



Consulting Engineering Project Management

Troopers 2019 NAT64 Day 2019 @ AWK

Troopers NGI 2019, 20 March 2019

Gabriel Müller, Principal Consultant

AWK Group

Facts and Figures



Activity	Consulting, engineering und project management for information technology and digital transformation
Founded in	1986
Employees	Over 300 staff
Clients	Over 400
Projects	Over 4'000
Site Locations	Zurich, Berne, Basle, Lausanne

Qualification of our Consultants

Professional experience More than 10 years 5 to 10 years < 5 years University degree Computer Electrical Engineering Other Science Additional qualifications P.h.D Business Degree . 0% 25% 50% 100% 75%

Turnover



Partners of AWK



From left to right: Christian Mauz Andreas Gumann Oliver Spiess Ralph Tonezzer Oliver Vaterlaus (CEO) Roger Mosimann André Arrigoni Adrian Wägli

AWK GROUP

Introduction

- ► Test Setup
- ► Test Results
- ► Test Results (other)
- Conclusion
- Backup Slides

Introduction

Motivation

"the proof of the pudding is in the eating"

Can we do it ?

How complex is the setup ?

Alternative to dual stack setup ?





Introduction

NAT64 / DNS64 Recap

Enable IPv6-only clients to access IPv4 content:

- Based on DNS response modifications
- If no AAAA exists, an AAAA response with prefix 66:ff9B::/96 is created and returned to client → DNS64
- Client then initiates an IPv6 connection to this IPv6 address, the NAT64 router does IPv6 to IPv4 translation → NAT64



Source: www.researchgate.net





- Test Results
- ► Test Results (other)
- Conclusion
- Backup Slides

Test setup – the big picture



Technical details



ge-0/0/0.0 ge-0/0/1.1012

// Interface Configuration

// IPv6 client network

set interfaces ge-0/0/0 unit 0 family inet6 address 2001:1702:6:6::10/64
set interfaces ge-0/0/0 unit 0 family inet6 address fe80::6:0:0:0:10/64

// Dualstack transport network

set interfaces ge-0/0/1 vlan-tagging set interfaces ge-0/0/1 unit 1012 vlan-id 1012 set interfaces ge-0/0/1 unit 1012 family inet address 10.1.241.30/24 set interfaces ge-0/0/1 unit 1012 family inet6 address 2001:1702:6:1012::30/64 set interfaces ge-0/0/1 unit 1012 family inet6 address fe80::1012:0:0:30/64 // NAT64 set security nat static rule-set NAT64 from zone Clients-IPv6 set security nat static rule-set NAT64 rule NAT64 INET match destination-address 64:ff9b::/96 set security nat static rule-set NAT64 rule NAT64 INET then static-nat inet // NAT46 set security nat static rule-set NAT46 from zone Transport-IPv4 set security nat static rule-set NAT46 rule NAT46_Pool match source-address 0.0.0.0/0 set security nat static rule-set NAT46 rule NAT46 Pool match destination-address 192.168.21. 1/28/25 set security nat static rule-set NAT46 rule NAT46 Pool then static-nat prefix 2001:1702:6:6::80/121 // DNS64 < nothing > // using dns doctoring feature of Junos, enabled by default

The packet destination ip is not same as source ip version, drop it

Technical details – stateless vs. stateful NAT64

In our test setup we use stateless / static NAT64

• Any idea why?

Stateless NAT64	Stateful NAT64
1:1 translation	1:N translation
No conservation of IPv4 address	Conserves IPv4 address
Assures end-to-end address transparency and scalability	Uses address overloading, hence lacks in end-to-end address transparency
No state or bindings created on the translation	State or bindings are created on every unique translation
Requires IPv4-translatable IPv6 addresses assignment	No requirement on the nature of IPv6 address assignment
Requires either manual or DHCPv6 based address assignment for IPv6 hosts	Free to choose any mode of IPv6 address assignment viz. Manual, DHCPv6, SLAAC

Source: Cisco IOS Advanced Webinars, NAT64 Technology: NAT64, IPv6 Branch Functionality

Addressing

Using DHCPv6

• Any idea why?

2001:1702:6:6::80 <-> 192.168.21.128 2001:1702:6:6::81 <-> 192.168.21.129 2001:1702:6:6::82 <-> 192.168.21.130 ... 2001:1702:6:6::ff <-> 192.168.21.255

• Motivation: Creating a 1to1 relationship / enabling bi-directional traffic

// **NAT46**

set security nat static rule-set NAT46 from zone Transport-IPv4 set security nat static rule-set NAT46 rule NAT46_Pool match source-address 0.0.0.0/0 set security nat static rule-set NAT46 rule NAT46_Pool match destination-address 192.168.21.128/25 set security nat static rule-set NAT46 rule NAT46 Pool then static-nat prefix 2001:1702:6:6::80/121

// DHCPv6

set access address-assignment pool IPv6-Pool01 family inet6 prefix 2001:1702:6:6::/64 set access address-assignment pool IPv6-Pool01 family inet6 range 1 low 2001:1702:6:6::80/128 set access address-assignment pool IPv6-Pool01 family inet6 range 1 high 2001:1702:6:6::ff/128 set access address-assignment pool IPv6-Pool01 family inet6 dhcp-attributes maximum-lease-time 1800 set access address-assignment pool IPv6-Pool01 family inet6 dhcp-attributes grace-period 300 set access address-assignment pool IPv6-Pool01 family inet6 dhcp-attributes dns-server 64:ff9b::0a01:4732 set access address-assignment pool IPv6-Pool01 family inet6 dhcp-attributes dns-server 64:ff9b::0a01:4733

Technical details – the beauty of static NAT @ Junos





Technical details – remark

Junos flow processing

• In which regard is this important ?



