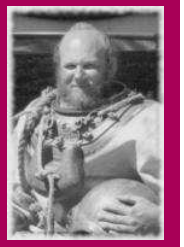
Monitoring (and) IPv6

Benedikt Stockebrand
Dipl. Inform.

<me@benedikt-stockebrand.de>

October 28, 2009

Open Source Monitoring Conference
Nürnberg, Germany



IPv6 and Monitoring

Intended Audiences

- Monitoring tool users
- Check script/plugin developers
- Monitoring tool developers

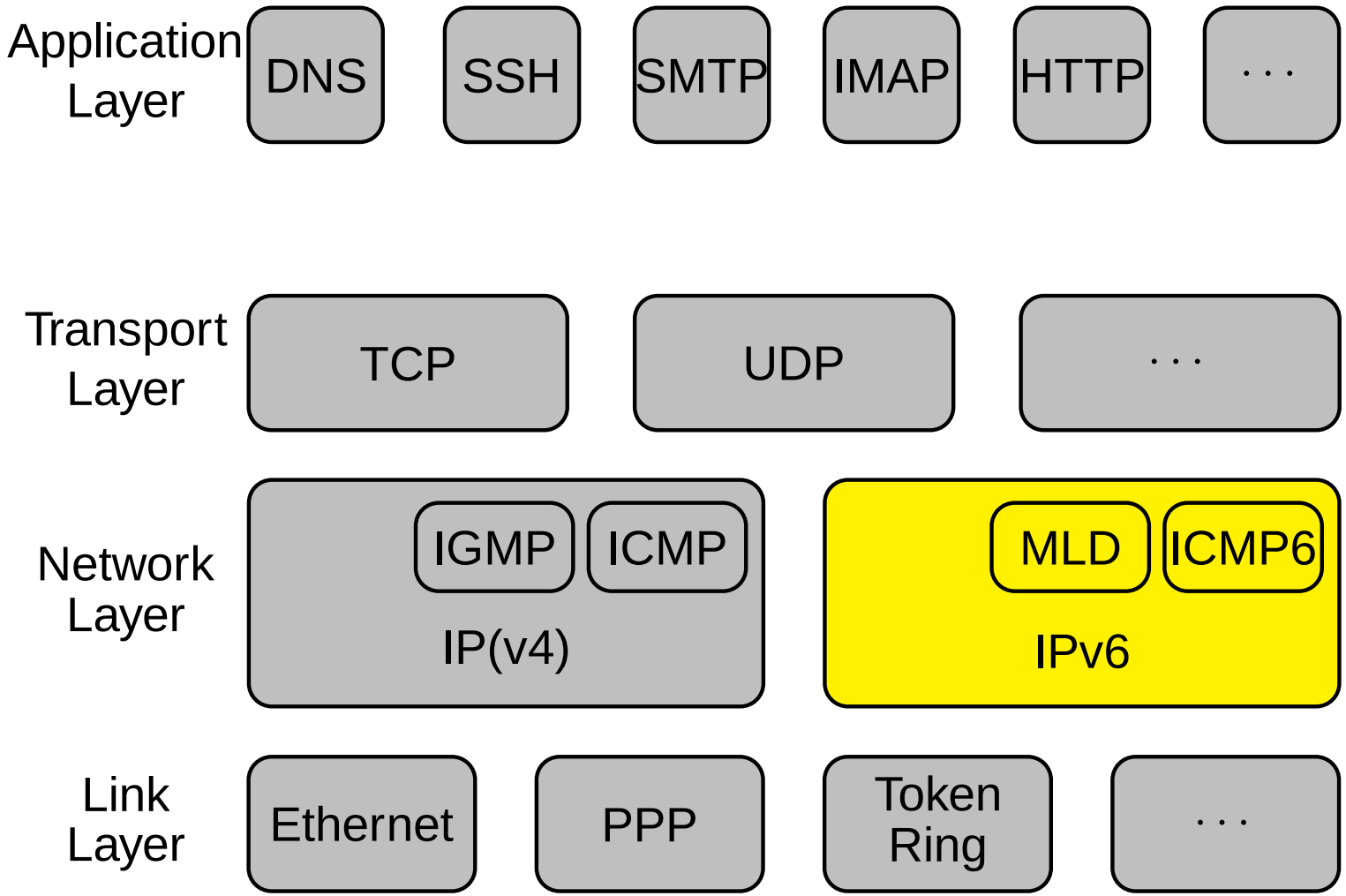
Relationships between Monitoring and IPv6

- Monitoring and IPv6 Deployments
- Monitoring IPv6
- Monitoring with IPv6

Monitoring and IPv6 Deployment

- Most things won’t break when IPv6 is deployed,
- . . . but IPv6 can potentially break anything.
- During a deployment, make sure everything works.
- Don’t deploy IPv6 without comprehensive monitoring.
- Help management understand the importance of monitoring:-)

What is IPv6? I



What is IPv6? II

- IPv4 and IPv6 can be run in parallel.
- IPv6 can’t solve problems outside the network layer.
- IPv6 can’t solve fundamental design deficiencies of the TCP/IP stack.
- Application porting should be easy. . .
- . . . but still must be done.
- Monitoring should be affected in only few areas.

The IPv6 (Non-)Impact

Unaffected are:

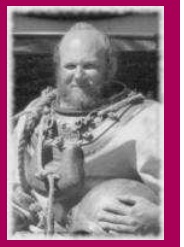
- Local checks (disk usage, CPU load, . . .)
- Anything IPv4-specific

Possibly affected are:

- Network applications (depending on check method)
- Network communications within monitoring software (depending on transport used)

Always affected are:

- IPv6-specific checks
- New monitoring features requiring IPv6



Monitoring and the IPv6 Way of Networking

- Scopes
- IPv6 Addressing
- Helpful New Mechanisms

Scopes

- Link-local scope is new.
- Site-local scope is still available.
- ARP has become ICMPv6 Neighbor Discovery (ND).
- Link-local features may require a satellite (NRPE or such) per subnet.
- Consider a 802.1Q trunk interface on your monitoring server.

