# Performance of SNMP over SSH/TLS/DTLS

Jürgen Schönwälder

Jacobs University Bremen
Bremen, Germany

23. NMRG Meeting 2007

# Motivation

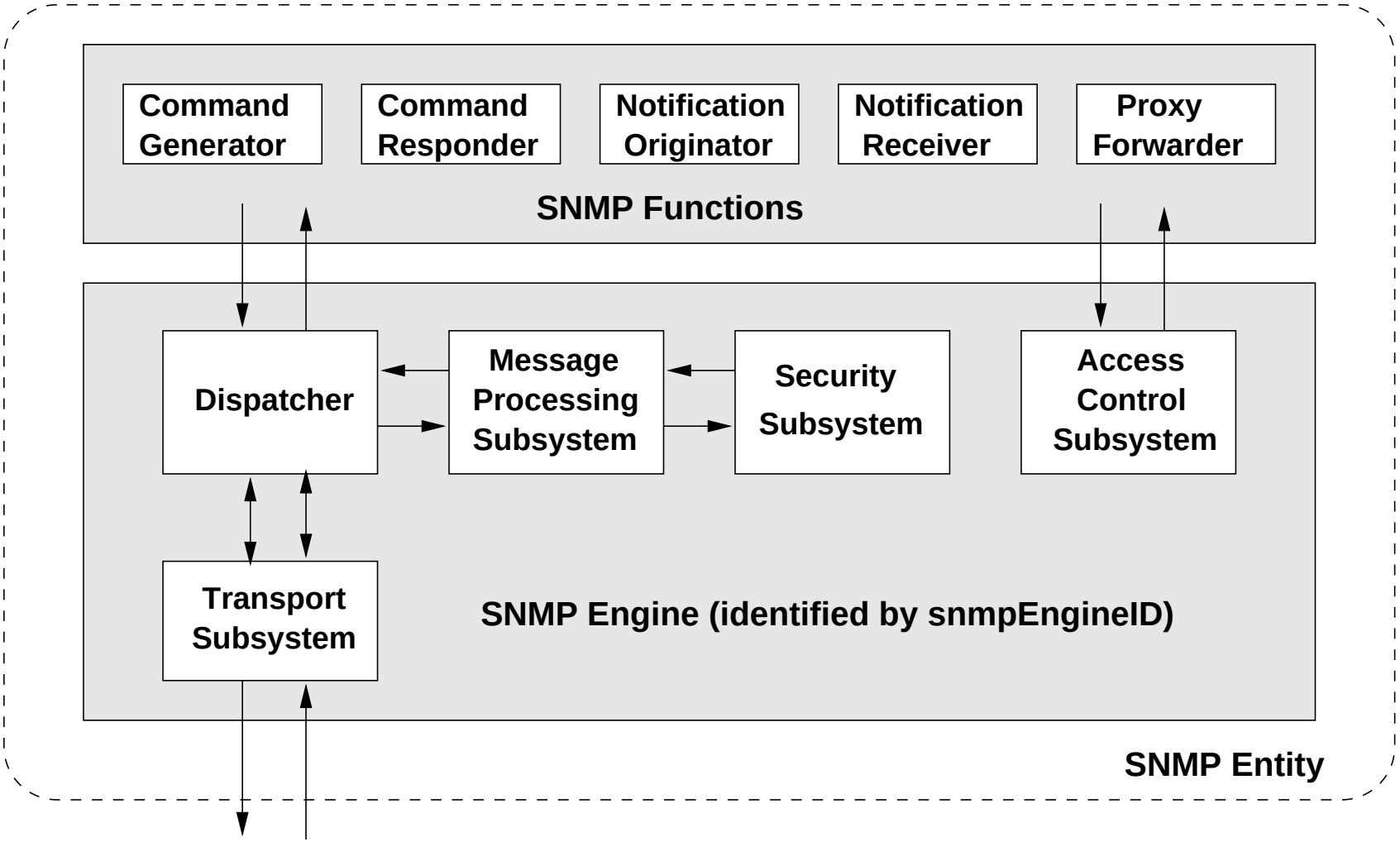
Network operators have reported that deploying another user and key management infrastructure just to secure SNMP is expensive and a reason to not deploy SNMPv3.

- So why not run SNMP over existing security protocols?
- Basic idea is not really new (see IM 2001 paper [1]).
- IETF ISMS WG (Security Area) is working out the details.
- As usual, the devil is in the details!