Technical details – Junos dns doctoring feature

// C:\ Ser Add	// DNS querry for entry with non-existing AAAA record C:\Users\Mug>nslookup -type=aaaa tagi.ch Server: UnKnown Address: 64:ff9b::a01:4732											
Nic	cht autorisi	lerende Antwort:								DNS querry ·	client per	spective
No.	Time 10.000000 20.002142	source 2001:1702:6:6::8c 64:ff9b::a01:4732	Destination 64:ff9b::a01:4732 2001:1702:6:6::8c	Length Protocol 87 DNS 123 DNS	™ Standard Standard	query query	0x0003 A response	AAA tagi 0x0003	i.ch AAAA	tagi.ch AAAA	64:ff9b::	97fc:a7e
// RT: RT: RT: RT: RT: RT:	<pre>- 20.002142 64:ff9b::a01:4732 2001:1702:6:6::8c 123DNS Standard query response 0x0003 AAAA tagi.ch AAAA 64:ff9b::97fc:a7e // SRX trace KT: Receive an A response from V4 server to V6 client KT: The response for the duplicate A query KT: Translating A response to AAAA response KT: DNS All RRs Offset Start Update KT: ************************************</pre>											
RT : RT : RT :	<pre>I: Modify offset from (12) to (25) I: Translating A response(151.252.10.126) to AAAA response(64:ff9b:0:0:0:0:0:97fc:a7e) I: Reinject the dup jbuf from A to AAAA I: Success to xlate reply from A to AAAA</pre>											

Test Methodology

Validation / fault finding done by

- Testing application
- Windows log
- Wireshark
- TCPview

		594 C					
🚠 TCPView - Sysinternals: wv	ww.sysinternals.com	m					
File Options Process Vi	ew Help						
陆 🔺 🕼							
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State 7
🙆 hdnClSvc.NET.exe	19224	TCP	0.0.0.0	8413	0.0.0.0	0	LISTENING
💽 PulseSetupClient.exe	23612	TCP	127.0.0.1	3355	0.0.0.0	0	LISTENING
T System	4	TCPV6	[2001:1702:6:6:0:0:0:80]	7718	[64:ff9b:0:0:0:0:a01:4714]	445	ESTABLISHED
0 OUTLOOK.EXE	1824	TCPV6	[2001:1702:6:6:0:0:0:80]	7557	[64:ff9b:0:0:0:0:a01:473c]	443	ESTABLISHED
🗖 OUTLOOK.EXE	1824	TCPV6	[2001:1702:6:6:0:0:0:80]	7569	[64:ff9b:0:0:0:0:a01:473c]	443	ESTABLISHED
🗖 OUTLOOK.EXE	1824	TCPV6	[2001:1702:6:6:0:0:0:80]	7575	[64:ff9b:0:0:0:0:a01:473c]	443	ESTABLISHED
0UTLOOK.EXE	1824	TCPV6	[2001:1702:6:6:0:0:0:80]	7577	[64:ff9b:0:0:0:0:a01:473c]	443	ESTABLISHED
01 OUTLOOK.EXE	1824	TCPV6	[2001:1702:6:6:0:0:0:80]	7585	[64:ff9b:0:0:0:0:a01:473c]	443	ESTABLISHED
🗖 OUTLOOK.EXE	1824	TCPV6	[2001:1702:6:6:0:0:0:80]	7591	[64:ff9b:0:0:0:0:a01:473c]	443	ESTABLISHED
01 OUTLOOK.EXE	1824	TCPV6	[2001:1702:6:6:0:0:0:80]	7601	[64:ff9b:0:0:0:0:a01:473c]	443	ESTABLISHED
🜀 lync.exe	4180	TCPV6	[2001:1702:6:6:0:0:0:80]	7613	[64:ff9b:0:0:0:0:a0a:1e47]	5061	ESTABLISHED
S lync.exe	4180	TCPV6	[2001:1702:6:6:0:0:0:80]	7684	[64:ff9b:0:0:0:0:a01:473c]	443	ESTABLISHED
McsClient.exe	5292	TCPV6	[2001:1702:6:6:0:0:0:80]	7702	[64:ff9b:0:0:0:0:340e:bed4]	443	ESTABLISHED
📧 svchost.exe	5896	TCPV6	[2001:1702:6:6:0:0:0:80]	7547	[64:ff9b:0:0:0:0:2843:ffc7]	443	ESTABLISHED
🔕 hdnClUI.exe	10656	TCPV6	[2001:1702:6:6:0:0:0:80]	7659	[64:ff9b:0:0:0:0:a01:4746]	1433	ESTABLISHED
💽 SkypeApp.exe	13444	TCPV6	[2001:1702:6:6:0:0:0:80]	7672	[64:ff9b:0:0:0:0:a83f:2b7b]	443	ESTABLISHED
📧 SkypeApp.exe	13444	TCPV6	[2001:1702:6:6:0:0:0:80]	7683	[64:ff9b:0:0:0:0:d5e:d371]	443	ESTABLISHED
📧 SkypeApp.exe	13444	TCPV6	[2001:1702:6:6:0:0:0:80]	7694	[64:ff9b:0:0:0:0:2843:fc3d]	443	ESTABLISHED
📧 SkypeApp.exe	13444	TCPV6	[2001:1702:6:6:0:0:0:80]	8041	[2606:2800:147:ff8:129b:22eb:20b:1347]	443	ESTABLISHED
🔇 WhatsApp.exe	18060	TCPV6	[2001:1702:6:6:0:0:0:80]	7580	[64:ff9b:0:0:0:0:a937:4a2a]	443	ESTABLISHED
🜀 UcMapi.exe	19220	TCPV6	[2001:1702:6:6:0:0:0:80]	7712	[64:ff9b:0:0:0:0:a01:473c]	443	ESTABLISHED



- Introduction
- Test Setup

- ► Test Results (other)
- Conclusion
- Backup Slides

Introduction

Conditions:

- AWK clients in IPv6-only network segment
- Within the trust zone, access to all internal IPv4 resources
- Access to the IPv4 and IPv6 internet
- Focus on AWK internal applications as well as on applications used by consultants within projects



Basics

// IP Configuratin Client (DHCPv6)

Ethernet-Adapter Ethernet:



Basics

// Routing Table Client TPv4-Routentabelle Aktive Routen: Netzwerkziel Netzwerkmaske Gateway Schnittstelle Metrik 127.0.0.0 255.0.0.0 Auf Verbindung 127.0.0.1 331 127.0.0.1 255.255.255.255 Auf Verbindung 127.0.0.1 331 // ... only directly connected networks (virtual box, etc.) // no IPv4 default route IPv6-Routentabelle Aktive Routen: If Metrik Netzwerkziel Gateway fe80:0:0:6::10 2 261 ::/0 Auf Verbindung 331 ::1/128 1 261 2001:1702:6:6::/64 Auf Verbindung 2 2 261 2001:1702:6:6::80/128 Auf Verbindung 22 281 fe80::/64 Auf Verbindung // ...

AWK GROUP

Basics

// Furthe	r Infor	mation						
C:\Users\	Mug> net	sh interface	ipv6 show in	terface				
Idx M	let	MTU	State	Name				
1	75	4294967295	connected	Loopback Pseudo-Ir	nterface 1			
28	25	1500	connected	Ethernet 19				
C:\Users\Mug> netsh int ipv6 show int 28								
Parameter	für di	e Schnittste	lle "Ethernet	19"	-			
•••								
Standortp	oräfixlä	nge	: 6	4				
… Angekündi …	gte Rou	terlebensdau	er : 1	800 Sekunden 🔶	// Router Lifetim	e		



Basics

// Router Perspective								
mug2@SRX300-T2019> show dhcpv6 server binding								
Prefix	Session Id	Expires	State	Interface	Client DUID			
2001:1702:6:6::86/128	7	86358	BOUND	ge-0/0/0.0	LL_TIME0x1-0x1fa9321e-54:ee:75:			
2001:1702:6:6::80/128	1	81466	BOUND	ge-0/0/0.0	LL_TIME0x1-0x221dd129-54:e1:ad:			

mug2@SRX300-T2019> show security flow session nat
Session ID: 2573, Policy name: 000_AllowAll/4, Timeout: 1394, Valid
In: 2001:1702:6:6::81/52603 --> 64:ff9b::a27d:1285/443;tcp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 116, Bytes: 72289,
Out: 162.125.18.133/443 --> 192.168.21.129/52603;tcp, Conn Tag: 0x0, If: ge-0/0/1.1012, Pkts: 181, Bytes: 27069,

Session ID: 4164, Policy name: 000_AllowAll/4, Timeout: 1388, Valid
In: 2001:1702:6:6::81/53284 --> 64:ff9b::a27d:1285/443;tcp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 92, Bytes: 50602,
Out: 162.125.18.133/443 --> 192.168.21.129/53284;tcp, Conn Tag: 0x0, If: ge-0/0/1.1012, Pkts: 145, Bytes: 22545,

Session ID: 5124, Policy name: 000_AllowAll/4, Timeout: 298, Valid
In: 2001:1702:6:6::82/49611 --> 64:ff9b::2843:fe24/443;tcp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 16, Bytes: 3322,
Out: 40.67.254.36/443 --> 192.168.21.130/49611;tcp, Conn Tag: 0x0, If: ge-0/0/1.1012, Pkts: 14, Bytes: 5212,



Basics – Findings – nslookup and ping

\checkmark

```
// nslookup and ping
mug@T420s:~$ nslookup ps10.awkgroup.com
Server:
              127.0.0.53
Address: 127.0.0.53#53
Non-authoritative answer:
       ps10.awkgroup.com
Name:
Address: 10.1.71.55
Name: ps10.awkgroup.com
Address: 64:ff9b::a01:4737
mug@T420s:~$ ping ps10.awkgroup.com
PING ps10.awkgroup.com(64:ff9b::a01:4737 (64:ff9b::a01:4737)) 56 data bytes
64 bytes from 64:ff9b::a01:4737 (64:ff9b::a01:4737): icmp seq=1 ttl=125 time=1.28 ms
64 bytes from 64:ff9b::a01:4737 (64:ff9b::a01:4737): icmp seq=2 ttl=125 time=1.15 ms
^C
--- ps10.awkgroup.com ping statistics ---
                                                                   Tip:
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
                                                                   You can also use IPv4 address notation:
rtt min/avg/max/mdev = 1.156/1.218/1.280/0.062 ms
mug@T420s:~$
                                                                   ping 64:ff9b::10.1.71.55
```



Basics – Findings – DNS registration



eignis 8015, DNS Client Events	Process	
Allgemein Details	 Client sending SOA query for <pc-name><domain< li=""> </domain<></pc-name>	>
	Response is SOA record	
mit den folgenden Einstellungen: Adaptername: {EB36F8B3-DE4D Hostname: PC-0LSRSR Primäres Domänensuffix: awkgr DNS-Serverliste: 64:ff9b::a01:4732, 64:ff9b::a01 Server, an den das Update geser IP-Adresse(n) : 2001:1702:6:6::8c Diese Ressourceneinträge konnten auf	<pre>Arctentrage (a our Adda) in termetawapper > Frame 4: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0 > Ethernet II, Src: JuniperN_d7:3a:00 (ec:13:db:d7:3a:00), Dst: LcfcHefe_1b:6e:33 (54:e1:ad:1b:6e > Internet Protocol Version 6, Src: 64:ff9b::a01:4732, Dst: 2001:1702:6:6::80 > User Datagram Protocol, Src Port: 53, Dst Port: 52354 > Domain Name System (response) Transaction ID: 0x970f > Flags: 0x8580 Standard query response, No error Questions: 1 Answer RRs: 2 Authority RRs: 0 Additional RRs: 2 > Queries > awkgroup.com: type NS, class IN, ns ad11.awkgroup.com > awkgroup.com: type NS, class IN, ns ad10.awkgroup.com > Additional records > ad11.awkgroup.com: type A, class IN, addr 10.1.71.50 Request In: 31</pre>	: 33
	[Time: 0.001710000 seconds]	
	This is what you can configure on the SRX, the DNS64 is a standard RFC and you	

