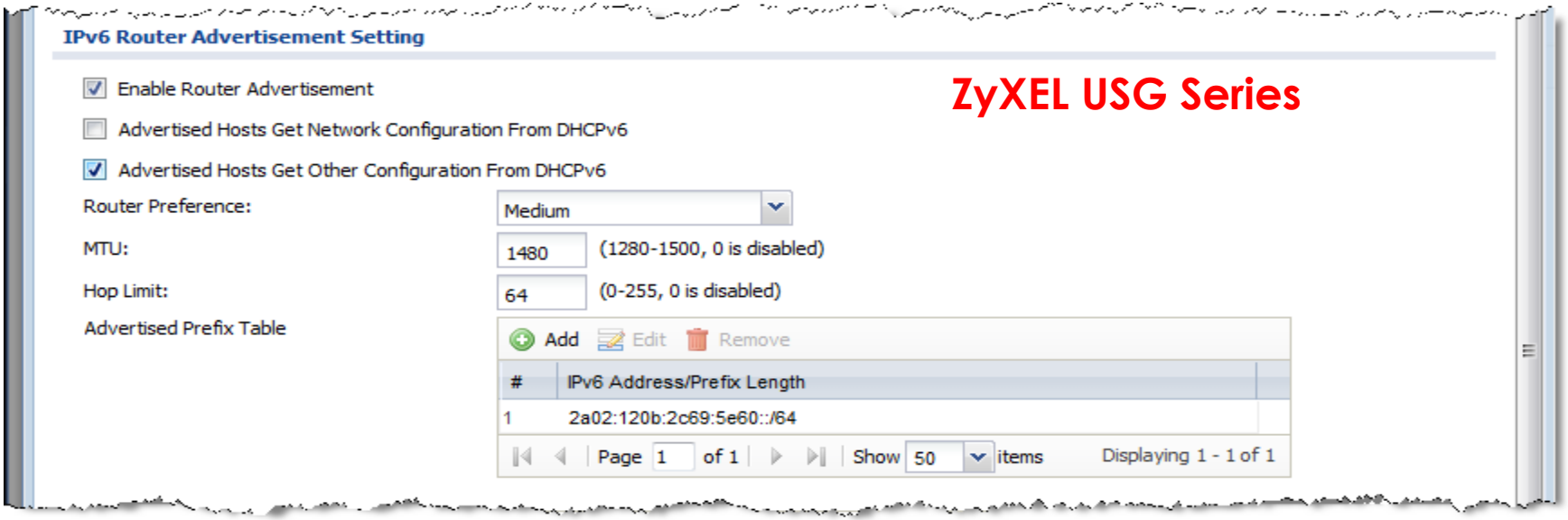
Client parameters	Stateless Auto Address Config. RFC2462	Stateless DHCP Service for IPv6 RFC3736	Stateful DHCPv6 RFC3315
Subnet Prefix & Mask	From Router Advertisements (O-Flag=0 M-Flag=0)	From Router Advertisements (O-Flag=1 / M-Flag=0)	From Router Advertisements (O-Flag=1 / M-Flag=1)
Interface Identifier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

Router Configuration Examples:



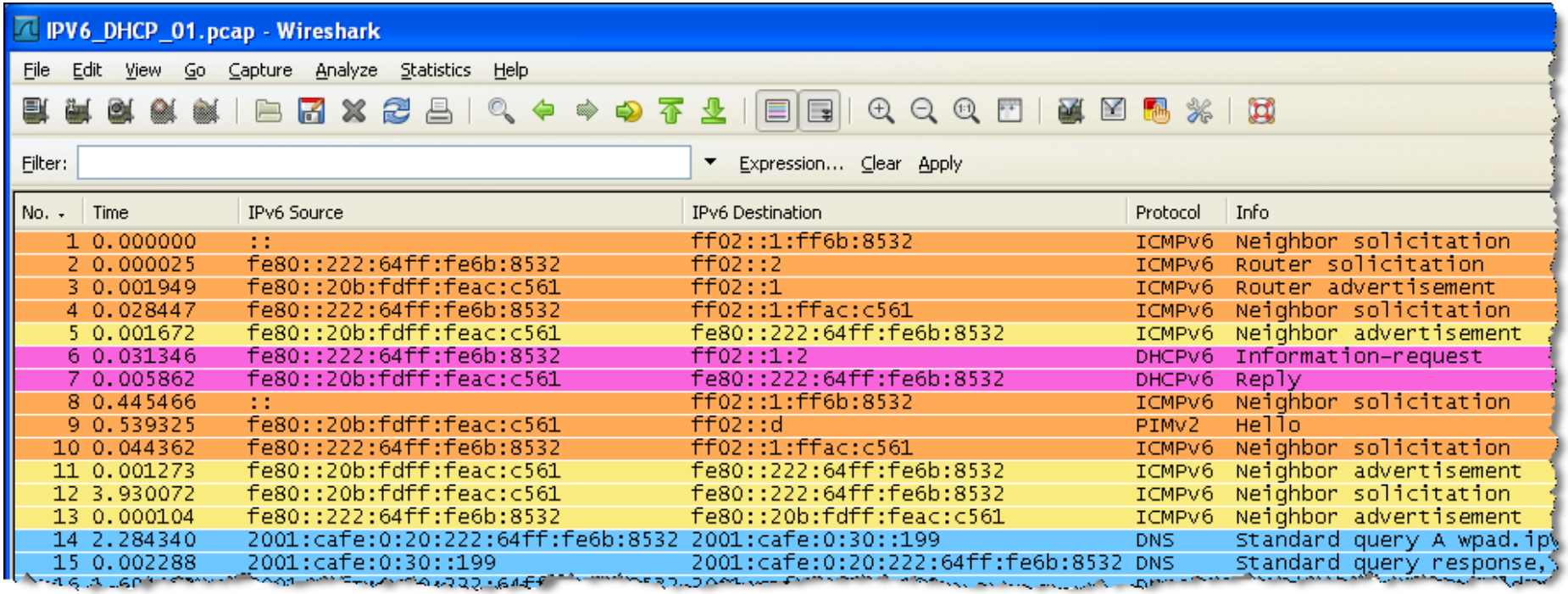


Host configuration with DHCPv6

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

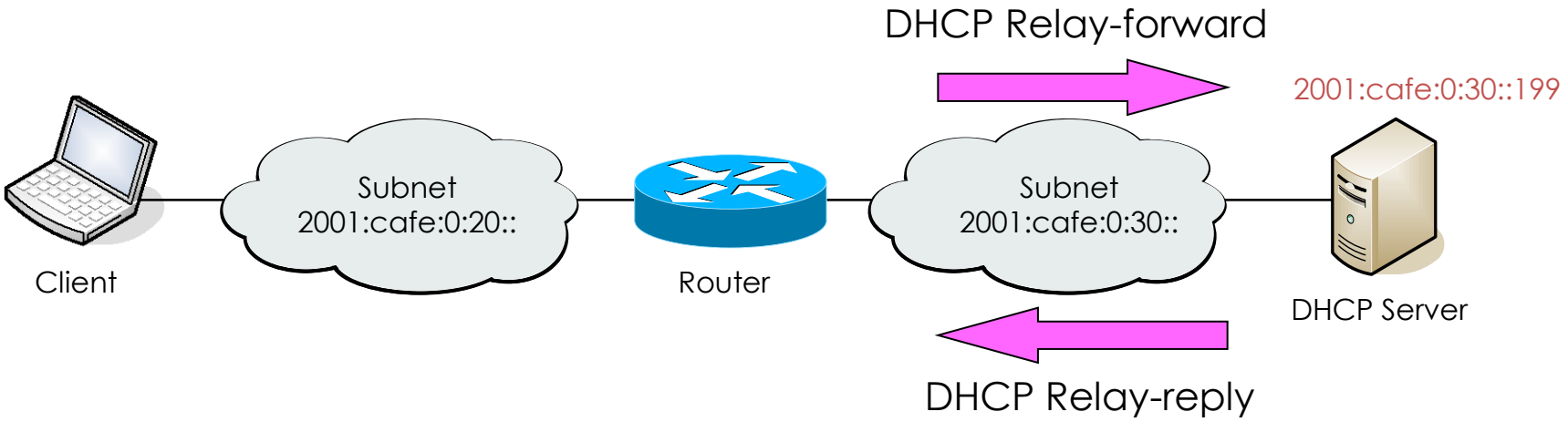
Frame #

- 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.



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



IPV6_DHCP_Relay_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	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
```

