TROOPERS

ERNW providing security.

Case Study: Building a Secure and Reliable IPv6 Guest WiFi Network

Christopher Werny, cwerny@ernw.de

Who am I

- Network geek, working as security researcher for
- Germany based ERNW GmbH
  - Independent
  - Deep technical knowledge
  - Structured (assessment) approach
  - Business reasonable recommendations
  - We understand corporate

- Blog: www.insinuator.net

- Twitter: @bcp38_

Agenda

- General Notes when building a conference WiFi network
- Specifics of IPv6 in (802.11) WiFi Networks
- How to Reduce the Chatter of IPv6 in WiFi Networks
- Troopers Network Infrastructure
  - We will also discuss my goal of going IPv6-only for the whole management ;-)
- Troopers Monitoring System
  - With statistics for the first day of the IPv6 Security Summit.

General Rules when building a Conference Network

General Notes On Conference WLANs

Guidelines

- Important Rule to keep in mind when building a wireless network:
  - The network is primarily radios, and only secondarily digital,
  - The 2,4GHz band is shared with other equipment like
    - cordless phones,
    - cordless microphones
    - Bluetooth

General Notes On Conference WLANs

Do a site survey to find out what the situation is!

- Find the network and power jacks in your area.
- Are there other WiFi signals in the area, and on what channels are they?
- Looking for interference in the area.
- Think about which effect walls or other moveable partitions have on your Signal.

Speaking of Interference…..

MAC Address	SSID	Channel	# Detecting Radios
00:04:0e:d4:b1:5c	Pollux	1	5
00:13:1a:40:84:30	REAPER	3	8
00:16:9d:73:ec:20	HDMWLAN02	1	7
00:16:9d:73:ec:21	HDMWLAN	1	8
00:16:9d:73:ec:22	HDMSECWLAN	1	7
00:16:9d:73:ec:24	Telekom_HDM	1	7
00:16:9d:73:f0:50	HDMWLAN02	11	5
00:16:9d:73:f0:51	HDMWLAN	11	6
00:16:9d:73:f0:52	HDMSECWLAN	11	5
00:16:9d:73:f0:54	Telekom_HDM	11	5
00:16:9d:73:f2:50	HDMWLAN02	11	5
00:16:9d:73:f2:51	HDMWLAN	11	3
00:16:9d:73:f2:52	HDMSECWLAN	11	2
00:16:9d:73:f2:54	Telekom_HDM	11	3
00:16:9d:7c:37:d0	HDMWLAN02	6	1
00:16:9d:7c:37:d1	HDMWLAN	6	1
00:16:9d:7c:37:d2	HDMSECWLAN	6	1
00:16:9d:7c:37:d4	Telekom_HDM	6	1
00:1b:d4:86:8e:10	Telekom	11	2

Rogues

124 APs 1 Clients

Entries 1 - 50 of 118

1 2 3

General Notes On Conference WLANs

some useful advices

- Encourage the use of 5 GHz channels.
- Turn power down on 2.4 GHz to allow for more access points without overlapping footprints
- Run DHCP on a central server.
  - This allows access points to act as bridges for mobile devices to roam from one AP to another without having to get new IP addresses.

General Notes On Conference WLANs

some useful advices

- Disable slow speeds.
  - If you can disable the 802.11b entirely
  - If you can control what devices are in use and make sure they are all 802.11n capable, you can disable 802.11g as well.
- Disable connection tracking. Connection tracking can be a very significant overhead on the CPU and RAM of the AP.
- Set short inactivity timers to avoid APs spending resources on trying to track devices that have moved or been turned off.
- With hundreds to thousands of users, you will never have enough Internet bandwidth to satisfy everyone.
  - ACLs, QoS, Proxy

Specifics of IPv6 in (802.11) WiFi Networks

The Multicast problem

The Multicast Problem [1]

- WLANs are a shared half-duplex: one station transmits all others must be silent.
- A multicast / broadcast transmission from an AP is physically transmitted to all WiFi clients.
- No other node can use the wireless medium at that time.
- Behavior as a Ethernet hub.

IPv6 Multicast Use [2]

- Duplicate Address Detection.
- Router Solicitations.
- Router Advertisements.
  - One multicast RAs every [RA interval] seconds * one solicited RA per host joining the network
- Neighbor solicitations.

IPv6 Multicast Use

- Different wireless clients may use different transmission encodings and data rates.
- A lower data rate effectively locks the medium for a longer time per bit.
- AP is constrained to transmit all multicast or broadcast frames at the lowest rate possible.

IPv6 Multicast Use

- Often translated to rates as low as 1 Mbps or 6 Mbps, even when the rate can reach a hundred of Mbps and above.
- Sending a single multicast frame can consume as much bandwidth as dozens of unicast frames.