Basics – Findings – GPO processing

		\checkmark
×		

eignis 1502, GroupPolicy	(Microsoft-Windows-GroupPo	olicy)		
Allgemein Details				
Die Gruppenrichtliniene erkannt und angewend	einstellungen für den Compute et.	er wurden erfolgreich	verarbeitet. Es wurden neue 28-Gruppenrichtlinienobjekte	-
Protokollname:	System			
Quelle:	GroupPolicy (Microsoft-Winc	Protokolliert:	28.01.2019 15:51:14	
Ereignis-ID:	1502	Aufgabenkategorie:	Keine	
Ebene:	Informationen	Schlüsselwörter:		
Benutzer:	SYSTEM	Computer:	PC-0LSRSR.awkgroup.com	
Vorgangscode:	(1)			
	Onlinehilfe			



llgemein Details			
Der Zeitanbieter "NtpC	lient" empfängt derzeit	gültige Zeitdaten von AD10.a	awkgroup.com (ntp.d [::]:123->[64:ff9b::a01:4732]:123).
 	C 1		
Protokoliname:	System		
Quelle:	Time-Service	Protokolliert:	28.01.2019 15:58:06
Ereignis-ID:	37	Aufgabenkategorie:	Keine
Ebene:	Informationen	Schlüsselwörter:	
Benutzer:	Lokaler Dienst	Computer:	PC-0LSRSR.awkgroup.com
	Info		
Vorgangscode:	inio		



Windows 10 client looses default GW information after 1 hour

	Update	
Ethernet-Adapter Ethernet:	 Used wrong fe80 address: fe80::6:0:0:0:10/64 	(should be fe80::6:0:0:10/64)
	• Once fixed, aw information is no longer lost	(,
Verbindungsspezifisches DNS-Suffix:	• Chec fixed, gw information is no fonger fost	/
Beschreibung :	Intel(R) Ethernet Connection (4) I219-V	
Physische Adresse	54-E1-AD-1B-6E-33	/
DHCP aktiviert	Ja	
Autokonfiguration aktiviert :	Ja	
IPv6-Adresse	2001:1702:6:6::80(Bevorzugt)	
Lease erhalten :	Donnerstag, 31. Januar 2019 07:27:22	
Lease läuft ab :	Freitag, 1. Februar 2019 07:27:21	
Verbindungslokale IPv6-Adresse . :	fe80::9878:6afa:d5d5:a16d%2(Bevorzugt)	/
IPv4-Adresse (Auto. Konfiguration):	169.254.161.109(Bevorzugt)	/
Subnetzmaske	255.255.0.0	_
Standardgateway :		
DHCPv6-IAID	39117229	-
DHCPv6-Client-DUID :	00-01-00-01-22-1D-D1-29-54-E1-AD-1B-6E-33	
DNS-Server	64:ff9b::a01:4732	
	64:ff9b::a01:4733	
NetBIOS über TCP/IP :	Deaktiviert	

Findings – AWK internal – various

Working

- File Access (network drives)
- Sharepoint
- RDP (mstsc.exe)
- Skype for Business
 - PTSN -> IPv6 client
 - IPv6 client -> PTSN
 - IPv4 client -> IPv6 client Video Call
 - IPv6 client -> IPv4 client Video Call
- Printing (sending job to print server)
- Abacus (ERP) (java based)
- Outlook
- Citrix Netscaler RDP

Findings – AWK internal – various



Not Working

- Microsoft Teams
 - IPv6 client -> IPv4 client Video Call
 - IPv4 client -> IPv6 client Video Call X
- Swisscom Storebox



Finding – AWK external – various

Working

- OpenVPN
- SSH
- Skype
- Speedtest (web based)
- google drive
- Whatsapp desktop app



64:ff9b::510

Password for

login as:



Using 64:ff9b::<IPv4 address>

ast login: Fri Jan 18 14:42:15 2019 from 178.38.116.71

net:

PuTTY

Using keyboard-interactive authentication.

Findings – AWK external – various



Not working

- Speedtest (app)
- Vmware Horizon (both, web-based and local application)



Findings – Other

Problematic

- IPv6 not properly working
- Why?
- No fallback to IPv4 (happy eyeballs, etc.)



- Introduction
- ► Test Setup
- ► Test Results
- Test Results (other)
- Conclusion
- Backup Slides

Test setup – the big picture (WLAN)



SRX Configuration

// Interface Configuration // IPv6 client network (WLAN) set interfaces ge-0/0/2 unit 0 family inet6 address 2001:1702:6:7::10/64 set interfaces ge-0/0/2 unit 0 family inet6 address fe80::7:0:0:0:10/64 // NAT64 set security nat source rule-set NAT64-2 to zone Transport-IPv4 set security nat source rule-set NAT64-2 rule NAT64 Source match source-address 2001:1702:6:7::/64 set security nat source rule-set NAT64-2 rule NAT64 Source match destination-address 0.0.0/0 set security nat source rule-set NAT64-2 rule NAT64 Source then source-nat interface // **NAT46** < empty / none > // DNS64 < nothing > // using dns doctoring feature of Junos, enabled by default // SLAAC (including RDNSS) & DHCPv6 set protocols router-advertisement interface ge-0/0/2.0 managed-configuration set protocols router-advertisement interface ge-0/0/2.0 dns-server-address 64:ff9b::0808:0808 set protocols router-advertisement interface ge-0/0/2.0 dns-server-address 64:ff9b::0808:0404 set protocols router-advertisement interface ge-0/0/2.0 prefix 2001:1702:6:7::/64

set access address-assignment pool IPv6-Pool02 family inet6 dhcp-attributes dns-server 64:ff9b::0808:0808 set access address-assignment pool IPv6-Pool02 family inet6 dhcp-attributes dns-server 64:ff9b::0808:0404