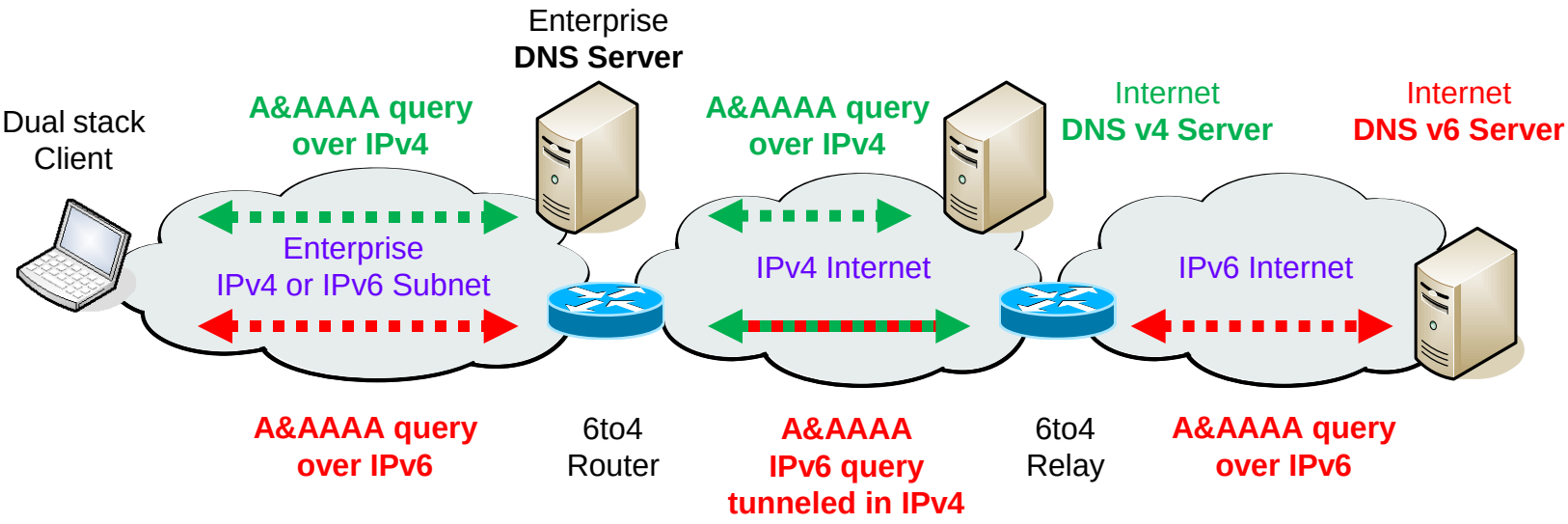
Agenda

- Address Autoconfiguration
- Neighbor discovery, Router discovery
- Host configuration with DHCPv6
- New DNS AAAA record
- Transition technologies, 6rd Tunnel

IPv6 Domain Name System (DNS)

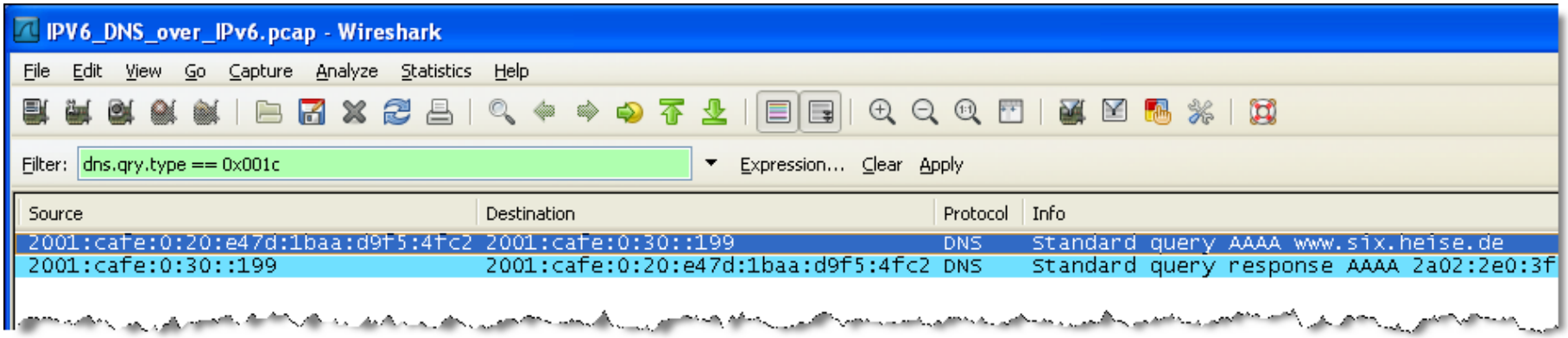
New AAAA resource record

- Due to the unhandy IPv6 address, DNS plays an important role in IPv6
- A new resource record type AAAA (called quad-A) has been defined
- During migration, DNS servers will support dual stack IPv4/IPv6
- IPv6 record queries and responses may be transmitted over IPv4 or IPv6

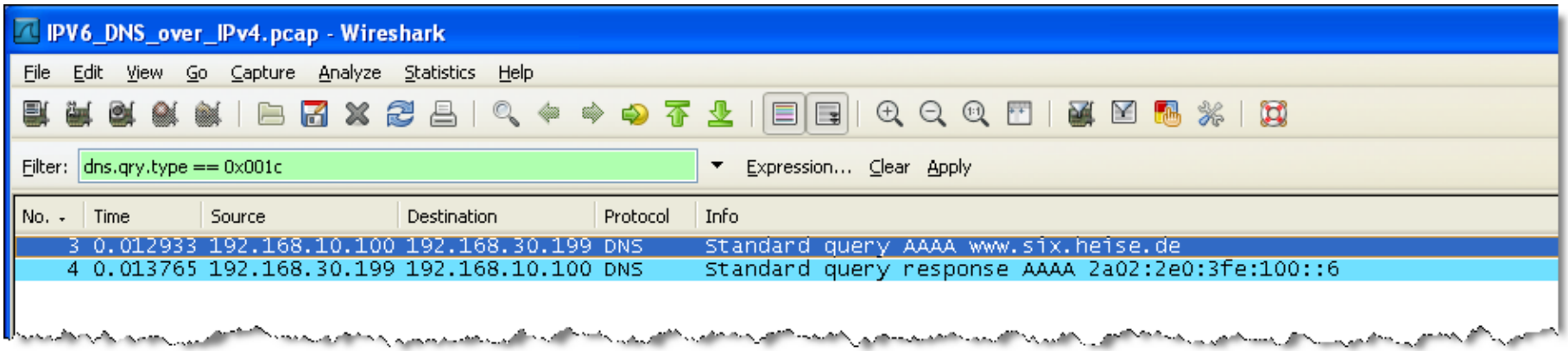


IPv6 Domain Name System (DNS)

- A & AAAA record query & response over IPv6 transport



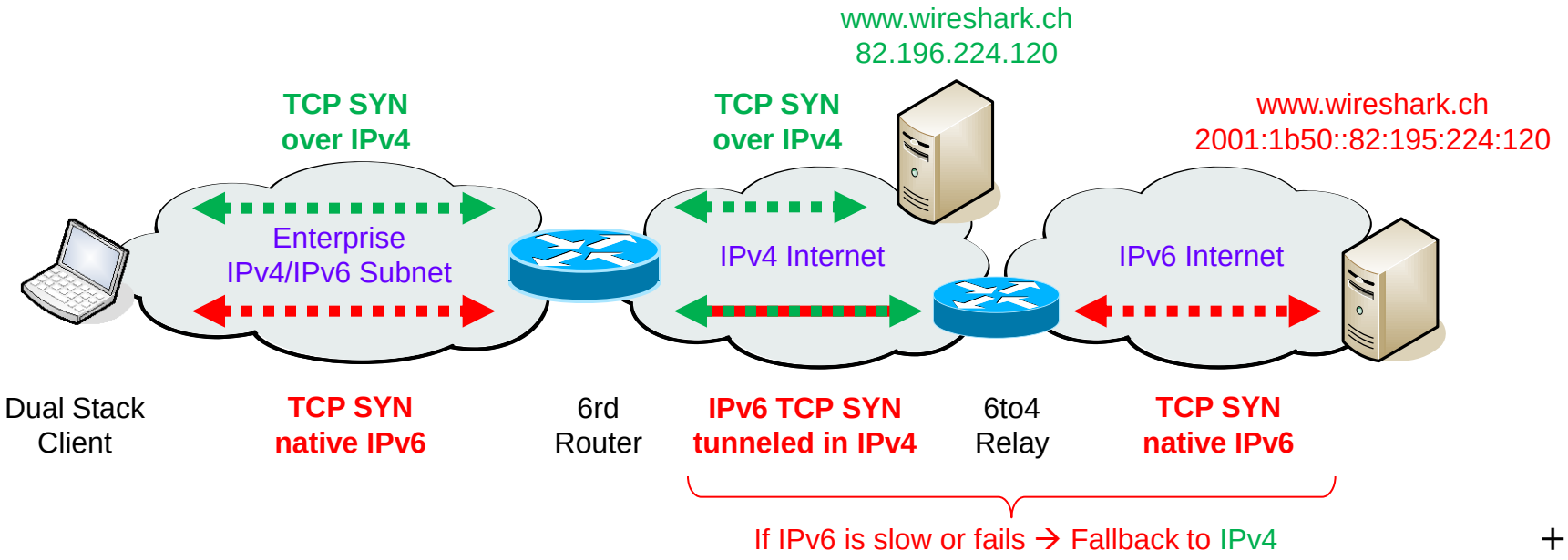
- A & AAAA record query & response over IPv4 transport



IPv6 Domain Name System (DNS)

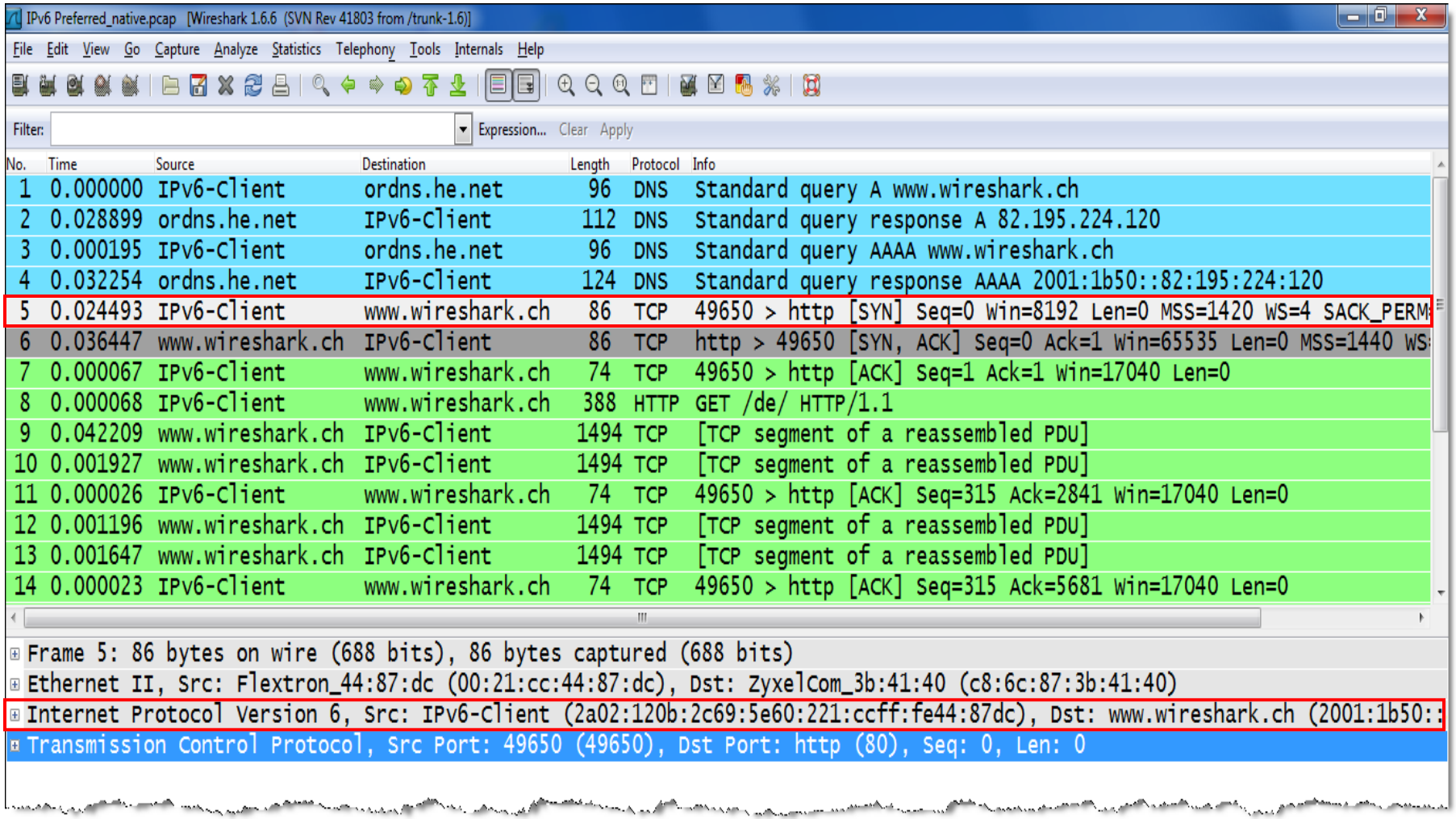
