



IBM Tivoli zSeries and Performance Automation

SNMPv3 Managagement and Security Meeting of the Minds

Laura Knapp

ljknapp@us.ibm.com

1-919-949-1617

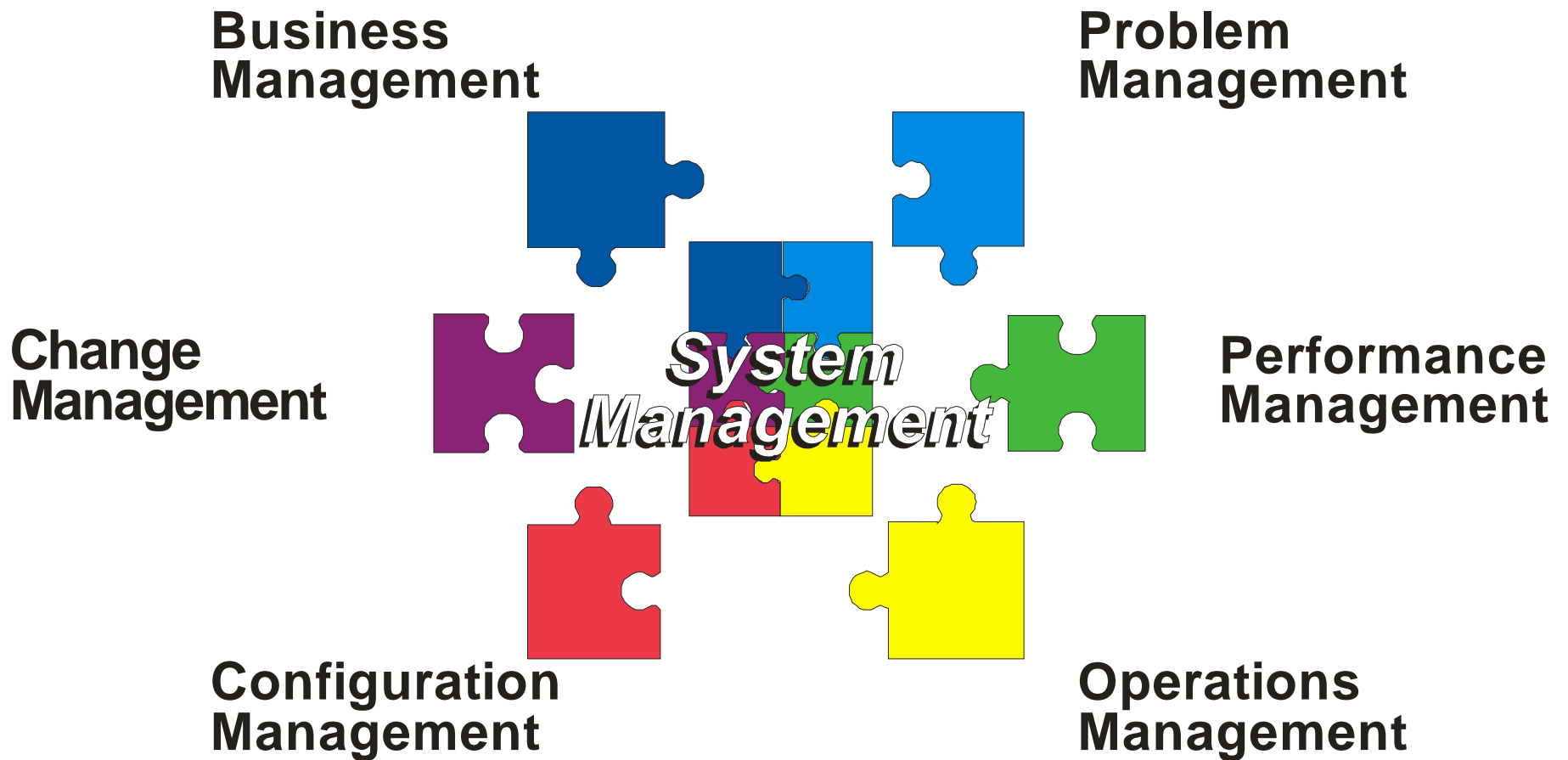


ON DEMAND BUSINESS™

© 2005 IBM Corporation

March 2006 : IBM Software Group : Share User Group

Success Systems Management



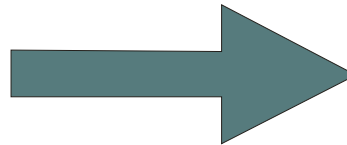
What is SNMP?

Simple Network Management Protocol

Internet standard

Initially tied to
TCP/IP protocol

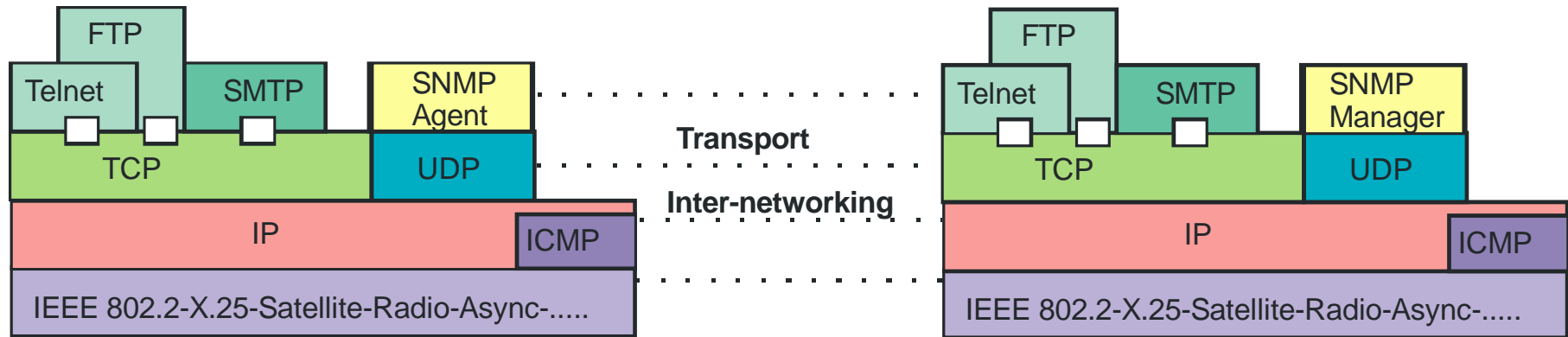
Set of functions
monitor network elements
control network elements



Routers, switches, Unix
hosts, bridges, hubs,
agents for many
operating systems, etc



