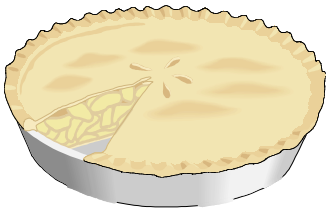
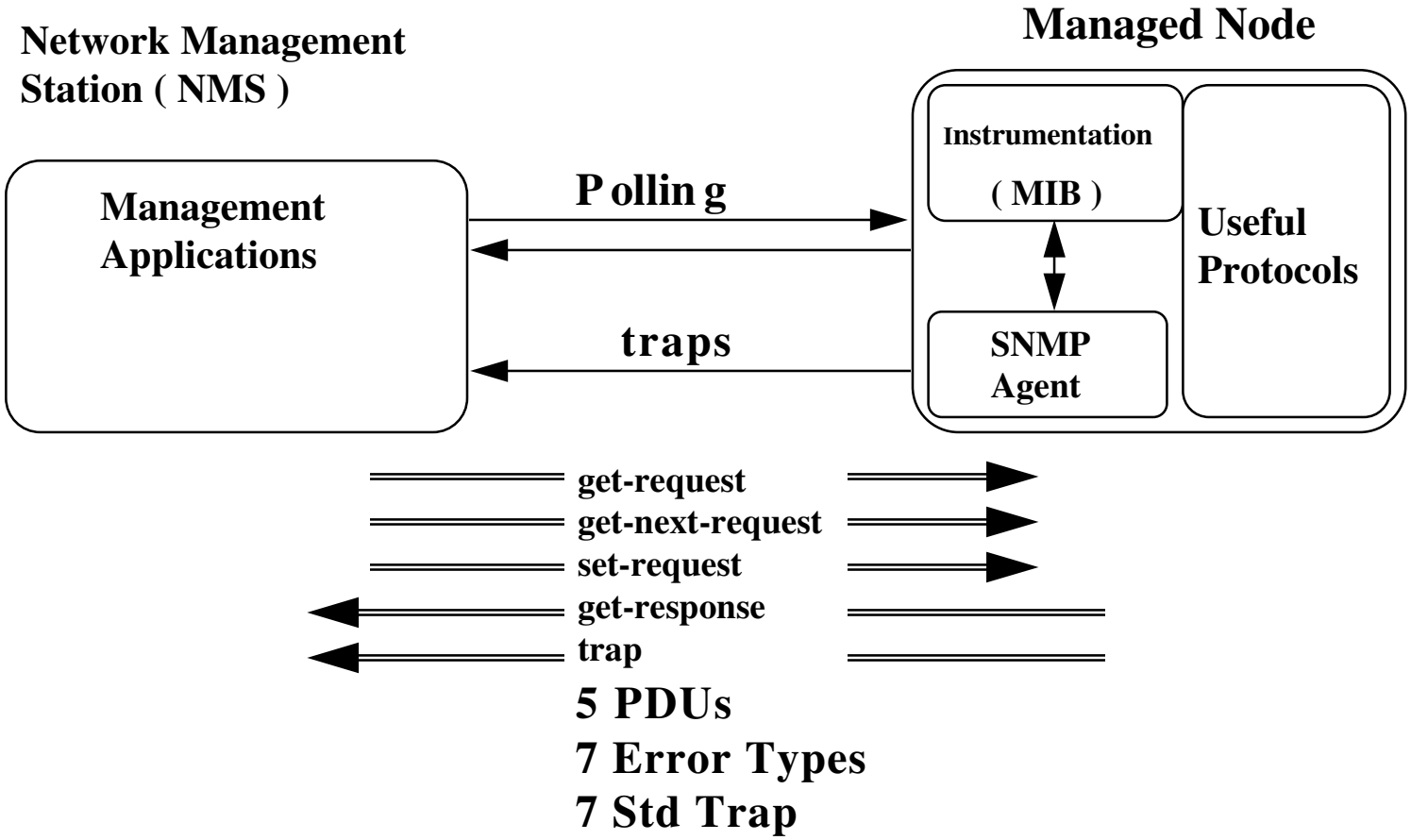
SNMPv2 Brown Bag Lunch



- *A Guided Tour Through SNMPv2*
- **12:05 SNMPv1 Review**
- **12:10 History**
- **12:15 SNMPv2 Features**
  - **12:20 New Messages (PDUs)**
    - **get-bulk**
    - **snmpv2 trap**
    - **inform-request**
  - **12:30 Security Features**
    - **Parties**
    - **Authentication Wrappers**
    - **Privacy Wrappers**
  - **12:45 Other SNMPv2 Goodies**