How to force the Client to use IPv6 protocol

- If a global IPv6 address is provided, most newer OSs prefer IPv6 over IPv4
- Some content providers use a separate namespace (www.six.heise.de)
- Newer Browsers will try to resolve A and AAAA record of an URI
- If an A and an AAAA record is available, IPv6 will be preferred
- Happy Eyeball (RFC6555) solves problem with slow fallback if IPv6 fails



IPv6 Domain Name System (DNS)

IPv6 preferred before IPv4 (WIN7 Client with Firefox 12.0)



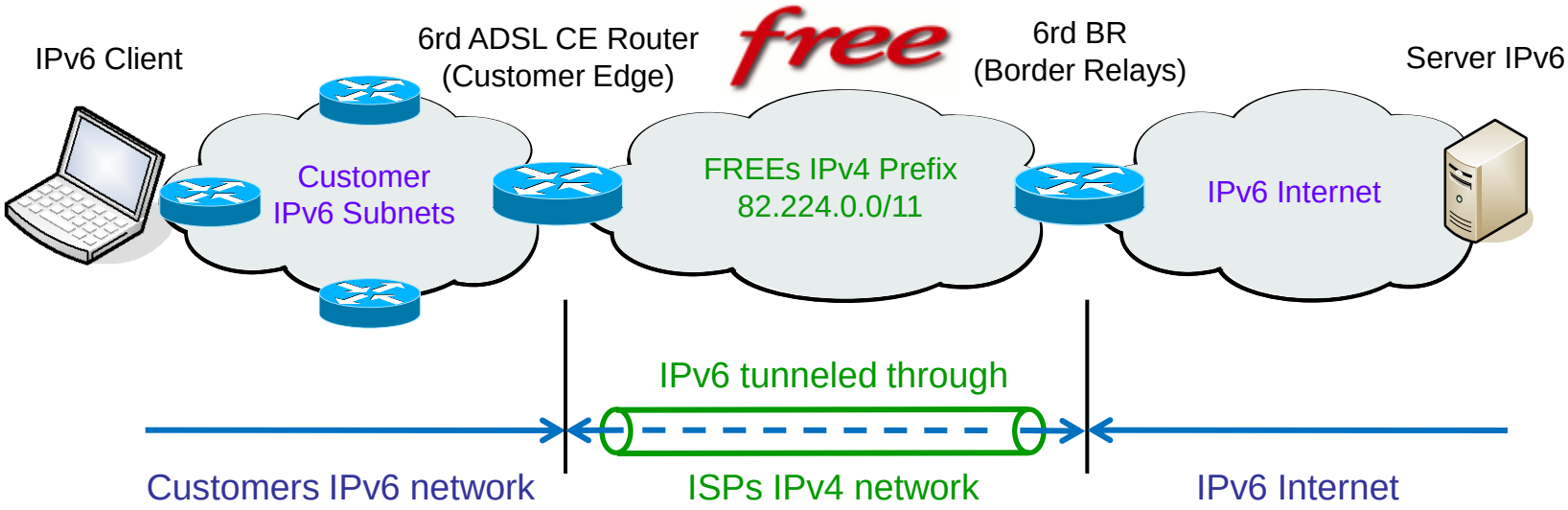
Agenda

- Address Autoconfiguration
- Neighbor discovery, Router discovery
- Host configuration with DHCPv6
- New DNS AAAA record
- Transition technologies, 6rd Tunnel

Transition Technologies, 6rd

6rd Rapid Deployment Tunnel

- Named after inventor Remi Despres / France
- First deployed by large French ISP ***FREE*** within 5 weeks in 2007