SNMP Layering



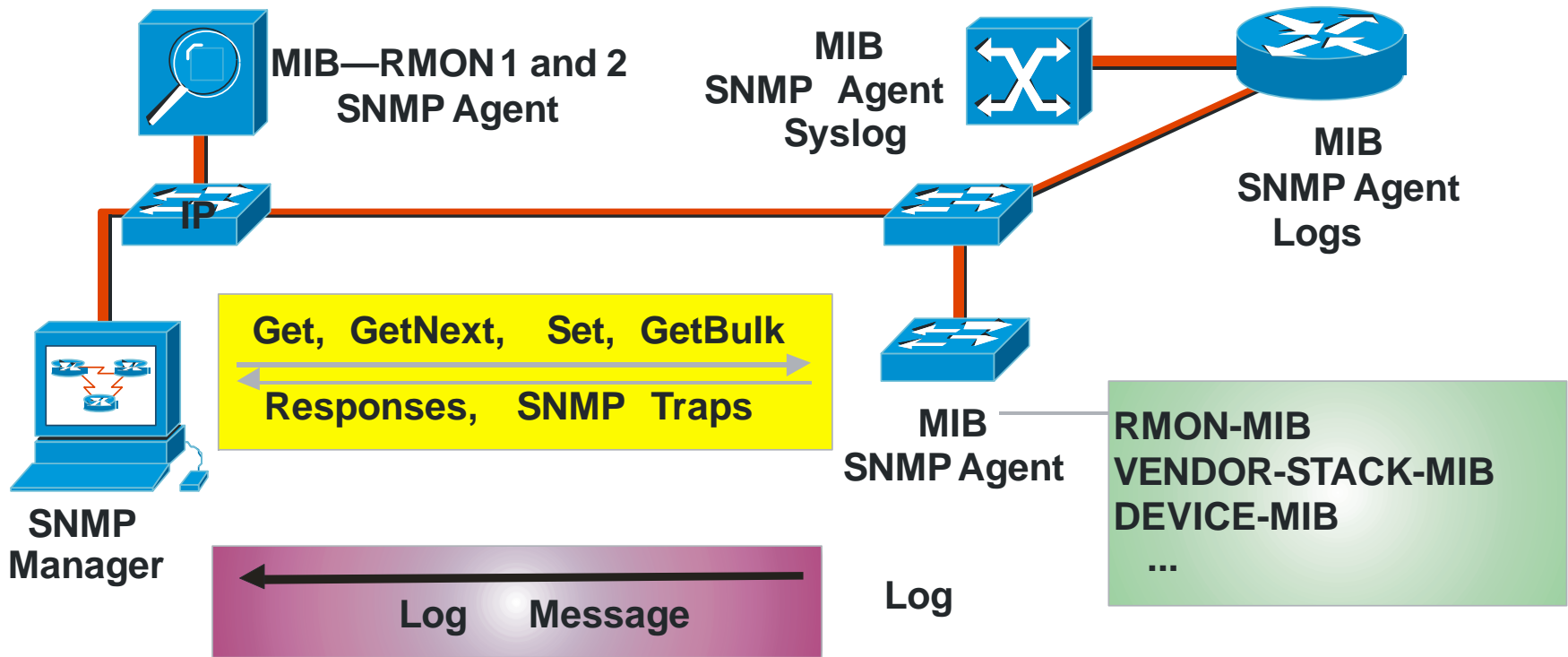
ICMP - Internet Control Message Protocol
 UDP - User Datagram Protocol
 Telnet Remote Access

- NFS Network File System
- RPC Remote Procedure Call
- SMTP Simple Mail Transfer Protocol

Manager/Agent Model

- Agent acts as "server"
- Manager acts as "client"
- Manager polls agents for information
- Agent keeps information and responds
- Agent may proactively send information as traps
- Opens UDP port 161, 162, 391, 1993

SNMP Flows



IP Connectivity

SNMP Traps/RMON

Log

Network Time Protocol

Vendor Specific

Management Information Base - MIB

How do the agents keep the information ?

Universe of network managed objects is called the Management Information Base (MIB).



Items within the network elements which are manageable are called managed objects

Objects within the MIB are organized into the following groups:

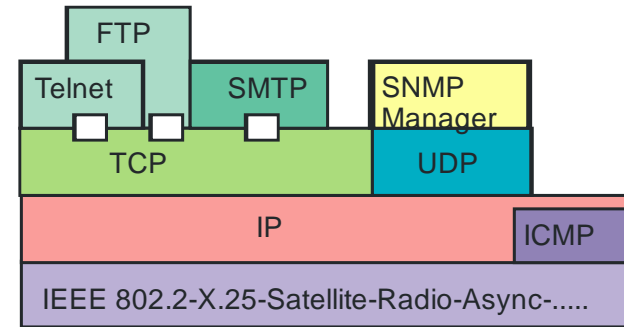
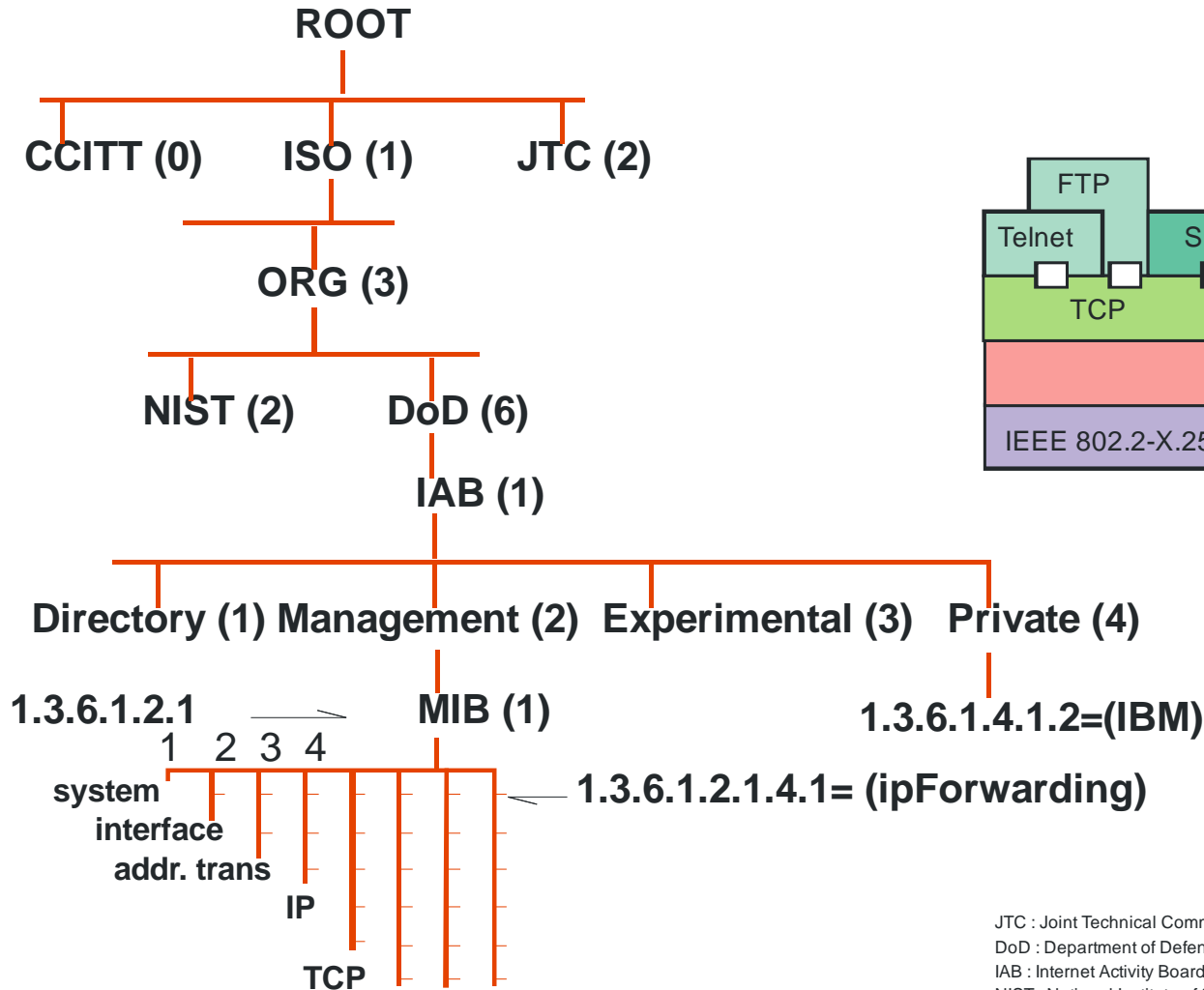
MIB(114)