Lowest WiFi rate	Highest WiFi rate	Mcast frame %-age	WiFi Utilization by Mcast
1 Mbps	11 Mbps	1 %	9 %
6 Mbps	54 Mbps	1 %	9 %
6 Mbps	54 Mbps	5 %	45 %
6 Mbps	54 Mbps	10 %	90 %

WiFi Utilization by Multicast [1]

Acknowledgements

- No acknowledgement mechanism (ARQ).
- Frames can be missed and NDP does not take this packet loss into account.
- Could have a negative impact for Duplicate Address Detection (DAD)

WiFi Error Rate

- Assuming a error rate of 8% of corrupted frame.
- 8% chance of loosing a complete frame.
- 16% chance of not detecting a duplicate address.

Host Sleep Mode

Host sleep Mode

- Host wakes up and sends multicast Router Solicitation.
- Triggers a Router Advertisement message from all adjacent routers.
- Duplicate Address Detection for its link-local and global addresses.
- Transmitting at least two multicast Neighbor Solicitation messages.
- Repeated by the AP to all other WiFi clients.

IPv6 Multicast Use

- Multicast Router Solicitation from the WiFi client, received by the AP and broadcasted again over the wireless link if not optimized.
- Multicast Neighbor Solitication for the host LLA from the WiFi client, received by the AP and transmitted back over the wireless link if not optimized.
- Same behavior per global address
- 6 WiFi “broadcast” packets plus the unicast replies on each wake-up cycle of the device.

WiFi Clients	Wake-up Cycle	Mcast packet/sec	Mcast bit/sec	Lowest WiFi Rate	Mcast Utilization
100	600 sec	1	960 bps	1 Mbps	0.1 %
1 000	600 sec	1	9600 bps	1 Mbps	1.0 %
5 000	600 sec	50	48 kbps	1 Mbps	4.8 %
5 000	300 sec	100	96 kbps	1 Mbps	9.6 %

IPv6 Multicast[1]

Multicast WiFi Usage by Sleeping Devices

Low Power WiFi Clients

- To save their batteries, Low Power (LP) hosts go into radio sleep mode until there is a local need to send a wireless frame.
- LP clients wake up periodically to listen to the WiFi beacon frames indicating whether there is multicast-traffic waiting.
- ALL LP hosts must stay awake to receive all multicast frames.

IPv6 Multicast [1]

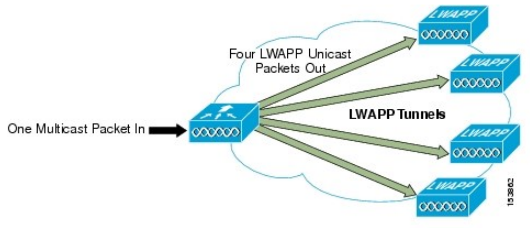
Multicast WiFi Impact on Low Power Hosts

Beacon frames/sec	Mcast frames/sec	Mcast frame size (bytes)	Lowest WiFi Rate	Awake time/sec
10	0	300 bytes	1 Mbps	2.4 %
10	5	300 bytes	1 Mbps	3.6 %
10	10	300 bytes	1 Mbps	4.8 %
10	50	300 bytes	1 Mbps	14.4 %

The Multicast Distribution Problem

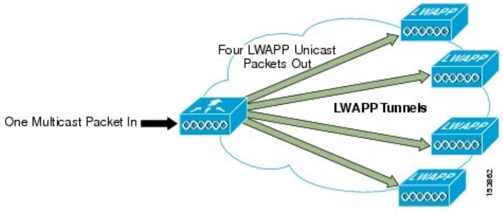
On Controller based WiFi Networks in Cisco Space

Multicast Distribution Problem [4]



- Controller delivered multicast packets to WLAN clients by making copies.
- Forwarding packets through a unicast Lightweight Access Point Protocol (LWAPP) tunnel to each AP connected to the controller.

Multicast Distribution Problem [4]



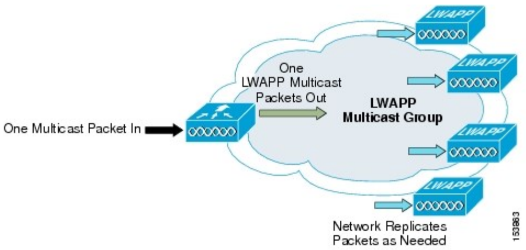
- Depending on the number of APs, the controller might need to generate up to 300 copies of each multicast packet.
- Places a large processing burden on the controller.
- Flooding the network with a large number of duplicate unicast packets.

Beware

- Take care: This “feature” DOES NOT solve the IPv6 multicast problem discussed above but just discusses WLC <-> AP multicast distribution.

