Integrated Security Model For SNMP (ISMS)

Wes Hardaker
<hardaker@tislabs.com>

2004.Aug.09

Overview

- 05m Agenda Bashing
- 20m Problem History
- 15m Requirements Bashing
- 30m Charter Bashing
- 40m Proposal Bashing
  - EUSM
  - KSM
  - SBSM
- 40m Proposals Comparison

Meeting requirements

Need someone to:

- Take minutes
- Jabber scribe
- Blue sheets

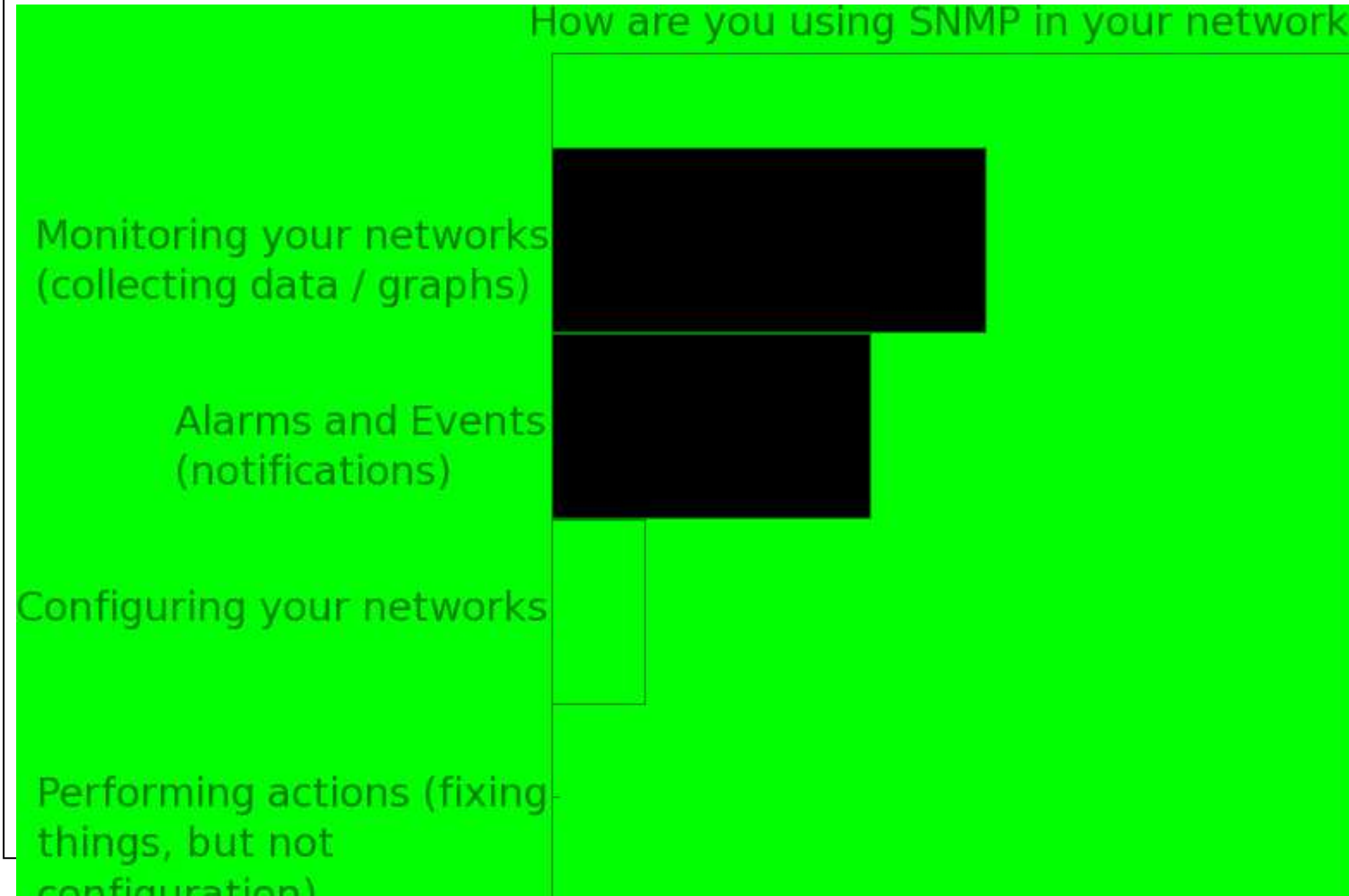