- 1) System
- 2) Interface
- 3) Address Translation
- 4) IP
- 5) ICMP
- 6) TCP
- 7) UDP
- 8) EGP

MIB-2(171)

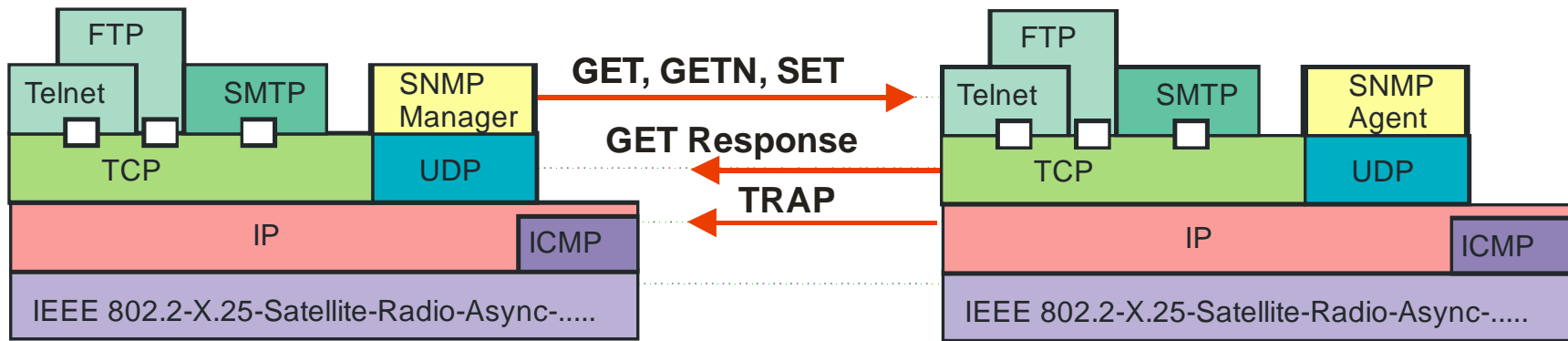
- 1) System
- 2) Interface
- 3) Address Translation
- 4) IP
- 5) ICMP
- 6) TCP
- 7) UDP
- 8) EGP
- 9) CMOT
- 10) Transmission
- 11) SNMP I

Object Registration Hierarchy



JTC : Joint Technical Committee
 DoD : Department of Defense (U.S.)
 IAB : Internet Activity Board
 NIST : National Institute of Standards and Technology (U.S.)

SNMP Components



SNMP Client - NMS

Executes management application that monitor/control agents

Issues SNMP commands (GET, GETN, SET)

Processes SNMP Msg (GET response, TRAPs)

SNMP Server - Agent

Allows access to management data (SNMP MIB)

Responds to SNMP commands via GET Response

Forwards unsolicited TRAPs to defined clients

Connectionless so no guarantees
Uses timeouts and retry counts

SNMP and RMON

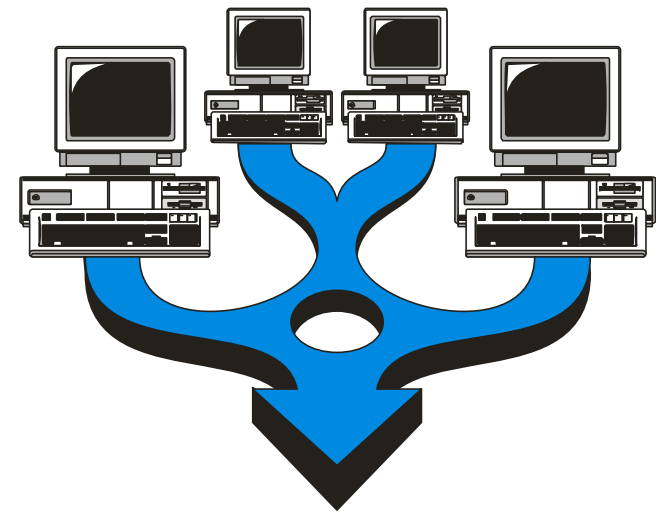
**RMON is a special MIB : RFC 1271/1757 :
Remote Network Monitoring MIB**

Uses standard SNMP transport

**RMON is not continuously on-line with
the SNMP manager**

RMON functions:

- **Collects and analyzes**
- **Configured to notify SNMP manager of events**
- **Diagnoses and logs events**
- **Detects, log, and reports errors**