- 6rd does NOT use the 6to4 global address prefix 2002:WWXX:YYZZ::/48
- Uses IPv6 prefix provided by ISP instead (i.e. Swisscom 2a02:1200::/28)
- Minimal changes on ISPs IPv4 infrastructure

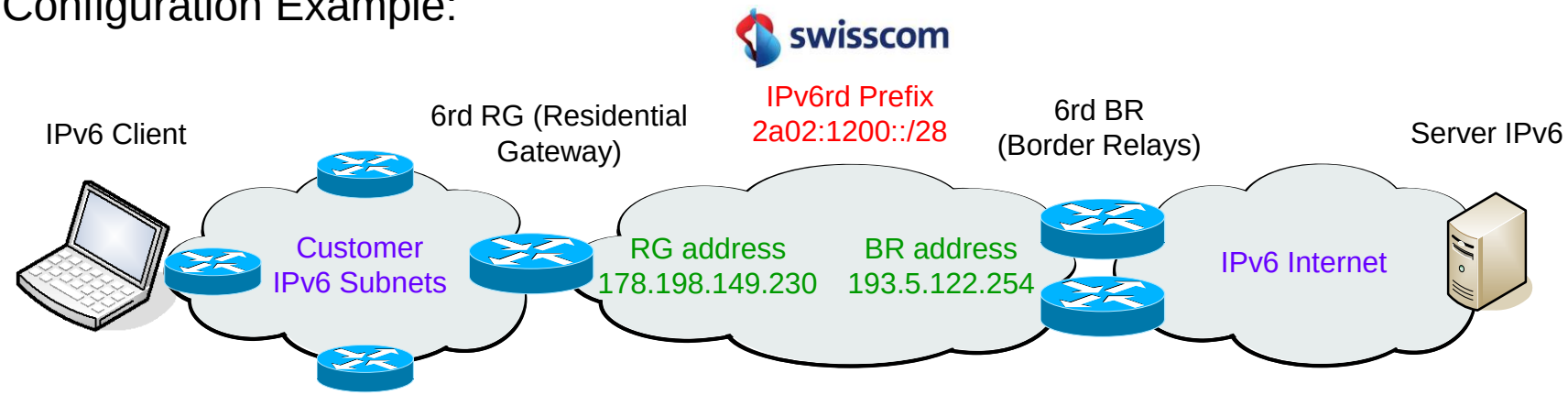


Transition Technologies, 6rd

6rd Rapid Deployment Tunnel

- Swisscom is providing public IPv4 address to Residential Gateway (RG)
- Swisscom is using IPv4 anycast address 193.5.122.254 for 6rd Border Relays
- Border Relays are stateless, traffic flow through any BR in both directions
- Works with global IPv4 and NAT44 addresses in customers network

Configuration Example:

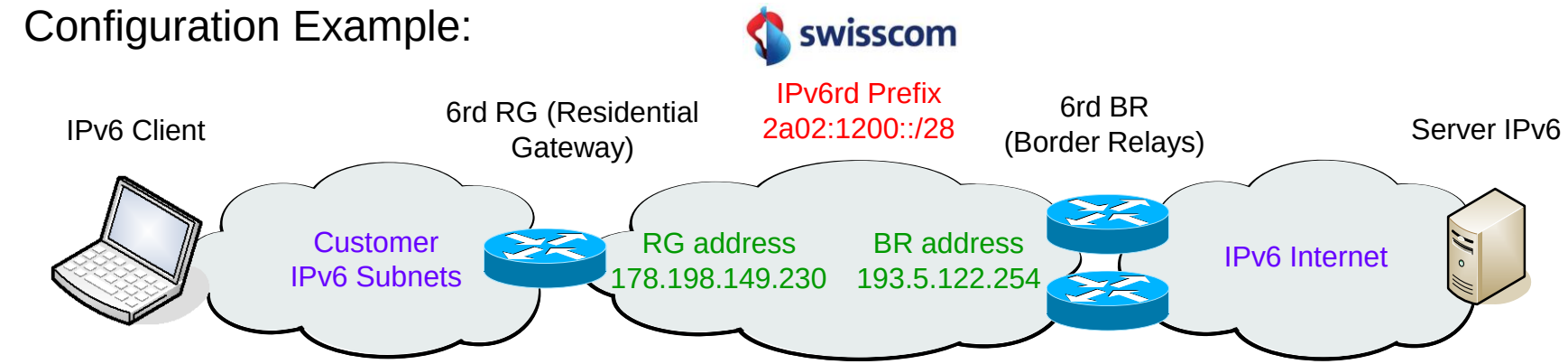


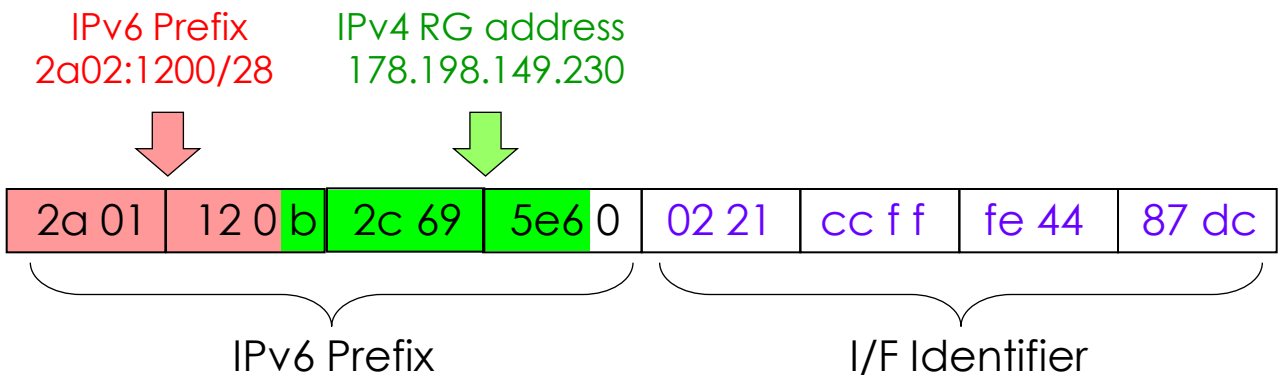
Transition Technologies, 6rd

6rd Rapid Deployment Tunnel

- IPv6 Client derives prefix from Swisscoms IPv6 and IPv4 prefixes

Configuration Example:



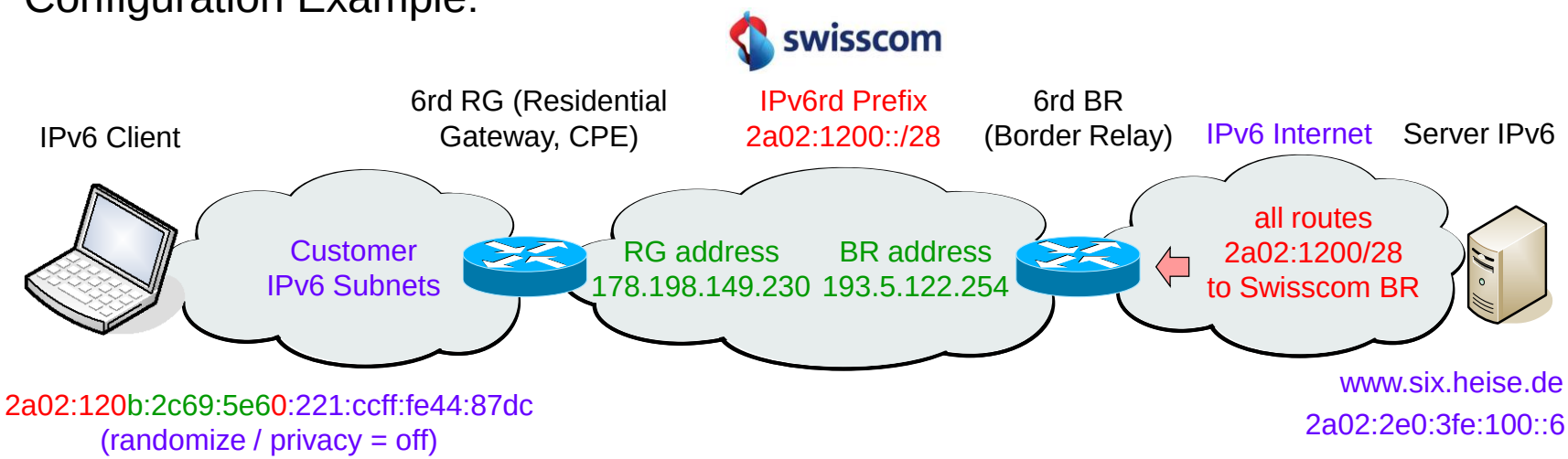