David’s slides

Problem History

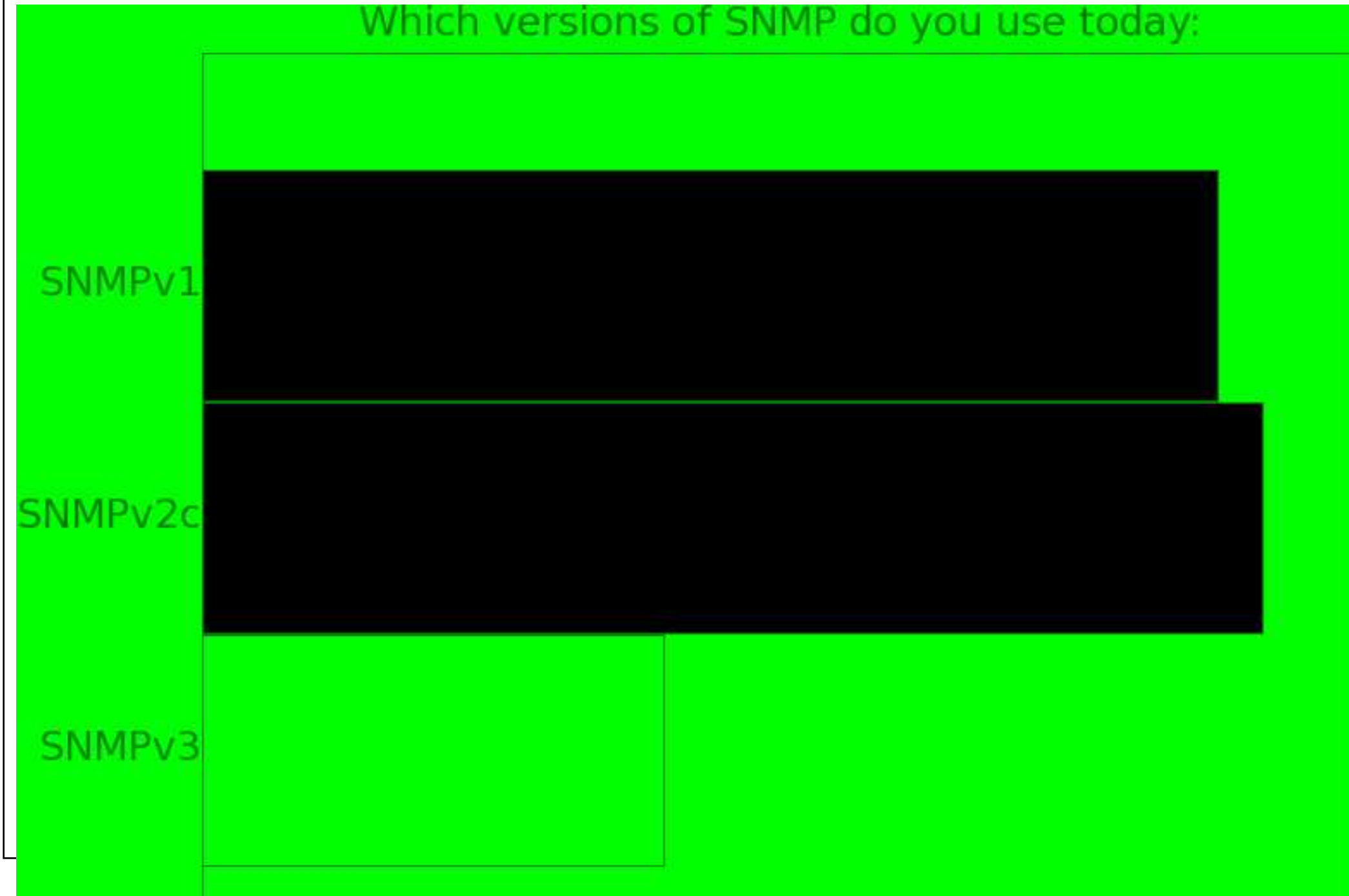
- This is the second BOF
  - Last time: unanimous audince support.
  - But... no operators were present.
    - ADs needed operator opinion
- Since then:
  - Operators polled at NANOG
  - Electronic survey
    - 149 responses
    - Overwhelmingly a problem
- And beyond:
  - Primary goal of this BOF: A charter
  - Secondary goal: technical