RMON Groups

**Statistics
History
Host top "n"
Matrix
Alarm
Filter
Packet capture
Event
Token-ring**

SNMP : Review

Agents maintain management information in their MIB

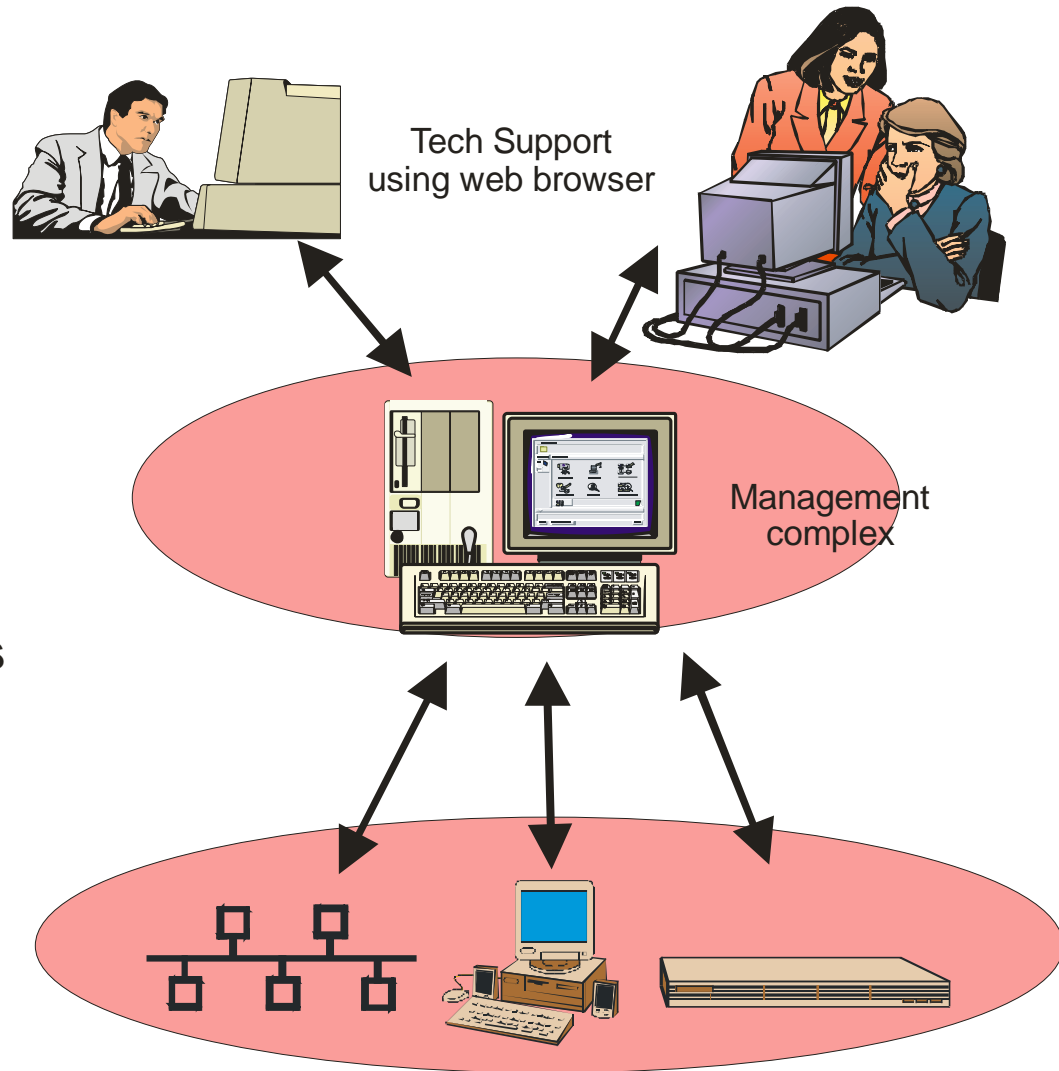
Management stations poll agents for MIB values

Multiple polls required to determine data

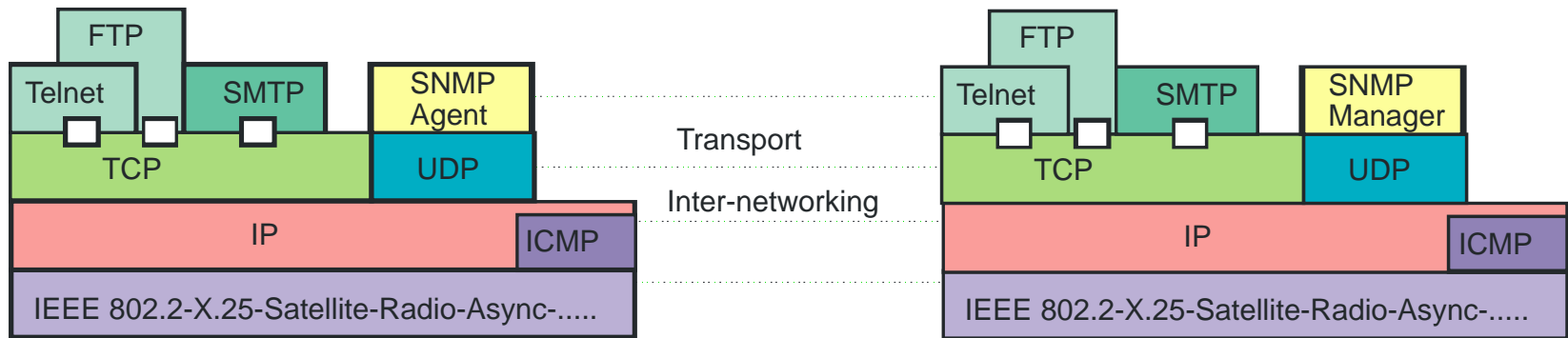
Agents may also send traps

Community names used for authentication

RMON allows distributed management functions



SNMP Deficiencies



SNMP version 3

SNMP version 1 and 2

- Version 1 showing age
- Large counters
- Limited security
- Poor WAN protocol
- No bulk data retrieval

- User Security Module (USM)**
- Authenticates users**
- Multiple administrative levels**
- Multiple user levels**
- Encrypts PDUs**
- Distributes management**
- Confirmed notifications**
- 64 bit counters**
- Bulk data retrieval**

