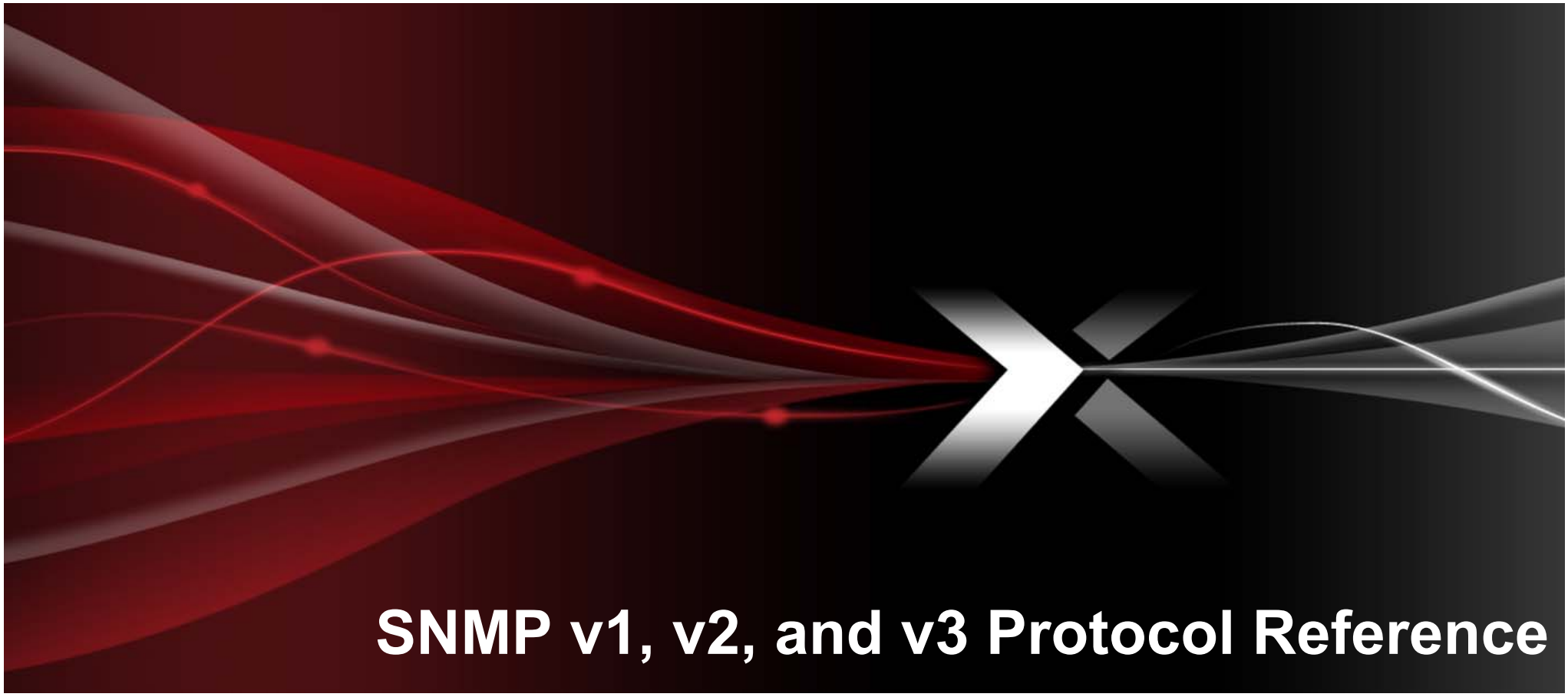


SNMP v1, v2, and v3 Protocol Reference

Benoît H. Dicaire <Benoit.Dicaire@INFRAX.com>

Version: July, 2006

This is a snapshot of an on-line document. Paper copies are valid only on the day they are printed.

Please refer to the author if you are in any doubt about the currency of this document.

While every effort has been taken to verify the accuracy of this information, neither INFRAX incorporated nor the author of this publication can accept any responsibility or liability for errors, omissions, or damages resulting from the use of the information herein.

The current electronic of the document will be found at : www.INFRAX.com/Publications

INFRAX®

Publication's Information

Version: July, 2006

This document was created on 9 April 2001 and is based on the best information available at revision time.