Survey Results -- Respondents

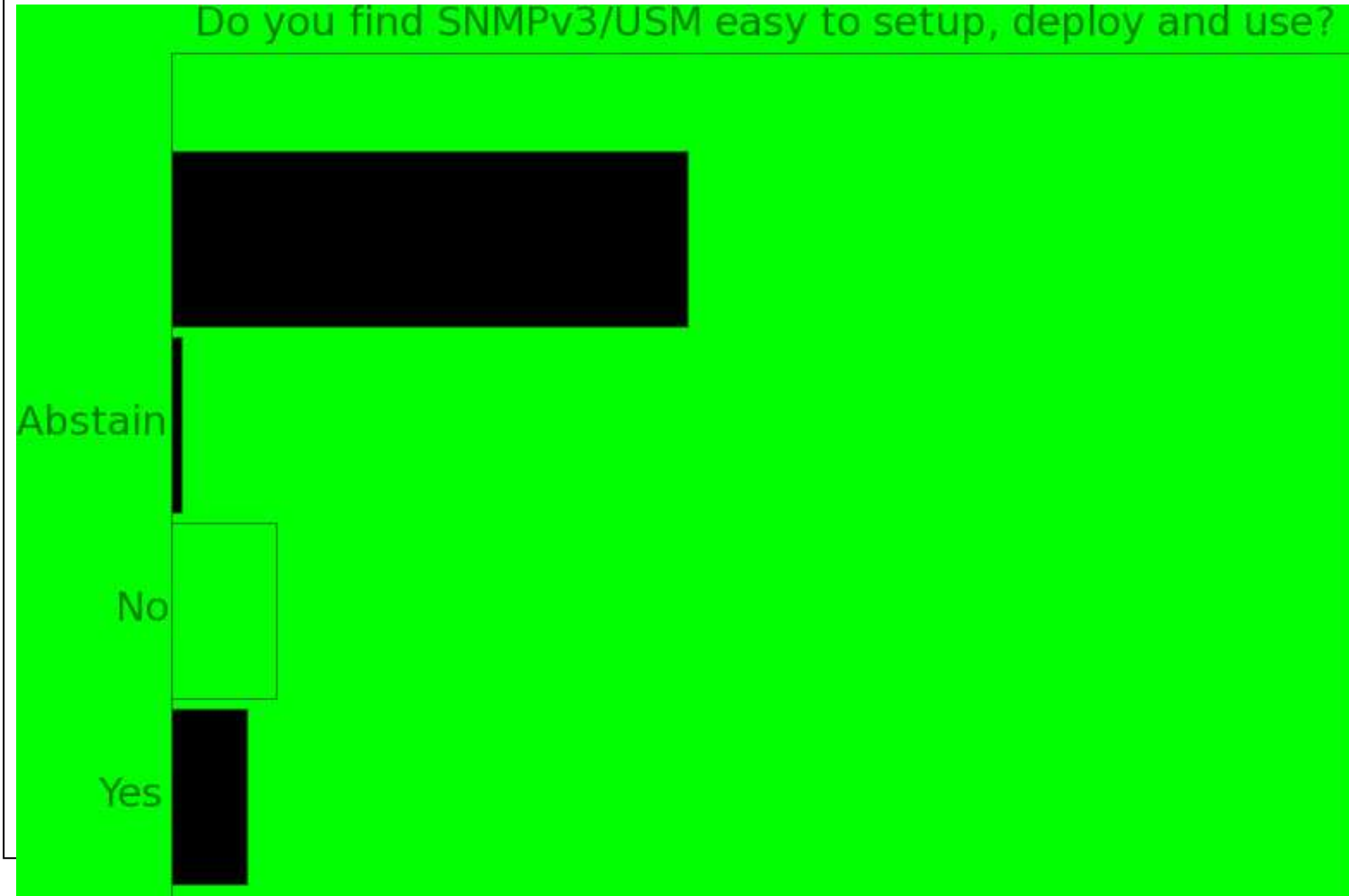
Survey Results -- Current SNMP Usage