# Some Design Issues

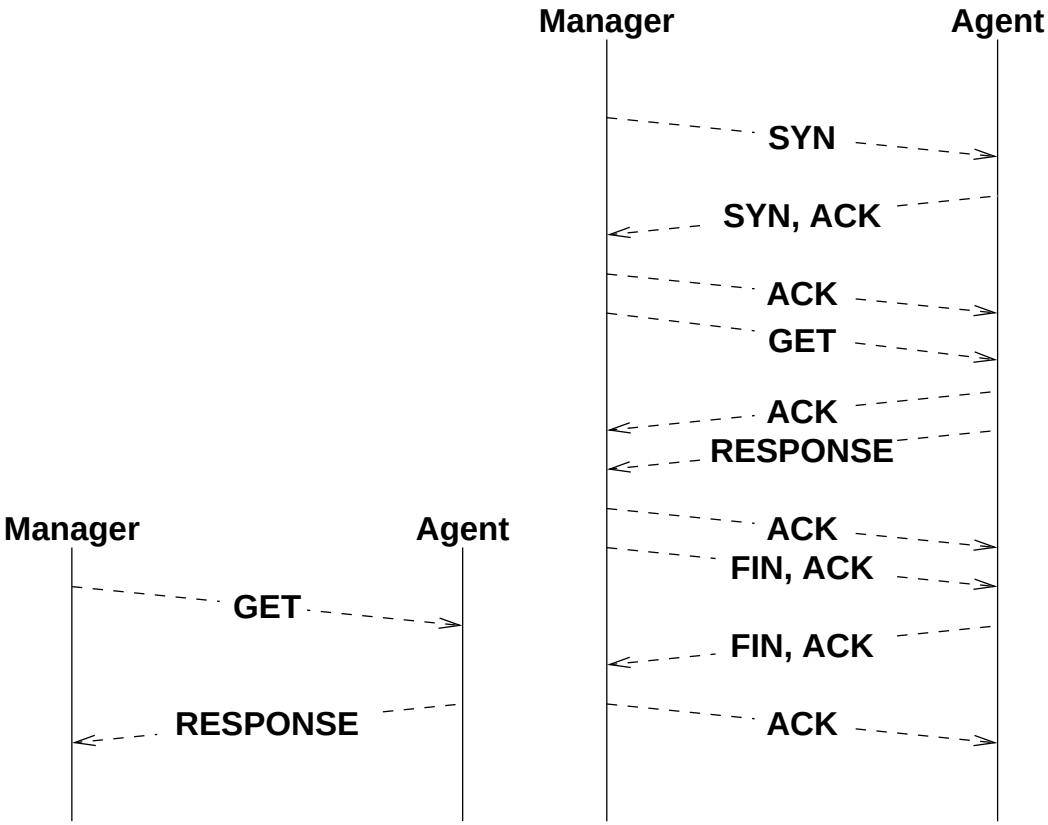
- SNMP does not really have a transport subsystem — so how to we properly add secure transports?
- SNMP architecture assumes security is provided by the security model called from the message processing model — how do we pass security parameters from a secure transport up to where the architecture expects things?
- Which secure transport to choose? SSH or TLS or . . . ?
- How do we map secure transport specific parameters into `securityName`, `securityLevel`, `securityModel`?
- How do session keys fit into the architectural framework?
- How do we deal with notifications — reverse authentication?