SNMP: Difficulties in High Speed Networks



Counters could not handle gigabit traffic

Interface Speed

32-bit counter wraparound times

**10 Mbps
100 Mbps
155 Mbps
1 Gbps**

**57.26 minutes
5.73 minutes
3.69 minutes
0.57 minutes**

SNMPv3 New Terminology

SNMP Agents and Managers are now SNMP entities

Each SNMP entity contains one SNMP engine

All SNMP applications are within the SNMP entity

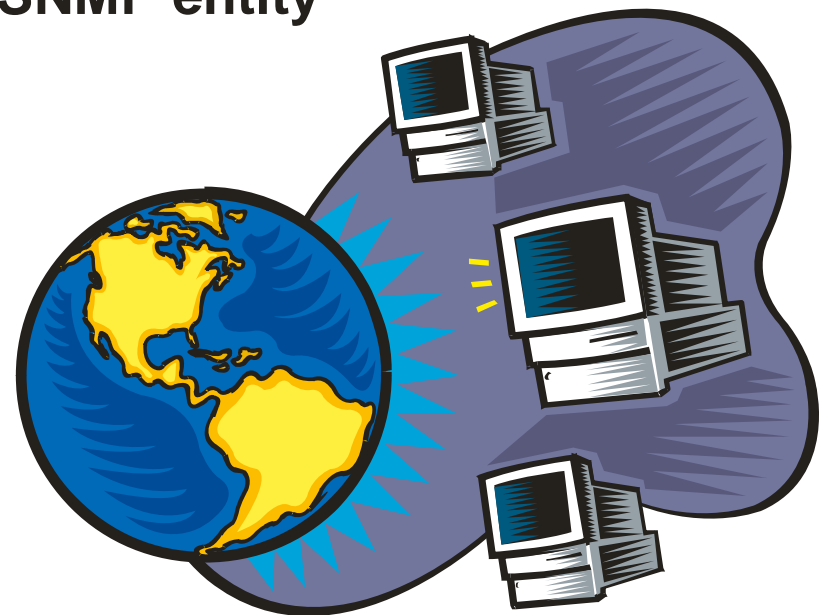
command generators

command responders

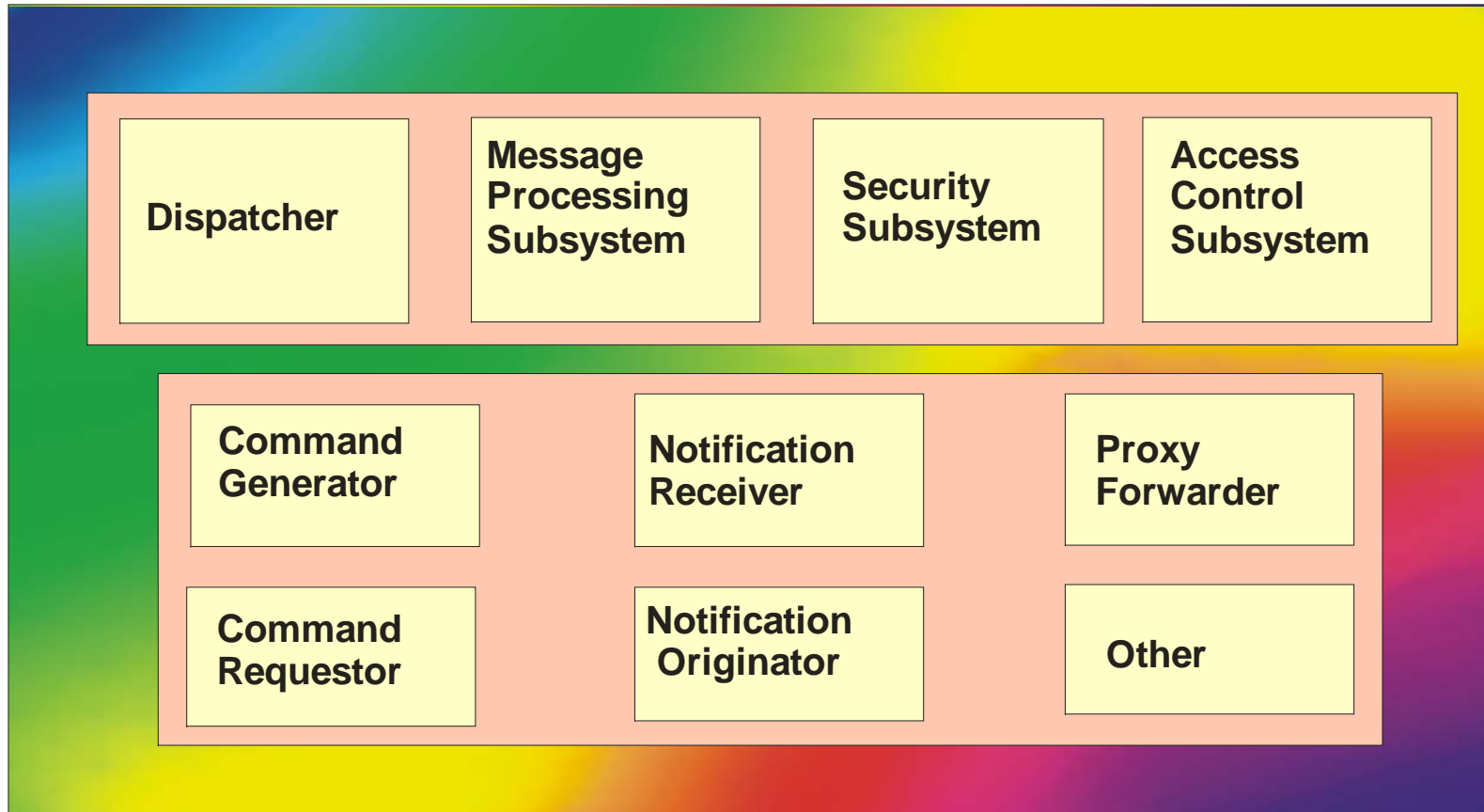
notification originators

notification receivers

proxy forwarders

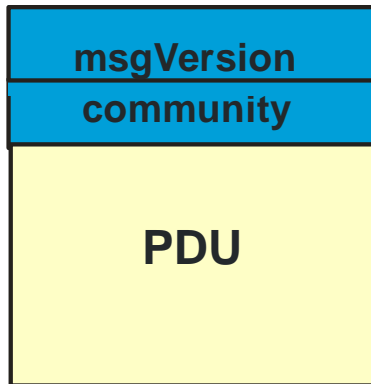


SNMPv3 New Framework

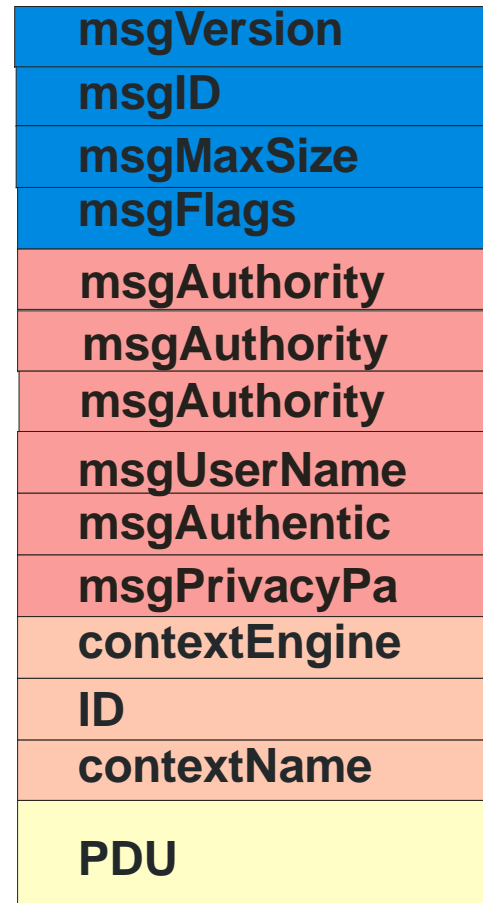


SNMPv3 New PDU

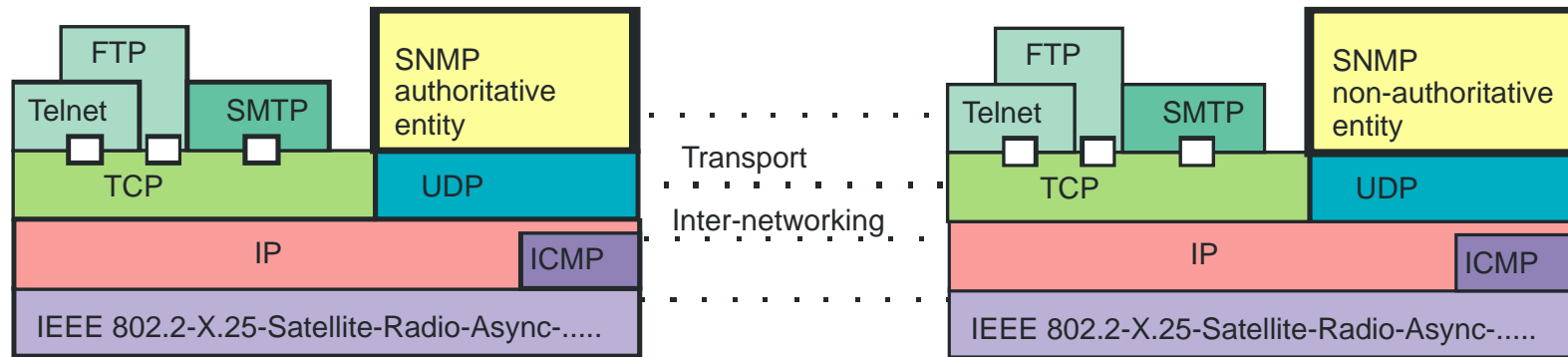
SNMPv1



SNMPv3



SNMPv3 : Authoritative



Authoritative entity
 receives requests
 responds to requests
 generates traps

Non-authoritative entity
 generates requests
 receives traps

Exception is for an 'Inform' message – the receiver is always authoritative

SNMPv3: Why Implement Security



Has the message been altered?

