



CASE STUDY: BUILDING A SECURE AND RELIABLE IPv6 GUEST WIFI NETWORK

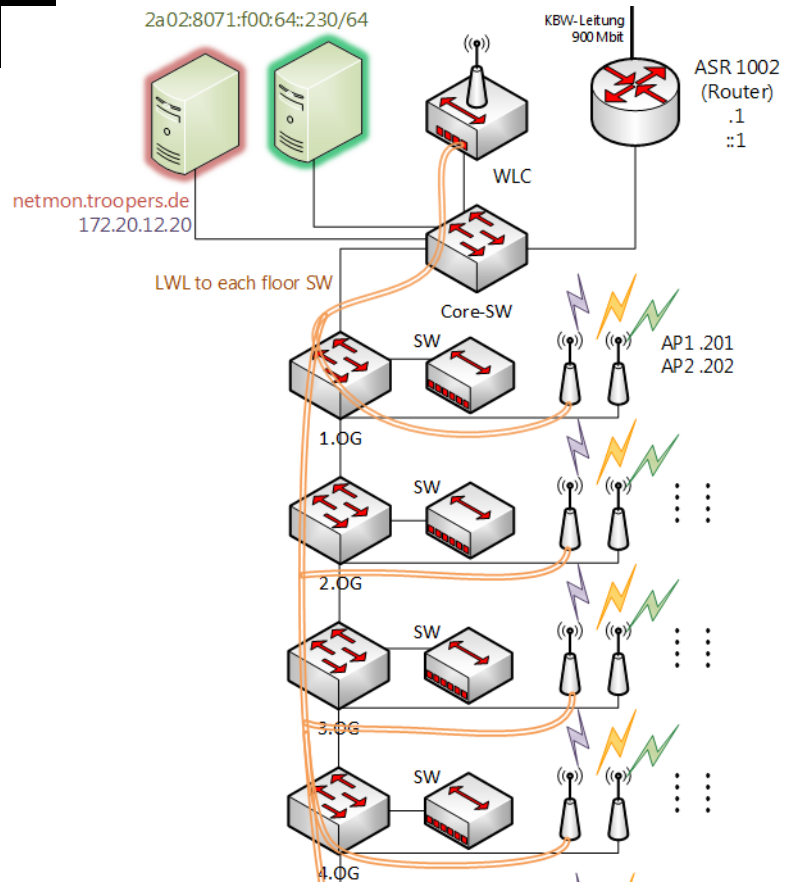


Christopher Werny, cwerny@ernw.de

Network Overview



- Network diagram
- Components
- Monitoring Infrastructure
- NAT64, implementation details



VLAN 10 – SSID: **Troopers15**
172.20.12.0/22
2a02:8071:f00:10: /64

VLAN 30 – SSID: **Troopers15-NAT64**
2a02:8071:f00:64: /64

VLAN 40 – SSID: **trp-noc**
172.20.40.0/24
2a02:8071:f00:40: /64

Network Design Overview

netmon.troopers.de
(Network Monitor)



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.
- Bring an AP with you to plug in and find out where you can hear it.



Speaking of Interference.....

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

Rogues

124 APs 1 Clients

Entries 1 - 50 of 118





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



Network Overview Devices

- Gateway (Fully Dual-Stack)

- Cisco ASR 1002 running

Cisco IOS Software, ASR1000 Software
(PPC_LINUX_IOSD-ADVENTERPRISEK9-M),
Version 15.4(3)S2



Network Overview Devices

- WLCs
 - Cisco 2504 running
Product Version.....8.0.110.0



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



Access Points

Cisco 1242 & 1602 models



Monitoring Infrastructure



Goals:

- Traffic overview
- Split into IPv4 and IPv6
- How many clients in total
- How many IPv4 only or 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