Transition Technologies, 6rd

6rd Rapid Deployment Tunnel

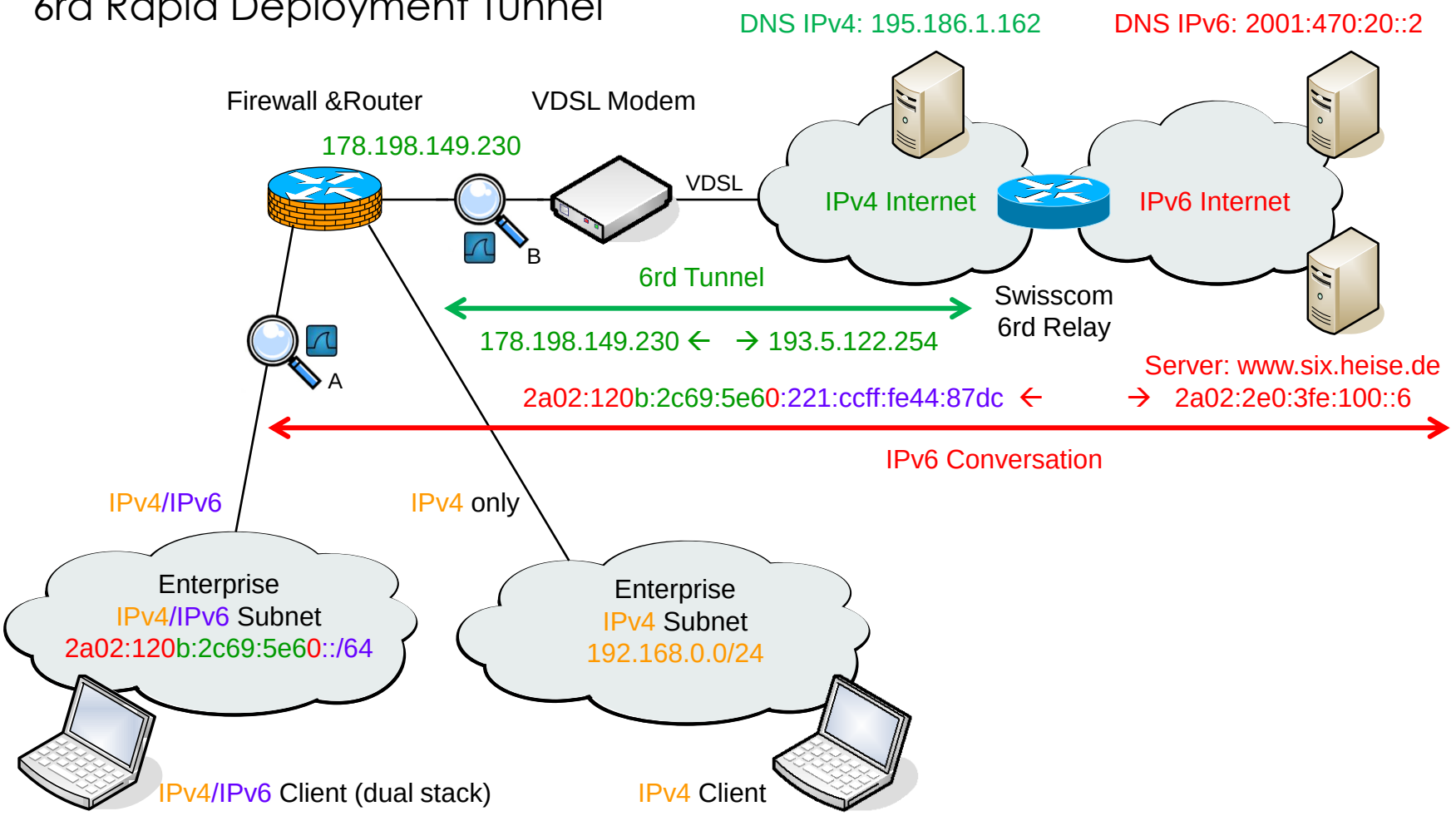
- Easy and fast deployments for ISPs
- Simple, stateless, automatic IPv6-in-IPv4 encap and decap functions
- IPv6 traffic automatically follows IPv4 Routing between CPE and BR
- From Swisscom offered as IPv6 Service (Pilot, today ~22'000 customers)
- Provides native IPv6 access to home user

Configuration Example:



Transition Technologies, 6rd

6rd Rapid Deployment Tunnel

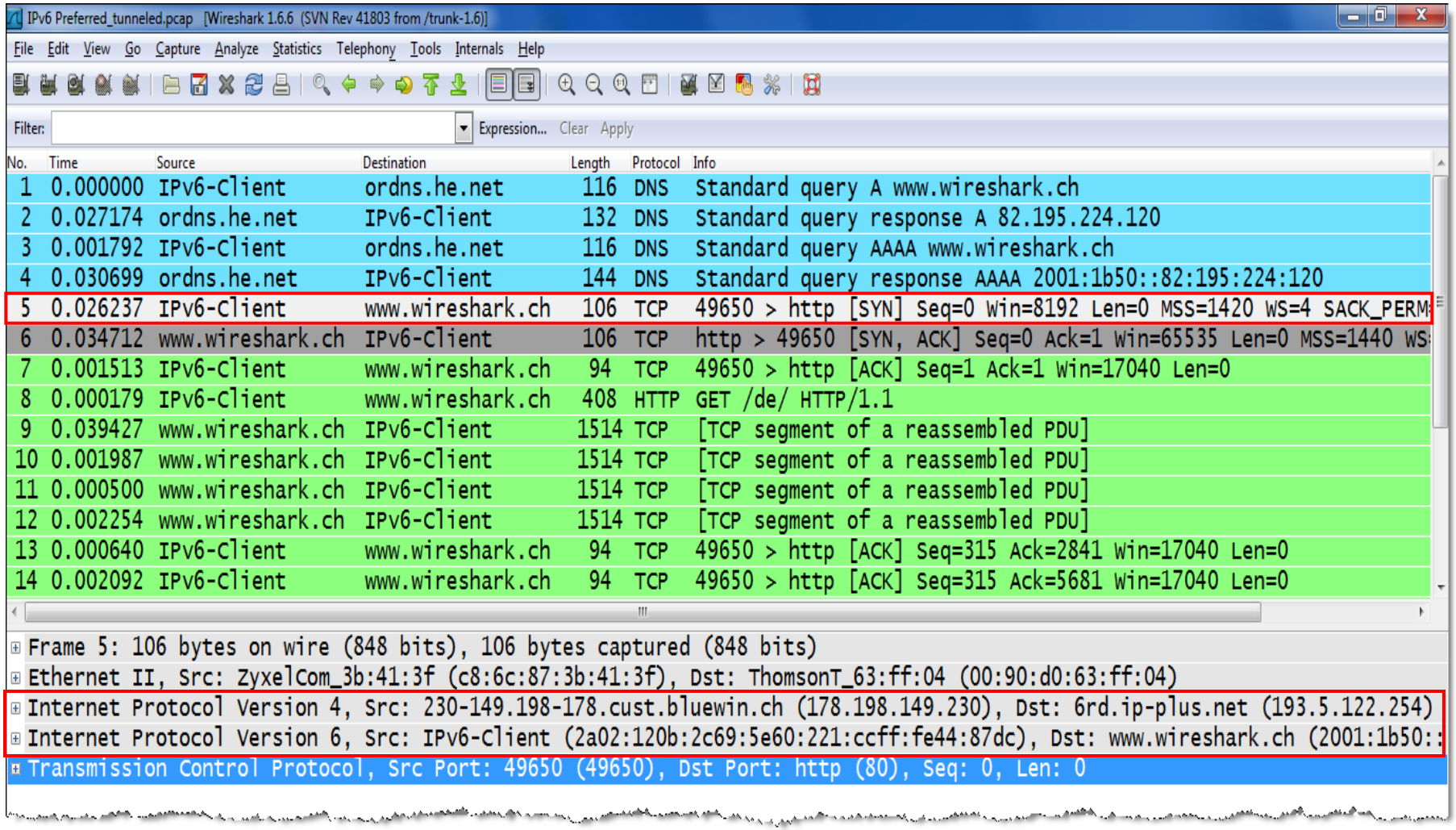


2a02:120b:2c69:5e60:221:ccff:fe44:87dc
(randomize / privacy = off)

Swisscom Präfix: 2a02:1200::/28
6rd Relay: 6rd.swisscom.com 193.5.122.254

Transition Technologies, 6rd

6rd Rapid Deployment Tunnel



IPv6 Session Summary

- Verify IPv6 readiness of your suppliers
- Verify IPv6 readiness of your applications
- IPv6 can perfectly coexist with IPv4