AWK GROUP

NAT64 Day @AWK

Preparation	Communication	NAT64 Day
 Configuration of SRX Testing with Android mobile Testing with iOS mobile Testing with Ubuntu PC 	 Email sent 1 week in advance Reminder sent 1 day in advance Information sent before activation Information sent at end of day 	 Switched to NAT64 at 08:00 Presence in lounge Switched back to normal at 11:00



Do. 07.03.2019 07:59 Müller, Gabriel **ZH: NAT64 DAY 2019 - Reminder**

An AWKGROUP

Hallo Zusammen

Kurzer Reminder, die Umschaltung (AWKWLAN) wird in wenigen Minuten erfolgen. ausschalten und sicherstellen, dass ihr mit AWKWLAN verbunden seid. Dann das me Rückmeldung an mich,

- Persönlich bei mir in der Lounge. In bin die ganze Zeit in der Lounge anwese
- Per Excel: Feedback NAT64-Day 2019.xlsx (solltet ihr keinen Zugriff haben,



NAT64 Day @AWK – Monitoring

Basic monitoring

- On SRX
- Using ntopng
- Observium

mug@SRX300-T2019> show ipv6 neighl	oours					
IPv6 Address	Linklayer Address	State	Exp	Rtr	Secure	Interface
2001:1702:6:7:480:13d2:24b3:c64	40:9c:28:5a:xx:xx	stale	366	no	no	ge-0/0/2.0
2001:1702:6:7:548:51cd:288b:482b	98:00:c6:27:xx:xx	stale	53	no	no	ge-0/0/2.0
2001:1702:6:7:6b1:67ff:fe2a:xxxx	04:b1:67:2a:xx:xx	stale	488	no	no	ge-0/0/2.0
fe80::4e66:41ff:fefc:xxxx	4c:66:41:fc:xx:xx	stale	141	no	no	ge-0/0/2.0
fe80::740c:8fb3:29b1:8981	24:18:1d:f3:xx:xx	stale	947	no	no	ge-0/0/2.0
fe80::8ef5:a3ff:fe82:xxxx	8c:f5:a3:82:xx:xx	stale	22	no	no	ge-0/0/2.0
fe80::8ef5:a3ff:fe82:xxxx	8c:f5:a3:82:xx:xx	stale	167	no	no	ge-0/0/2.0
fe80::b6cd:27ff:fea1:xxxx	b4:cd:27:a1:xx:xx	stale	777	no	no	ge-0/0/2.0

•••

NAT64 Day @AWK – Monitoring



Networks

10 - IP Version-

Network Name	Chart	Hosts	Alerts	Seen Since	Breakdown	Throughput	Traffic
2001:1702:6:7:3e18:a0ff:fe0c:f3b1/64		47	0	56 min, 35 sec	Sent Rcvd	630.7 kbit/s -	1.52 GB
Remote Networks	-	178	0	56 min, 35 sec	Sent Rcvd	652.13 kbit/s -	545.55 MB
fe80::3e18:a0ff:fe0c:f3b1/64		33	0	56 min, 32 sec	Sent F	2.33 kbit/s 🛧	1.35 MB

Showing 1 to 3 of 3 rows

NOTE: In case you have defined overlapping networks:

1. You will see both network entries in the above table.

2. The broader network will not include hosts defined in smaller networks.



NAT64 Day @AWK – Monitoring





NAT64 Day @AWK – Monitoring





NAT64 Day @AWK – Results

Biggest hassle with Window 10 laptops

• Were not able to configure an IPv6 address

Flapping internet / spontaneous disconnects

• Reported by 2 users (both Android (version 6 and 9)

Other than that only very little problems detected

• Revolut app: Verification SMS not received



Test Results (other)