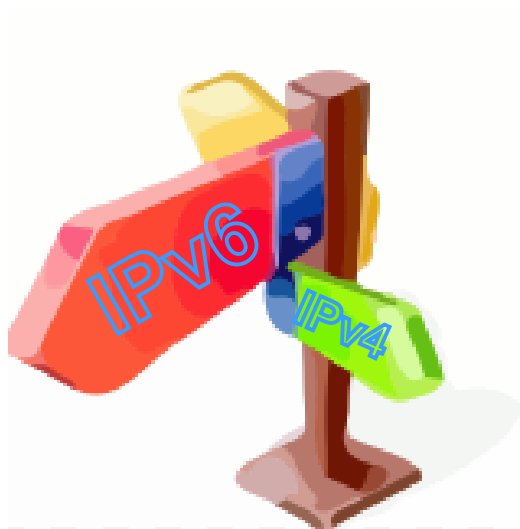
Monitoring Infrastructure



- Linux with a webserver and some dirty Scripts ;)
 - Details later on
- Monitoring system c3netmon
 - customized to achieve our goals
 - <https://github.com/FremaksGmbH/c3netmon-public>
- Collecting information via SNMPv3



NAT64 & DNS64



- Unbound on FreeBSD for DNS64
 - <https://github.com/Flast/unbound-dns64>
 - Version 1.5.2
- 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 1.5.2 with dns64
configuration



```
## See unbound.conf(5) man page, version 1.5.2.
## The server clause sets the main parameters.
server:
    # specify the interfaces to answer queries from by
    ip-address.    interface: 2a02:8071:f00:64::230

    # specify the interfaces to send outgoing queries
    to authoritative
    # server from by ip-address.
    outgoing-interface: 2a02:8071:f00:64::230
    outgoing-interface: 172.20.40.22

    # 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
<output omitted>
ip address 10.10.10.1 255.255.255.0
<output omitted>
nat64 enable
```

```
interface GigabitEthernet0/0/1.30
<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 other-config-flag
ipv6 nd router-preference High
ipv6 nd ra dns server 2A02:8071:F00:64::230
```



ASR NAT 64 Config



```
ipv6 dhcp pool NAT64
  dns-server 2a02:8071:f00:64::230
  domain-name troopers.net

ipv6 access-list nat64-acl
  permit ipv6 any 2003:60:4010:6464::/96

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

nat64 v4 pool nat64-pool 10.10.10.3
10.10.10.254

nat64 v6v4 list nat64-acl pool nat64-pool
overload
```



Basic Connectivity Test

```
C:\Users\sMk>ping blackout-problems.com
```

```
Pinging blackout-problems.com [2003:60:4010:6464::3e9f:60b3] with 32 bytes of data:  
Reply from 2003:60:4010:6464::3e9f:60b3: time=11ms  
Reply from 2003:60:4010:6464::3e9f:60b3: time=11ms  
Reply from 2003:60:4010:6464::3e9f:60b3: time=11ms  
Reply from 2003:60:4010:6464::3e9f:60b3: time=11ms
```

```
Ping statistics for 2003:60:4010:6464::3e9f:60b3:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 11ms, Maximum = 11ms, Average = 11ms
```

```
C:\Users\sMk>ping www.cisco.com
```

```
Pinging e144.dscb.akamaiedge.net [2a02:26f0:6a:287::90] with 32 bytes of data:  
Reply from 2a02:26f0:6a:287::90: time=8ms  
Reply from 2a02:26f0:6a:287::90: time=8ms  
Reply from 2a02:26f0:6a:287::90: time=8ms  
Reply from 2a02:26f0:6a:287::90: time=8ms
```

```
Ping statistics for 2a02:26f0:6a:287::90:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 8ms, Maximum = 8ms, Average = 8ms
```

```
TRP-GW1#show nat64 statistics
NAT64 Statistics
```

```
Total active translations: 43 (0 static, 43 dynamic; 43 extended)
Sessions found: 21726533
Sessions created: 8977
Expired translations: 8936
Global Stats:
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 12840831
    MAP-T: 0
  Packets translated (IPv6 -> IPv4)
    Stateless: 0
    Stateful: 8894681
    MAP-T: 0
```

Interface Statistics

```
GigabitEthernet0/0/0.30 (IPv4 not configured, IPv6 configured):
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 0
    MAP-T: 0
  Packets translated (IPv6 -> IPv4)
    Stateless: 0
    Stateful: 8894681
    MAP-T: 0
  Packets dropped: 162
GigabitEthernet0/0/0.1 (IPv4 configured, IPv6 configured):
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 12840831
    MAP-T: 0
```

Some Statistics from the ASR



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 Solicitation 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 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.
- AP to store unicast and multicast frames.
- 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.