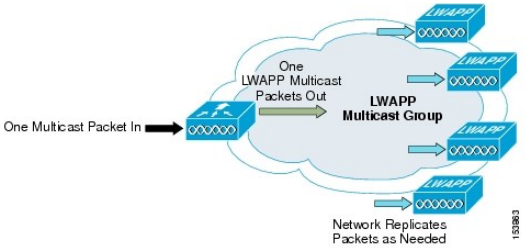
Multicast Distribution Problem [4]

And how to solve it the Cisco way



- Multicast performance has been optimized, by introducing a more efficient way of delivering multicast traffic from the controller to the access points.
- LWAPP multicast group is used to deliver the multicast packet to each access point.
- Allows routers in the network to use standard multicast techniques to replicate and deliver multicast packets to the APs.

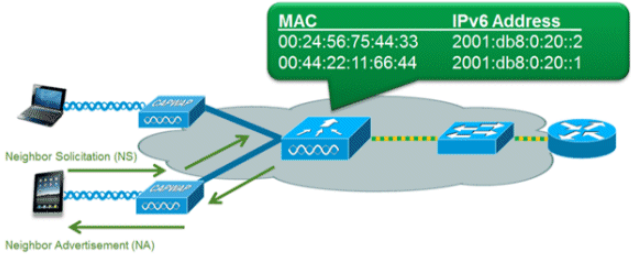
Multicast -> Multicast Distribution [4]



- Multicast packet are transmitted to the LWAPP multicast group via the management interface.
- Multicast packet are being delivered to each of the access point using the normal multicast mechanisms in the routers.

How to Reduce the Chatter of IPv6 in WiFi Networks

NDP Proxy



- Neighbor discovery caching allows the controller to act as a proxy and respond back to NS queries that it can resolve.
- Is made possible by the underlying neighbor binding table present in the controller.

Neighbor Binding Table on WLC

10.20.40.10 - PuTTY

```
summary         Display the IPv6 Neighbor Binding Table

(Cisco Controller) >show ipv6 neighbor-binding SUMmary
Binding Table has 173 entries, 173 dynamic (limit 11000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk             0004:Orig access
0008:Orig trusted trunk     0010:Orig trusted access    0020:DHCP assigned
0040:Cga authenticated      0080:Cert authenticated     0100:Statically assigned


    IPv6 address                                MAC Address        Port  VLAN Type      prlvl age  state     Time left
-- ------------------------------------------- ----------------- ----- ---- --------- ----- ---- --------- ----------
ND  fe80::fedb:b3ff:fe48:d6e6                   fc:db:b3:48:d6:e6    AP   10 wireless  0005    5 STALE      87917
ND  fe80::dafc:93ff:fe8b:6faa                   d8:fc:93:8b:6f:aa    AP   10 wireless  0005   36 STALE      88191
ND  fe80::bef5:acff:fef8:9ce5                   bc:f5:ac:f8:9c:e5    AP   30 wireless  0005    7 STALE      88784
ND  fe80::aebc:32ff:fed2:de8f                   ac:bc:32:d2:de:8f    AP   10 wireless  0005   11 STALE      89981
ND  fe80::ad24:85f3:b84a:7347                   18:5e:0f:eb:1f:27    AP   10 wireless  0005    5 STALE      90461
ND  fe80::aa66:7fff:fe1a:66c8                   a8:66:7f:1a:66:c8    AP   10 wireless  0005    3 REACHABLE  122
ND  fe80::a6e4:b8ff:fe51:8390                   a4:e4:b8:51:83:90    AP   10 wireless  0005   30 STALE      86388
ND  fe80::a65e:60ff:fed2:729                    a4:5e:60:d2:07:29    AP   10 wireless  0005   11 STALE      87166
ND  fe80::9ad6:f7ff:fe96:bd66                   98:d6:f7:96:bd:66    AP   30 wireless  0005   11 STALE      88756
ND  fe80::8938:cac5:6c54:47                     5c:51:4f:87:e7:c7    AP   40 wireless  0005    3 REACHABLE  118
ND  fe80::868e:dfff:fee7:cc1c                   84:8e:df:e7:cc:1c    AP   10 wireless  0005   38 STALE      88401
ND  fe80::80ec:8805:f2a1:1f3f                   dc:f1:10:8b:5b:20    AP   10 wireless  0005   21 STALE      88366
ND  fe80::7ed1:c3ff:fee8:a8bb                   7c:d1:c3:e8:a8:bb    AP   30 wireless  0005    2 REACHABLE  178

--More-- or (q)uit
```

IPv6 RA Throttling

RA Throttle Policy > Edit

Enable RA Throttle Policy	☑	
Throttle Period (10-86400 seconds)	600	
Max Through (0-256)	5	No Limit ☐
Interval Option	Throttle ▼	
Allow At-least (0-32)	1	
Allow At-most (0-256)	1	No Limit ☐

- Routers which are configured to send RAs very often (e.g. every 3 seconds) can be trimmed back to a minimum frequency that will still maintain IPv6 client connectivity.
- Allows airtime to be optimized by reducing the number of multicast packets that must be sent.
- If a client sends an RS, then an RA will be allowed through the controller. Ensures no negatively impact by RA throttling.