SNMPv1 Big Picture



History

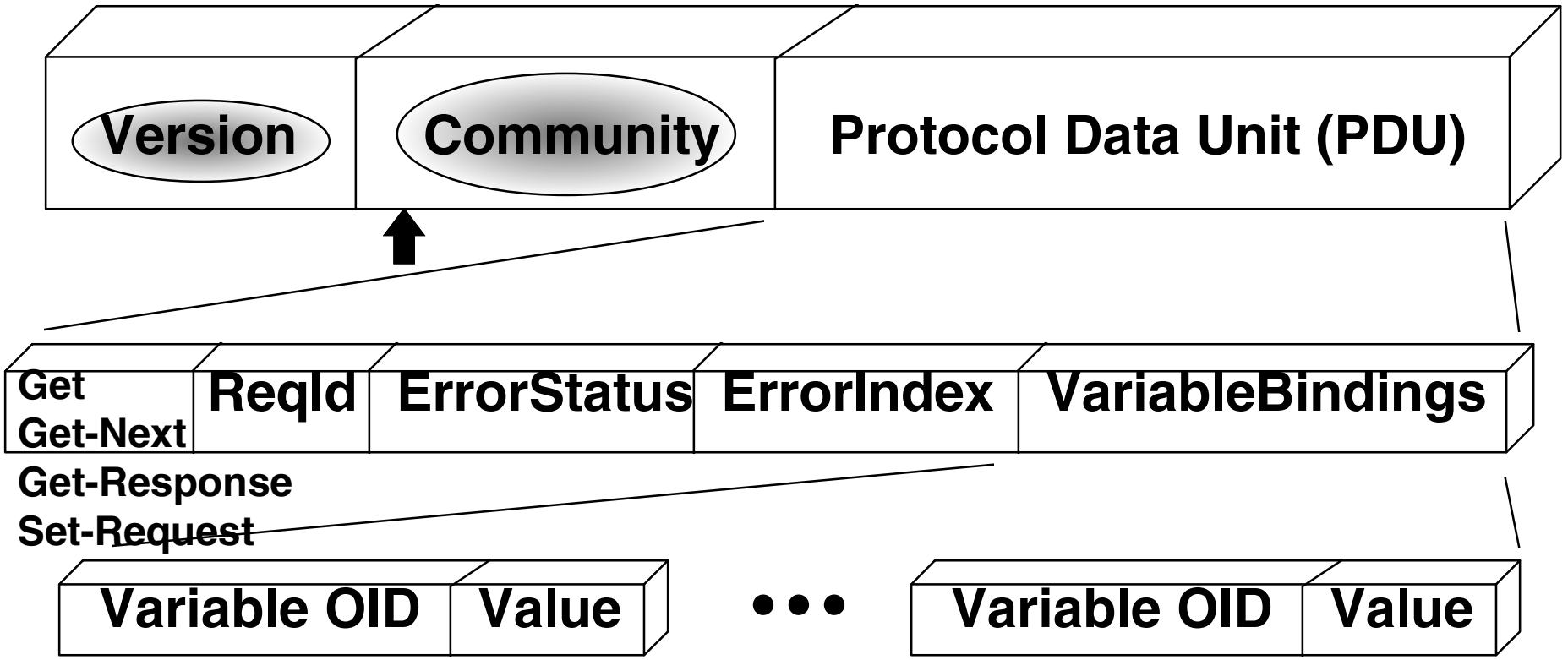
- Several IETFs - NM AD-SNMPv1 problems?
- March '92 - RFP to evolve Framework
- July '92 - SMP BOF
  - Gang of Four - Case, McCloghrie, Rose, Waldbusser
- Nov '92 - SNMPv2 WG begins - few changes
- Feb '93 - SNMPv2 moved to draft
  - SNMPv1 - defined in 3 RFCs
  - SNMPv2 - 12 RFCs - "That's progress for you"
- Few implementations as commercial products

What is new in SNMPv2?

- **New PDUs**
- **Added Security**
- **Greater information in Errors**
- **Row creation mechanism defined**
- **Textual conventions defined**
- **Manager-of-managers (M2M MIB)**
- **Proxy relationships**
- **SNMPv2 MIB**
- **more...**

SNMPv1 Messages

- **Community - Authentication/Authorization**
- **String sent in Clear Text**
- **Explicit Community Profile - access and view**



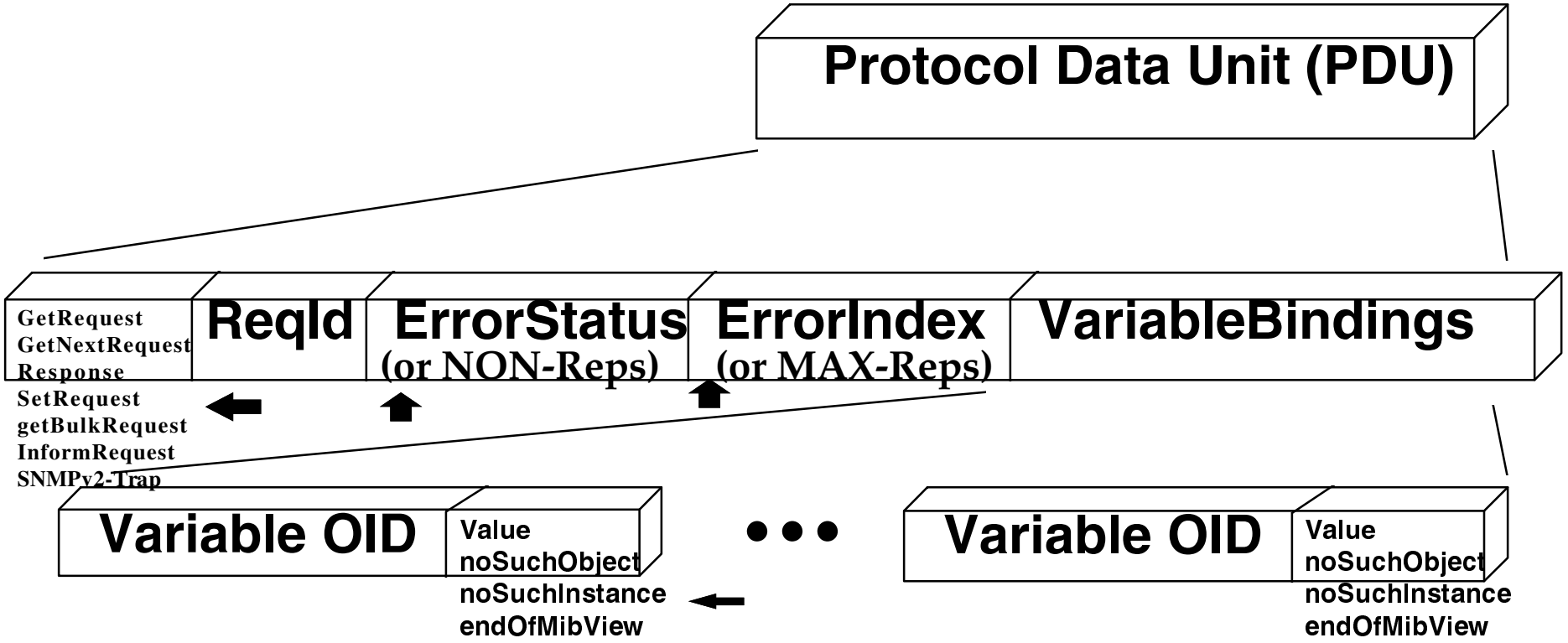
SNMPv2 Specifications

- *SNMPv2 Defined in the 12 RFC Series:*
- **rfc1441 Introduction to SNMPv2**
- **rfc1442 SMI for SNMPv2**
- **rfc1443 Textual Conventions for SNMPv2**
- **rfc1444 Conformance Statements for SNMPv2**
- **rfc1445 Administrative Model for SNMPv2**
- **rfc1446 Security Protocols for SNMPv2**
- **rfc1447 Party MIB for SNMPv2**
- **rfc1448 Protocol Operations for SNMPv2**
- **rfc1449 Transport Mappings for SNMPv2**
- **rfc1450 MIB for SNMPv2**
- **rfc1451 Manager to Manager MIB**
- **rfc1452 SNMPv2 and SNMPv2 Coexistence**