# Extended SNMP Architecture (ISMS)



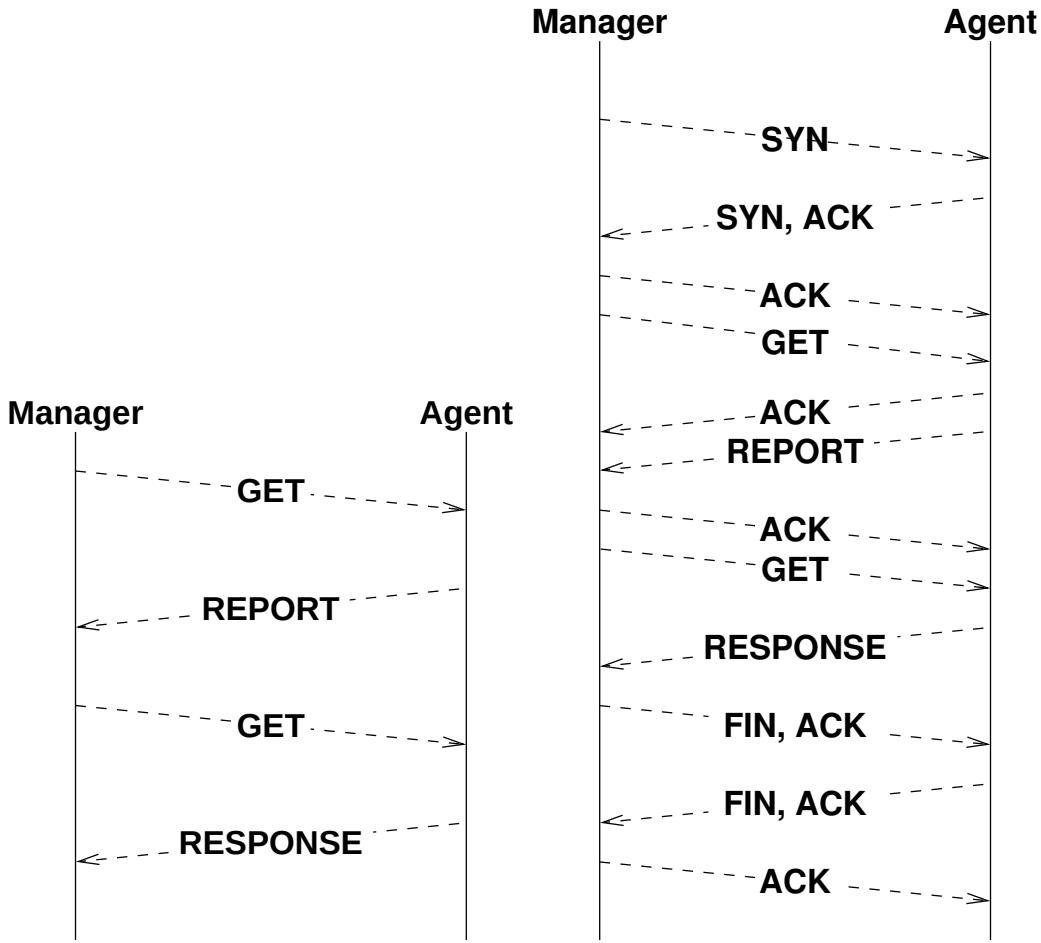

- See `draft-ietf-isms-tmsm-xx.txt` for details

# SNMPv2c over UDP and TCP



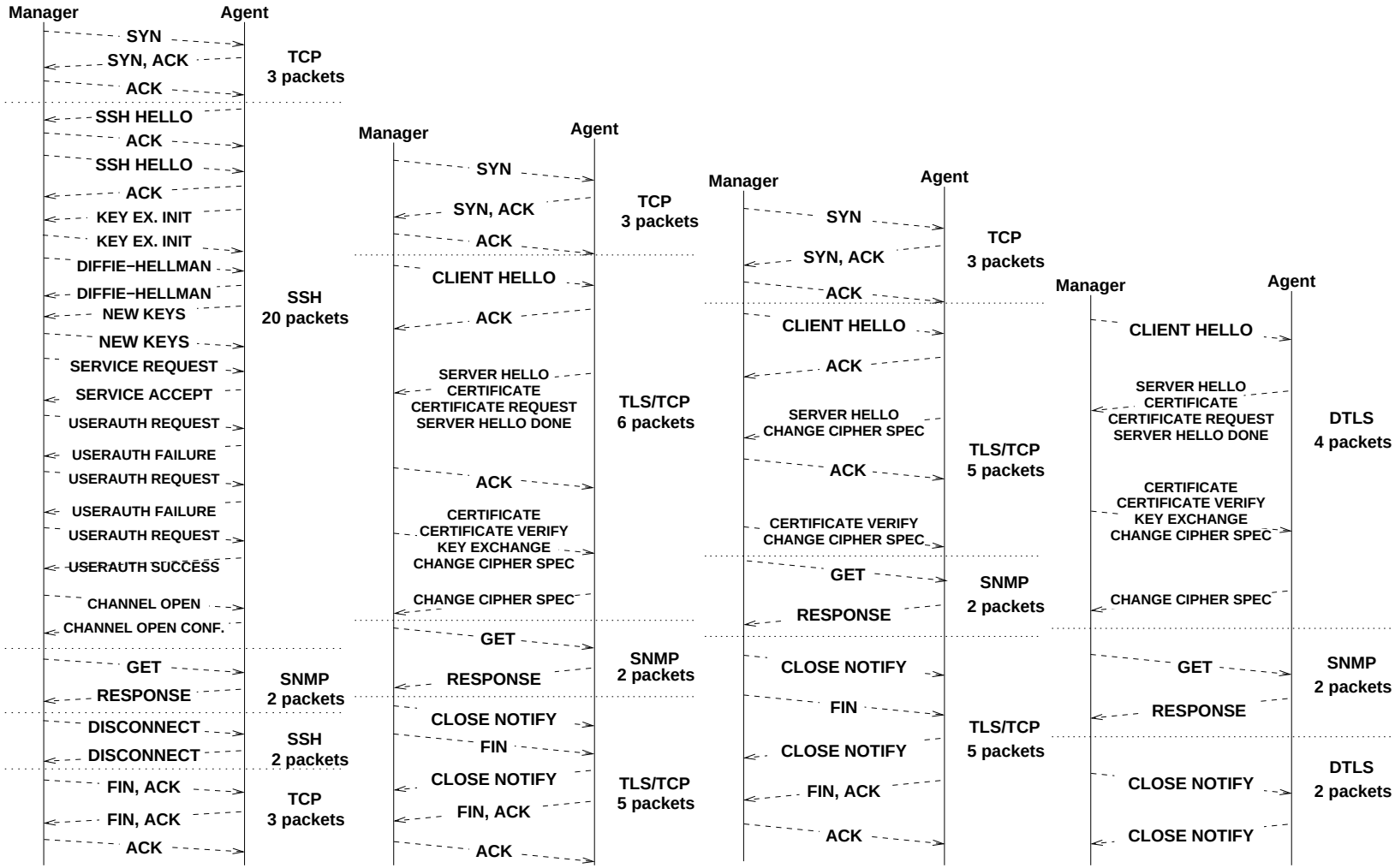

- We all know this...

# SNMPv3/USM over UDP and TCP




- and we also all know this...

# SNMPv3/TSM over SSH/TLS/DTLS




- but I am sure not everybody knows all this!

# Experimental Setup

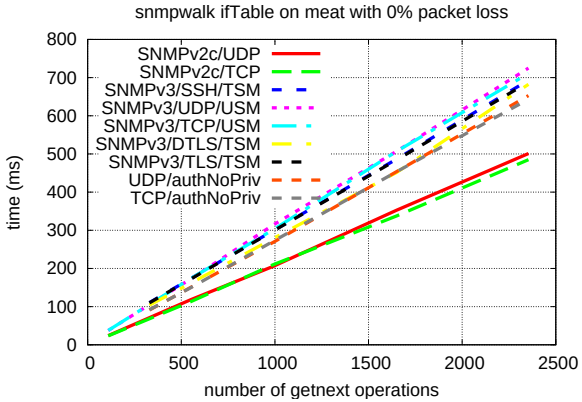
- Implemented SNMP over SSH/TLS/DTLS using NET-SNMP 5.3.0.1, libssh, and openssl