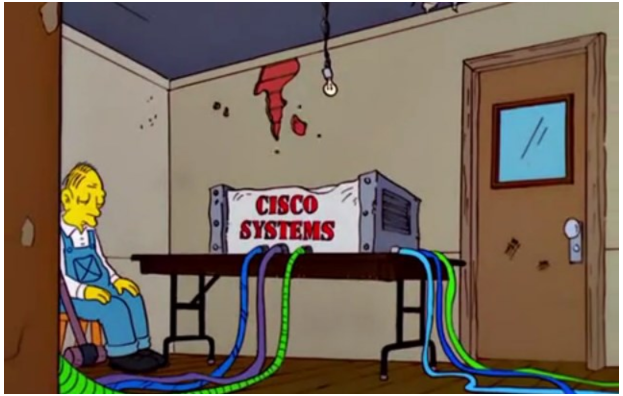
Gateway Configuration

- To reduce the multicast traffic the following parameters were adjusted:
- Router lifetime to 9000 seconds
- Reachable lifetime to 900 Seconds
- Unicast solicited RAs
- Inspired by Andrew Yourtchenko
  - Thank You!

How to Properly Secure an IPv6 WiFi Network

Cisco First-Hop-Security Features on the WLC

Cisco First-Hop-Security



- Cisco term for various security features in the IPv6 space
- The WLC does support a number of features discussed below

Cisco IPv6 Snooping

- IPv6 Snooping is the basis for several FHS security mechanisms
- Used to build the security binding table on the WLC for the following FHS features

RA Guard

- Implements *isolation* principle similar to other L2 protection mechanisms already deployed in v4 world.
- RFC 6105
- Acts a stateless ACL filter for ICMPv6 type 134

DHCPv6 Guard

- Similar functionality to DHCP Snooping in the IPv4 world
  - But more sophisticated
- Blocks reply and advertisement messages that originates from “malicious” DHCP servers and relay agents
- Provides finer level of granularity than DHCP Snooping.
- Messages can be filtered based on the address of the DHCP server or relay agent, and/or by the prefixes and address range in the reply message.

IPv6 Source Guard

- Prevents a wireless client spoofing an IPv6 address of another client.
- IPv6 Source Guard is enabled by default but can be disabled via the CLI.

IPv6 ACLs

- v6 Access Control Lists (ACLs) can be used to identify traffic and permit or deny it.
- IPv6 ACLs support the same options as IPv4 ACLs including source, destination, source port, and destination port (port ranges are also supported).

FHS on WLC Controller

FHS Feature	Default	Configurable
RA Guard	Enabled	Yes (only on AP)
DHCPv6 Guard	Enabled	No
IPv6 Source Guard	Enabled	Yes
IPv6 ACLs	Disabled	Yes

RA Guard Configuration

IPv6 ACL on WLC

Seq	Action	Source IPv6/Prefix Length	Destination IPv6/Prefix Length	Protocol	Source Port	Dest Port	DSCP	Direction	Num
1	Deny	:: / 0	:: / 0	UDP	Any	5353	Any	Any	0
2	Permit	:: / 0	:: / 0	Any	Any	Any	Any	Any	0

Summar

- Given the nature of IPv6 link layer behavior, reducing the amount of chatter must be taken care of.

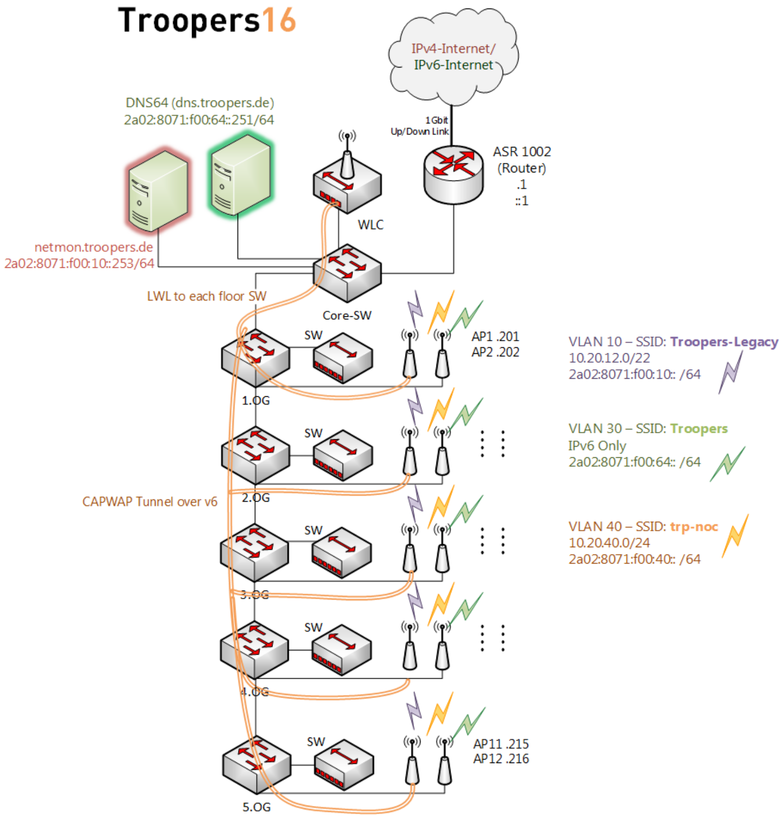
- By means of configuration tweaks in regards to multicast traffic as well as supporting features on the WiFi Controller.