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

IPv6 Multicast [1]

Multicast WiFi Impact on Low Power Hosts



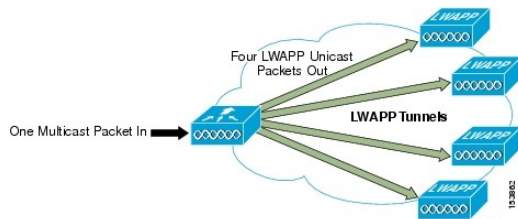
The Multicast Distribution Problem

On Controller based WiFi Networks in Cisco Space





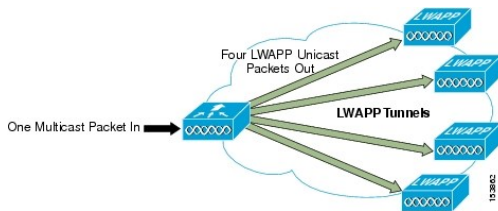
Multicast Distribution Problem [4]



- 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

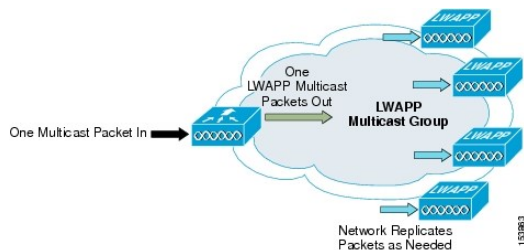


- Take care: This “feature” DOES NOT solve the IPv6 multicast problem discussed above but just discusses WLC <-> AP multicast distribution.



Multicast Distribution Problem [4]

And how to solve it the Cisco way

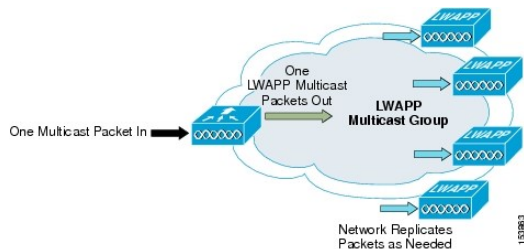


- Multicast performance has been optimized, by introducing a more efficient way of delivering multicast traffic from the controller to the access points.
- LWAPP multicast group is used to deliver the multicast packet to each access point.
- Allows routers in the network to use standard multicast techniques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



Multicast -> Multicast Distribution [4]

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





Considerations



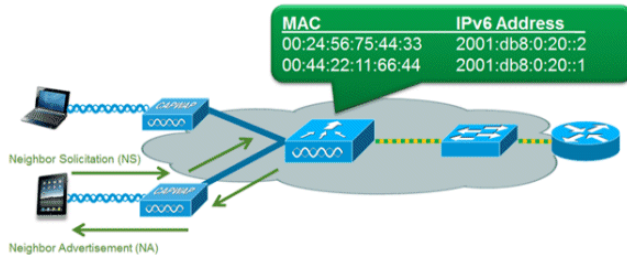
- Multicast packets received on the VLAN from the first hop router is transmitted over the wireless network, including HSRP hellos and all router EIGRP and PIM multicast packets.
- Could seriously degrade the WLAN throughput for clients if e using millisecond hellos with HSRP on the client VLAN.



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.



IPv6 RA Throttling

TODO BILD VON CONFIG PARAMETER

- 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
- Inspired by Andrew Yourtchenko
 - Thank You!



ASR Interface Configuration

```
interface GigabitEthernet0/0/1.10
description ===CON===
encapsulation dot1Q 10
ip address 172.20.12.1 255.255.252.0
ip access-group DENY_MGMT in
no ip redirects
no ip proxy-arp
ipv6 address FE80::1 link-local
ipv6 address 2003:60:4010:2010::1/64
ipv6 enable
ipv6 mtu 1300
ipv6 nd reachable-time 900000
ipv6 nd other-config-flag
ipv6 nd router-preference High
ipv6 nd ra lifetime 9000
no ipv6 redirects
ipv6 dhcp server CON
ipv6 traffic-filter DENY6_MGMT in
```



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).