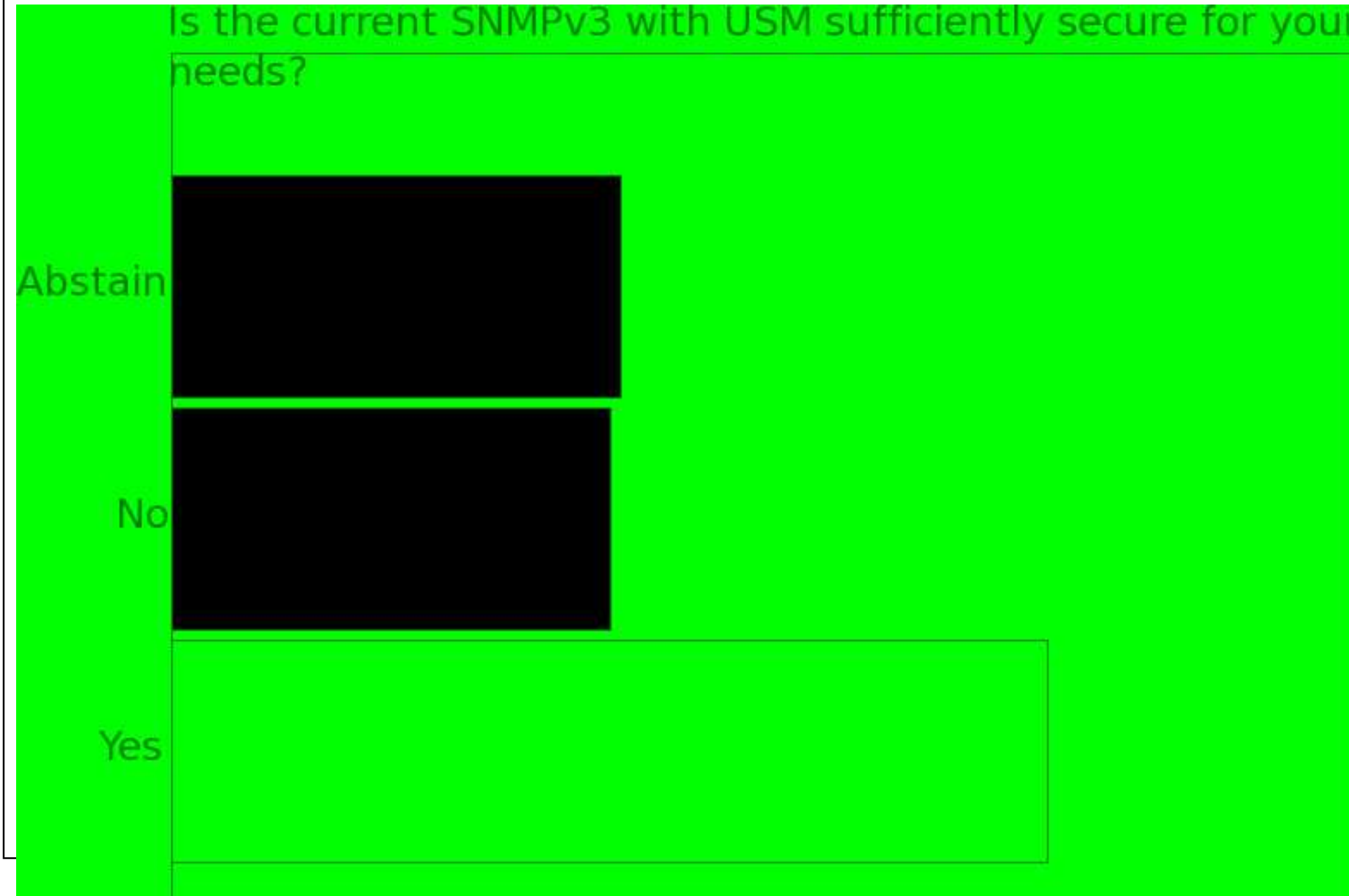
Survey Results -- Current SNMP Usage



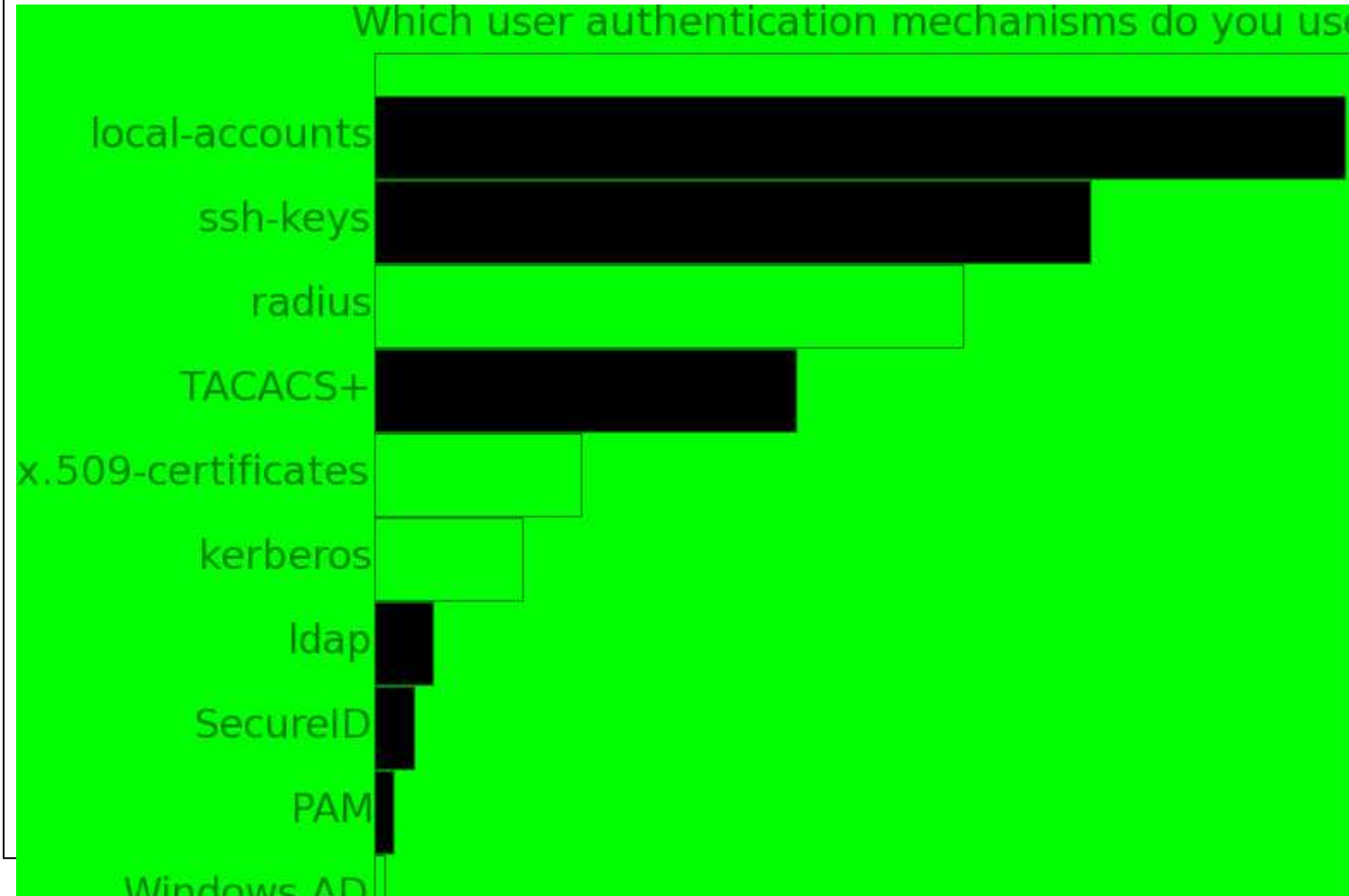