- The WLC supports quite a lot of FHS security mechanisms which are enabled in the default state.

Troopers Network Infrastructure

Network Overview

- Network diagram
- Components
- NAT64, implementation details
- Monitoring Solution and statistics



Network Design Overview

Network Devices

- Cisco ASR 1002 Gateway
  - `Cisco IOS Software, ASR1000 Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.5(3)S2`
- Also provides NAT64 functionality for the "Troopers" SSID
- Might be a little bit oversized, but in Germany we have a saying „viel hilft viel" ;-)
  - See RFC 1925 truth nr. 9 :-)

Network Devices

- Cisco 4948E as Core Switch
- Provides connectivity to all floor distribution switches

Network Devices

- WLCs
  - Cisco 2504 running

```
Product Version..........8.2.100.0
```

- No HA besides a second WLC as cold standby down in the basement ,)

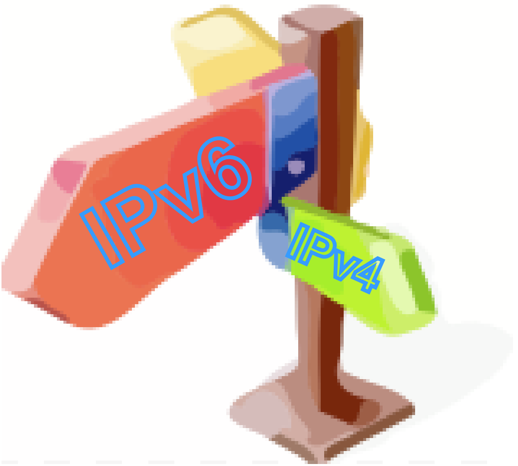
Access Points

Cisco 1602 model with internal and external antennas.

17 APs in total deployed

NAT64 Deployment@Troopers

NAT64 & DNS64



- Unbound on FreeBSD for DNS64
  - https://github.com/Flast/unbound-dns64
  - `Version 1.5.7`
- Stateful NAT64 implemented on ASR 1002

DNS64

Unbound Version 1.4.20 with dns64 licensed under the BSD license

- Unbound is installed as part of the base system in FreeBSD since version 10.0.
- It is a DNS server designed for high-performance.

- The Ecdysis Project (open-source implementation of NAT64) released a patch for support of DNS64 in unbound
  - http://ecdysis.viagenie.ca/instructions.html

DNS64

Unbound Version 1.5.7 with dns64 configuration


```
## See unbound.conf(5) man page, version 1.5.7.
## The server clause sets the main parameters.
server:
     # specify the interfaces to answer queries from by
     ip-address.    interface: 2a02:8071:f00:64::251

     # specify the interfaces to send outgoing queries
     to authoritative
     # server from by ip-address.
     outgoing-interface: 2a02:8071:f00:64::251
     outgoing-interface: 10.20.40.51

     # Enable IPv6
     do-ip6: yes
```

DNS64


```
# module configuration of the server.
# A string with identifiers separated by spaces.
module-config: "dns64 iterator‟

# DNS64 prefix. Must be specified when
# DNS64 is in use.
dns64-prefix: 2003:60:4010:6464::/96
```

ASR NAT 64 Config


```
interface GigabitEthernet0/0/0.30
 <output omitted>
 description ====TRP-NAT64===
 encapsulation dot1Q 30
 ipv6 address FE80::1 link-local
 ipv6 address 2A02:8071:F00:64::1/64
 ipv6 enable
 ipv6 mtu 1280
 ipv6 nd reachable-time 900000
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
 ipv6 nd ra solicited unicast
 ipv6 nd ra lifetime 9000
 ipv6 nd ra interval 4
 ipv6 nd ra dns server 2A02:8071:F00:64::251
 ipv6 dhcp server DHCP-TRP-NAT64-v6-POOL
 nat64 enable
```

ASR NAT 64 Config


```
ipv6 dhcp pool DHCP-TRP-NAT64-v6-POOL
 dns-server 2A02:8071:F00:64::251
 domain-name troopers.net

nat64 prefix stateful 2003:60:4010:6464::/96

nat64 v4 pool NAT64-POOL 10.50.50.3
10.50.50.254

nat64 v6v4 list NAT64-ACL pool NAT64-POOL
overload
```

