Default IPv6 Local Only Addressing for Non-Internet Devices

draft-smith-v6ops-local-only-addressing-00

IETF-106

Mark Smith
markzzzsmith@gmail.com

New Home Printer

- Wifi/Wired/USB
- IPv6 (not enabled by default)
- Supports many protocols over IPv6

Spec. Sheet - IPv6

NDP, RA, DNS resolver, mDNS, LLMN responder, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP Server, TELNET Server, HTTP/HTTPS server, TFTP client and server, SMTP Client, SNMPv1/v2c, ICMPv6, Web Services (Print), CIFS Client, SNTP Client

Factory Default listening **TCP** ports on IPv6 **GUA**

nmap -6 -v -n -sT -p0-65535 -sV --version-all -O -oN

80/tcp open http Debut embedded httpd 1.30 (Brother/HP printer http admin)

443/tcp open ssl/http Debut embedded httpd 1.30 (Brother/HP printer http admin)

515/tcp open printer

631/tcp open http Debut embedded httpd 1.30 (Brother/HP printer http admin)

9100/tcp open jetdirect?

Factory Default listening **UDP** ports on IPv6 **GUA**

nmap -6 -v -n -sU -p0-65535 -sV --version-all -O -oN

69/udp open|filtered tftp

161/udp open snmp SNMPv1 server; 0 SNMPv3 server (public)

3702/udp open ventrilo Ventrilo 2.1.2+

5353/udp open mdns DNS-based service discovery

5355/udp open|filtered llmnr

41470/udp open|filtered unknown

Factory Default listening **Protocols** on IPv6 **GUA**

nmap -6 -v -n -sO -sV --version-all -O -oN

6 open tcp

17 open udp

43 open ipv6-route

58 open ipv6-icmp

Yeah, Nah.

515/tcp open printer
9100/tcp open jetdirect?

- Unauthenticated printing from the Internet.

69/udp open|filtered tftp

- TFTP???

161/udp open snmp SNMPv1 server; 0 SNMPv3 server (**public**)

- RW is not **private**, but not much better

3702/udp open ventrilo Ventrilo 2.1.2+

- “Ventrilo is a proprietary VoIP software that includes text chat.” - Wikipedia. ??????????????????

5353/udp open mdns DNS-based service discovery

- Exploit/exhaust via unicast?

Printer does not need a GUA address

All network printing and other access from within my network

- i.e. Only from Link-Local or ULA addresses

Trouble Is

Single SSID

GUA and ULA prefix – RA PIOs A=1, L=1

Printer configures unneeded GUA

Create new ULA only SSID?

Convenient mDNS doesn’t work.

Upstream Network Firewall?

Maybe. Can’t be sure.

Device can only assure what it can control.

Non-Technical User

At home I try to think like a (non-technical) user.

Create ULA only SSID? ✗

Check Network Firewall? ✗

Beyond my (imaginary) technical capability.

“Internet Proof” network software?

All IPv6 hosts configure GUAs by default

GUAs imply Internet connectivity.

Implied assumption of all network facing software is “Internet Proof”? Evidence shows otherwise.

“Internet Unsafe by default”?

End-to-End Argument Applies?

“The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system.”

More generally:

Do things where the results matter the most.

Do things where the best knowledge of what is and isn’t required is available.

If you want something done properly,

you need to do it yourself.

Default IPv6 Local Only Addressing for Non-Internet Devices

Proposal:

If **clear** and **obvious** to vendor that device doesn't need Internet access by default:

Only configure (SLAAC)/ accept (stateful DHCPv6) ULA addresses

Only accept packets from ULAs and LLAs.

Much reduced attack surface.

Attacks can only come from local network (ULA, LLA).

“Internet Safe by default”

“Configure All Addresses” switch

Override for a system admin.

Then configures GUAs too.

Manufacturer Usage Description (RFC 8520) (MUD)?

Somewhat similar goal

Network enforces policy/security instead of device

Much more discrete

Requires supporting MUD servers/infrastructure

Assumes local network administrator to choose/manage policies

Default IPv6 Local Only Addressing for Non-Internet Devices

Simple to implement –

- just ignore non-ULA RA PIOs or non-ULA stateful DHCPv6 IA_NAs and IA_TAs

Doesn’t require technical network administrator.

Adds defence depth -

- compliment to MUD and Network Firewall

Another Example

AMI Electricity Smartmeters

Must use ULAs

Implied Internet via GUAs make them vulnerable to DDoS, electrity network sabotage

This proposed mechanism would enforce Internet isolation by enforced ULAs only.

On-demand GUAs?

Firmware upgrade only reason for GUAs?

Only generate (SLAAC) or acquire (stateful DHCPv6) GUA address when checking for/downloading firmware upgrade.

Deprecate/release GUA when finished.

All other times, ULA (+LLA) only.

Thoughts?

Questions?