Is the message coming from a valid user?

Has the message been maliciously delayed?

Is the message being replayed?

Can sensitive information be protected against eavesdroppers?

Is the user allowed to access the MIB objects specified in the message?

Defenses against denial of service and traffic analysis are not covered in the security model used

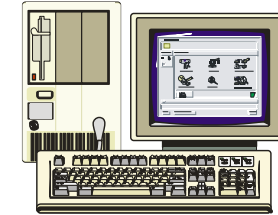
SNMPv3: Timeliness

Timeliness prevents
Intentional delay
Replay by a malicious party

Every message contains a timestamp which when examined upon receipt to determine the difference between the timestamp and the internal clock - if too old then it is rejected

**Uses a loosely synchronized clock
(Must be received within 150-second window)**

Authoritative entity maintains a clock
engine boots (number of times engine rebooted)
engine time (time since last reboot)
when engine time wraps - engine boots incremented



Non-authoritative Entity



Authoritative Entity

SNMPv3: Security

Three levels of security

Without authentication and privacy

With authentication but without privacy

With authentication and privacy

Authentication protocols

HMAC-MD5-96

HMAC-SHA-96

Framework allows for others

Encryption protocols

CBC-DES

Framework allows for others

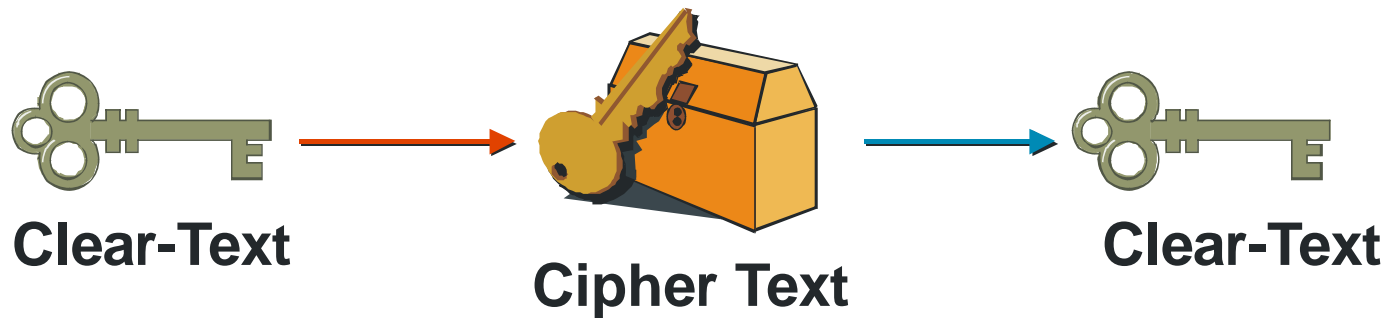
Can use PKI (public key infrastructure)

Especially to protect the secret key distribution

Receipt of messages in a timely manor



SNMPv3: Use of Public Key Infrastructure



Components

- Keys
- Mathematical algorithms
- Message digest

PKI
Public Key Infrastructure

Types

- Secret (symmetric)
- Public (asymmetric)

International politics
Used by SNMPv3



SNMPv3: PKI Review

Secret Key - Symmetric

Same key used by sender and receiver

Key used to encrypt and decrypt data

Rely on users to protect the key

Very fast

Used since the 1970's

Most popular
DES
(Data Encryption Standard)

Most widely used today

Public Key - Asymmetric

Two keys
public and private

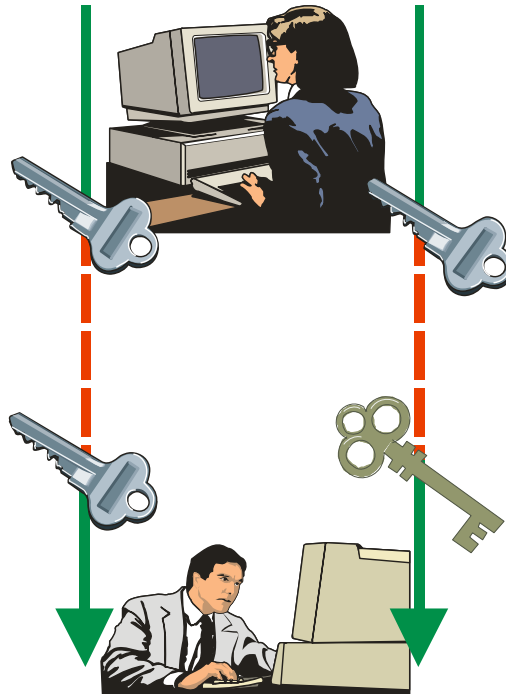
Public key known

Private key kept
confidential by owner

Slower than symmetric key

More complex
- key distribution

Most popular
RSA



SNMPv3: Key Derivation

A user/operator 'owns' the keys that he shares with the remote SNMP engines he manages

Key is derived from passwords entered by the user by using a very strong hash function concatenated many times