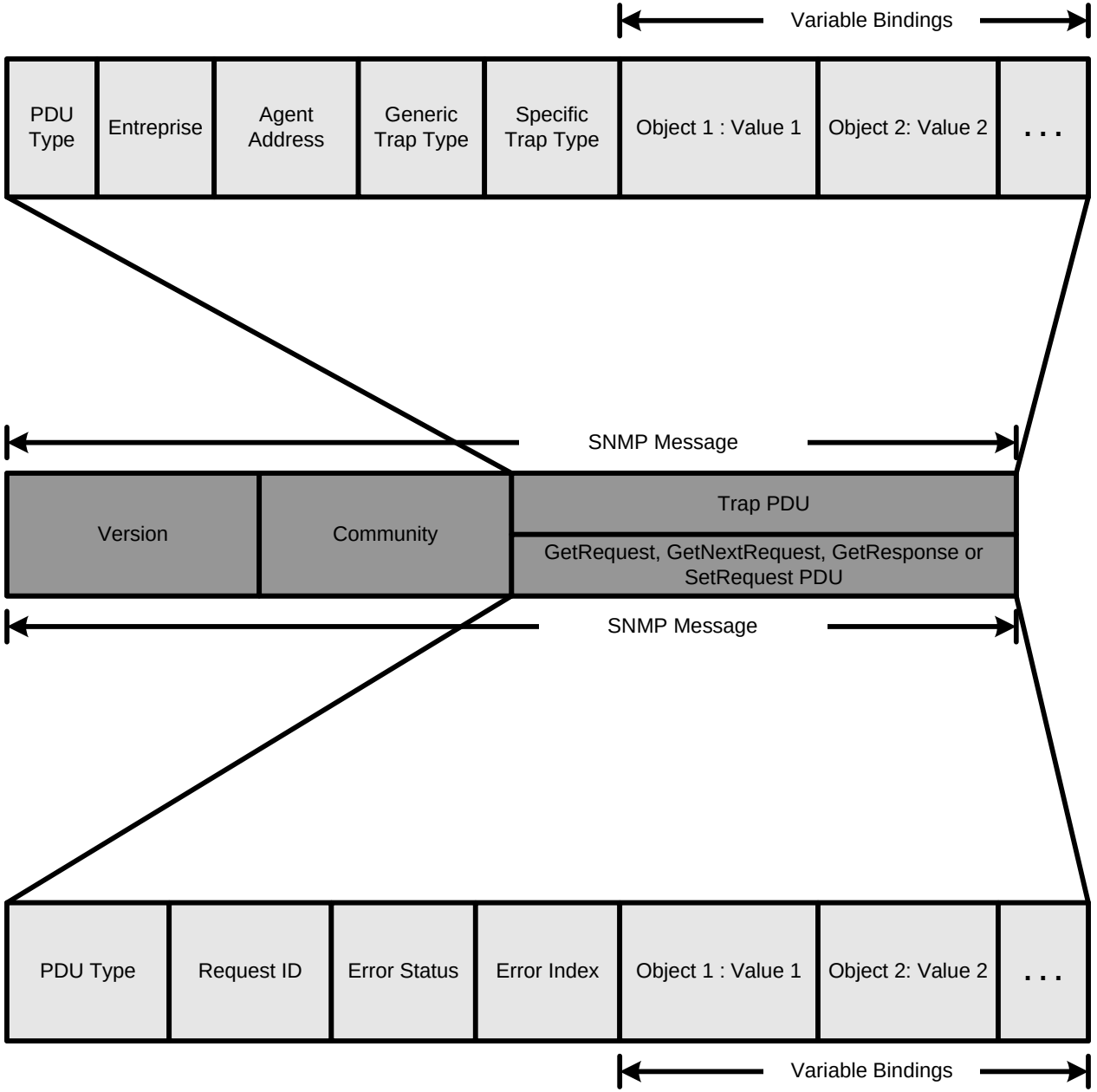
About the Author
Benoît H. Dicaire is the founder and Information Security Strategist for INFRAX.

With nearly two decades of experience providing key strategies and technology solutions for managing information security risks, Dicaire now focuses his work on Security Posture Assessment and Enterprise Architecture for organizations in Canada and around the world.

A trusted advisor, Dicaire is frequently consulted by leaders of private and government organizations.

