DENOG
German Network Operators Group

ERNW
providing security.

Reliable & Secure DHCPv6

Christopher Werny

cwerny@ernw.de

Who I Am

- Network/IPv6 geek of vendor independent network consulting & security assessment company ERNW.
  - 42 members of staff.
  - Mainly serving global enterprise orgs.
- Involved with IPv6 since 2007 and regularly blogging at www.insinuator.net.
- Host of annual **Troopers IPv6 Security Summit**.

Disclaimer

- There will be some unpleasant truths/news in this talk.
- Please don‘t shoot the messenger.

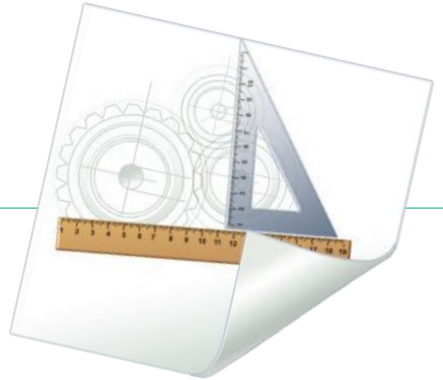
Agenda

In this talk it‘s all about DHCPv6

- How It Is Designed & Specified
  - Some Basics & Main Differences wrt v4
- How You Might Think (and Wish) It Worked
  - Expectations... & Frustrations
- How You Can still (somewhat) Succeed
  - Requirements re: Tech & Implementation
  - Requirements re: Organization & Processes

How It Is Designed & Specified

Some Basics

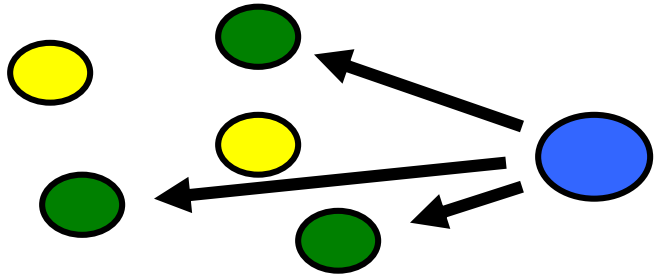


DHCPv6

- Specified (initially|mainly) in RFC 3315.
- Uses UDP Ports 546 (Clients) and 547 (Server/Relays).
- DHCPv6 uses multicast packets in IPv6.
- Clients/Server will be identified by:
  - DUID + IAID(s)
- Components of a DHCPv6 Infrastructure
  - DHCPv6 Clients
  - DHCPv6 Server
  - DHCPv6 Relay Agents

DHCPv6 Multicast Addresses

- All_DHCP_Relay_Agents_and_Servers (FF02::1:2)
  - A link-scoped multicast address used by a client to communicate with neighboring (i.e., on-link) relay agents and servers. All servers and relay agents are members of this multicast group.



- All_DHCP_Servers (FF05::1:3)
  - A site-scoped multicast address used by a relay agent to communicate with servers, either because the relay agent wants to send messages to all servers or because it does not know the unicast addresses of the servers.

DHCPv6 DUID

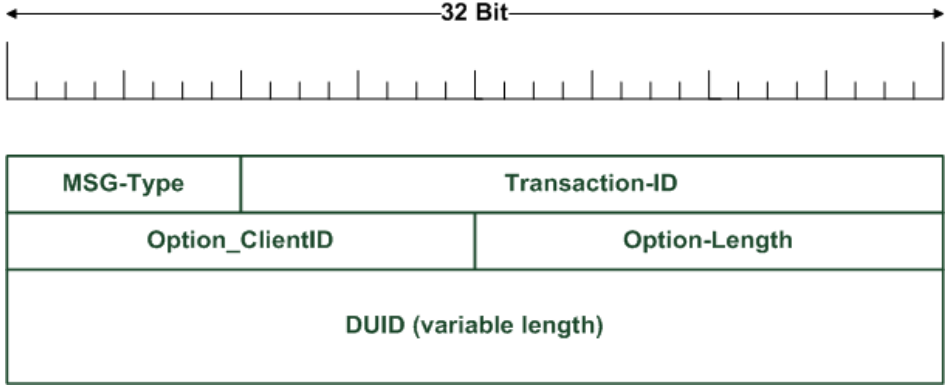
- DUID = DHCP Unique Identifier
  - Identifies Servers and Clients
  - Unique
  - Should not change (even if the NIC is changed)

  - **Methods to generate the DUID:**
  1. Based on the MAC address with a timestamp
  2. Static UID defined by the manufacturer based on an “Enterprise Number”
  3. Based on the MAC address
  4. DUID-UUID (RFC 6355)

- IAID = Identity Association Identifier
  - At least one per interface
  - Generated by the clients.
  - Does not change once DHCP client is rebooted.