Two keys per user per engine: one for authentication and one for encryption

Authoritative entity needs secret keys

Changing keys

Generate a new password

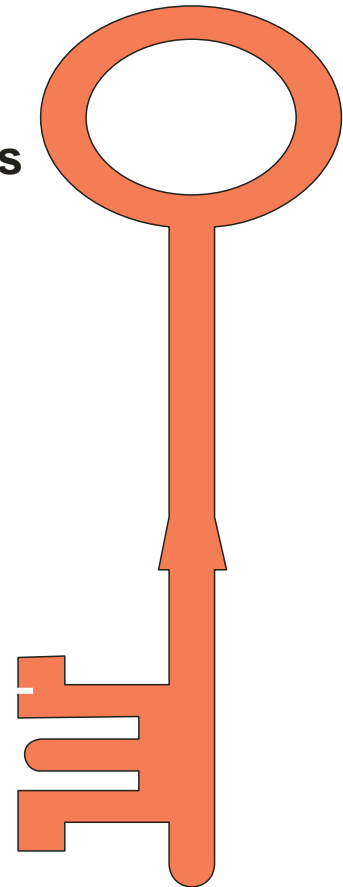
Get localized key

Generate a random value

Calculate a delta value

Concatenate random and delta values

Eavesdroppers cannot use delta value unless they have original key



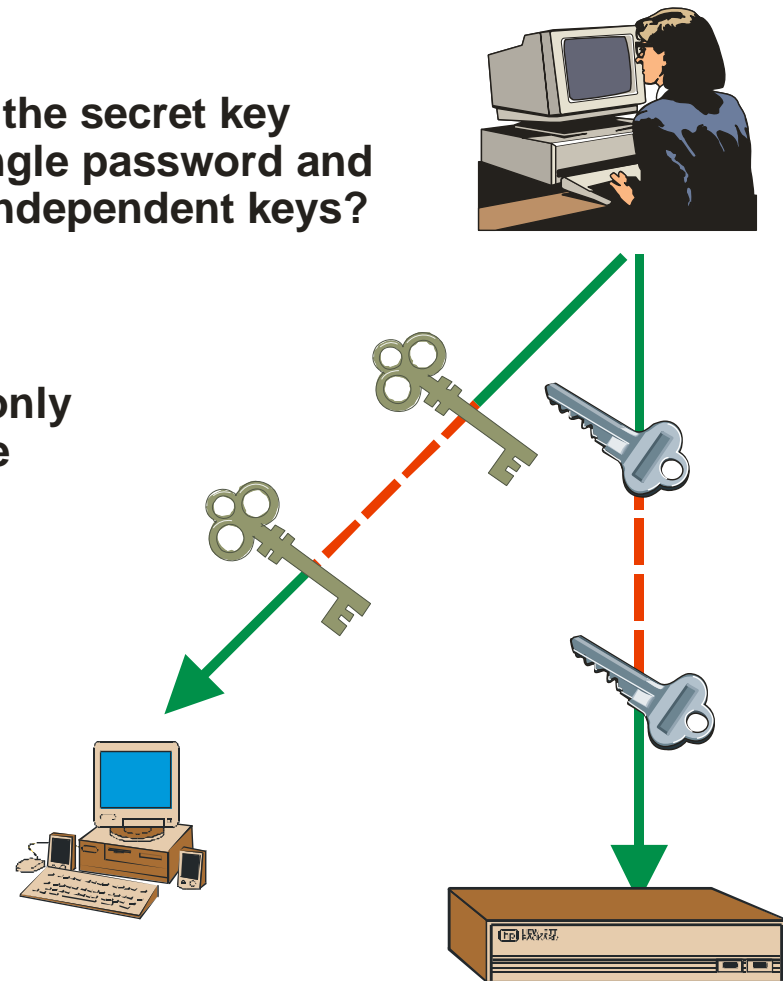
SNMPv3: Key Localization

If a user password is associated with the secret key how do you allow a user to have a single password and allow each managed engine to have independent keys?

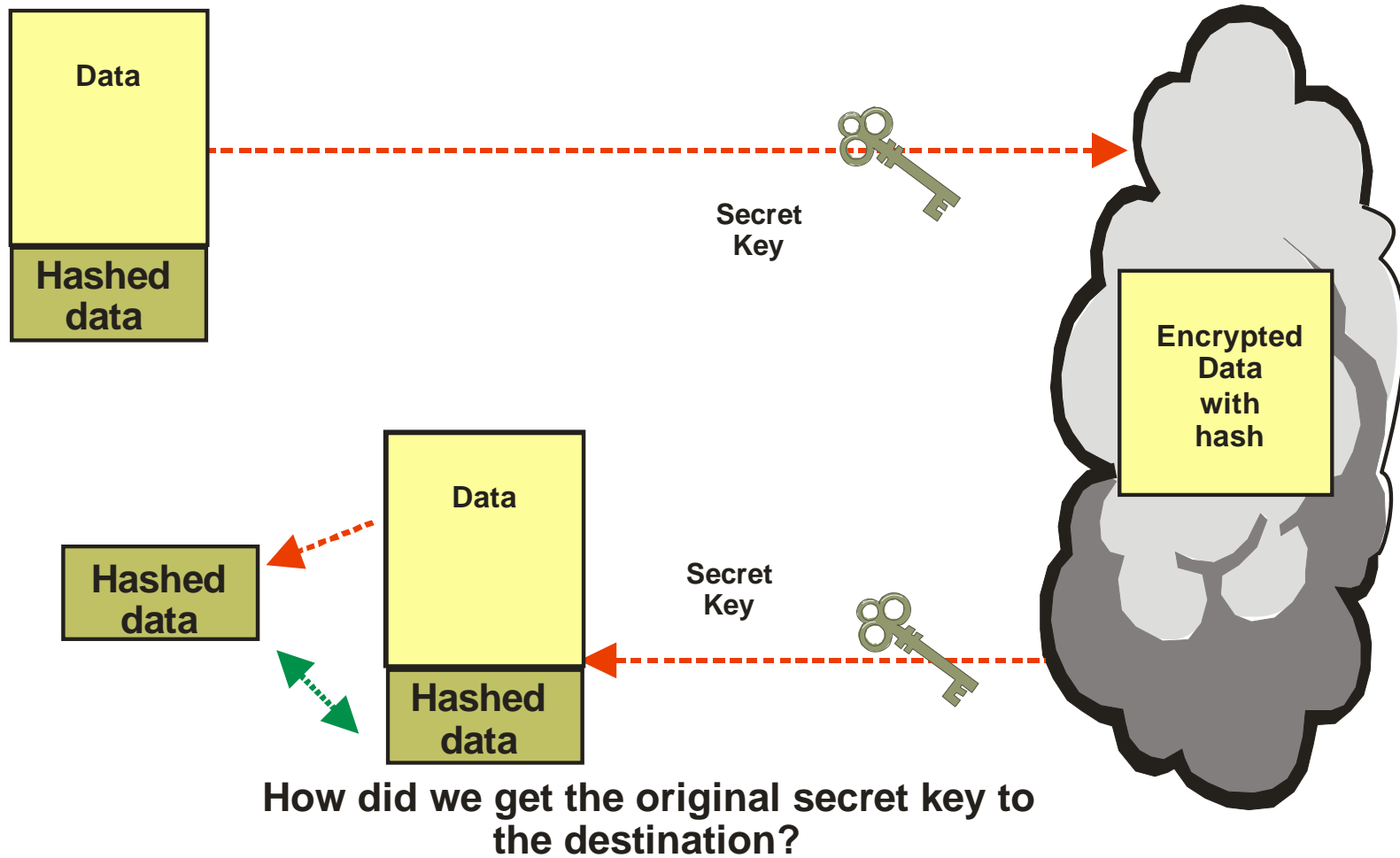
Use the concept of key localization

The generation of the secret key not only uses the user's password but also the managed engines publicly known identifier to produce the key

If an SNMP engine is compromised, then only the communications between the user and that single engine is compromised and not all communications from the user