Plain Vanilla Unicast Addresses

- NAT is dead.
- . . . and so is STUN.
- There are enough addresses.
- Use Unique-local Addresses (ULA) with site-local scope where applicable.
- Multiple addresses per interface:
  - Check all, not just a “primary” one.
- Hosts may use randomized temporary addresses (aka. “Privacy Extensions”, RFC 3041).
- Multiple addresses from DNS:
  - Check services with all.
  - Watch for excessive timeouts.
  - Beware of `ping6` limitations.
  - Check DNS queries via TCP.

Multicast

IPv6 multicast offers

- all the addresses you need,
- actually working multicast routing (within scalability limits) and
- enormous potential for new functionalities.

Multicast routing monitoring:

- Use multicast ping (with `mcjoin`) for simple tests.
- Possibly check from multiple subnets.

Anycast

- Now a standard, no longer a hack
- Difficult to test without actual failover
- Use whitebox style local checks

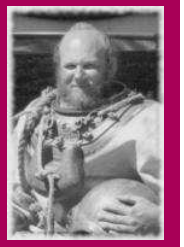
Helpful New Mechanisms

Autoconfiguration

- Much better than DHCP address management.
- Check lifetimes locally on host.
- Check for (possibly multiple) default routes on hosts.

Duplicate Address Detection

- Should appear locally in `syslog`.



Monitoring Dual Stack Environments

- Tunnels
- Gateway Mechanisms
- Where to Put Your Monitoring Server

Tunnels

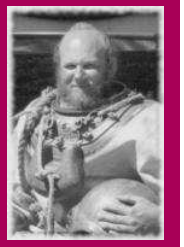
- Do IPv6 blackbox tests through tunnels.
- Do IPv4 whitebox tests of tunnel routes if possible.
- Check for unexpected tunnels
  in security-critical environments
  (especially Teredo, UDP 3544).

Gateway Mechanisms

- Application level gateways/proxies are basically unchanged.
- Protocol translators (TRT, NAT-PT) can be troublesome.
  - Avoid them, they are deprecated anyway.
  - Don’t rely on `ping` to work through them.
  - Check the application instead.
- Transparent proxies (`socat` et al.) can also be somewhat troublesome.
  - `Pings` are answered by the proxy.

Where to Put Your Monitoring Server

- Preferably keep your monitoring server dual-stacked.
  - This may require a minor downtime of the monitoring server.
  - Consider adding a dedicated IPv6 interface, rather than dual-stacking an existing one.
- If that’s impossible, use satellites.
- If that’s impossible, use (transparent) proxies.
- **Don’t** force all clients to be dual-stacked.



Monitoring With IPv6

- Intermediate Protocols
- Monitoring Protocols
- Adding IPv6 Support
- Summary

Ssh and SSL

- Ssh works without problems.
- SSL too, unless `openssl s_client` and `s_server` are used with `popen(3)` or scripts.
- The multiple addresses issue may cause undesirable effects.

Standard Protocols

SNMP

- `netsnmp` works fine.
- But many appliances (routers, switches, . . .) don't.

Syslog

- The Linux `sysklogd` doesn't support IPv6.
- Use `syslog-ng` or `rsyslog` on Linux.
- Many appliances don't support IPv6.

Workarounds:

- make the monitoring servers/satellites dual stacked,
- use satellites,
- or proxies.

Nagios and IPv6 I

- Works fine over Ssh.
- Works fine through Apache.
- But (sorry about the nagging. . .):

Nagios and IPv6 II

From: Jens Link [...]
Subject: IPv6 Monitoring

Moin,

was fuer deinen Vortrag. Falls du einen der Entwickler dabei hast.

```
root@calo-ila# ./check_nrpe -H 2001:6f8:1138::1
Invalid host name '2001:6f8:1138::1'
```

(Auch mit nur Hostname, [], ...)

```
root@calo-ila# ./check_nrpe
Incorrect command line arguments supplied

NRPE Plugin for Nagios
Copyright (c) 1999-2008 Ethan Galstad
(nagios@nagios.org)
Version: 2.12
Last Modified: 03-10-2008
```

Jens

Adding IPv6 Support

- Software is usually easy to port,
  - . . . but still requires doing so.
  - Code samples at my home page
    `http://www.benedikt-stockebrand.de/`
- TCP is simple, UDP can involve a bit of work.
- Alternative I: Run over existing protocols, like Ssh.
- Alternative II: Use a high level language.
- Review all code sections touching raw IP addresses.
- Expect minor fun with configuration syntax issues.

Show that Open Source is a step (or ten) ahead!

Making Use of IPv6

Developers

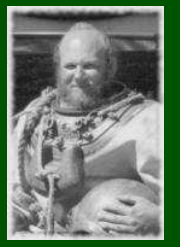
- Multicast routing is worth some real thought.
- Neighbor Discovery may simplify ARPwatch style functionality.

Users

- Consider using dedicated addresses for monitoring access.

Everybody

- Forget about NAT, STUN and similar diseases.



Summary: Monitoring With IPv6

- IPv6 needs proper monitoring.
- Monitoring stays largely unchanged.
- Some details need work.
- IPv6 simplifies monitoring in a number of respects.
- IPv6 offers some nice infrastructure features.

Contact Information

Benedikt Stockebrand
Dipl.-Inform.

Fichardstr. 38
D-60322 Frankfurt/Main

contact@benedikt-stockebrand.de
http://www.benedikt-stockebrand.de/