Basic Connectivity Test

```
C:\Users\sMk>ping www.troopers.de

Pinging www.troopers.de [2003:60:4010:1090::40] with 32 bytes of data:
Reply from 2003:60:4010:1090::40: time=64ms
Reply from 2003:60:4010:1090::40: time=105ms
Reply from 2003:60:4010:1090::40: time=45ms
Reply from 2003:60:4010:1090::40: time=89ms

Ping statistics for 2003:60:4010:1090::40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 105ms, Average = 75ms

C:\Users\sMk>ping www.twitter.com

Pinging twitter.com [2003:60:4010:6464::68f4:2ac1] with 32 bytes of data:
Reply from 2003:60:4010:6464::68f4:2ac1: time=35ms
Reply from 2003:60:4010:6464::68f4:2ac1: time=54ms
Reply from 2003:60:4010:6464::68f4:2ac1: time=16ms
Reply from 2003:60:4010:6464::68f4:2ac1: time=59ms

Ping statistics for 2003:60:4010:6464::68f4:2ac1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 59ms, Average = 41ms
```

Some Statistics from the ASR

```
trp-gw1#show nat64 statistics
NAT64 Statistics

Total active translations: 291 (0 static, 291 dynamic; 291 extended)
Sessions found: 17474823
Sessions created: 71432
Expired translations: 71255
Global Stats:
   Packets translated (IPv4 -> IPv6)
      Stateless: 0
      Stateful: 11208720
      MAP-T: 0
   Packets translated (IPv6 -> IPv4)
      Stateless: 0
      Stateful: 6337649
      MAP-T: 0
```

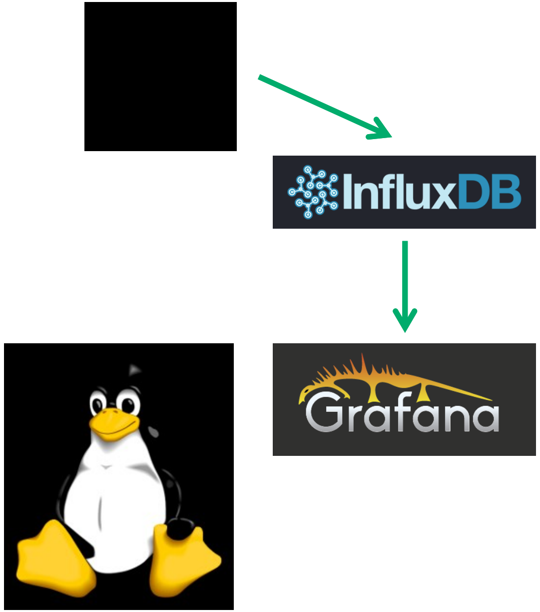
IPv4/IPv6 Traffic/Client Statistics

During the IPv6 Security Summit

Monitoring Infrastructure

- Goals:
  - Traffic overview
  - Split into IPv4 and IPv6
  - How many clients in total
  - How many IPv4 only, Dual-Stack or IPv6 only clients are active
  - WLAN usage overview
    - 802.11b, 802.11g, and 802.11n on 2.4GHz band
    - 802.11a and 802.11n on 5GHz band

Monitoring Infrastructure



- Linux webserver
- Collector: collectd
  - Collecting information via SNMPv3
  - And some additional scripts
- Database: influxdb
- Frontend: Grafana

How it gets collected

https://collectd.org/

Net-SNMP

- Collecting the data with collectd via SNMPv3
  - ```
    <Plugin snmp>
    <Data "gw.bandwidth.v4">
       Type "if_octets"
       Table true
       Instance "IF-MIB::ifName"
       InstancePrefix "ipv4."
       Values "$MIB-IN" "$MIB-OUT"
    </Data>
    ```
- Additional data is collected via SNMPv3 with the net-snmp tools
- `snmpget -v3 -u $RUSER -l authPriv -a sha -A $AUTH -x aes -X $PASS udp6:[$IPv6] $MIB`
- `snmpwalk -v3 -u $RUSER -l authPriv -a sha -A $AUTH -x aes -X $PASS udp6:[$IPv6] $MIB`
- Every 300sec
    ```

How it get stored and displayed

https://influxdata.com/time-series-platform/influxdb

http://grafana.org/

- The Collected data are stored into the Influxdb Database
  - Good database for storing time series data
- The fronted Grafana is used to display the collected data
  - Request the stored data from the Influxdb
  - Example request for the RX Bandwidth of the GW Interface:
  - ```
    SELECT non_negative_derivative("value", 1s) FROM "snmp_rx" WHERE "host" = 'gw.troopers.net' AND "type_instance" = 'Gi0_0_1' AND $timeFilter
    ```
    ```