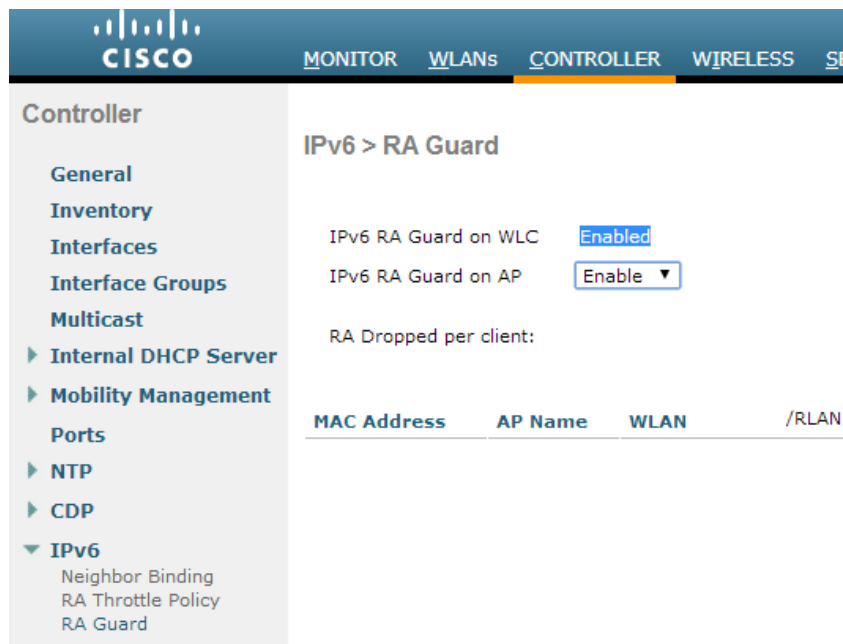


FHS on WLC Controller

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



The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The left sidebar lists various configuration categories, with 'IPv6' expanded to show 'Neighbor Binding', 'RA Throttle Policy', and 'RA Guard'. The main content area is titled 'IPv6 > RA Guard' and contains the following settings:

- IPv6 RA Guard on WLC: Enabled
- IPv6 RA Guard on AP: Enable ▼
- RA Dropped per client:

MAC Address	AP Name	WLAN	/RLAN
-------------	---------	------	-------



IPv6 ACL on WLC

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



IPv4/IPv6 Traffic/Client Statistics

During the IPv6 Security Summit



How it gets collected

The Scripts



Net-SNMP

- Collecting the data via SNMPv3 with the net-snmp tools
- ```
snmpget -v3 -u $RUSER -l authPriv -a sha -A $AUTH -x aes -X $PASS $IP $MIB
```
- ```
snmpwalk -v3 -u $RUSER -l authPriv -a sha -A $AUTH -x aes -X $PASS $IP $MIB
```
- Every 30sec



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 ifHCOctets
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 ipIfStatsHCOctets
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



- MIB AIRESpace-WIRELESS-MIB
Object bsnDot11EssNumberOfMobileStations
OID 1.3.6.1.4.1.14179.2.1.1.1.38
- MIB AIRESpace-WIRELESS-MIB
Object bsnDot11EssVpnIkeLifetime
OID 1.3.6.1.4.1.14179.2.1.1.1.25



Clients

IPv4 & IPv6 Clients per VLAN



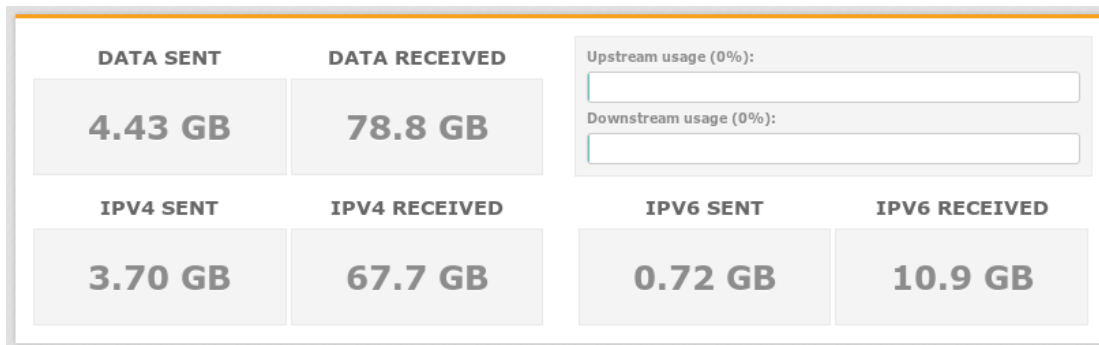
- MIB IP-MIB
- Object ipNetToPhysicalPhysAddress
- OID 1.3.6.1.2.1.4.35.1.4.\$VLAN.ipv4
- OID 1.3.6.1.2.1.4.35.1.4.\$VLAN.ipv6