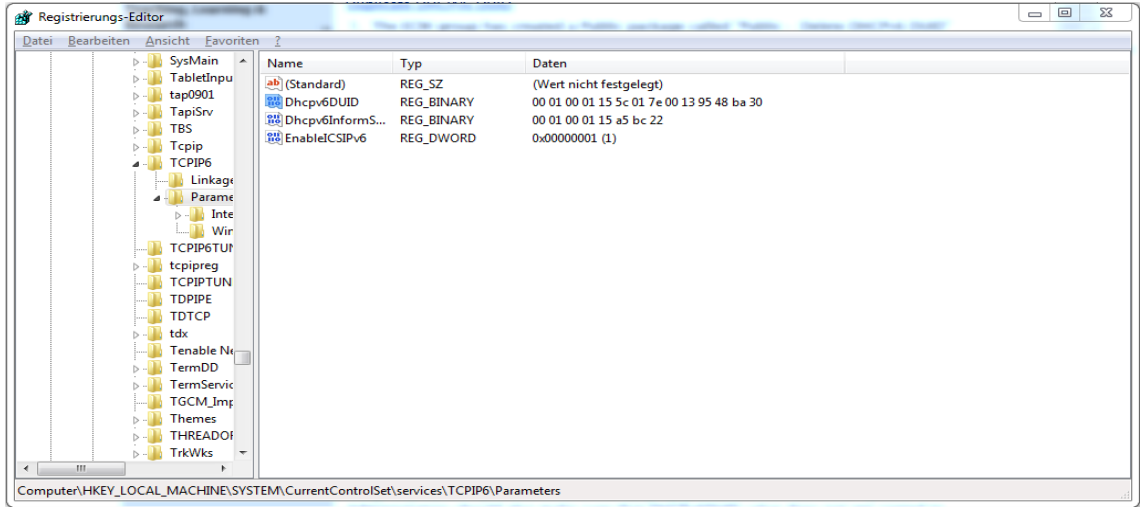
DUID – Overview

- DHCP Unique Identifier (DUID)
  - Specified in RFC 3315
  - Identifies each DHCP client and each DHCP server
    - Client: identify server messages
    - Server: identify clients for selection of configuration parameters
  - DUID is carried in the option fields of DHCPv6 and may be of variable length.



DUID - Windows

- Windows 7
  - Default type code 1 (“Link-layer address plus time”)



