Implementing Existing Management Protocols on Constrained Devices

Jürgen Schönwälder

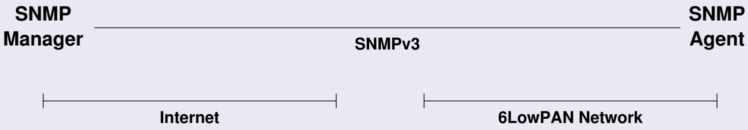
JACOBS UNIVERSITY

IETF 81, Quebec, 2011-07-26

1. SNMP on Constrained Devices
2. NETCONF on Constrained Devices (NETCONF Light)
3. Discovery (mDNS) and Infrastructure (NTP, SYSLOG)
4. Summary and References

SNMP and 6LoWPAN: End-to-End

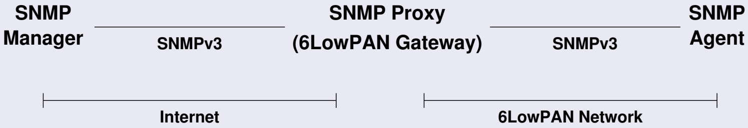
SNMPv3 end-to-end



- \+ Straightforward direct access to individual 6LoWPAN nodes
- \+ Reuse of existing deployed SNMP-based tools
- o End-to-end security, end-to-end key management
- \- Message size and potential fragmentation issues
- \- 6LoWPAN nodes must run an SNMP engine
- \- Trap-directed polling nature of SNMP has high (energy) costs

SNMP and 6LoWPAN: Proxies

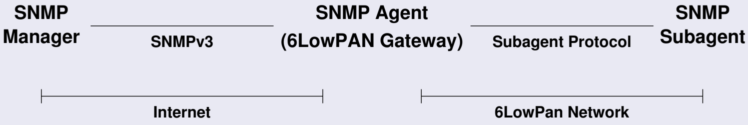
SNMPv3 proxies



+ Indirect access to individual 6LoWPAN nodes
+ Alternate transport encoding can reduce message sizes
o Reuse of existing SNMP-based tools supporting proxies
o Two security domains, different key management schemes
- 6LoWPAN nodes must run an SNMP engine
- Trap-directed polling nature of SNMP has high (energy) costs

SNMP and 6LoWPAN: Subagents

SNMPv3 subagents



+ Indirect access to individual 6LoWPAN nodes
+ Alternate transport encoding can reduce message sizes
o Reuse of existing SNMP-based tools supporting contexts
o Two security domains, different key management schemes
o 6LoWPAN nodes must run an SNMP subagent
- Trap-directed polling nature of SNMP has high (energy) costs

SNMP and 6LoWPAN: Data Fusion Protocols

SNMPv3 interfacing to data fusion protocols

SNMP Manager	SNMPv3	SNMP Agent (6LowPAN Gateway)	data fusion protocol	WSN Peer

Internet	6LowPan Network

- \+ Indirect access to individual 6LoWPAN nodes
- \+ Leveraging data fusion protocols (in-network aggregation)
- \+ SNMP agent acting as a cache, no expensive polling
- o Reuse of existing SNMP-based tools supporting contexts
- o Two security domains, different key management schemes
- ? No direct advantage of 6LoWPAN technology — oops

Contiki-SNMP Overview

General features / limitations

- SNMP messages up to 484-byte length
- `Get`, `GetNext` and `Set` operations
- SNMPv1 and SNMPv3 message processing models
- USM security model, no VACM access control model
- API to define and implement managed objects

USM security algorithms

- HMAC-MD5-96 authentication protocol (RFC 3414)
- CFB128-AES-128 symmetric encryption protocol (RFC 3826)

Implemented MIB Modules and Static Memory Usage

MIB modules

- `SNMPv2-MIB` – SNMP entity information
- `IF-MIB` – network interface information (no 802.14.5 ifType)
- `ENTITY-SENSOR-MIB` – temperature sensor readings

SNMPv1 and SNMPv3 enabled

- 31220 bytes of ROM (around 24% of the available ROM)
- 235 bytes of statically allocated RAM

SNMPv1 enabled

- 8860 bytes of ROM (around 7% of the available ROM)
- 43 bytes of statically allocated RAM

Flash ROM and Static Memory Usage

Memory usage by software module (bytes)

Module	Flash ROM	RAM (static)
snmpd.c	172	2
dispatch.c	1076	26
msg-proc-v1.c	634	6
msg-proc-v3.c	1184	30
cmd-responder.c	302	0
mib.c	1996	6
ber.c	4264	3
usm.c	1160	122
aes_cfb.c	9752	40
md5.c	10264	0
utils.c	416	0