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



Generated Traffic

Since Sunday to Monday 20:00



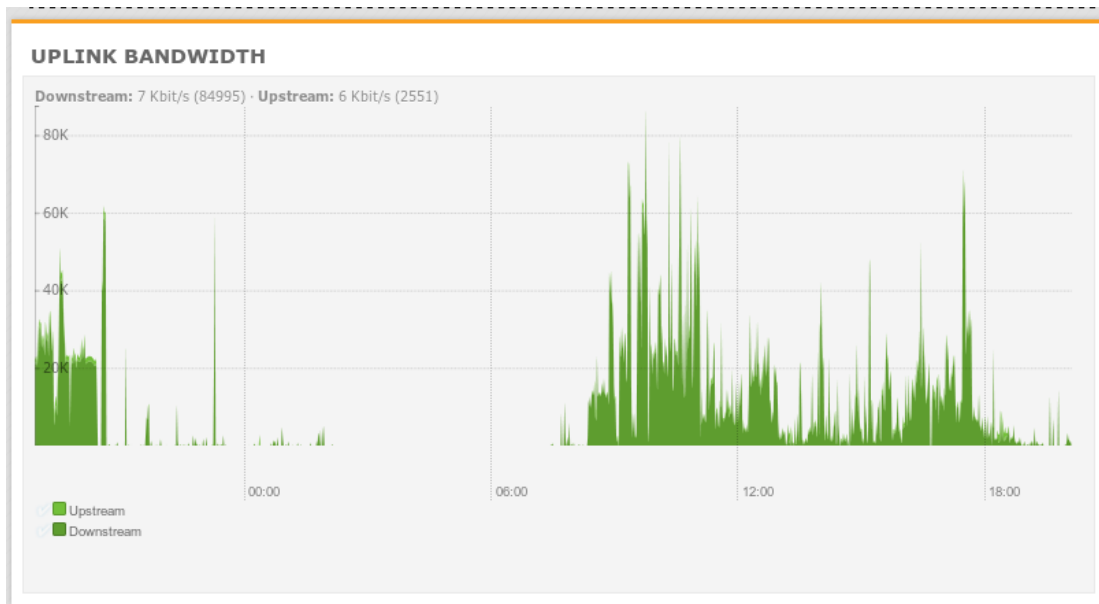


Uplink Bandwidth Statistics

Since Sunday to Monday 20:00

Max down: 84995 kbit/s \approx 10,6 MB/s

Max up: 2551 kbit/s \approx 0,3 MB/s



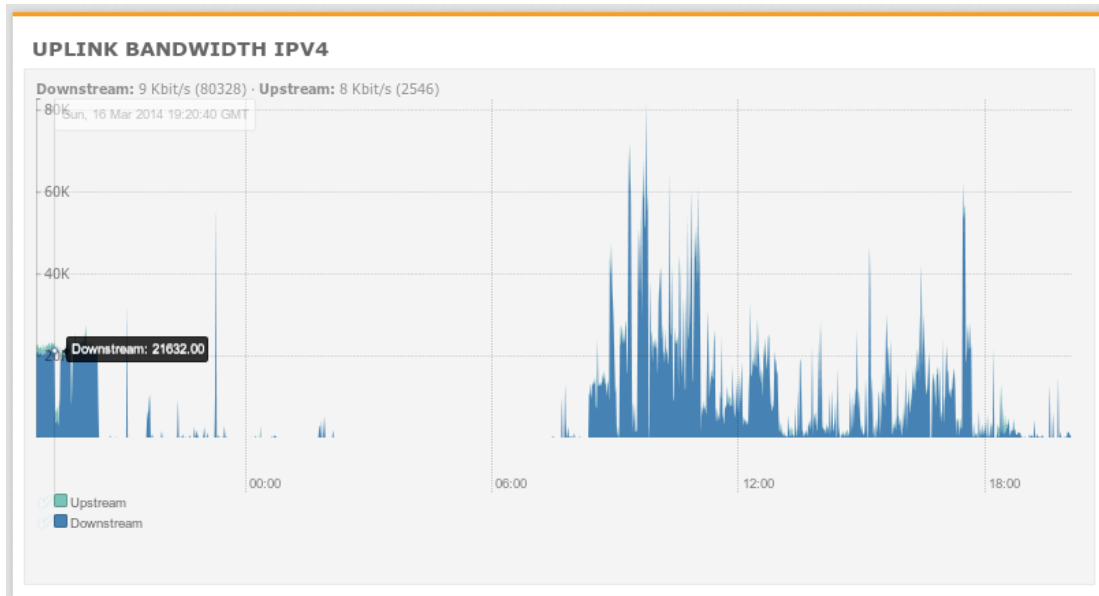


Uplink Bandwidth only IPv4

Since Sunday to Monday 20:00

Max down:80328kbit/s \approx 10 MB/s