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Dhcpv6DUID

DUID - Linux

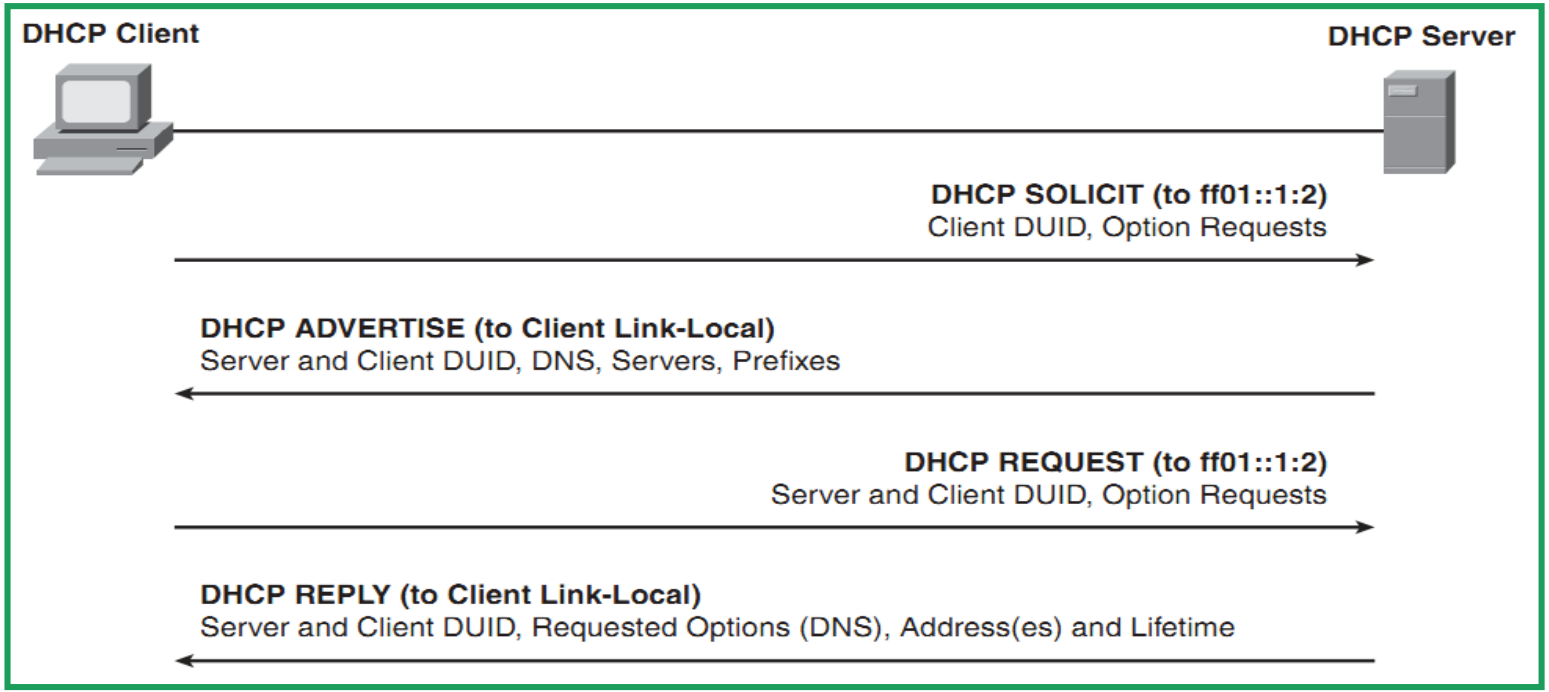
- Linux
  - Mostly type code 1 (“Link-layer address plus time”)
  - Generated when the DHCPv6 client is installed and stored in /var/lib/dhcpv6/dhcp6c_duid

```
root@test:/# hexdump -C /var/lib/dhcpv6/dhcp6c_duid
00000000  0e 00 00 01 00 01 16 66  7e 75 00 0c 95 48 ba 30  |.......f~u...H.0|
00000010
root@test:/#
```

DHCPv6 Message Types

DHCPv6 Message Type	DHCPv4 Message Type
SOLICIT (1)	DHCPDISCOVER
ADVERTISE (2)	DHCPOFFER
REQUEST (3), RENEW (5), REBIND (6)	DHCPREQUEST
REPLY (7)	DHCPACK/DHCPNAK
RELEASE (8)	DHCPRELEASE
INFORMATION-REQUEST (11)	DHCPINFORM
DECLINE(9)	DHCPDECLINE
CONFIRM (4)	- No equivalent -
RECONFIGURE (10)	DHCPFORCERENEW
RELAY-FORW (12), RELAY REPLY (13)	- No equivalent -

DHCP Message Exchange ["M-Flag Variant"]

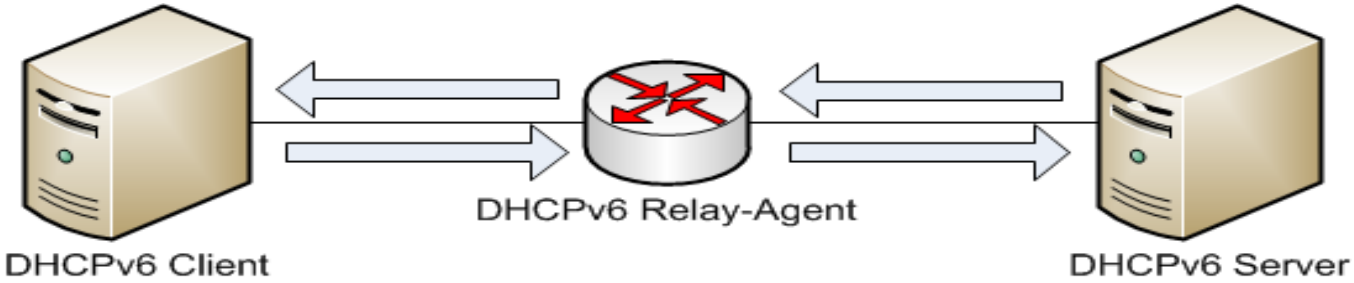


Message Types in DHCPv6

- SOLICIT
  - A client sends a Solicit message to locate servers.
- ADVERTISE
  - A server sends an Advertise message to indicate that it is available for DHCP service, in response to a Solicit message received from a client.
- REQUEST
  - A client sends a Request message to request configuration parameters, including IP addresses, from a specific server.
- REPLY
  - A server sends a Reply message containing assigned addresses and configuration parameters in response to a Solicit, Request, Renew, Rebind message received from a client.