- Some code fine tuning was necessary
- Some debugging of libraries was also necessary
- SSH uses libpam for password authentication
- Machines used during the measurements:

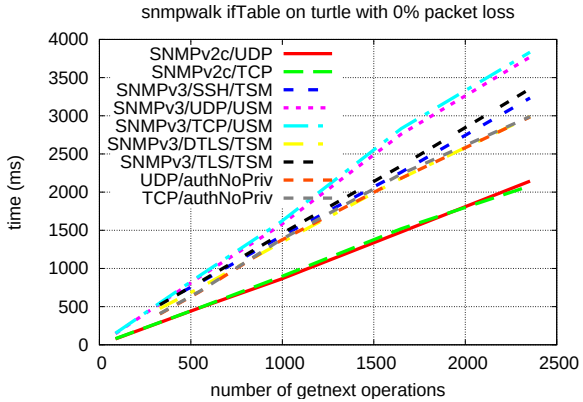
| Name | CPUs | RAM | Ethernet | Kernel |
|---|---|---|---|---|
| `meat` | 2 Xeon 3 GHz | 2 GB | 1 Gbps | 2.6.16.14 |
| `veggie` | 2 Xeon 3 GHz | 1 GB | 1 Gbps | 2.6.12.6 |
| `turtle` | 1 Ultra Sparc IIi | 128 MB | 100 Mbps | 2.6.16.14 |