NAT64 Day @AWK – Results





1: SMS validation not working

Unifi – No IPv6 support

\checkmark
\land

U	C	UĥiFi							CURR CHZ	ENT SITE	JSERNAME ° su_mug ∨ °
6	ALL (33) WIRELESS (33) WIRED (0)	ALL (33) USER	S (33) GUESTS (0)			+ 4	ADD CLIENT ALL	CONFIGURED CLIENT	S Search	Q
Π_		NAME	IP ADDRESS	CONNECTION ↑	AP/PORT	ACTIVITY ↔	ACTIVITY DOWN	ACTIVITY UP	UPTIME	ACTIONS \leftrightarrow	<u>о</u> , 1
	8	DeniseMrsiPhone	10.1.113.58	AWKWLAN	CHZH01NAP11		19.1 MB	883 KB	2h 5m 50s		C RECONNECT
\bigcirc	8	iPhonevonErdinc	169.254.228.205	AWKWLAN	CHZH01NAP14		764 KB	393 KB	30m 36s		
0	8	04:b1:	10.1.113.165	AWKWLAN	CHZH01NAP15		72.7 MB	68.4 MB	1h 33m 15s		
0	8	Mayas-iPhone	10.1.113.246	AWKWLAN	CHZH01NAP99		1.83 MB	465 KB	2h 29m 33s	Ø BLOCK	
口	8	Kevs-iPhone	10.1.113.233	AWKWLAN	CHZH01NAP12		79.9 KB	54.1 KB	13m 23s		C RECONNECT
\bigtriangledown	8	iPhone-von-kai	169.254.28.31	AWKWLAN	CHZH01NAP15	-	26.6 MB	3.06 MB	14m 44s	Ø BLOCK	C RECONNECT
业	8	Galaxy-S9	-	AWKWLAN	CHZH01NAP15		10 MB	809 KB	14m 58s		
	8	iPhonevfanRiedi	169.254.227.43	AWKWLAN	CHZH01NAP14		1.64 MB	628 KB	1h 11m 58s	BLOCK	C RECONNECT
	8	iPhonevonMarisa	10.1.113.67	AWKWLAN	CHZH01NAP13		100 KB	235 KB	1h 23m 28s	Ø BLOCK	C RECONNECT
	8	Samsung-Galaxy-S7	10.1.113.238	AWKWLAN	CHZH01NAP15		435 KB	260 KB	2h 37m 37s		
	8	Daniels-iPhone	10.1.113.182	AWKWLAN	CHZH01NAP14		6.2 MB	1.59 MB	1h 47m 11s		C RECONNECT
(j)	8	Galaxy-S8	-	AWKWLAN	CHZH01NAP15		52 KB	47.7 KB	10m 34s	BLOCK	C RECONNECT
	8	48:02:	10.1.113.198	AWKWLAN	CHZH01NAP13		13 MB	14.4 MB	1d 19h 43m 21s		C RECONNECT
*	8	Samuels-iPhone	10.1.113.69	AWKWLAN	CHZH01NAP15		0.98 KB	6.41 KB	2m 58s		C RECONNECT
<u> </u>	8	MR	169.254.63.169	AWKWLAN	CHZH01NAP13		273 MB	102 MB	33m 4s		C RECONNECT
	8	mrshorty	169.254.125.31	AWKWLAN	TestAP01		4.37 MB	916 KB	1h 5m 29s		
	8°	android-6,0000000,02000	10.1.113.152	AWKWLAN	TestAP02		26 MB	5.4 MB	16d 1h 32m 35s		C RECONNECT



M and O flags – IPv6 address configuration

Managed Address Configuration flag (M)

• instructs the host to use a configuration protocol to obtain stateful addresses

Other Stateful Configuration flag (O)

• instructs the host to use a configuration protocol to obtain other configuration settings

Flag states	Theoretical client behavior
	Client shall use information contained in router advertisements to configure network interface. No DHCPv6 service available
	Client shall use DHCPv6 protocol to configure IPv6 addresses on interface. For all other information router advertisement information should be used.
M = 0 O = 1	Client shall use DHCPv6 only for other configuration information, and using router advertisements for address configuration (> stateless DHCPv6)
M = 1 O = 1	Client shall use DHCPv6 for IPv6 address configuration and other configuration settings (> stateful DHCPv6)



M and O flags – Juniper SRX300

Example: M and O set (1) set protocols router-advertisement interface ge-0/0/2.0 managed-configuration set protocols router-advertisement interface ge-0/0/2.0 other-stateful-configuration

Looking at RA message sent by SRX

```
Example: M and O set (1)
root@T420s:/home/mug# tcpdump -vvvv -ttt icmp6 and 'ip6[40] = 134'
tcpdump: listening on enp0s25, link-type EN10MB (Ethernet), capture size 262144 bytes
00:00:00.000000 IP6 (hlim 255, next-header ICMPv6 (58) payload length: 96) gateway > ip6-allnodes:
[icmp6 sum ok] ICMP6, router advertisement, length 96
        hop limit 64, Flags [managed, other stateful], pref medium, router lifetime 180s, ...
          source link-address option (1), length 8 (1): ec:13:db:d7:3a:02
            0x0000: ec13 dbd7 3a02
          rdnss option (25), length 40 (5): lifetime 1800s, addr: 64:ff9b::808:808 addr: 64:ff9b::...
            0x0000: 0000 0000 0708 0064 ff9b 0000 0000 0000
            0x0010: 0000 0808 0808 0064 ff9b 0000 0000 0000
            0x0020: 0000 0808 0404
          prefix info option (3), length 32 (4): 2001:1702:6:7::/64, Flags [onlink, auto], valid time ...
            0x0000: 40c0 0027 8d00 0009 3a80 0000 0000 2001
            0x0010: 1702 0006 0007 0000 0000 0000 0000
```

M and O flags – Some more testing

• Used wrong fe80 address: fe80::7:0:0:0:10/64 (should be fe80::7:0:0:10/64)

• DHCPv6 server needed reset as well



Flag	DHCPv6	Windows 10	Windows 10	Ubuntu	Mac OS X
states	enabled	10.0 (Build 10240)	1709 (Build 16299.431)	18.04.1 LTS	10.10.5
	No	SLAAC – no gw No IP addr. configured	SLAAC – OK No IP addr. configured	SLAAC – OK SLAAC – OK	SLAAC – OK SLAAC – OK
	Yes	SLAAC – no DNS DHCPv6 - OK	SLAAC – OK No IP addr. configured	SLAAC – OK SLAAC – OK	SLAAC – OK SLAAC – OK
M = 1	No	SLAAC – NO DNS	SLAAC – OK	SLAAC – OK	SLAAC – OK
O = 0		SLAAC – NO DNS	SLAAC – NO DNS	SLAAC – OK	SLAAC – OK
M = 1	Yes	SLAAC – NO DNS	DHCPv6 – OK	DHCPv6 – OK	DHCPv6 – OK
O = 0		DHCPv6 - OK	No IP addr. configured	DHCPv6 – OK	SLAAC – OK
M = 0	No	SLAAC – NO DNS	SLAAC – NO DNS	SLAAC – OK	SLAAC – OK
O = 1		SLAAC – NO DNS	SLAAC – NO DNS	SLAAC – OK	SLAAC – OK
M = 0	Yes	SLAAC – NO DNS	SLAAC – OK	SLAAC – OK	SLAAC – OK
O = 1		SLAAC – OK	No IP addr. configured	SLAAC – OK	SLAAC – OK
M = 1	No	SLAAC – NO DNS	SLAAC – OK	SLAAC – OK	SLAAC – OK
O = 1		SLAAC – NO DNS	No IP addr. configured	SLAAC – OK	SLAAC – OK
M = 1	Yes	SLAAC – NO DNS	DHCPv6 – OK	DHCPv6 – OK	DHCPv6 – OK
O = 1		SLAAC – OK	SLAAC – OK	DHCPv6 – OK	SLAAC - OK