DHCPv6 – Relay-Agents

- Primary Role of the “Relay-Agent” is the forwarding of DHCP Messages if client and server are in different subnets.
  - Works across multiple hops.



Main Differences

On the Protocol Level

- There is no “route option“ in DHCPv6
- Concept of DUID
- The (Non-) Role of DHCPv6 in IPv6‘s “Subnet Model“ (RFC 5942)

Differences (I)

There Is no *Route Option*

- And I doubt there will ever be one. Nuff said.
- From an architecture perspective this means that – at least in routed networks ;-) – something else is needed to (further) provision the nodes.
- Ofc, this has some impact on operations.
  - Do not underestimate this.
  - Do not! More on this later.

Differences (II)

The Concept of DUID

- In scenarios with DHCPv6 relaying (read: in all large networks) DHCPv6 server doesn‘t get to see a client‘s MAC address anymore.
- Again, this has huge operational implications in many networks
  - Reservations no longer possible.
  - Some types of “poor man‘s access control“ no longer possible/feasible.
  - Correlation of IPv4 & IPv6 addresses via MAC address can‘t be done.
- There is a “cure“ (RFC 6939) but that‘s not (yet) widely supported. Again, more on this later.

Differences (III)

The (Non-) Role in the Subnet Model

See also:

- Technically this means that DHCPv6 addresses don‘t have their “on-link“ flag set.
  - “I don‘t have any neighbors“.
- This has *huge* operational implications.
  - Actually this might be the biggest, yet widely underestimated protocol difference of all.
  - It‘s one of my favorite picks for “why & where IPv6 is different from v4“.
  - Its main impact/property is, let‘s say: inconspicuousness.
  - Again, a more detailed discussion tbd below.

Differences

Here‘s another one not to strictly blame on the protocol itself.

- (Informational) RFC 6434 IPv6 Node Requirements, sect. 5.9.5:
  - “[A]ll hosts SHOULD implement address configuration via DHCPv6.”
- For the record, RFC 2119 states:
  - “SHOULD This word[…] mean[s] that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.”

DHCPv6 Support by OSs

~~What could possibly go wrong?~~ Who could possibly deviate?

https://code.google.com/p/android/issues/detail?id=32621

- “Marking [Support for DHCPv6] declined until there is a compelling use case.
  - -- Lorenzo Colitti (Google) on Dec 07 2014
  - See also: http://mailman.nanog.org/pipermail/nanog/2015-June/thread.html#75916
- → No DHCPv6 on Android
  - Except for the *Fairphone.*
- There are people who expect that Android is going to be one of the major OS for #IoT...

Ok, ok, but still…

- Once we‘ve understood those pesky technical differences AND all our – current – nodes support DHCPv6, we‘re good to go, right?

  [read: implement the same provisioning & operations model as in our IPv4 networks]

- Well, unfortunately... no.

Once upon a Time

When our ancestors did the initial specs of IPv6

- They had a certain place for DHCPv6 in mind, within the IPv6 universe.
- This happened to be a very different role from the (at the time developing) role of DHCP in IPv4.
- Tell you what: this is going to haunt you.

What Do You Mean?

Can you please elude?

- DHCPv4 was meant to be *exclusive*.
  - Either configure basic IPv4 properties manually *or* get the stuff from DHCPv4.
  - Once DHCPv4 is used, it‘s used for everything.
- DHCPv6 is meant to be *complementary*.
  - It can (and must) be mixed with other spicy stuff.
  - Add some #RFCambiguity to the mix.
- To fully understand what this means, let‘s step back one step and look at...

How You Might Think (and Wish) It Worked

Expectations... & Frustrations

Expectations wrt DHCP

Conscious ones & unconscious ones

From an architecture perspective

- It shall be the one+only parameter provisioning system.
  - Thou shall not get any information from other sources.
- It‘s fully able to fill this role as it‘s able to provision everything that‘s needed.
- In an ideal environment, we can run it in a centralized way, by $IT_OPS team.
  - Feel free to replace $IT_OPS by $OUTSOURCING_PARTNER.

Expectations (II)

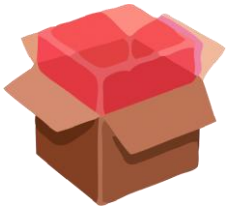
- It‘s independent.
  - Thou shall not rely on something else.
  - Except for a working network, maybe.

- It‘s predictable.
  - It behaves in a certain way, usually.

Expectations (III)

Some technical odds and ends

- We can force a node to (mostly only) use DHCPv6 with reasonable operational effort.
  - I mean that‘s the way it worked in DHCPv4 anyway.