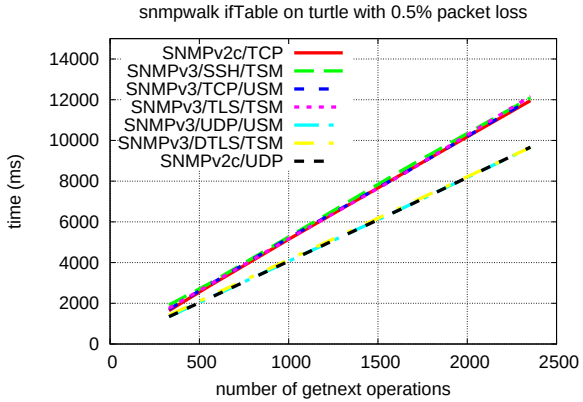
# Session Establishment Overhead

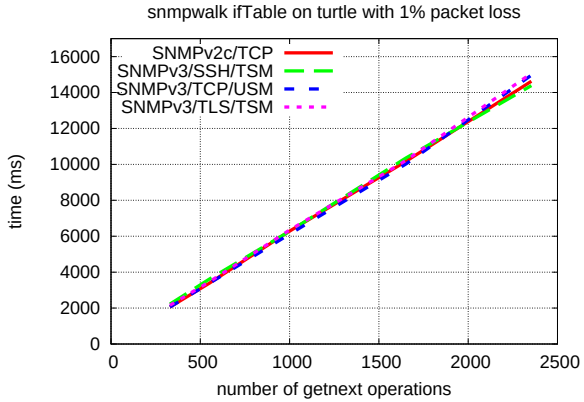
| Protocol | Time (meat) | Time (turtle) | Data | Packets |
|---|---|---|---|---|
| SNMPv2c/UDP | 1.03 ms | 0.70 ms | 232 bytes | 2 |
| SNMPv2c/TCP | 1.13 ms | 1.00 ms | 824 bytes | 10 |
| SNMPv3/USM/UDP | 1.97 ms | 2.28 ms | 668 bytes | 4 |
| SNMPv3/USM/TCP | 2.03 ms | 3.03 ms | 1312 bytes | 12 |
| SNMPv3/SSH | 17.00 ms | 103.27 ms | 4200 bytes | 29 |
| SNMPv3/TLS | 16.04 ms | 67.16 ms | 3987 bytes | 16 |
| SNMPv3/TLS/sr | 2.00 ms | 6.14 ms | 1737 bytes | 15 |
| SNMPv3/DTLS | 16.12 ms | 68.94 ms | 18895 bytes | 56 |

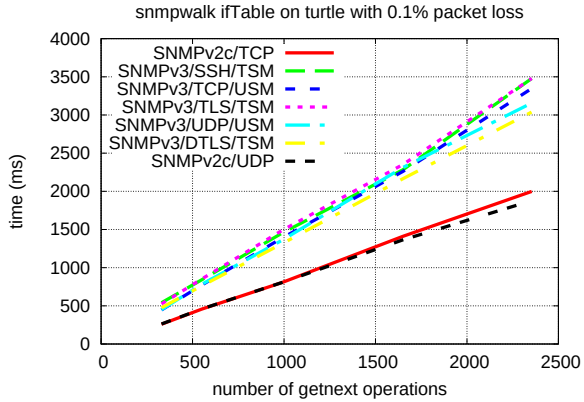
- Session resumption is key to port existing applications that usually do not maintain long-term session
- SSH really fails badly here — was it the right choice?
- TLS requires less messages and this shows
- Large number of DTLS messages seem to be a bug

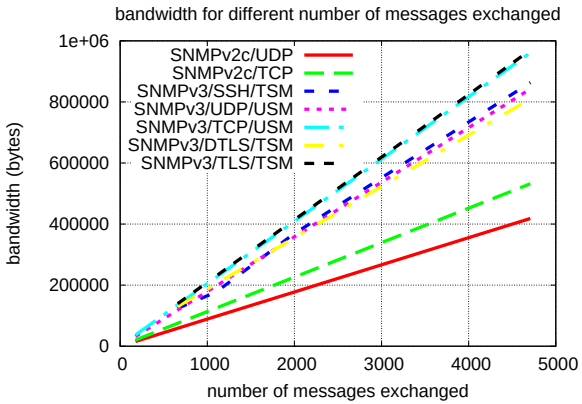

snmpwalk ifTable on meat with 0% packet loss
time (ms)
number of getnext operations
SNMPv2c/UDP
SNMPv2c/TCP
SNMPv3/SSH/TSM
SNMPv3/UDP/USM
SNMPv3/TCP/USM
SNMPv3/DTLS/TSM
SNMPv3/TLS/TSM
UDP/authNoPriv
TCP/authNoPriv