M and O flags – Some more testing (rev. 2 – after fixing wrong fe80 address)



Flag	DHCPv6	Windows 10	Windows 10	Ubuntu	Mac OS X
states	enabled	10.0 (Build 10240)	1709 (Build 16299.431)	18.04.1 LTS	10.10.5
	No	SLAAC – no DNS SLAAC – no DNS	SLAAC – OK SLAAC – OK	SLAAC – OK SLAAC – OK	SLAAC – OK SLAAC – OK
	Yes	DHCPv6 – OK DHCPv6 – OK	DHCPv6 – OK DHCPv6 – OK	SLAAC – OK SLAAC – OK	SLAAC – OK SLAAC – OK
M = 1	No	SLAAC – no DNS	SLAAC – OK	SLAAC – OK	SLAAC – OK
O = 0		SLAAC – no DNS	SLAAC – OK	SLAAC – OK	SLAAC – OK
M = 1	Yes	DHCPv6 – OK	DHCPv6 – OK	DHCPv6 – OK	DHCPv6 – OK
O = 0		DHCPv6 – OK	DHCPv6 – OK	DHCPv6 – OK	SLAAC – OK
M = 0	No	SLAAC – no DNS	SLAAC – OK	SLAAC – OK	SLAAC – OK
O = 1		SLAAC – no DNS	SLAAC – OK	SLAAC – OK	SLAAC – OK
M = 0	Yes	DHCPv6 – OK	DHCPv6 – OK	SLAAC – OK	SLAAC – OK
O = 1		DHCPv6 – OK	DHCPv6 – OK	SLAAC – OK	SLAAC – OK
M = 1	No	SLAAC – no DNS	SLAAC – OK	SLAAC – OK	SLAAC – OK
O = 1		SLAAC – no DNS	SLAAC – OK	SLAAC – OK	SLAAC – OK
M = 1	Yes	DHCPv6 – OK	DHCPv6 – OK	DHCPv6 – OK	DHCPv6 – OK
O = 1		DHCPv6 – OK	DHCPv6 – OK	DHCPv6 – OK	SLAAC - OK

- Introduction
- ► Test Setup
- ► Test Results
- ► Test Results (other)
- **Conclusion**
- Backup Slides

Conclusion

Summary

Getting it up and running was fast and easy

- Most time consuming: Planning and preparations
- DNS doctoring feature 'build-in', no additional DNS server required

Test Results

- Within our TRUST zone (internal network)
- Much better than expected
- Nevertheless not an option due to missing support for key features

Test Results (other)

- Again, much better than expected
- Most challenging seems to be address assignment / configuration on Windows



Conclusion

Discussion

IPv6-only setup less complex ?

- really?
- At least for IPv4 traffic you will see both (v6/v4) depending on network segment you are looking at
- So for me it looks more and more like you should first
 - Enable your server infrastructure / internal resources dualstack (or IPv6-only with dualstack GW)
 - (optional) Create IPv6 'islands'
 - Then switch clients to IPv6 only with NAT64 / DNS64 for accessing external IPv4 resource
- By tendency, the more content is available native via IPv6 the better / easier you can move the client site to an IPv6-only network
- Your opinion

Conclusion

Challenges

1. AWK VPN

2. Android IPv4 URL



- Introduction
- ► Test Setup
- Test Results
- ► Test Results (other)
- Conclusion
- Backup Slides



Complete configuration SRX300

set version 15.1X49-D45 set system host-name SRX300-T2019 set system root-authentication encrypted-password ... set system login class read-only-local permissions snmp set system login user mug uid 2000 set system login user mug class super-user set system login user mug authentication encrypted-password ... set system services ssh set system services dns forwarders 10.1.71.50 set system services dns dns-proxy interface ge-0/0/0.0 set system services dns dns-proxy interface qe-0/0/2.0 // added after NAT64 Day set system services dhcp-local-server dhcpv6 overrides interface-client-limit 200 set system services dhcp-local-server dhcpv6 group IPv6-Group01 interface ge-0/0/0.0 set system services dhcp-local-server dhcpv6 group IPv6-Group02 interface ge-0/0/2.0 // added after NAT64 Day set security alg traceoptions file DebugDNS set security forwarding-options family inet6 mode flow-based set security nat source rule-set NAT64-2 from zone Clients-IPv6 set security nat source rule-set NAT64-2 to zone Transport-IPv4 set security nat source rule-set NAT64-2 rule NAT64 Source match source-address 2001:1702:6:7::/64 set security nat source rule-set NAT64-2 rule NAT64 Source match destination-address 0.0.0.0/0 set security nat source rule-set NAT64-2 rule NAT64 Source then source-nat interface set security nat static rule-set NAT64 from zone Clients-IPv6 set security nat static rule-set NAT64 rule NAT64 INET match destination-address 64:ff9b::/96 set security nat static rule-set NAT64 rule NAT64 INET then static-nat inet