SNMP-MIBs

Bandwidth and Traffic

- MIB IF-MIB-
  Object ifHCInOctets
  OID 1.3.6.1.2.1.31.1.1.1.6.$INTERFACE
- MIB IF-MIB
  Object ifHCOutOctets
  OID 1.3.6.1.2.1.31.1.1.1.10.$INTERFACE
- MIB IP-MIB
  Object ipIfStatsHCInOctets
  OID 1.3.6.1.2.1.4.31.3.1.6.IPv4.$INTERFACE
  OID 1.3.6.1.2.1.4.31.3.1.6.IPv6.$INTERFACE
- MIB IP-MIB
  Object ipIfStatsHCOutOctets
  OID 1.3.6.1.2.1.4.31.3.1.33.IPv4.$INTERFACE
  OID 1.3.6.1.2.1.4.31.3.1.33.IPv6.$INTERFACE

WLAN

WLAN-Clients per Band

- Queries the client IDs per wireless band
  - MIB AIRESPACE-WIRELESS-MIB
    Object bsnMobileStationProtocol
    OID .1.3.6.1.4.1.14179.2.1.4.1.25

- Queries the association of client ID to SSID
  - MIB AIRESPACE-WIRELESS-MIB
    Object bsnDot11EssSsid
    OID .1.3.6.1.4.1.14179.2.1.1.1.2

- Queries the number of clients connected to SSID
  - MIB AIRESPACE-WIRELESS-MIB
    Object bsnDot11EssNumberOfMobileStations
    OID .1.3.6.1.4.1.14179.2.1.1.1.38

Clients

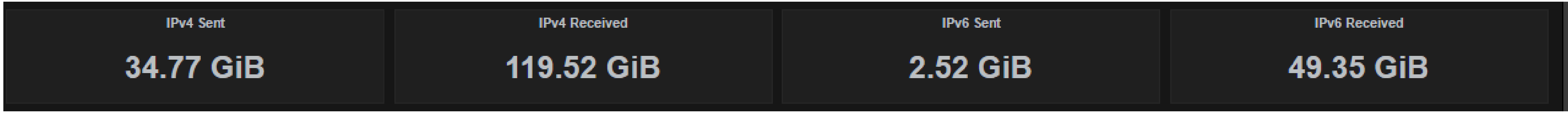
IPv4 & IPv6 Clients per VLAN

- MIB IP-MIB
- Object ipNetToPhysicalPhysAddress
- OID 1.3.6.1.2.1.4.35.1.4.$VLAN.ipv4
- OID 1.3.6.1.2.1.4.35.1.4.$VLAN.ipv6

- Compare ARP and Neighbor cache tables with a python script to get the IPv4, Dual-Stack and IPv6 number of clients

Generated Traffic

- Sunday to Tuesday 8:00

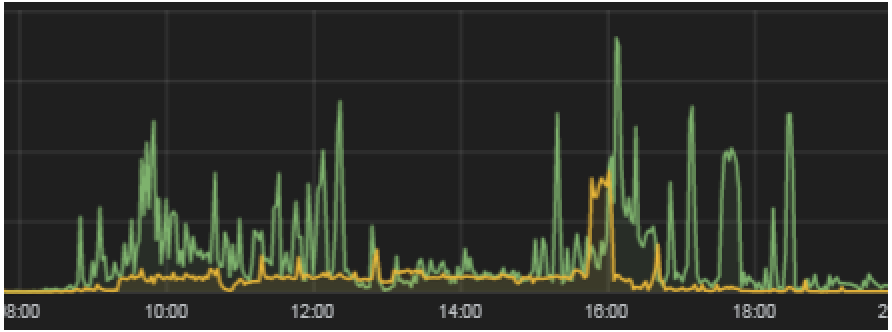


Uplink Bandwidth Statistics (Total)