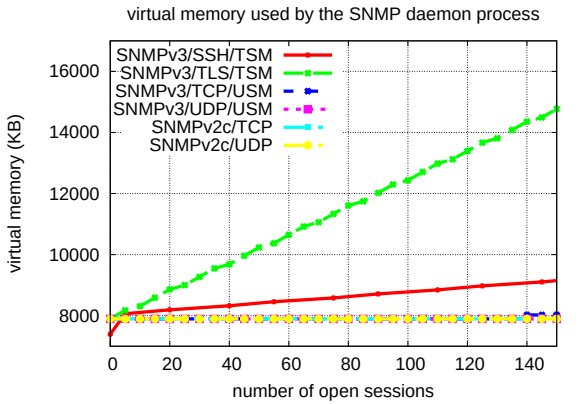

snmpwalk ifTable on turtle with 0% packet loss
time (ms)
number of getnext operations
SNMPv2c/UDP
SNMPv2c/TCP
SNMPv3/SSH/TSM
SNMPv3/UDP/USM
SNMPv3/TCP/USM
SNMPv3/DTLS/TSM
SNMPv3/TLS/TSM
UDP/authNoPriv
TCP/authNoPriv


snmpwalk ifTable on turtle with 0.5% packet loss
time (ms)
number of getnext operations
SNMPv2c/TCP
SNMPv3/SSH/TSM
SNMPv3/TCP/USM
SNMPv3/TLS/TSM
SNMPv3/UDP/USM
SNMPv3/DTLS/TSM
SNMPv2c/UDP


snmpwalk ifTable on turtle with 1% packet loss
time (ms)
number of getnext operations
SNMPv2c/TCP
SNMPv3/SSH/TSM
SNMPv3/TCP/USM
SNMPv3/TLS/TSM


snmpwalk ifTable on turtle with 0.1% packet loss
time (ms)
number of getnext operations
SNMPv2c/TCP
SNMPv3/SSH/TSM
SNMPv3/TCP/USM
SNMPv3/TLS/TSM
SNMPv3/UDP/USM
SNMPv3/DTLS/TSM
SNMPv2c/UDP


bandwidth for different number of messages exchanged
bandwidth (bytes)
number of messages exchanged
SNMPv2c/UDP
SNMPv2c/TCP
SNMPv3/SSH/TSM
SNMPv3/UDP/USM
SNMPv3/TCP/USM
SNMPv3/DTLS/TSM
SNMPv3/TLS/TSM


virtual memory used by the SNMP daemon process
virtual memory (KB)
number of open sessions
SNMPv3/SSH/TSM
SNMPv3/TLS/TSM
SNMPv3/TCP/USM
SNMPv3/UDP/USM
SNMPv2c/TCP
SNMPv2c/UDP

# References


X. Du, M. Shayman, and M. Rozenblit.

Implementation and Performance Analysis of SNMP on a TLS/TCP Base.
In *Proc. 7th IFIP/IEEE International Symposium on Integrated Network Management*, pages 453–466, Seattle, May 2001.

V. Marinov and J. Schönwälder.

Performance Analysis of SNMP over SSH.
In *Proc. 17th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM 2006)*, pages 25–36, Dublin, October 2006. Springer LNCS 4269.

D. Harrington and J. Schönwälder.

Transport Subsystem for the Simple Network Management Protocol (SNMP).
Internet Draft (work in progress) <draft-ietf-isms-tmsm-10.txt>, Huawei Technologies, Jacobs University Bremen, September 2007.

D. Harrington.

Transport Security Model for SNMP.
Internet Draft (work in progress) <draft-ietf-isms-transport-security-model-06.txt>, Huawei Technologies, September 2007.

D. Harrington and J. Salowey.

Secure Shell Transport Model for SNMP.
Internet Draft (work in progress) <draft-ietf-isms-secshell-08.txt>, Futurewei Technologies, Cisco Systems, September 2007.