Stack and Heap Usage

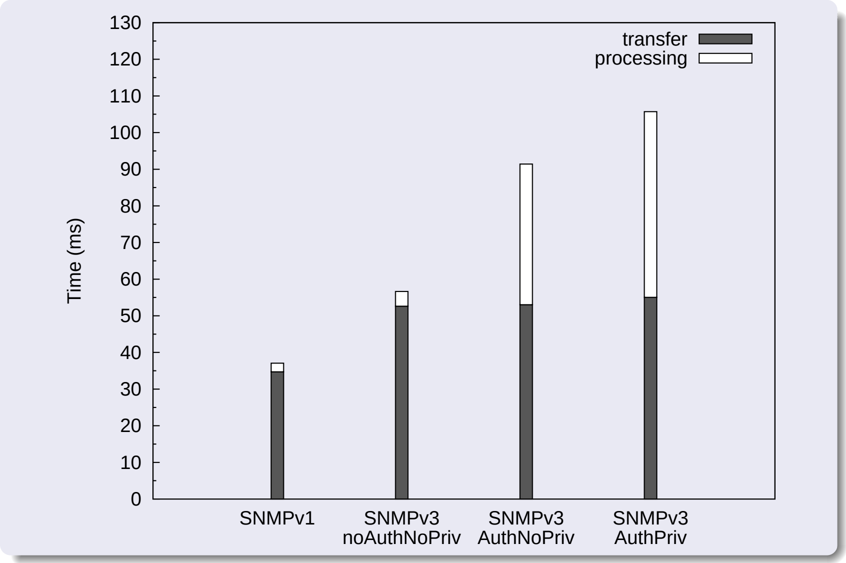
Maximum observed stack usage

Version	Security mode	Max. stack size
SNMPv1	–	688 bytes
SNMPv3	noAuthNoPriv	708 bytes
SNMPv3	authNoPriv	1140 bytes
SNMPv3	authPriv	1144 bytes

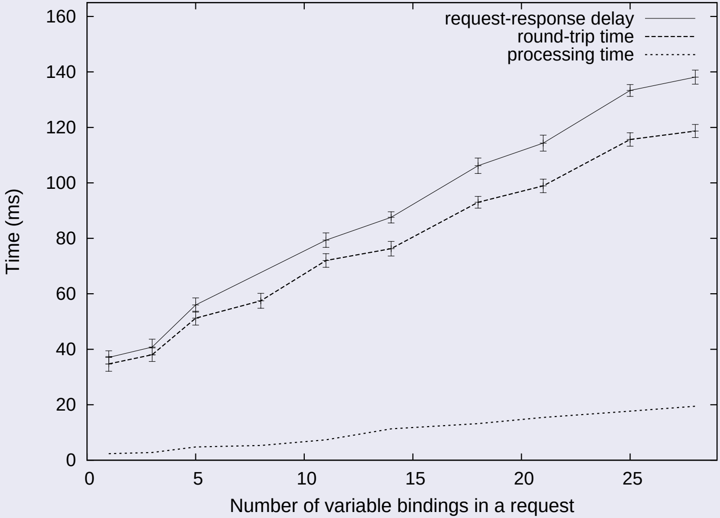
Heap usage

- not more than 910 bytes for storing an SNMPv1 message
- approximately 16 bytes for every managed object in the MIB
- if a managed object is of a string-based type, then additional heap memory is used to store its value

SNMP Request/Response Latency (varying security)



SNMPv1 Request/Response Latency (varying # varbinds)



Related Work at Jacobs University

SNMP applicability to constrained devices

- Guidelines how to fit SNMP into constrained devices
- Tricks like making VACM a simple read-only/read-write switch
- <draft-hamid-6lowpan-snmp-optimizations-02.txt>

RPL MIB module specification and implementation

- Definition of a MIB module for the RPL routing protocol
- Implementation and evaluation on Econotags
- <draft-sehgal-roll-rpl-mib-01.txt>

DTLS for constrained devices

- Contiki-SNMP over DTLS (RFC 5590, RFC 5591, RFC 5953)
- Pretty much future work at this point in time

NETCONF on Constrained Devices (NETCONF Light)

1. SNMP on Constrained Devices
2. NETCONF on Constrained Devices (NETCONF Light)
3. Discovery (mDNS) and Infrastructure (NTP, SYSLOG)
4. Summary and References

Motivation and Approach

Motivation

- Some applications (e.g., the Smart Grid) have a requirement to run a single management protocol on a set of devices with very different processing and storage capabilities.
- NETCONF (RFC 6241) provides a fairly feature complete solution for network devices such as routers and switches.
- Constrained devices may not be able to support NETCONF completely — so how "small" can NETCONF be?

Approach and Assumptions

- Define a proper subset of NETCONF that is appropriate for constrained devices.
- Assumption: On constrained devices, the amount of configuration data is small and the need to interact with multiple management systems concurrently is small.

NETCONF Light (NCL)

Reduced Protocol Operations

- NCL implementations are not required to support filtering on `<get-config>` and `<get>` operations.
- NCL implementations are not required to implement the `<edit-config>` operation (simply use `<copy-config>`).
- NCL implementations only support the `<running>` datastore.
- NCL implementations may choose to only support one concurrent session (makes `<lock>` and `<unlock>` trivial).
- NCL uses a different XML namespace to identify itself.