- We can prevent hosts from receiving false/rogue DHCP information with reasonable effort.
  - In IPv4 that‘s easy – use *DHCP Snooping* on switches.

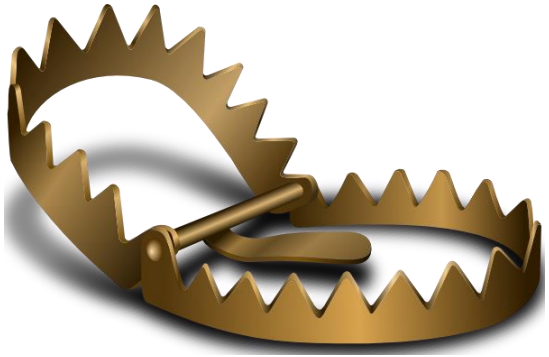
Overall, in some Heads there is this One

In the course of their IPv4 → IPv6 transition efforts.

- We can use and operate DHCPv6 in pretty much the same way we did it with DHCPv4.
- At this point in this presentation it should be obvious that this is *not* the case.
- Still let‘s have a closer look at the expectations.

Expectations & Frustrations (I)

- It shall be the one+only parameter provisioning system.

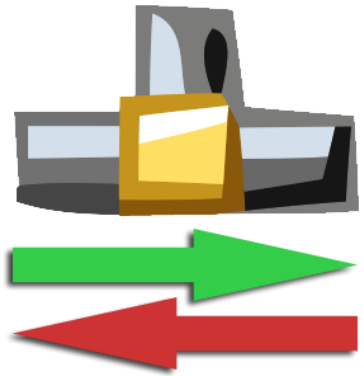


- In IPv6 it *can‘t*.
  - That‘s simply not the IPv6 approach. Nodes are supposed to have multiple addresses, from multiple sources, anyway.
  - And there‘s this (lack of) *route option* thing.

Expectations & Frustrations (II)

- “It‘s able to fill this role as it‘s able to provision everything that‘s needed.“
- In IPv6 it *can‘t*.
  - See above.

Expectations & Frustrations (III)

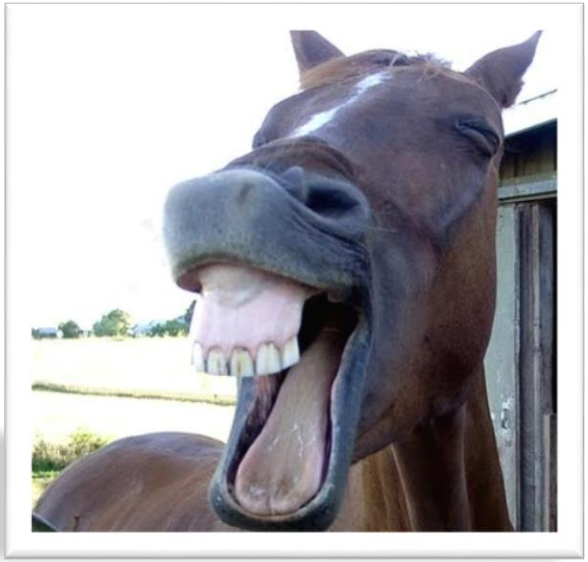


- In an ideal corp world, we can run it in a centralized way.
- You can do that, but it will not deliver properly as long as you don‘t control all L3 devices, of all networks, where DHCPv6 comes into play.
  - Incl. the rogue ones, of course.
- This can be a tough one.
  - How many subsidiaries/offices do you have where the network devices are operated by $SOME_OTHER_PARTY than DHCP?

Expectations & Frustrations (IV)

- It‘s independent.
- The actual way DHCPv6 works (“managed” vs. “other“) – and if it comes into play at all – is determined by IPv6 router advertisements.
  - Well, at least for the majority of OSs. More on this later.

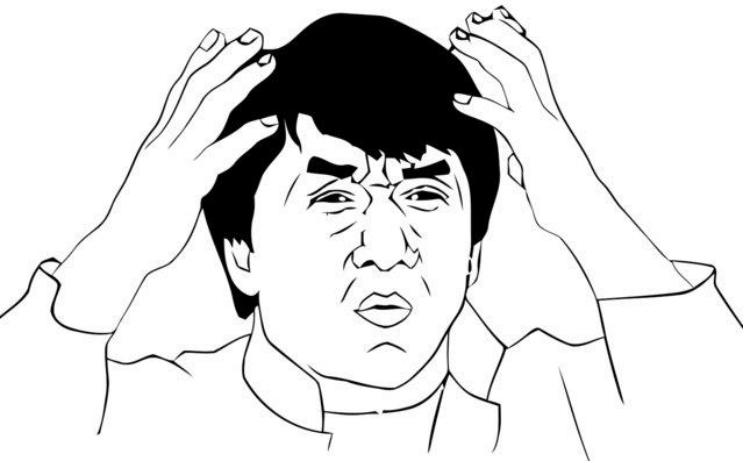
It‘s Predictable



- C‘mon. You don‘t expect any protocol interaction in the IPv6 world to be predictable (in a heterogeneous environment), do you?
- This was not to meant to be funny. Alas, I‘m serious here.