SNMPv2 Messages

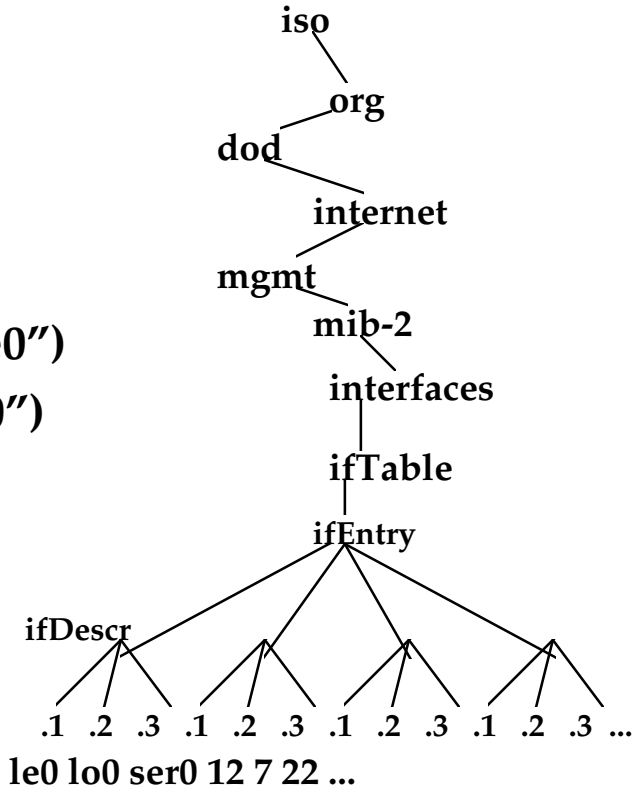
No more TRAP PDU, 3 alternative PDUs
Individual VarBinds Can be in error, others can still succeed

- **Expanded PDUs**



getBulk Message

- **SNMPv1 - worst case**
  - **get-next(ifDescr.0)...getResponse(ifDescr.1="ie0")**
  - **get-next(ifDescr.1)...getResponse(ifDescr.2="lo0")**
  - **:**
- **SNMPv2 - getBulk PDU**
- **getBulk(non-repeaters=1, max-repetitions=100, VarBinds=sysDescr.0, ifDescr.0)**
- **BUT..It is does not stop until max-reps exceeded**
- **Or EndOfMibView is reached**

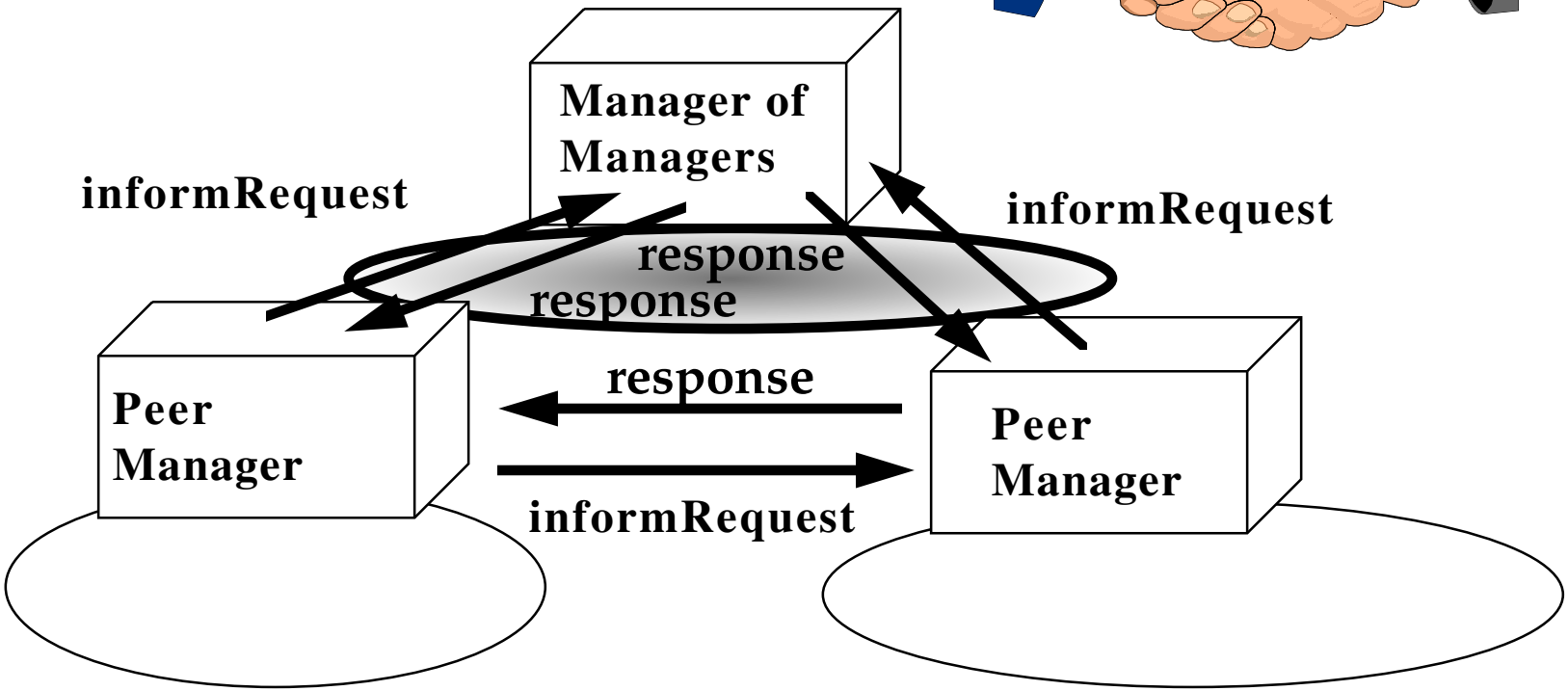


sysDescr.0
sysLocation.0
sysContact.0
sysName.0

	ifDescr	ifType	ifMtu	...	ifOperStatus	...
.1	le0	12	1500		UP(1)	
.2	lo0	7	1500		DOWN(2)	
.3	ser0	22	23590		TESTING(3)	

informRequest PDU

- Traps inherently unreliable
- Dumb devices shouldn't have to ...retransmit
- M2M communication