Things Kept Unchanged

- XML encoding of the configuration data (although XML format is less relevant since there is no `<edit-config>`).
- RFC 6241 framing (although this took effort to implement if memory is tight).

NETCONF Light Implementation Experience

Characteristics

- Contiki NETCONF Light implemented on AVR Raven motes (Class 1 devices, 16 KiB RAM, 128 KiB Flash)
- Uses NETCONF over plain TCP instead of SSH or TLS
- Uses Contiki's Coffee File System to store the configuration (and we had lots of "fun" with its implementation)
- Supports all the NETCONF operations as described before

Memory Consumption

- $\approx$ 13 KiB RAM (10 KiB Contiki, 0.5 KiB System Manager, 2.6 KiB NETCONF)
- $\approx$ 87 KiB Flash with $\approx$ 12 KiB reserved for the four files in the Coffee File System
- Further code optimizations are possible and file sizes in flash memory can be adapted

1 SNMP on Constrained Devices

2 NETCONF on Constrained Devices (NETCONF Light)

3 Discovery (mDNS) and Infrastructure (NTP, SYSLOG)

4 Summary and References

mDNS and SYSLOG and NTP

Multicast DNS for network management service discovery

- Managers use mDNS to discover manageable devices
- Devices discover management services via mDNS
- Contiki-mDNS implementation already running
- <draft-schoenw-opsawg-nm-srv-02.txt>

SYSLOG for logging

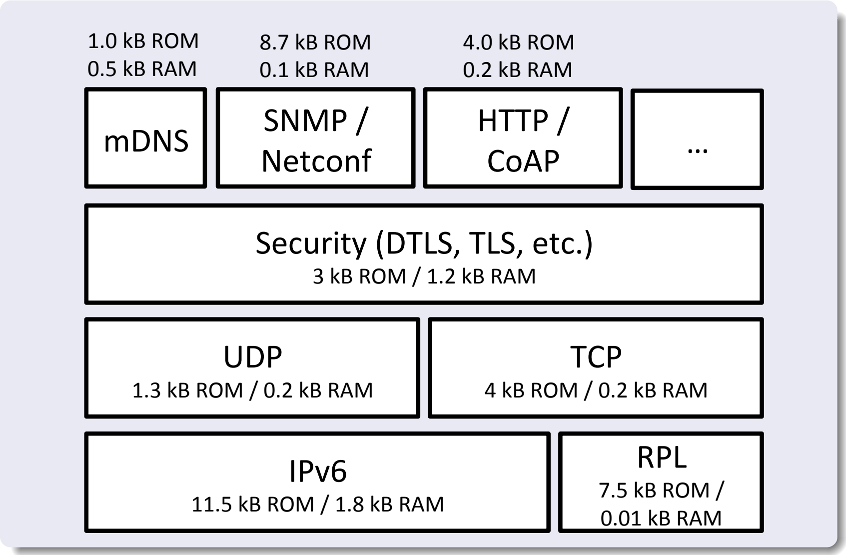
- Minimal SYSLOG implementation
- Using mDNS to discover a SYSLOG server
- Fallback assumes the default router can handle SYSLOG

NTP for time synchronization

- Minimal NTP client to pickup a notion of time

1. SNMP on Constrained Devices
2. NETCONF on Constrained Devices (NETCONF Light)
3. Discovery (mDNS) and Infrastructure (NTP, SYSLOG)
4. Summary and References

Implementations at Jacobs University



References

J. Ko, A. Terzis, S. Dawson-Haggerty, D. E. Culler, J. W. Hui, and P. Levis.
Connecting Low-Power and Lossy Networks to the Internet.
IEEE Communications Magazine, 49(4):96–101, April 2011.

S. Kuryla and J. Schönwälder.
Evaluation of the Resource Requirements of SNMP Agents on Constrained Devices.
In *Proc. of the 5th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2011)*, number 6734 in LNCS, pages 100–111. Springer, June 2011.

J. Schönwälder, H. Mukhtar, S. Joo, and K. Kim.
SNMP Optimizations for Constrained Devices.
Internet Draft <draft-hamid-6lowpan-snmp-optimizations-03.txt>, ETRI, Jacobs University, Ajou University, October 2010.

J. Schönwälder, T. Tsou, and C. Zhou.
DNS SRV Resource Records for Network Management Protocols.
Internet-Draft (work in progress) <draft-schoenw-opsawg-nm-srv-02>, Jacobs University, June 2011.

V. Perelman, J. Schönwälder, and M. Ersue.
Network Configuration Protocol for Constrained Devices (NETCONF Light).
Internet-Draft (work in progress) <draft-schoenw-netconf-light-00>, Jacobs University, Nokia Siemens Networks, June 2011.

K. Korte, A. Sehgal, and J. Schönwälder.
Definition of Managed Objects for the IPv6 Routing Protocol for Low power and Lossy Networks (RPL).
Internet Draft <draft-sehgal-roll-rpl-mib-01>, Jacobs University, March 2011.