About INFRAX
INFRAX is an independent Information Security consulting firm dedicated to providing our clients with top-level security solutions, advice and protection. Furthermore, unbiased in-depth INFRAXstructure analysis helps organizations make smarter enterprise architecture decisions adapted to today's increasingly complex environments.

SNMP v1 Message Formats



SNMP v1 Field Formats

Field	Description
Enterprise:	SNMP sysObject ID.
Agent Address:	IP address of SNMP Agent.
Generic Trap Type:	Specifies the message type. Values are: 0 = coldStart 1 = warmStart 2 = linkDown 3 = linkUp 4 = AuthenticationFailure 5 = egpNeighborLoss 6 = enterpriseSpecific
Specific Trap Type:	Trap code.
Timestamp:	Current value of that Agent's sysUpTime object.
Variable Bindings:	Pairing of object name and value.

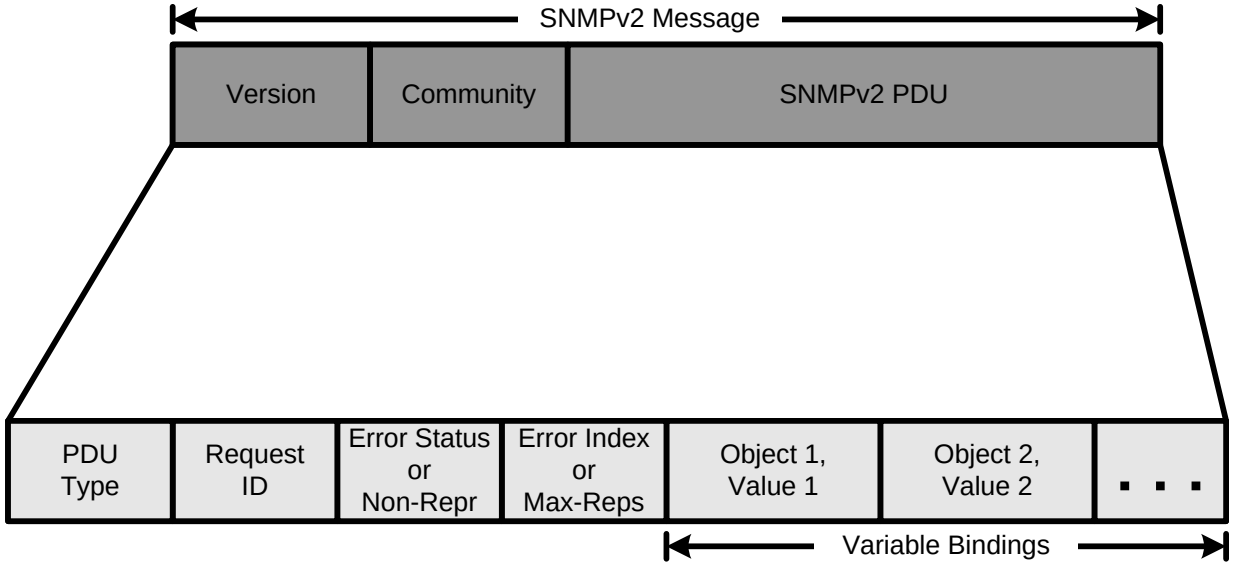
Field	Description
Version:	Protocol version.
Community:	Community name.
PDU Type:	Specifies the PDU being transmitted: 0 = GetRequest 1 = GetNextRequest 2 = GetResponse 3 = SetResponse 4 = Trap

Field	Description
Request ID:	Used to correlate the Request and Response.
Error Status:	Exception condition for the request. Values are: 0 = noError 1 = tooBig 2 = noSuchName 3 = badValue 4 = readOnly 5 = genErr
Error Index:	Pointer to Variable Binding that caused the error.
Variable Bindings:	Pairing of object name value.