Seriously, how could you expect predictability out of this?

Not much RFC 2119 in there, is it?



- RFC 4862, 5.5.2 *Absence of Router Advertisements*
  - “Even if a link has no routers, the DHCPv6 service to obtain addresses may still be available, and hosts may want to use the service.”
- RFC 4862, 5.6 *Configuration Consistency*
  - “If the same configuration information is provided by multiple sources, the value of this information should be consistent.”
  - “In any case, if there is no security difference, the most recently obtained values SHOULD have precedence over information learned earlier.”

Reality Check

On *Predictability*

	Scenario	Collected Information	Windows 7	Windows 8.1	Ubuntu 14	Centos 7	Fedora 21	MAC OS-X
1	A=1, M=0, O=0 DHCPv6 present	IPv6 address	router	both	router	router	router	router
		RDNSS	-	DHCPv6	router	router	router	router
2	A=1, M=0, O=1 DHCPv6 present	IPv6 address	router	router	router	router	router	router
		RDNSS	DHCPv6	DHCPv6	router	router/DHCPv6	router/DHCPv6	DHCPv6/router
3	A=1, M=0, O=1 no DHCPv6 present	IPv6 address	router	router	router	router	router	router
		RDNSS	-	-	router	router	router	router
4	A=1, M=1,O=1 DHCPv6 present	IPv6 address	both	both	both	both	both	both
		RDNSS	DHCPv6	DHCPv6	router	router/DHCPv6	router/DHCPv6	DHCPv6/router
5	A=1, M=1,O=1 no DHCPv6 present	IPv6 address	router	router	router	router	router	router
		RDNSS	-	-	router	router	router	router
6	A=0, M=0, O=0 DHCPv6 present	IPv6 address	-	DHCPv6	-	-	-	-
		RDNSS	-	DHCPv6	router	router	router	Router

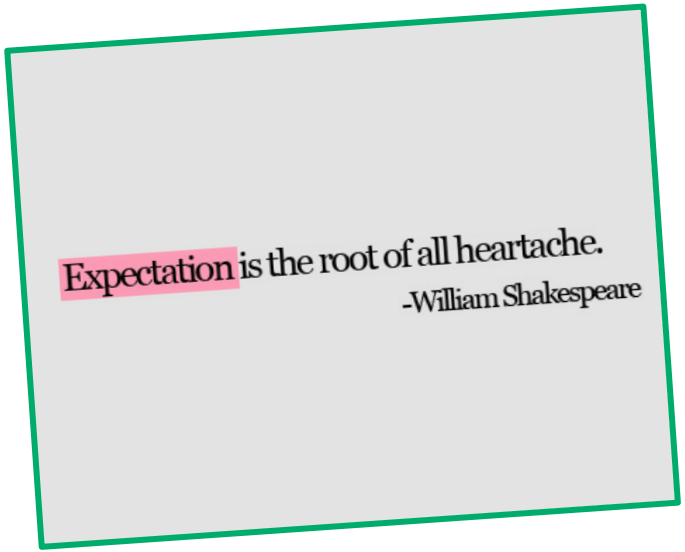
https://www.ernw.de/download/ERNW_Whitepaper_IPv6_RAs_RDNSS_DHCPv6_Conflicting_Parameters.pdf
https://tools.ietf.org/html/draft-ietf-v6ops-dhcpv6-slaac-problem-05

ERNW
providing security.