Complete configuration SRX300 (continued)

set security nat static rule-set NAT46 from zone Transport-IPv4 set security nat static rule-set NAT46 rule NAT46 Pool match source-address 0.0.0.0/0 set security nat static rule-set NAT46 rule NAT46 Pool match destination-address 192.168.21.128/25 set security nat static rule-set NAT46 rule NAT46 Pool then static-nat prefix 2001:1702:6:6::80/121 set security policies from-zone Clients-IPv6 to-zone Transport-IPv4 policy 000 AllowAll match source-address any set security policies from-zone Clients-IPv6 to-zone Transport-IPv4 policy 000 AllowAll match destination-address any set security policies from-zone Clients-IPv6 to-zone Transport-IPv4 policy 000 AllowAll match application any set security policies from-zone Clients-IPv6 to-zone Transport-IPv4 policy 000 AllowAll then permit set security policies from-zone Transport-IPv4 to-zone Clients-IPv6 policy 000 AllowAny match source-address any set security policies from-zone Transport-IPv4 to-zone Clients-IPv6 policy 000 AllowAny match destination-address any set security policies from-zone Transport-IPv4 to-zone Clients-IPv6 policy 000 AllowAny match application any set security policies from-zone Transport-IPv4 to-zone Clients-IPv6 policy 000 AllowAny then permit set security traceoptions file DebugDNS set security zones security-zone Clients-IPv6 interfaces ge-0/0/0.0 host-inbound-traffic system-services all set security zones security-zone Clients-IPv6 interfaces qe-0/0/2.0 host-inbound-traffic system-services all set security zones security-zone Transport-IPv4 interfaces ge-0/0/1.1012 host-inbound-traffic system-services all set security zones security-zone MGMT interfaces ge-0/0/1.1111 host-inbound-traffic system-services all set interfaces ge-0/0/0 unit 0 family inet6 address 2001:1702:6:6::10/64 set interfaces ge-0/0/0 unit 0 family inet6 address fe80::6:0:0:10/64 set interfaces ge-0/0/1 vlan-tagging set interfaces ge-0/0/1 unit 1012 vlan-id 1012 set interfaces ge-0/0/1 unit 1012 family inet address 10.1.241.30/24 set interfaces ge-0/0/1 unit 1012 family inet6 address 2001:1702:6:1012::30/64

AWK GROUP

Complete configuration SRX300 (continued)

set interfaces ge-0/0/1 unit 1012 family inet6 address 2001:1702:6:1012::30/64 set interfaces ge-0/0/1 unit 1012 family inet6 address fe80::1012:0:0:30/64 set interfaces ge-0/0/1 unit 1111 vlan-id 1111 set interfaces ge-0/0/1 unit 1111 family inet address 10.1.224.30/24 set interfaces ge-0/0/2 unit 0 family inet6 address 2001:1702:6:7::10/64 set interfaces ge-0/0/2 unit 0 family inet6 address fe80::7:0:0:10/64 set interfaces lo0 unit 0 family inet address 192.168.21.254/32 set snmp location CHZH01 set snmp contact "Gabriel Mueller <qabriel.mueller@awk.ch>" set snmp community ... authorization read-only set snmp community ... clients 10.1.233.0/24 set routing-options rib inet6.0 static route ::/0 next-hop 2001:1702:6:1012::10 set routing-options static route 0.0.0.0/0 next-hop 10.1.241.10 set routing-options static route 10.1.233.0/24 next-hop 10.1.224.10 set protocols router-advertisement interface ge-0/0/0.0 max-advertisement-interval 60 set protocols router-advertisement interface ge-0/0/0.0 min-advertisement-interval 5 set protocols router-advertisement interface ge-0/0/0.0 managed-configuration set protocols router-advertisement interface ge-0/0/0.0 other-stateful-configuration set protocols router-advertisement interface qe-0/0/0.0 prefix 2001:1702:6:6::/64 no-autonomous set protocols router-advertisement interface ge-0/0/0.0 prefix ::/0 valid-lifetime 36001 set protocols router-advertisement interface ge-0/0/0.0 prefix ::/0 preferred-lifetime 36000 set protocols router-advertisement interface qe-0/0/0.0 prefix ::/0 no-autonomous

AWK GROUP

Complete configuration SRX300 (continued)

set protocols router-advertisement interface ge-0/0/2.0 max-advertisement-interval 60 set protocols router-advertisement interface qe-0/0/2.0 min-advertisement-interval 5 set protocols router-advertisement interface ge-0/0/2.0 other-stateful-configuration set protocols router-advertisement interface qe-0/0/2.0 dns-server-address 64:ff9b::0808:0808 set protocols router-advertisement interface qe-0/0/2.0 dns-server-address 64:ff9b::0808:0404 set protocols router-advertisement interface ge-0/0/2.0 prefix 2001:1702:6:7::/64 set access address-assignment pool IPv6-Pool01 family inet6 prefix 2001:1702:6:6::/64 set access address-assignment pool IPv6-Pool01 family inet6 range 1 low 2001:1702:6:6::80/128 set access address-assignment pool IPv6-Pool01 family inet6 range 1 high 2001:1702:6:6::ff/128 set access address-assignment pool IPv6-Pool01 family inet6 dhcp-attributes maximum-lease-time 1800 set access address-assignment pool IPv6-Pool01 family inet6 dhcp-attributes grace-period 300 set access address-assignment pool IPv6-Pool01 family inet6 dhcp-attributes dns-server 64:ff9b::0a01:4732 set access address-assignment pool IPv6-Pool01 family inet6 dhcp-attributes dns-server 64:ff9b::0a01:4733 set access address-assignment pool IPv6-Pool02 family inet6 prefix 2001:1702:6:7::/64 set access address-assignment pool IPv6-Pool02 family inet6 range 1 low 2001:1702:6:7::20/128 set access address-assignment pool IPv6-Pool02 family inet6 range 1 high 2001:1702:6:7::ff:ff/128 set access address-assignment pool IPv6-Pool02 family inet6 dhcp-attributes maximum-lease-time 36000 set access address-assignment pool IPv6-Pool02 family inet6 dhcp-attributes grace-period 3600 set access address-assignment pool IPv6-Pool02 family inet6 dhcp-attributes dns-server 64:ff9b::0808:0808 set access address-assignment pool IPv6-Pool02 family inet6 dhcp-attributes dns-server 64:ff9b::0808:0404

Links / References

RFC 6052 - IPv6 Addressing of IPv4/IPv6 Translators