Sunday to Tuesday 8:00

Max down: 18,6 MB/s

Max up:2551: 8,5 MB/s

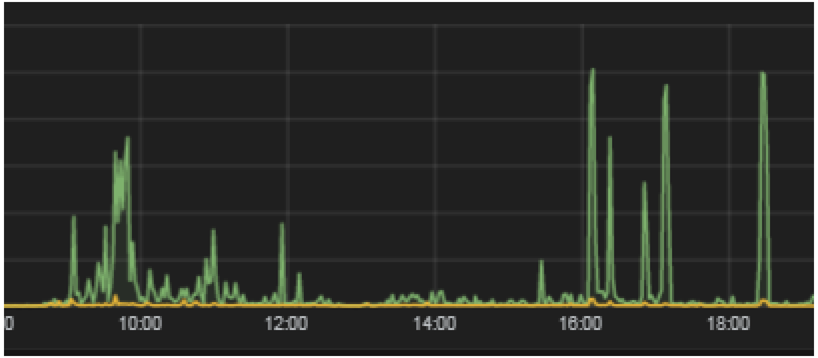


Uplink Bandwidth IPv6

Since Sunday to Monday 20:00

Max down:59810 kbit/s ≈ 11,5 MB/s

Max up:1957 kbit/s ≈ 0,5 MB/s



Clients per Wireless Band

Sunday to Tuesday 8:00

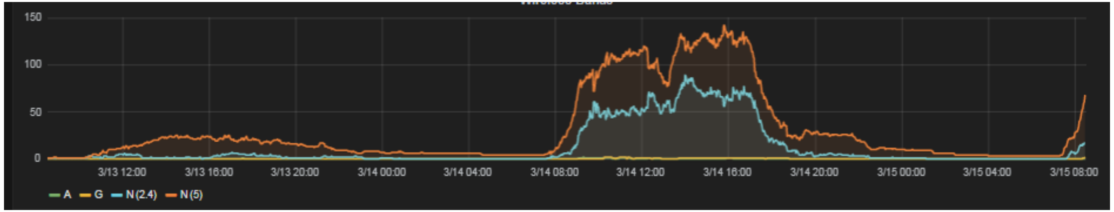
Max WLAN clients: 209

Max clients 802.11a: 1

Max clients 802.11g: 1

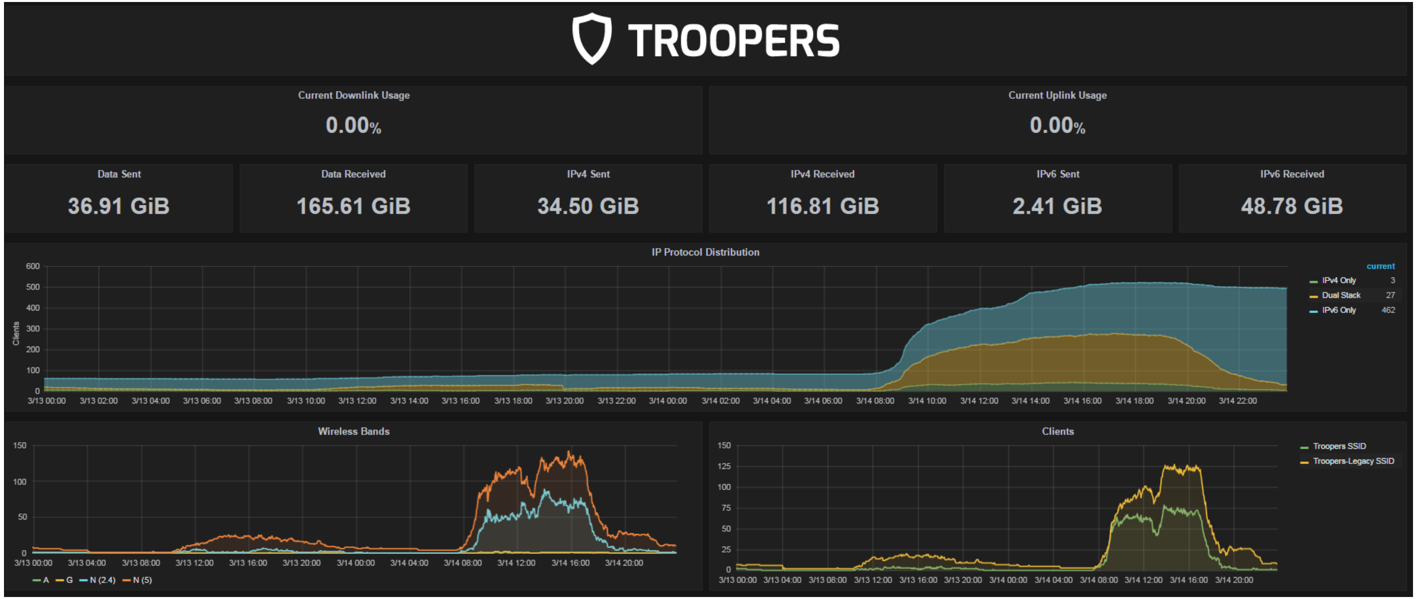
Max clients 802.11n: 86

Max clients 802.11n (5Gz): 142



Kudos to Pascal and Rafael for setting up this awesome monitoring !!

- Visit Troopers16 Network Monitor: netmon.troopers.de



There's never enough time…

THANK YOU… ...for yours!

Questions & Discussion

References

- [1] - Why Network-Layer Multicast is Not Always Efficient At Datalink Layer
  - http://tools.ietf.org/html/draft-vyncke-6man-mcast-not-efficient-01
- [2] - Reducing Multicast in IPv6 Neighbor Discovery
  - http://tools.ietf.org/html/draft-yourtchenko-colitti-nd-reduce-multicast-00
- [3] – Cisco WiFi Client IPv6 Deployment Guide
  - http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113427-cuwn-ipv6-guide-00.html
- [4] - Cisco Unified Wireless Multicast Design
  - http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/MCast.html
- [5] – Reducing Energy Consumption of Router Advertisements
  - https://www.rfc-editor.org/rfc/rfc7772.txt