How You Can still (somewhat) Succeed

Let‘s look for solutions

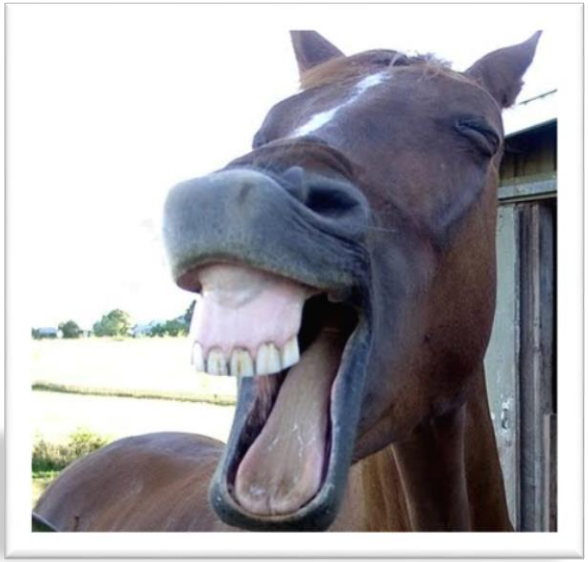
Quick Recap of Expectations



- One & only parameter provisioning system
- Provides everything that's needed
- Run it in a centralized way/control from one point
- Independent
- Predictable
- Imitation of DHCPv4 – Acting upon MAC address
- Imitation of DHCPv4 – Reservations
- Imitation of DHCPv4 – Local-link behavior
- Imitation of DHCPv4 – Prevent rogue players

DHCPv6 as the One & only Parameter Provisioning Source

Prerequisites on Org/Process Level



- Control *all* node-facing L3 devices involved
  - Routers incl. SOHO
  - Firewalls incl. SOHO

OR (at least)

- Make sure those all follow consistent configuration approach
  - Governance & guidance
  - In case network operations are outsourced include in contract, blueprints etc.

DHCPv6 as the One & only Parameter Provisioning Source

Technical Implementation

- Tweak router advertisements
  - Set M-flag, plus
  - Clear PIO OR
  - Clear A-flag
  - Keep in mind: clearing just PIO leaves on-link behavior (“don‘t have neighbors“) unsolved.
- Most probably you won‘t be able to achieve the goal on the node level
  - Can we configure nodes in a way so they consistently only process default route from RAs but do DHCPv6 for anything else?
    - Not as of OS behavior as of early 2015. See above.

DHCPv6 Provides Everything that's Needed

- All of the above.
  - PLUS (long-term strategy):
- Send people to IETF meetings (hint: 6man)…

Run it in a Centralized Way from one Point

- Nothing new here.
- Use IPAM system you already have or get a new one.
  - Large scale IPv6 without IPAM doesn‘t make sense.
  - Check IPv6 capabilities of $IPAM.
    - See also https://www.ernw.de/download/newsletter/ERNW_Newsletter_46_Evaluation_of_Commercial_IPAM_Solutions_IPv6_Capabilities.pdf

Independent

- Right now Win 8.1 seems the only major OS that does *not* need RAs trigger to perform DHCPv6.
  - See table above.
- From our perspective it‘s not clear if this is “allowed“ as of relevant RFCs.
  - Who cares anyway what‘s “allowed“...
- In short: most probably forget this!

Predictable

- Understand exact behavior of all node OS involved.
- Then try to tweak it
  - Windows registry, maybe.
  - `sysctl` parameters on Linux/Unix, maybe.
  - Did you just say you have smartphones?
- In short: most probably forget this!

Imitation of DHCPv4

In the end of the day you want DHCPv6 to do the same stuff as in IPv4 network, right?

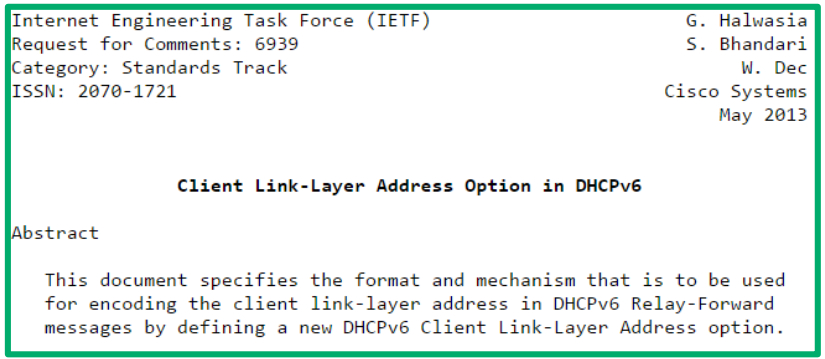
There‘re two main areas here:

- Stuff related to MAC address
  - Reservations
  - Logging
  - Correlation
  - Poor man‘s access control
- On-link behavior

Imitation of DHCPv4

Stuff related to client's MAC address

- RFC 6939 to the rescue
- Not yet widely supported
  - ISC DHCP since 4.3.1
    - → Probably all IPAM based on ISC as well, in their latest versions.
  - As relay
    - Cisco devices running IOS-XE do/have support by default.
    - Other vendors? Cisco IOS? → find out!