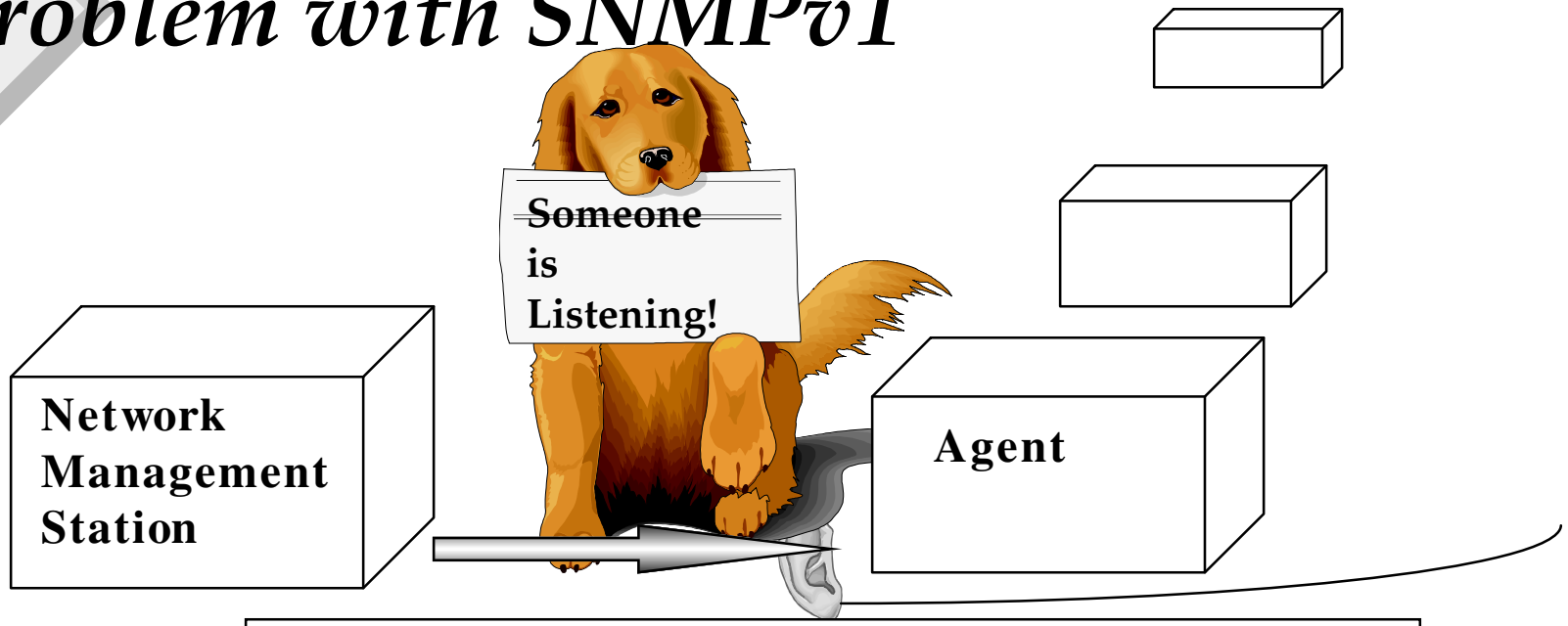


SNMPv2 Security

- Authentication
- Parties
- Party Database
- How Authentication Works
- Privacy Wrapper
- Clock Synch
- NVM Requirements
- Secret Distribution

French Hacker

Problem with SNMPv1



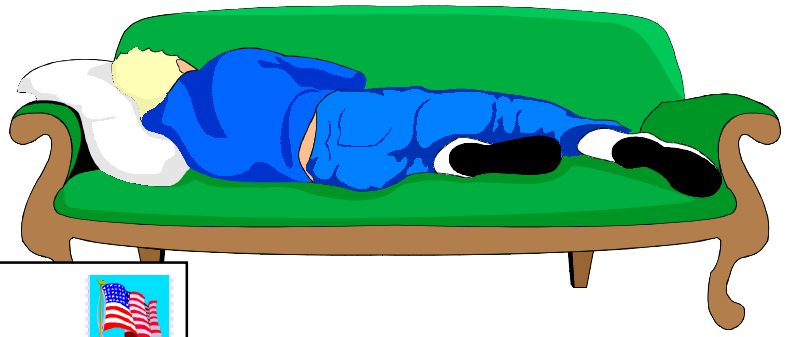
SNMP Msg | **Community=writeme, set (ifOperStatus.1 = DOWN)**

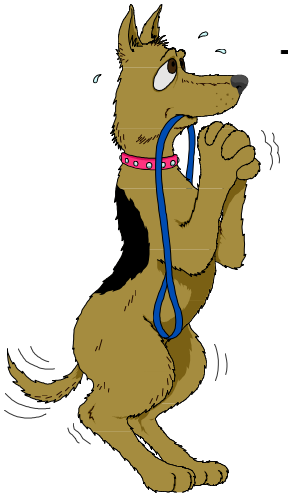
userid=community
pas s word=
loginProfile=communityProfile

So, guess the userid (community) and ...
you are afforded the rights of that userid (community) !!
Capture & replay also, ambigous destination machine, ...