Survey Results -- Current SNMP Usage



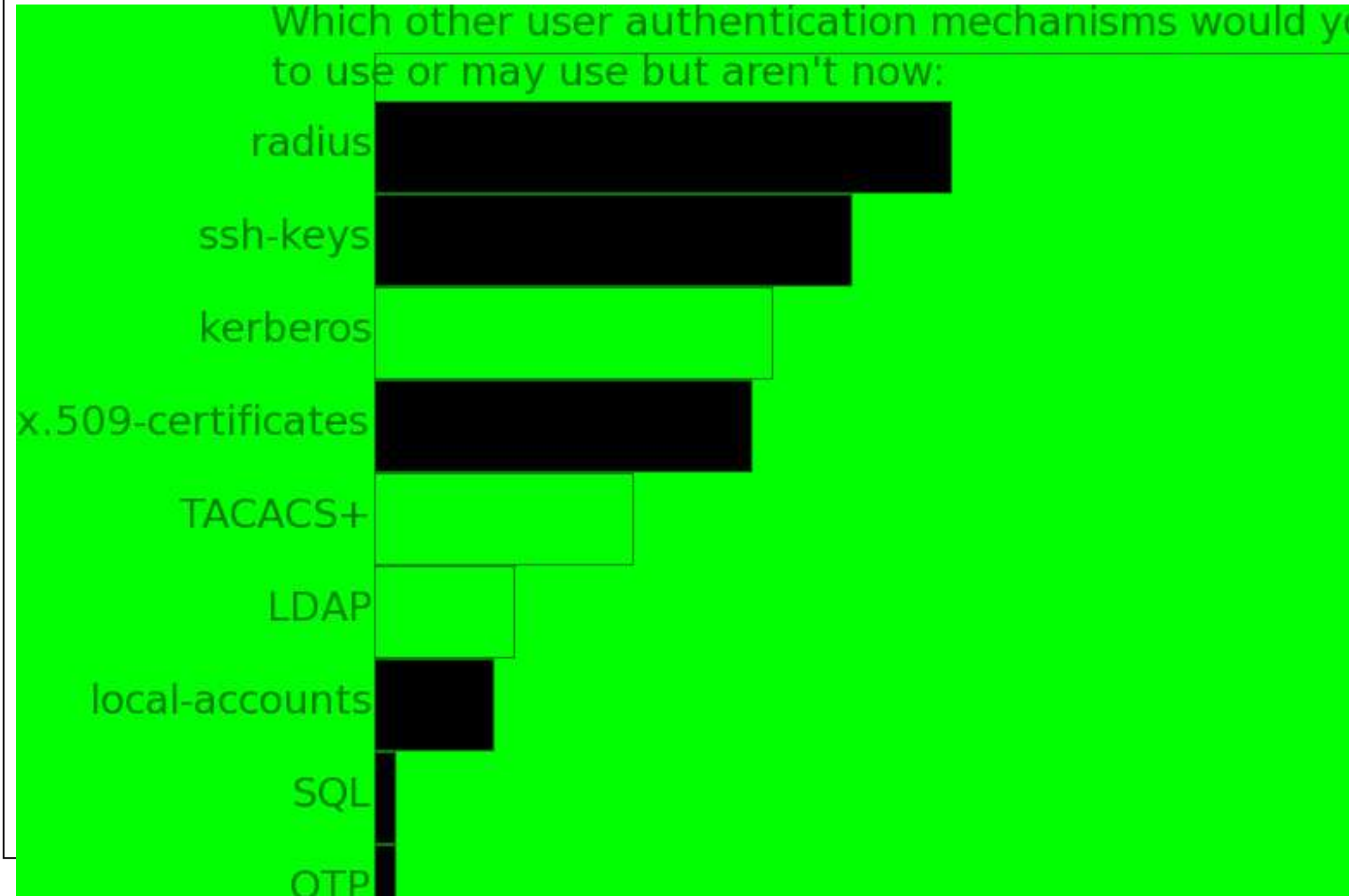
Survey Results -- Current SNMP Usage



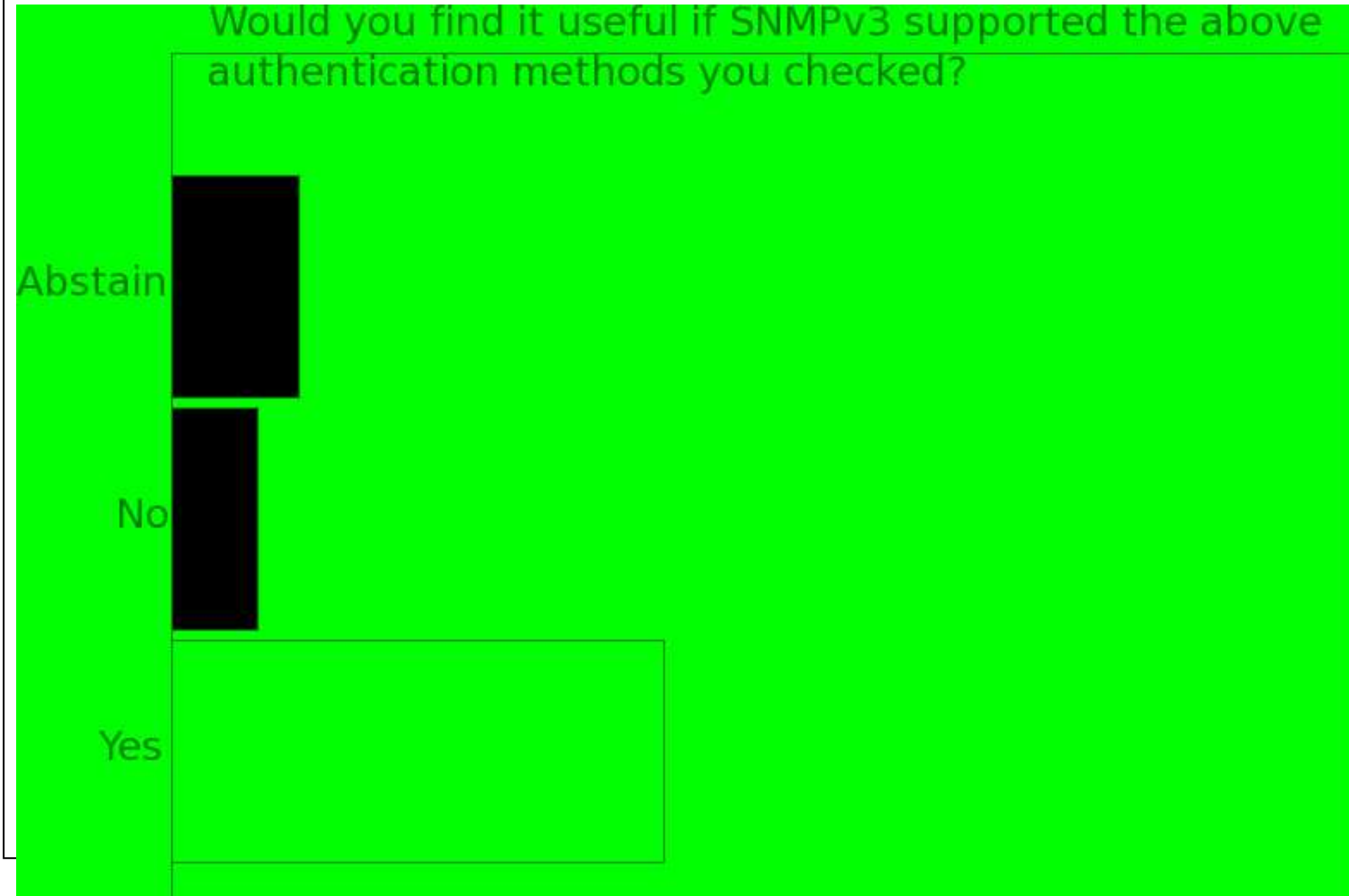
Survey Results -- Authentication Requirements