RFC	Subject
1155	Structure of Management Information
1157	Simple Network Management Protocol (SNMP)
1212	Concise MIB Definitions
1213	Management Information Base (MIB-II)
1214	OSI Internet Management MIB
1215	Convention for Defining Traps
1270	SNMP Communications Services
1303	Convention for Describing SNMP Agents
1418	SNMP over OSI
1419	SNMP over Apple Talk
1420	SNMP over IPX
1493	Managed Objects for Bridges

RFC	Subject
1512	FDDI MIB
1559	DECnet Phase IV MIB Extensions
1643	Managed Objects for Ethernet
1694	Managed Objects for the SMDS SIP Interface
1695	ATM MIB
1748	IEEE 802.5 Token Ring MIB
1757	Remote Network Monitoring (RMON) MIB
1850	OSPF Version 2 MIB
1901	Community-based SNMPv2
2021	RMON2 MIB
2115	Frame Relay DTE MIB
2271	SNMPv3

SNMP v2 Message Format



Version: Protocol version (SNMPv2 = 1).

Community: Community name.

PDU Type: Specifies the PDU being transmitted:

0 = GetRequest
1 = GetNextRequest
2 = Response
3 = SetRequest
4 = obsolete
5 = GetBulkRequest
6 = InformRequest
7 = SNMPv2-Trap
8 = Report

Request ID: Used to correlate the Request and Response.

Error Status:
Exception Condition for the request

0 = noError
1 = tooBig
2 = noSuchName
3 = badValue
4 = readOnly
5 = genErr
6 = noAccess
7 = wrongType
8 = wrongLength
9 = wrongEncoding
10 = wrongValue
11 = noCreation
12 = inconsistentValue
13 = resourceUnavailable
14 = commitFailed
15 = undoFailed
16 = authorizationError*
17 = notWritable
18 = inconsistentName

Error Index: Pointer to the Variable Binding in error.

Non-Repeaters: How many of the requested variables will not be processed repeatedly, e.g. single instances of variables. Used in GetBulkRequests only.

Max-Repetitions: Maximum number of repeated executions to retrieve specific variables. Used in GetBulkRequest only.

Variable Bindings: Pairing of object name and value.

SNMP v2 Protocol Reference Guide

SNMPv2 PDU	Agent		Manager	
	Generate	Receice	Generate	Receive
GetRequest		x	x	
GetNextRequest		x	x	
Response	x		x	x
SetRequest		x	x	
GetBulkRequest		x	x	
InformRequest			x	x
SNMPv2-Trap	x			x

When errors occur in the processing of SNMPv2 PDUs, the SNMPv2 entity prepares a Response PDU with the Error Status field set to indicate the error. Possible errors include:

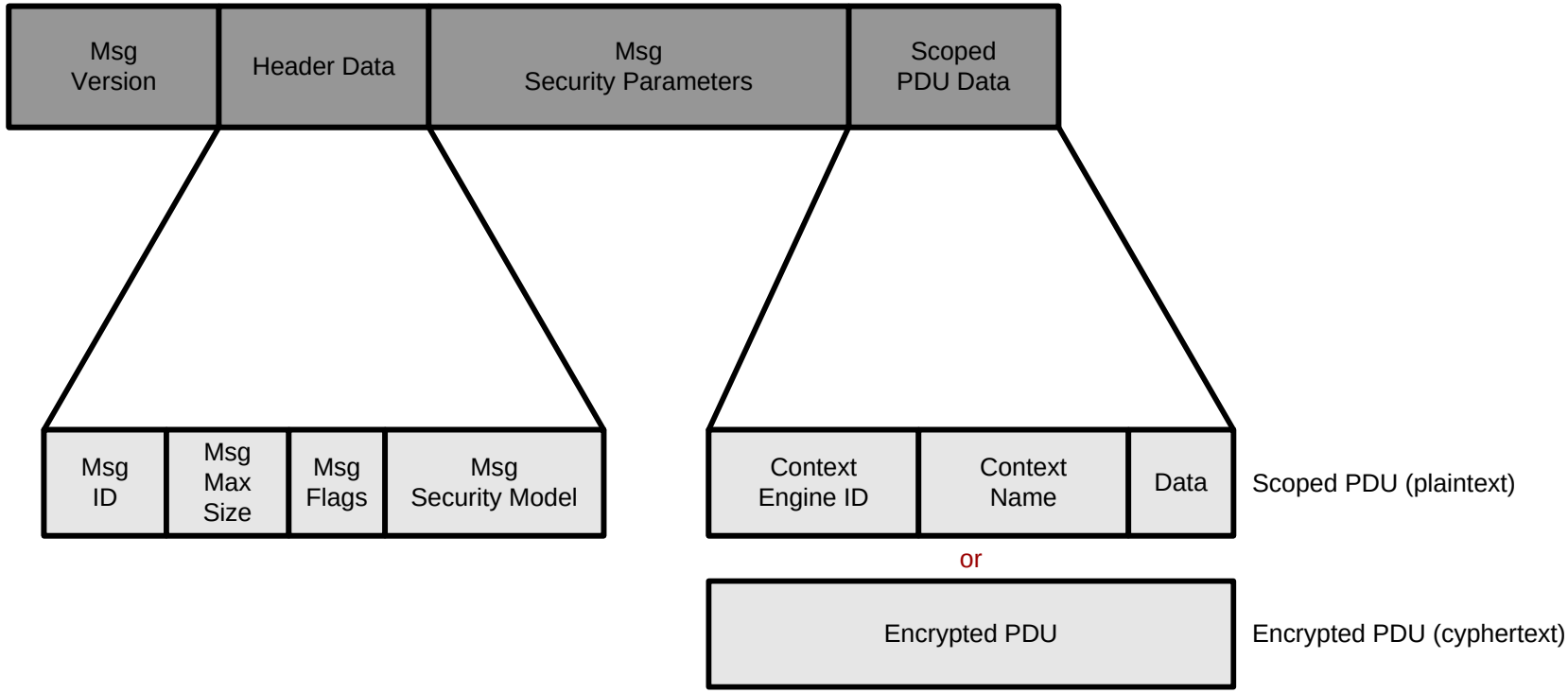
SNMPv2 Error	Get	GetNext	GetBulk	Set	Inform
noError	x	x	x	x	x
tooBig	x	x		x	x
noSuchName(b)					
badValue(b)					
readOnly(b)					
genErr	x	x	x	x	
noAcces				x	
wrongType				x	
wrongLength				x	
wrongEncoding				x	
wrongValue				x	
noCreation				x	
inconsistentValue				x	
resourceUnavailable				x	
commitFailed				x	
undoFailed				x	
authorizationError	x(a)	x(a)	x(a)	x(a)	x(a)
notWritable				x	
inconsistentName				x	