Authentication

- Identify the source and destination of the communication
- Elements of the new security model
  - SNMPv2 Communication
  - SNMPv2 Parties
  - SNMPv2 MIB Views
  - SNMPv2 Access Policies



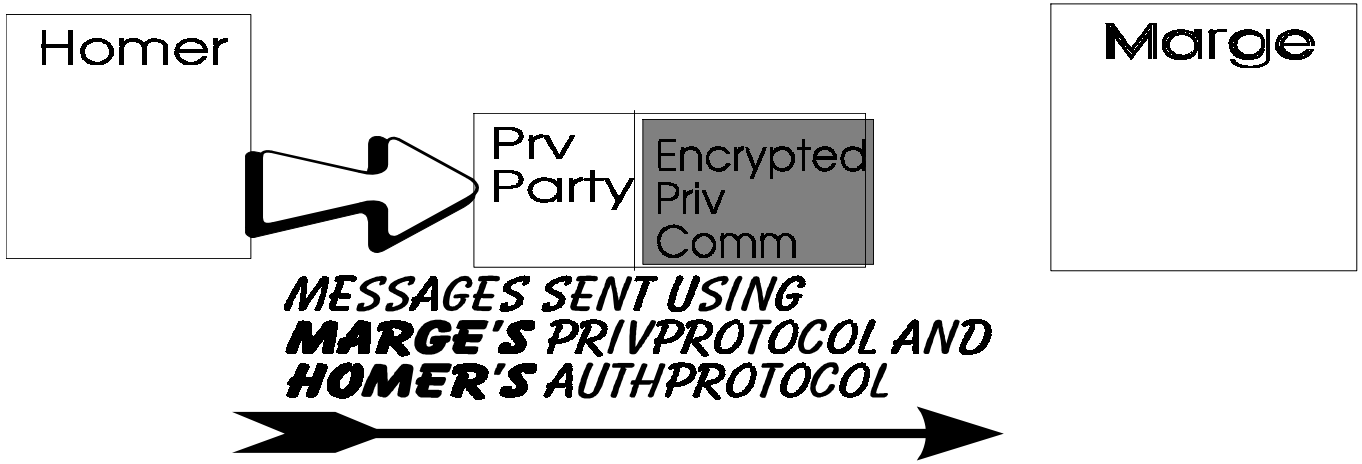


From: Morgan

To: Bill

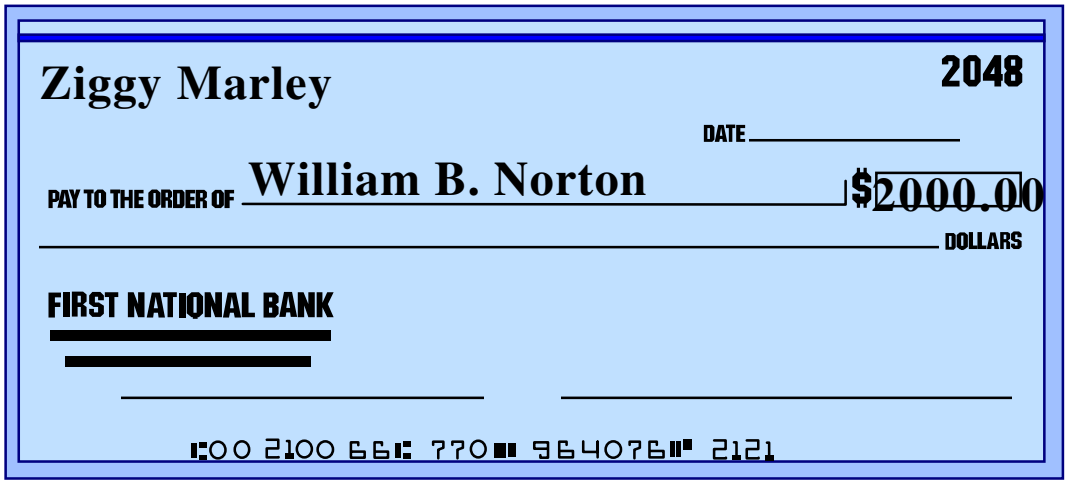
Party Database

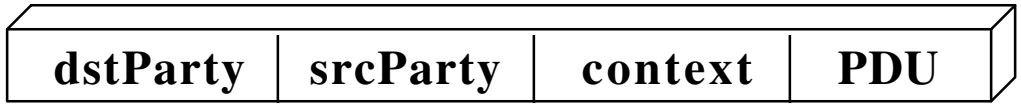
	Homer	Marge
Identity	*Homer*	Marge
TDomain	*snmpUDPDomain*	snmpUDPDomain
TAddress	*1.2.3.4, 161*	1.2.3.5, 161
MaxMessageSize	*1500*	1500
AuthProtocol	*v2md5AuthProtocol*	v2md5AuthProtocol
AuthClock	*0*	0
AuthPrivate	*0123456789ABCDEF*	GHIJK0123456789
AuthPublic		
AuthLifetime	*300*	300
PrivProtocol	*desPrivProtocol*	desPrivProtocol
PrivPrivate	*MNOPQR0123456789*	0123456789QRSTUV
PrivPublic		



SNMP Management Communication (snmpMgmtComm)