Survey Results -- Authentication Requirements

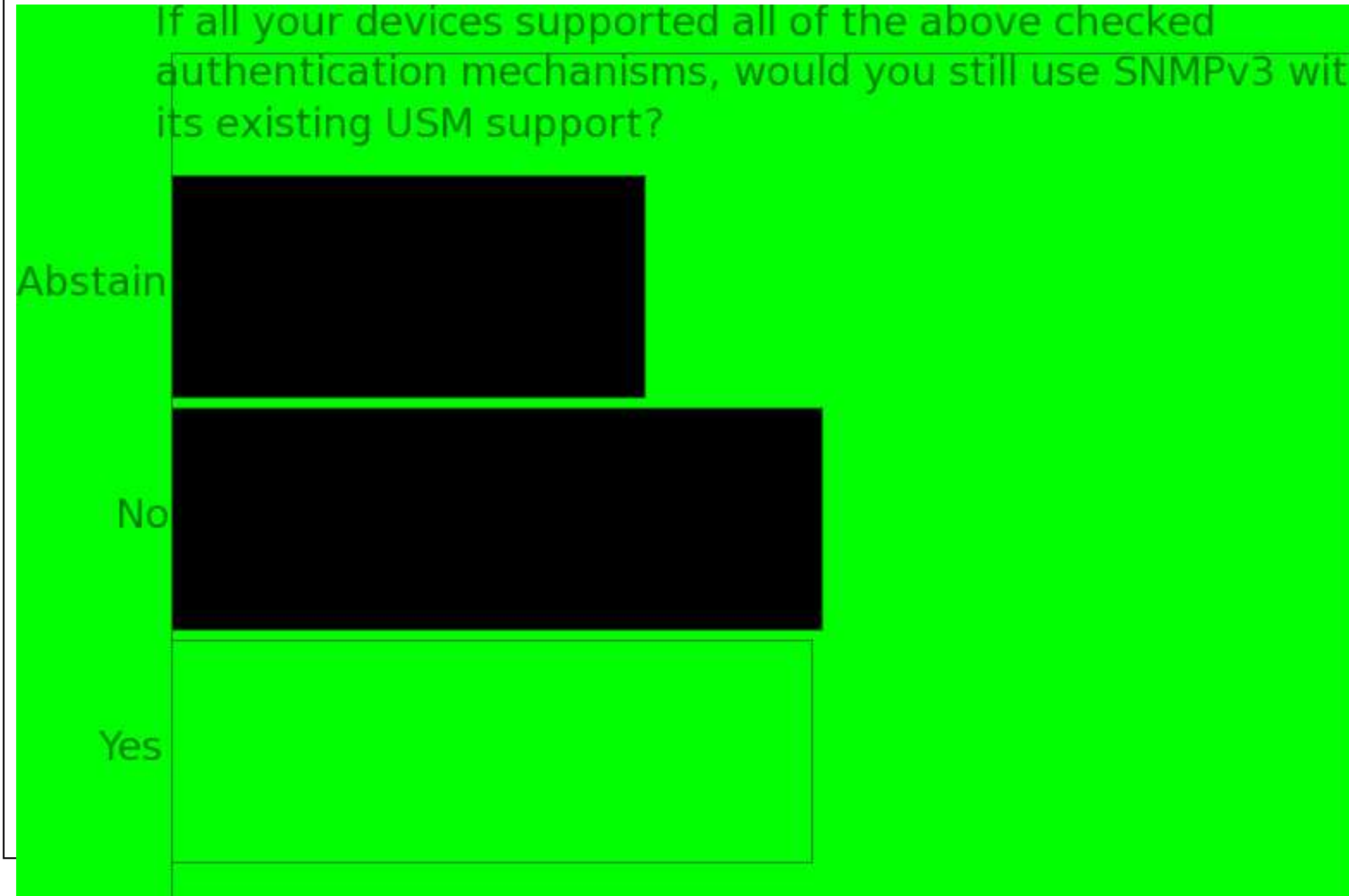


Survey Results -- Is ISMS needed



Survey Results -- Is ISMS needed

Survey Results -- Is ISMS needed



Requirements Discussion

- must be possible to integrate with existing infrastructure
- can’t be less secure than SNMPv3/USM
- must not modify SNMPv3 full standards documents
- must work with all SNMPv3v message types
- must be able to manage the box during times of network instability
- minimal impact on applications and agents
- minimal impact/setup/operation in the eyes of the users
- minimal impact on performance of network management tasks
- resulting system must be manageable by SNMP

Charter Bashing -- The Easy Part

Integrated Security Module for SNMP [ISMS]

- Chair(s):
  - TBD
- Security Area Director(s)
  - Steven Bellovin <smb@research.att.com>
  - Russell Housley <housley@vigilsec.com>
- Mailing Lists:
  - Address: sbsm@machshav.com
  - Subscribe: sbsm-request@machshav.com
  - Archive: https://www.machshav.com/mailman/listinfo/sbsm

Charter Bashing -- History

Version 3 of the Simple Network Management Protocol (SNMPv3) was completed recently and added security to the previous versions of the protocol. Although the enhanced protocol was secure, operators and administrators found that deploying it could be problematic in large distributions. This was due primarily to the addition o a SNMPv3-specific authentication database which must be supported in addition to existing deployed security infrastructures. Most of these devices already contained local accounts and/or the ability to negotiate with authentication servers (e.g. RADIUS servers). However, SNMPv3 did not make use of these authentication mechanisms, and this caused additional synchronization burdens.

Charter Bashing -- Goals

The ISMS working group will focus primarily on creating a security model for SNMPv3 that will meet the security and operational needs of network administrators. The work will include the ability to make use of existing and commonly deployed security infrastructure. Security infrastructures that must be usable by the end solution include:

- Local accounts
- Radius
- TACACS+

Additionally, the following account infrastructures should be considered:

- X.509 Certificates
- Kerberos
- SSH identities
- LDAP

Charter Bashing -- Requirements

The work should not modify the other aspects of SNMP protocol (EG, by adding new PDUs or behavior) in order to achieve these goal of integrated security. It should also be compliant with the security model architectural block of SNMPv3, as outlined in RFC 3411.

The working group may consider adding additional security features not present in SNMPv3's user based security model as long as the new features does not significantly impact the speed at which the newly designed security model is designed, implemented and deployed.

Charter Bashing -- Work items & Timeline

- Work Items:
  - A document defining an integrated authentication security model for SNMPv3.