Internet Engineering Task Force (IETF) — G. Halwasia
Request for Comments: 6939 — S. Bhandari
Category: Standards Track — W. Dec
ISSN: 2070-1721 — Cisco Systems
May 2013

Client Link-Layer Address Option in DHCPv6

Abstract

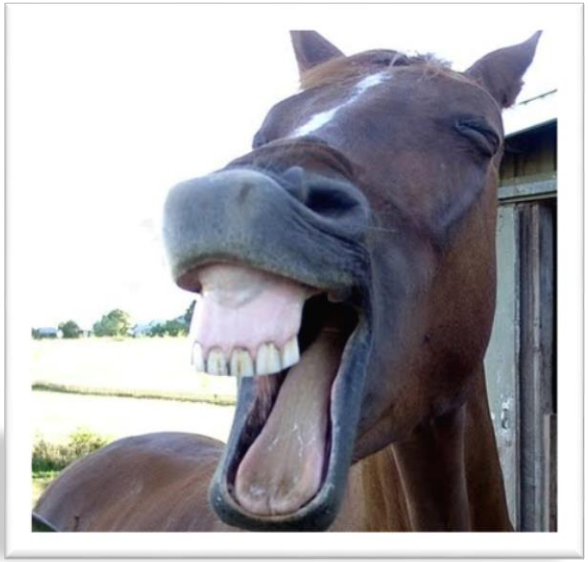
This document specifies the format and mechanism that is to be used for encoding the client link-layer address in DHCPv6 Relay-Forward messages by defining a new DHCPv6 Client Link-Layer Address option.

RFC 6939

http://www.insinuator.net/2015/02/is-rfc-6939-support-finally-here-checking-the-implementation-of-the-client-link-layer-address-option-in-dhcpv6/

Imitation of DHCPv4

Local-link behavior



- You can‘t force DHCPv6 provided addresses to have the on-link flag set.
  - You can not. See RFC 5942, sect. 3.
- But you can trick nodes into to a similar mode of operation.
  - If you don‘t (can‘t) do this trick (next slide) you have to rely on `ICMPv6 redirects`.
  - Which means a lot of fun with trouble-shooting then...

DHCPv4 like On-link Behavior

Let us know that trick.

- Let me paraphrase this for you first.
- Make sure the router(s) tell the nodes something along the lines of:
  - “Listen guys (nodes):
    here‘s some prefix information.
    You‘re not supposed to use this for address configuration (but we‘ll tell you nevertheless).
    However, you may keep this in mind to realize you‘re in an Ethernet environment.
    DHCPv6 forgot to tell you this – as it assumed you were RAS clients. I mean, who would ever use DHCPv6 over Ethernet, right?
  - Capisce?

DHCPv4 like On-link Behavior

Technical Implementation, Sample

- `Router(config-if)# ipv6 nd prefix 2001:db8:6:6::/64 2592000 86400 no-autoconfig`

- Of course, to implement this in a consistent way in your whole network
  - You must control all routers involved.
  - All of those routers must support this configuration tweak.
    - Have fun searching for it on SOHO boxes.

Imitation of DHCPv4

Prevent rogue players

- Use DHCPv6 Guard
  - If available on $PLATFORM.
  - Fully understand configuration & operation.
  - Be aware of limitations
    - => see Antonios‘ presentation (appendix)
- See also:
  http://www.insinuator.net/2015/01/dhcpv6-guard-do-it-like-ra-guard-evasion/

Quick Summary of this Section + Checklist

- Control all L3 devices involved
  - By policy or *privilege 15*.
- Tweak config.
- Take care of RFC 6939 support.
- Implement IPAM.
- Use *DHCPv6 Guard* if considered appropriate.
- Send people to IETF meetings.

Conclusions

- DHCPv6 is very very different from DHCPv4.
- To run it in a reliable & secure way a different operations model is needed.
- You will probably be able to achieve some objectives, but not all.

There’s never enough time…

THANK YOU…

...for yours!

Questions?

- You can reach us at:
  - cwerny@ernw.de, www.ernw.de
- Our blog:
  - www.insinuator.net

We Hire!

- Want to join our team of IPv6 practitioners?
- Work in large, challenging environments (and have quite some fun doing so, learning new things every day)?
- Then drop an e-mail to career@ernw.de

DENOG
German Network Operators Group

Guys, we would love to see you in Heidelberg!

ERNW
providing security.

March, 14-18 2016
Heidelberg, Germany
TROOPERS - Make the world a safer place.




More info & extensive archives @ www.troopers.de