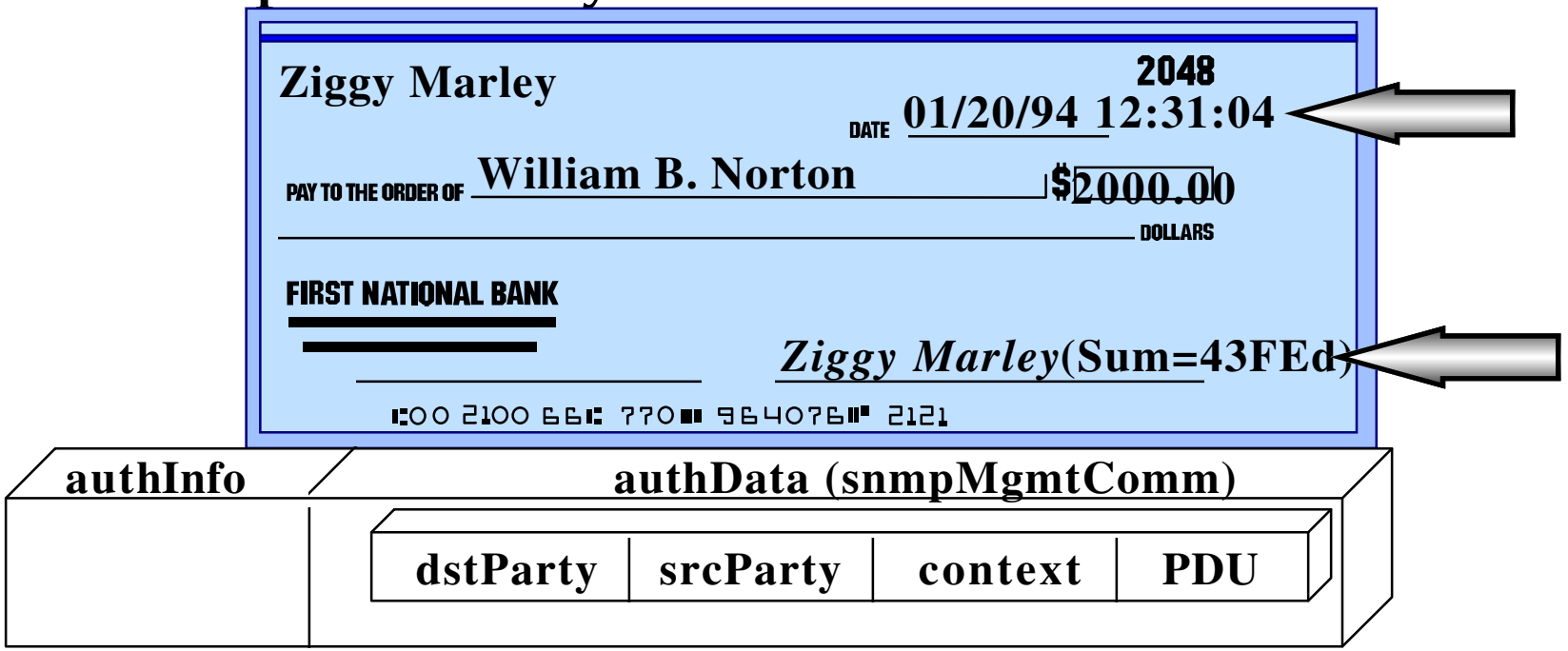
- a disambiguated SNMPv2 Operation
- Parties: 2 endpoints of communication
- a check with the payer, payee, and amount filled in





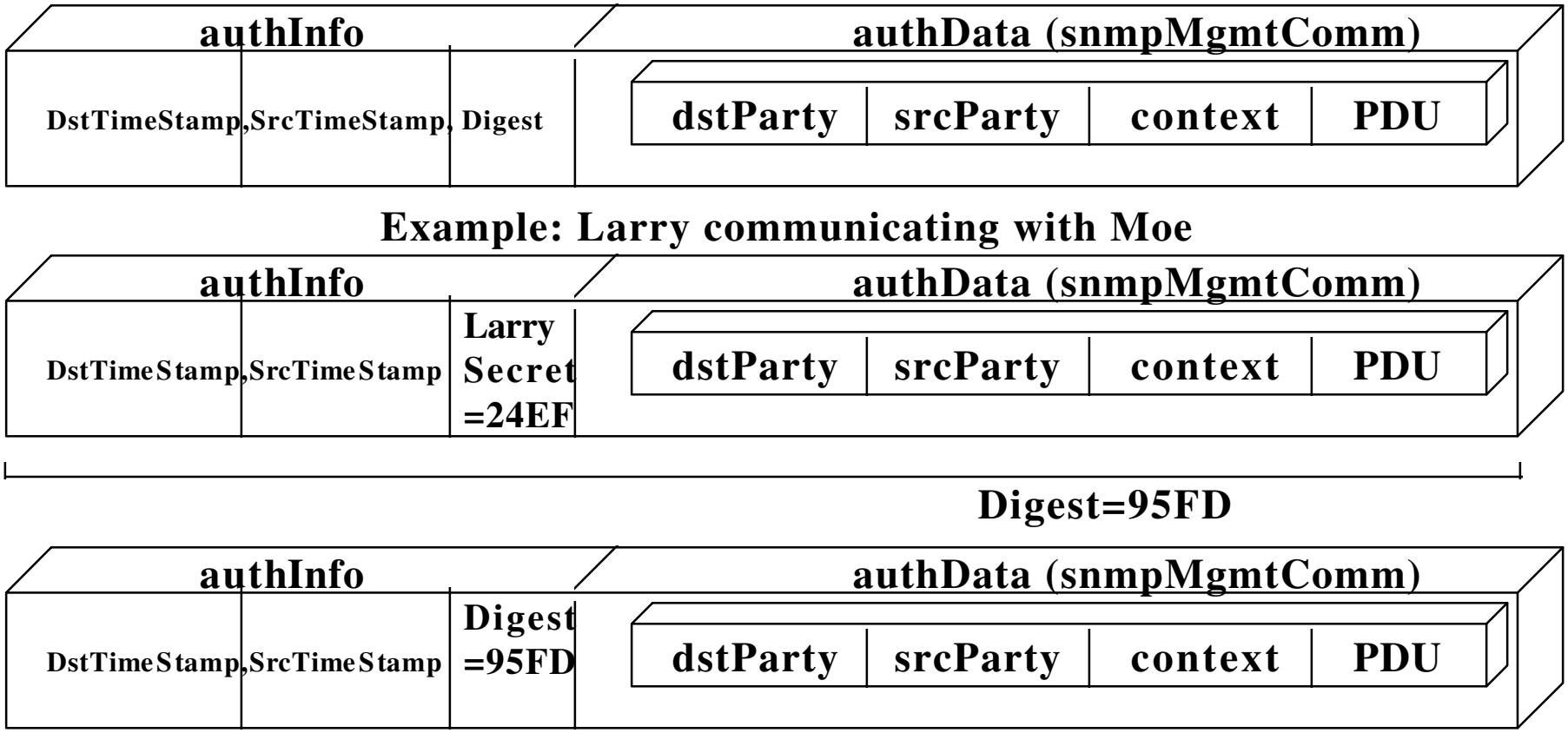
SNMP Authenticated Message (snmpAuthMsg)

- represents a SNMPv2 operation of reliable origin and integrity
- a check that is dated, signed in a technology dependent way