Notes:
(a) Unused with SNMPv2, per RFC 1901.
(b) Never generated by a SNMPv2 entity (proxy compatibility only), per RFC 1905.

Reference Documents

RFC	Subject
1901	Introduction to Community-based SNMPv2
1902	SMI for SNMPv2
1903	Textual Conventions for SNMPv2
1904	Conformance Statements for SNMPv2
1905	Protocol Operation for SNMPv2
1906	Transport Mapping for SNMPv2
1907	MIB for SNMPv2
1908	SNMPv1 and SNMPv2 Coexitence
1909	Administrative Infrastructure for SNMPv2
1910	User-based Security Model

SNMP v3 Message Format



msgVersion: Identifies the message as an SNMPv3 message when msgVersion = 3.

msgID: Used to coordinate request and response messages between the manager and the agent. The msgID in a response must be the same as the msgID in a request.

msgMaxSize: conveys the maximum message size that the sender can accept.

msgFlags: bit fields which control processing of the message:

Field	Meaning
....1	authFlag
.... ..1.	privFlag
.... .1..	reportableFlag
.... ..00	is OK, means noAuthNoPriv
.... ..01	is OK, means authNoPriv
.... ..10	reserved, must NOT be used
.... ..11	is OK, means authPriv

SNMPv3 Message Format-suite

msgSecurity Model:	identifies the Security Model used for the message generation and reception.
msgSecurityParameters:	used for communication between the Security Model modules.
scopedPduData:	either a plaintext scoped PDU, or a cyphertext encrypted PDU.
scopedPDU:	identifies an administratively-unique context and PDU.
contextEngineID:	determines the context to process this PDU, such as the correct application.
contextName:	identifies the context associated with the management information in the PDU.
data:	contains the SNMPv3 PDU, which must be one of the PDUs specified in RFC 1905: GetRequest, GetNextRequest, Response, SetRequest, GetBulkRequest, InformRequest, SNMPv2-Trap or Report.

SNMPv3 Protocol Reference Guide

RFC	Subject
2271	An Architecture for Describing SNMP Management Frameworks.
2272	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
2273	SNMPv3 Applications
2274	User-based Security Model (USM) for SNMPv3
2275	View-based Access Control Model (VACM) for SNMP