- Start experimenting using 6rd Tunnel
- Network migration can be done smoothly
- Train yourself and your people
- Wireshark is the perfect tool to learn and train
- Interesting IPv6 references:

How to get

www.worldipv6launch.org Organized by the Internet Society, World IPv6 Launch on 6 June 2012 is intended to motivate organizations across the industry to prepare for and permanently enable Internet Protocol version 6.

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

Our Trainings

NET-Analysis with Wireshark

2 days introduction to Network Analysis using Wireshark. A perfect quick start and overview of Wireshark's almost unlimited possibilities for troubleshooting and analysing problems in TCP/IP, WLAN, VoIP network.

WLAN Wireshark Network Analyser Training

3 days training providing in-depth knowledge and skills in WLAN 802.11a/b/g/n technology, analysing and troubleshooting problems using the Wireshark® network analyser and AirPcap USB WLAN Adapters.

TCP/IP Wireshark Network Analyser Training

3 days training providing in-depth knowledge and skills in TCP/IP network technology, analysing and troubleshooting problems using the Wireshark® network analyser. Covering also all important new features of TCP like Window Scaling, Selective Acknowledges, Time Stamp, Checksum & Chimney offloading, Win7 Auto tuning, Wireshark TCP Expert System & TCP Graph and many more.

VoIP Wireshark Network Analyser Training

2 days hands-on training analysing most popular VoIP protocols like Session Initiation Protocol (SIP), H.323 Protocol, Session Description Protocol (SDP), Skinny Client Control Protocol (SCCP), Real-time Transport Protocol (RTP), RTP Control Protocol (RTCP), Megaco/H.248 Gateway Control Protocol, Media Gateway Control Protocol (MGCP) using the Wireshark® network analyser.

IPv6 Wireshark Network Analyser Training

2 days training providing in-depth knowledge and skills in IPv6 network technology, analyzing and troubleshooting protocols & processes like "Automatic Address Configuration", "Neighbor & Router Discovery", "Multicast Listener Discovery" , Tunnelling Methods ISATAP, Teredo, 6to4, 6rd etc.

In-house Wireshark Training

If you need to train more than 4 students, please ask for customized in-house and onsite courses. All training are provided by highly experienced and certified network professionals from Leutert NetServices in English and German. Please ask for an offer through info@wireshark.ch

Our complete list of trainings & locations on http://www.wireshark.ch/de/wireshark-kurse/oeffentliche-kurse

Thanks for visiting

Rolf Leutert, Leutert NetServices, www.wireshark.ch