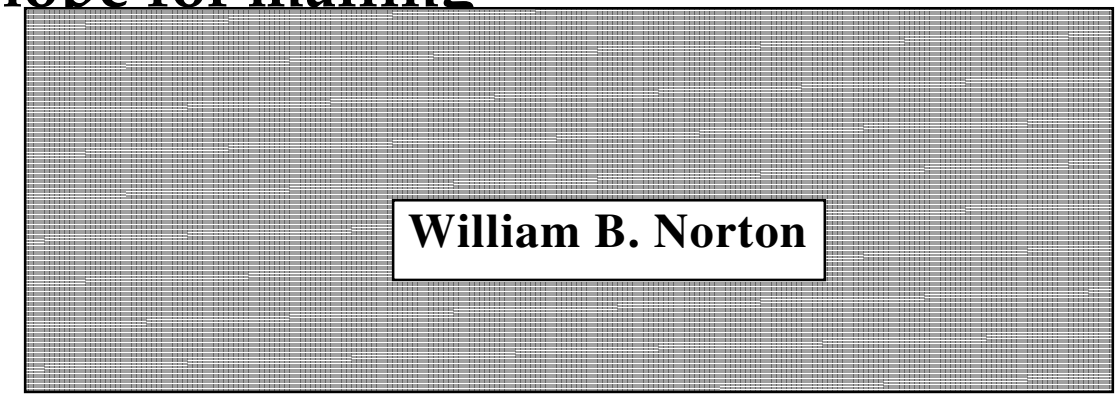
SNMP Authenticated Message

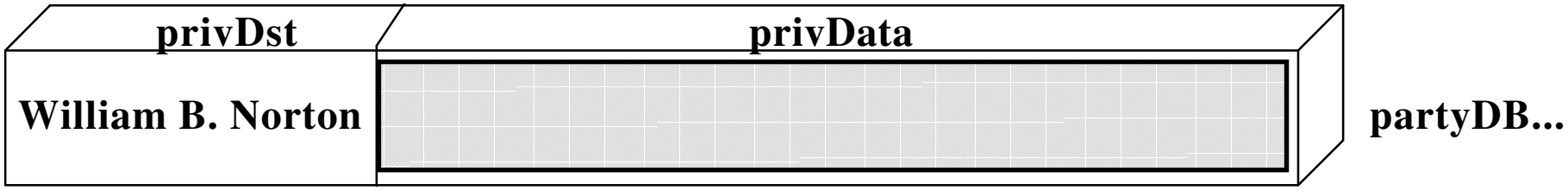
- *Example: How authentication works using MD5*



SNMP Privacy Message

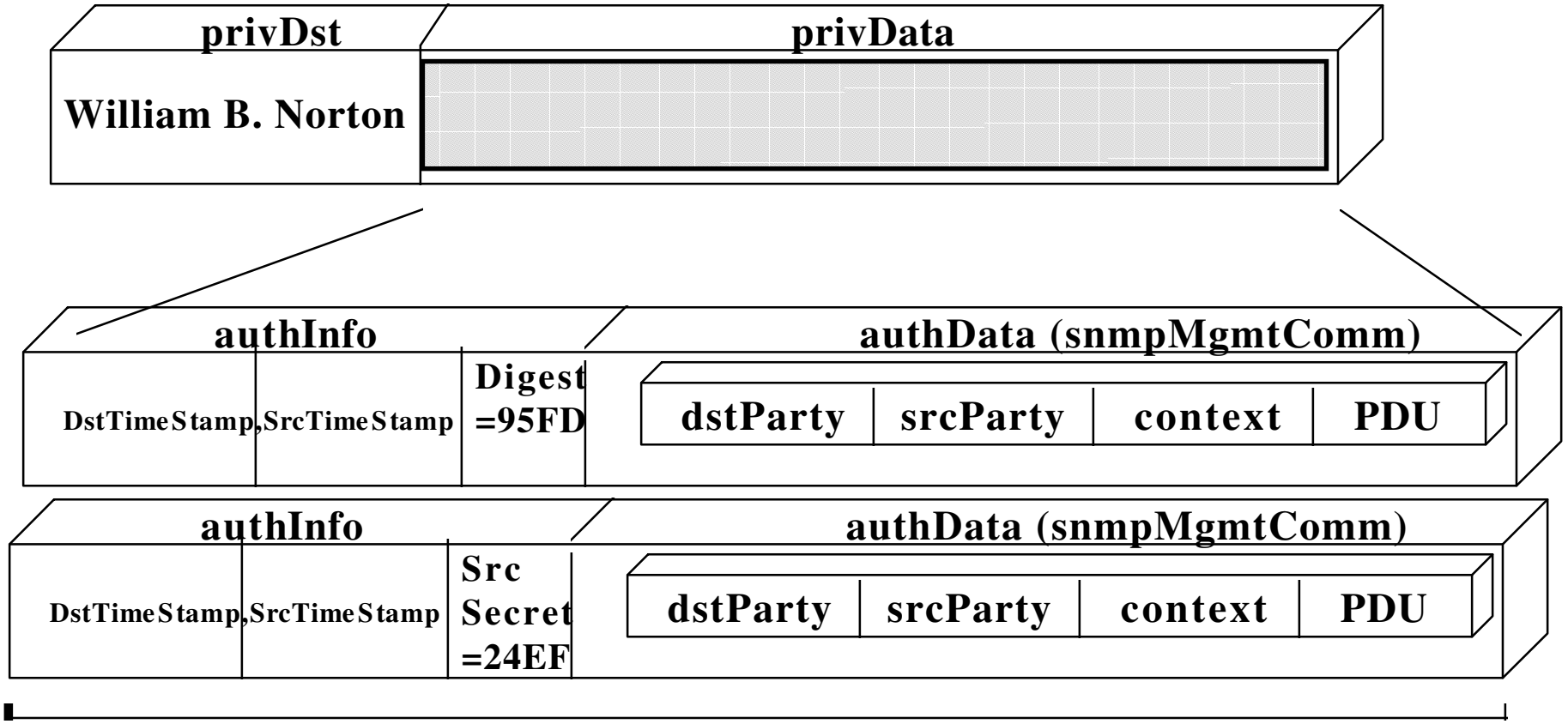
- a SNMPv2 message protected from Disclosure
- useful for exchanging secrets, captured RMON packets, etc
- a signed check in a more or less opaque, addressed envelope for mailing





SNMP Security Realized

Received this SNMPv2 Message:



Digest=95FD

My Calculated Digest=Transmitted digest...
Private, Authenticated, and integrity insured message!
It is that Easy! Ha!