Max up:2546 kbit/s \approx 0,3 MB/s



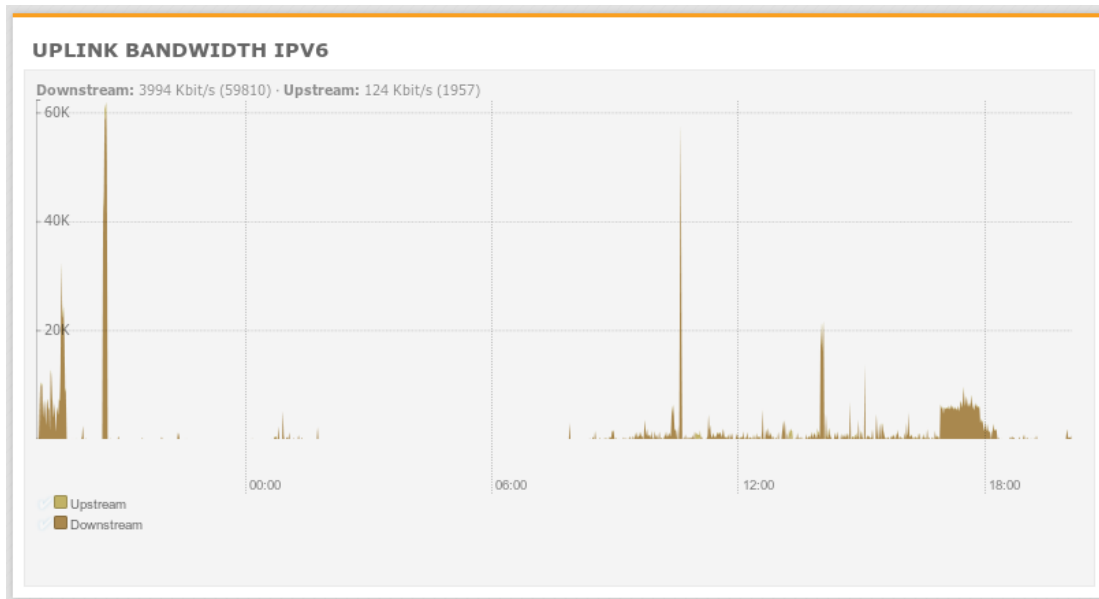


Uplink Bandwidth only IPv6

Since Sunday to Monday 20:00

Max down: 59810 kbit/s \approx 7,5 MB/s

Max up: 1957 kbit/s \approx 0,3 MB/s

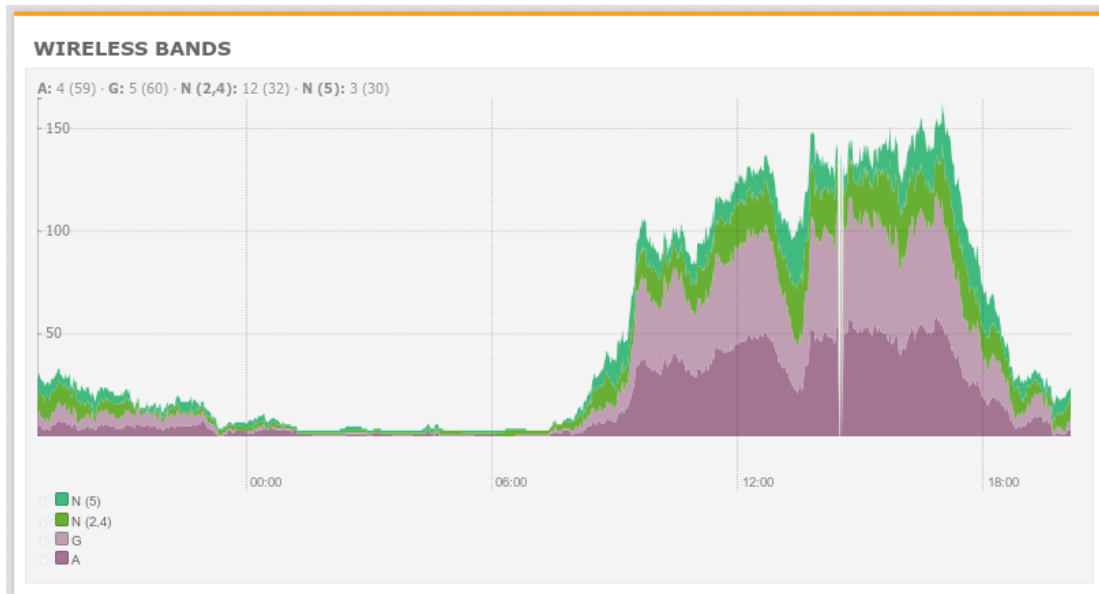




Clients per Wireless Band

Since Sunday to Monday 20:00

- Max WLAN clients: 181
- Max clients 802.11a: 59
- Max clients 802.11g: 60
- Max clients 802.11n: 32
- Max clients 802.11n (5Gz): 30