- Goals and Milestones:
  - Aug 04 BOF
  - Nov 04 Decision about which solution approach the WG will concentrate on and first publication of a WG solution draft
  - Nov 05 Work submitted to the IESG for publication as proposed

Technical Proposals

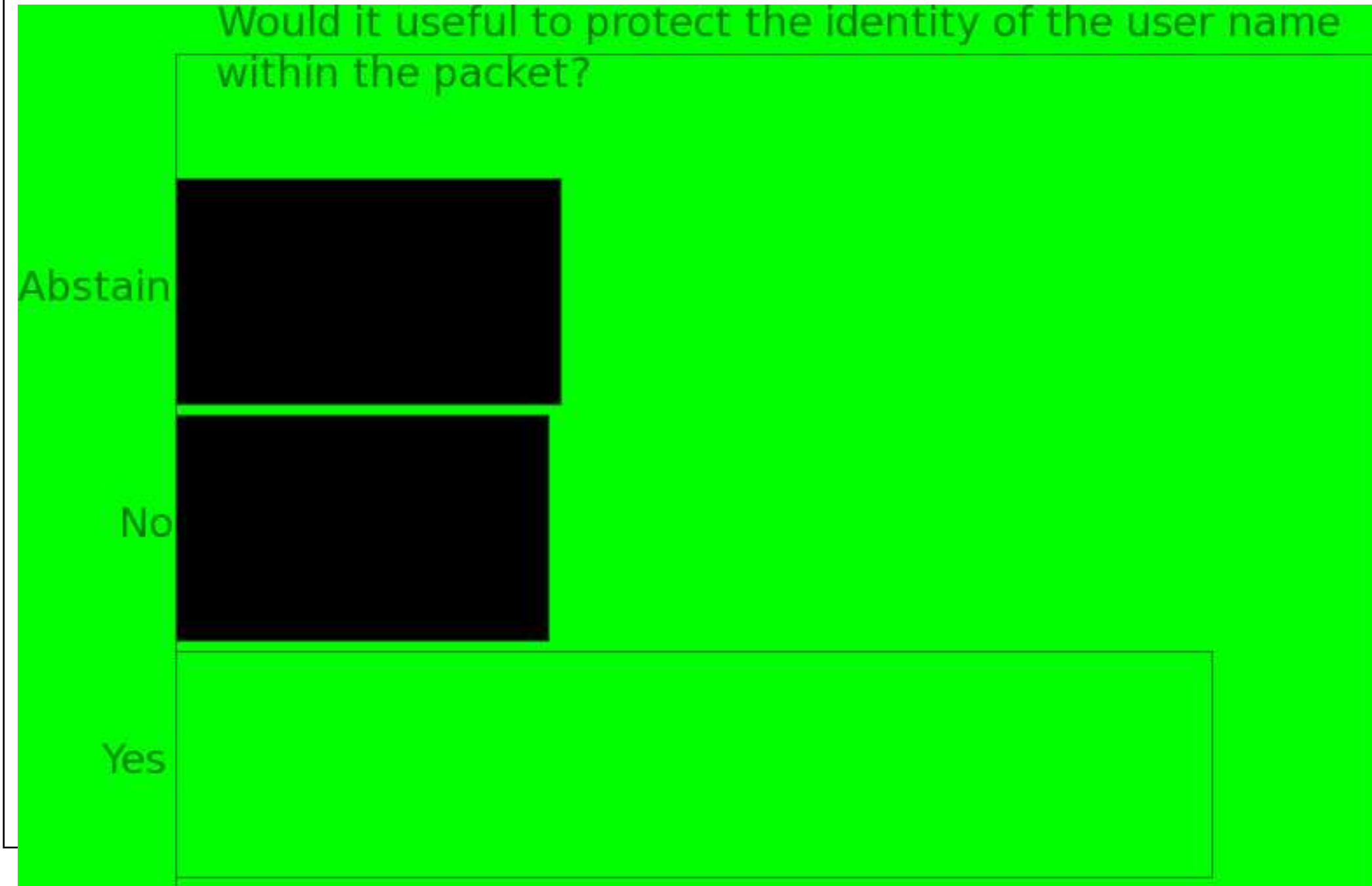
- Presentations about existing work:
  - EUSM: Extended User Based Security
  - KSM: Kerberos-based Security Model
  - SBSM: Session Based Security Model

- Ideas floated, no IDs yet:
  - TLS: Transport Layer Security

Comparison

	USM	EUSM	SBSM	TLS	KRB5
Can use account infrastructure	No	AAA	Yes	Yes	Yes 1/2
Flexible identification methods	No	AAA	Yes	Yes	Yes 1/2
session-keys;	No	Yes	Yes	Yes	central
ident != integrity					
(pair-wise dynamic keys)					
Negotiated auth/priv algorithms	No	No	Yes	Yes	central
Negotiated SNMP Params	Yes	Yes	Yes	No	Yes
True replay protection	No	No	Yes	Yes	Yes

Survey Results --



Path Forward

- WG creation -- AD approval?
- Decide on solution path: November