Access Control List

- snmpMgmtComm context used as key

Target	Subject	Context	Privileges
gracie	george	local	35 (Get, GetNext & GetBulk)
george	gracie	local	132 (Response & SNMPv2-Trap)

Defines the rights afforded to the parties in the given context.

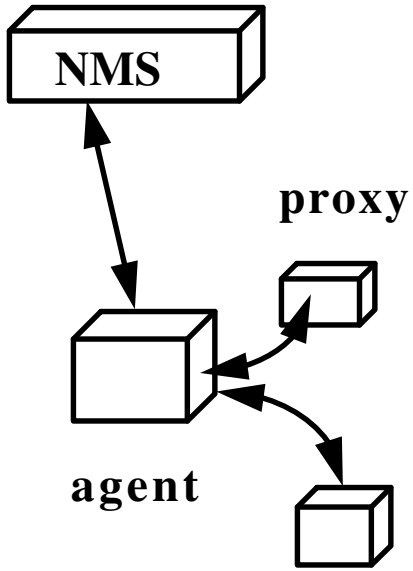
Analogous to the read-only/read-write community name configuration, but more flexible.

Get	1
GetNext	2
Response	4
Set	8
---unused	16
GetBulk	32
Inform	64
SNMPv2-Trap	128

Context and View Table

- From Context, determine view

Identity	View Index	ProxySrcParty	proxyDstParty	....
local	1			
peer	2	me_n_my	shadow	
box	2	laurel	hardy	

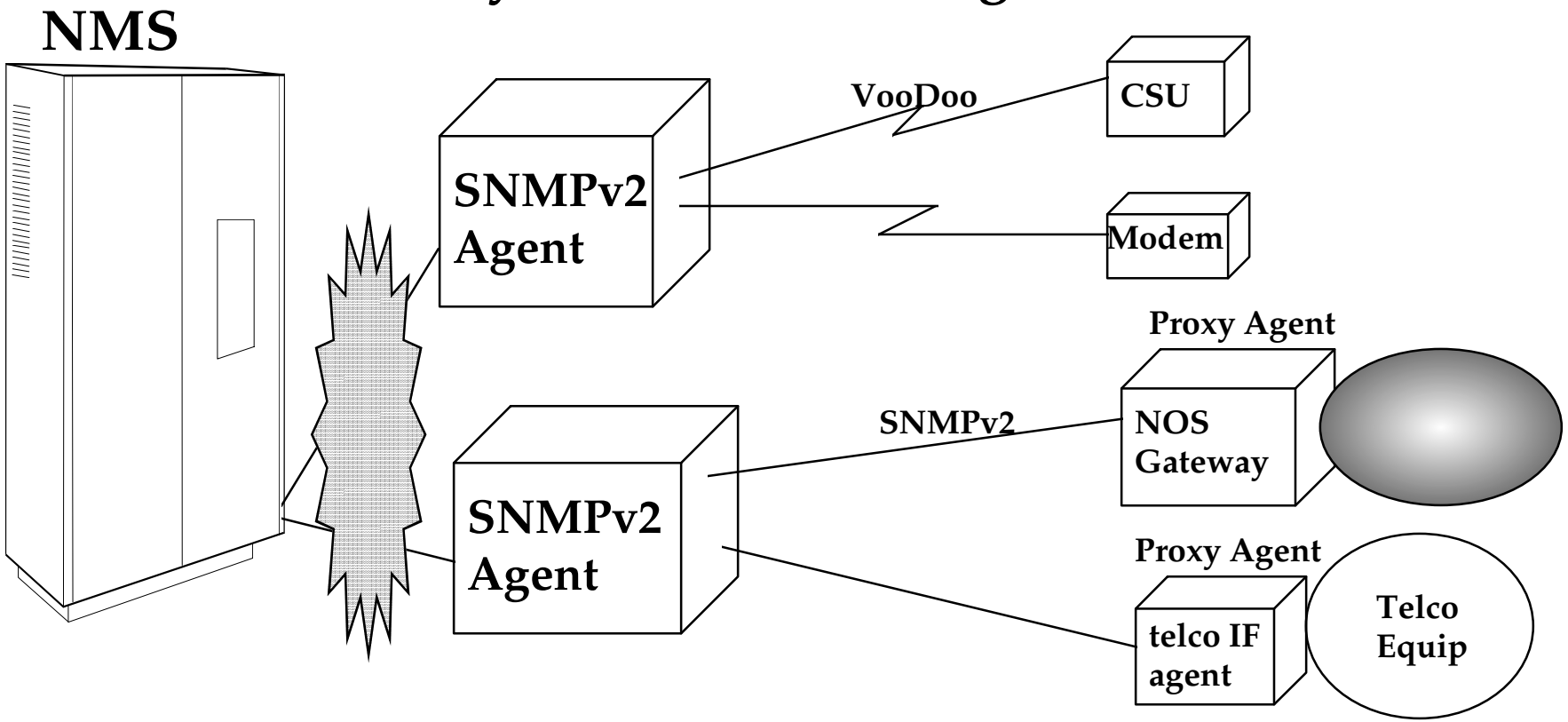


Index	Subtree	Mask(signif. subids)	Type ...
1	1.3.6.1.2.1	''B	inclusive
1	1.3.6.1.4.1.25	'1111101'B	inclusive
1	1.3.6.1.2.1.2.1	''B	exclusive
2	1.3.6.1.4.1	''	inclusive

Collectively, MIB View

Proxy Relationships

- **Foreign Proxy - manage non-snmp boxes**
- **Native Proxy - distribute management**



Other Features of SNMPv2

- **18 Error Status Values**
- **Instance level granulation**
- **MOM communication**
- **Textual Conventions**
- **SNMPv2 MIB (partyDB, contexts, views,**
- **Manager-to-manager MIB**

SNMPv2 References

- **rfc1441-rfc1452 - anonymous FTP**
- **The Simple Book, 2nd edition, Marshall T. Rose**
- **SNMP, SNMPv2, and CMIP, William Stallings**
- **The Simple Times, Electronic Publication, st-subscriptions@simple-times.org**
- **snmp@psi.com**
- **snmpv2-request@magellan.TIS.COM**