Only IPv4, Dual-Stack, only IPv6 - Clients

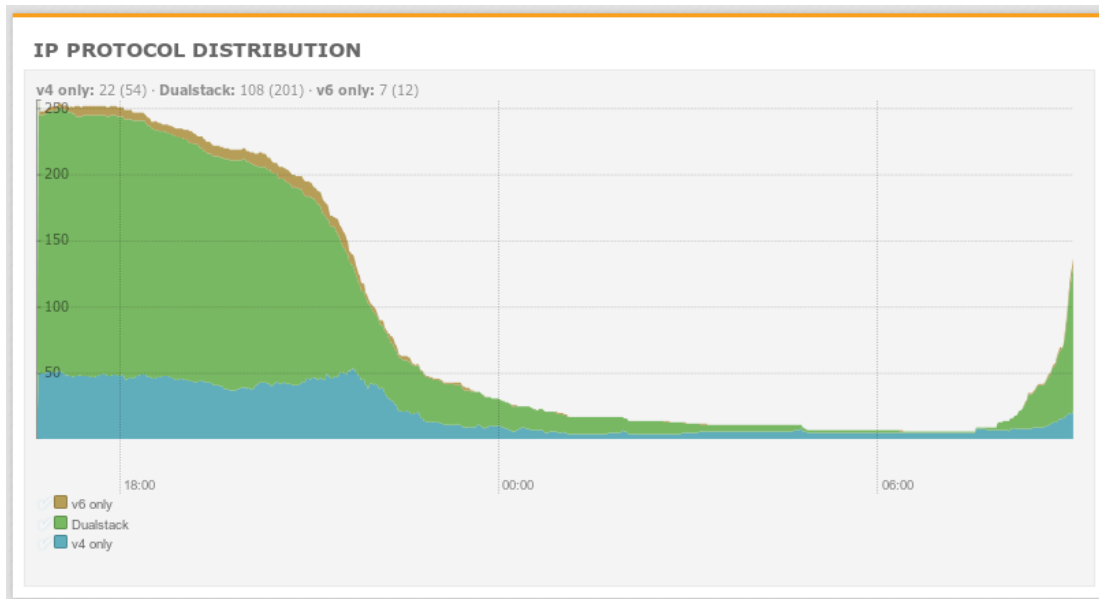
Since Monday to Tuesday 9:00

Max Devices: 262

Max IPv4 only: 52

Max Dual-Stack: 201

Max IPv6 only: 9

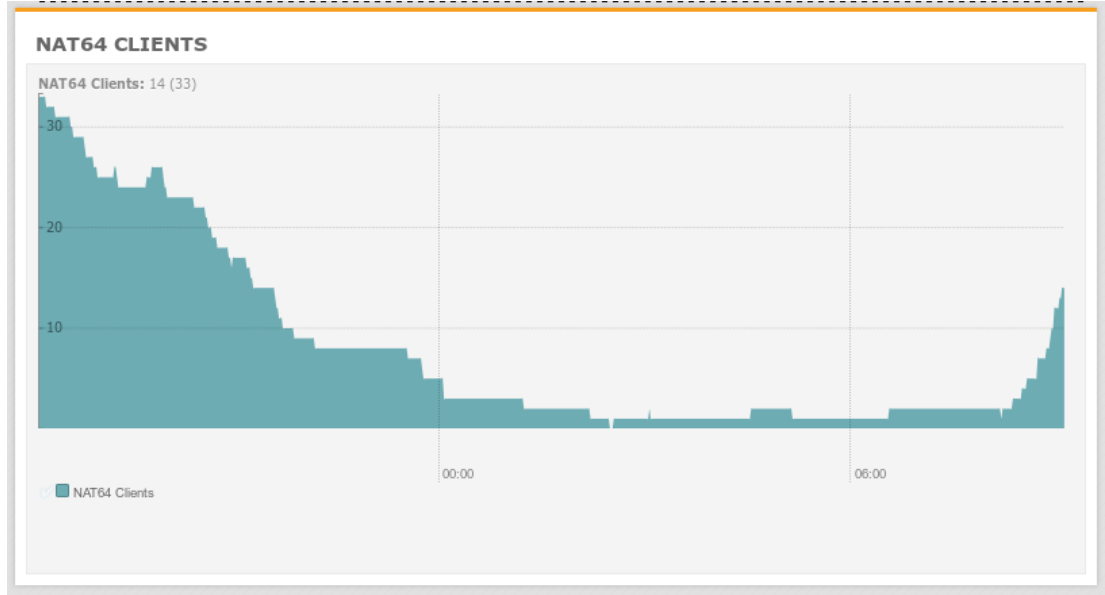




IPv6 only Clients NAT64-Vlan

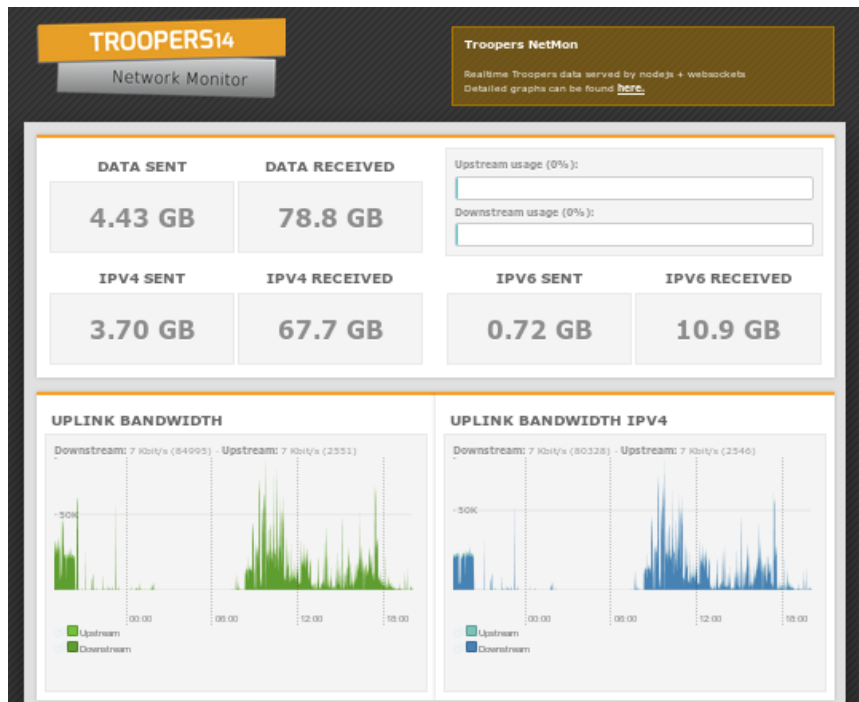
Since Monday to Tuesday 9:00

Max IPv6 only clients:33





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



Troopers Netmon

Visit Troopers15 Network Monitor: netmon.troopers.de



Summary etc.

- 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.



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>