SNMPv3: Authentication and Encryption

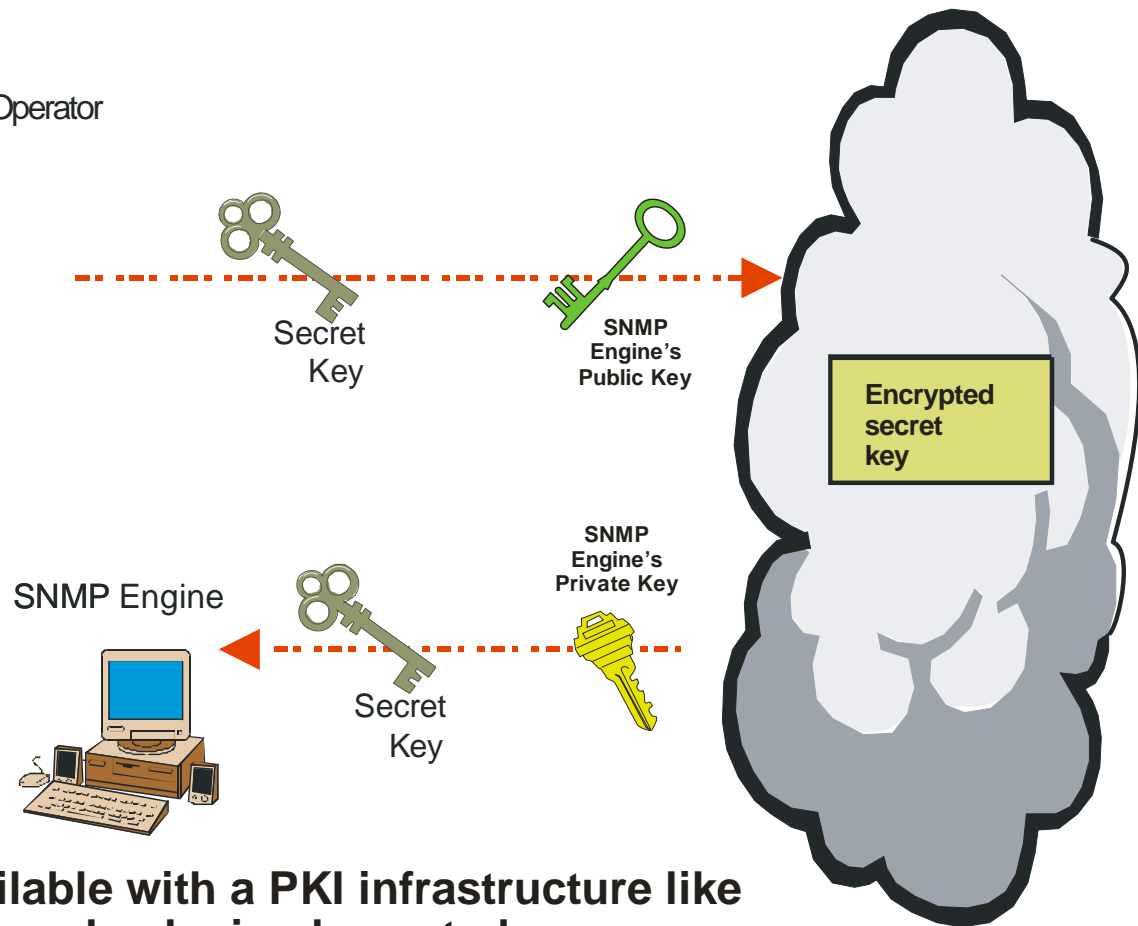


SNMPv3: Potential Use of PKI



User/Operator

We could also manually load the initial secret key in the remote SNMP engine (not very practical in a large enterprise network environment)



Other elements available with a PKI infrastructure like digital signatures can also be implemented

SNMPv3: Proxy Forwarding

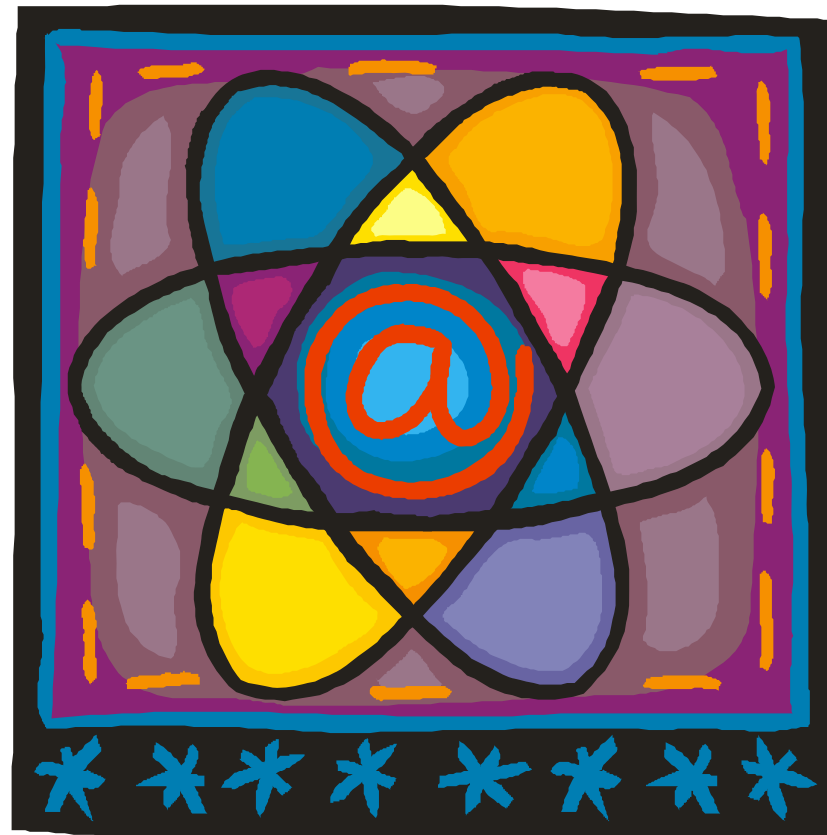
A proxy forwarder forwards and translates requests/responses and/or notifications to other SNMP entities

MIB tables will be used to define the message and target addresses

Entries can be added/removed

MIB tables

**Management Target
Notification
Proxy**



SNMPv3: Access Control

Maps requesting entity to a MIB view

MIBs now have ACL (access control lists)

Keep MIB views simple

- keeps management cost down
- easier to make changes
- reduces time trouble shooting
- maintenance is critical

Interaction between tables difficult
to trouble shoot

Determines what objects are accessed in the operation

What are the rights of the requestor with regard to the objects of the operation?



SNMPv3: Coexistence

Use proxies for SNMPv1 and SNMPv2

Translating notification messages

Handling Counter64 objects

Handling MIB views

Translating error status

Mapping SNMPv2 exceptions

Mapping community names
into new security



SNMPv3: RMON2

Protocol breakdown by segment

Protocol breakdown by network address

Protocol breakdown for traffic between network addresses

Protocol breakdown by application layer

Application traffic breakdown between network addresses



SNMP: Securing SNMPv1 and SNMPv2

Filter SNMP traffic for non authorized hosts

Change the default community string name

Disable stack execution

Segregate SNMP traffic on its own network

How do you identify who is running SNMP?

SNMPing - snmptool@sans.org

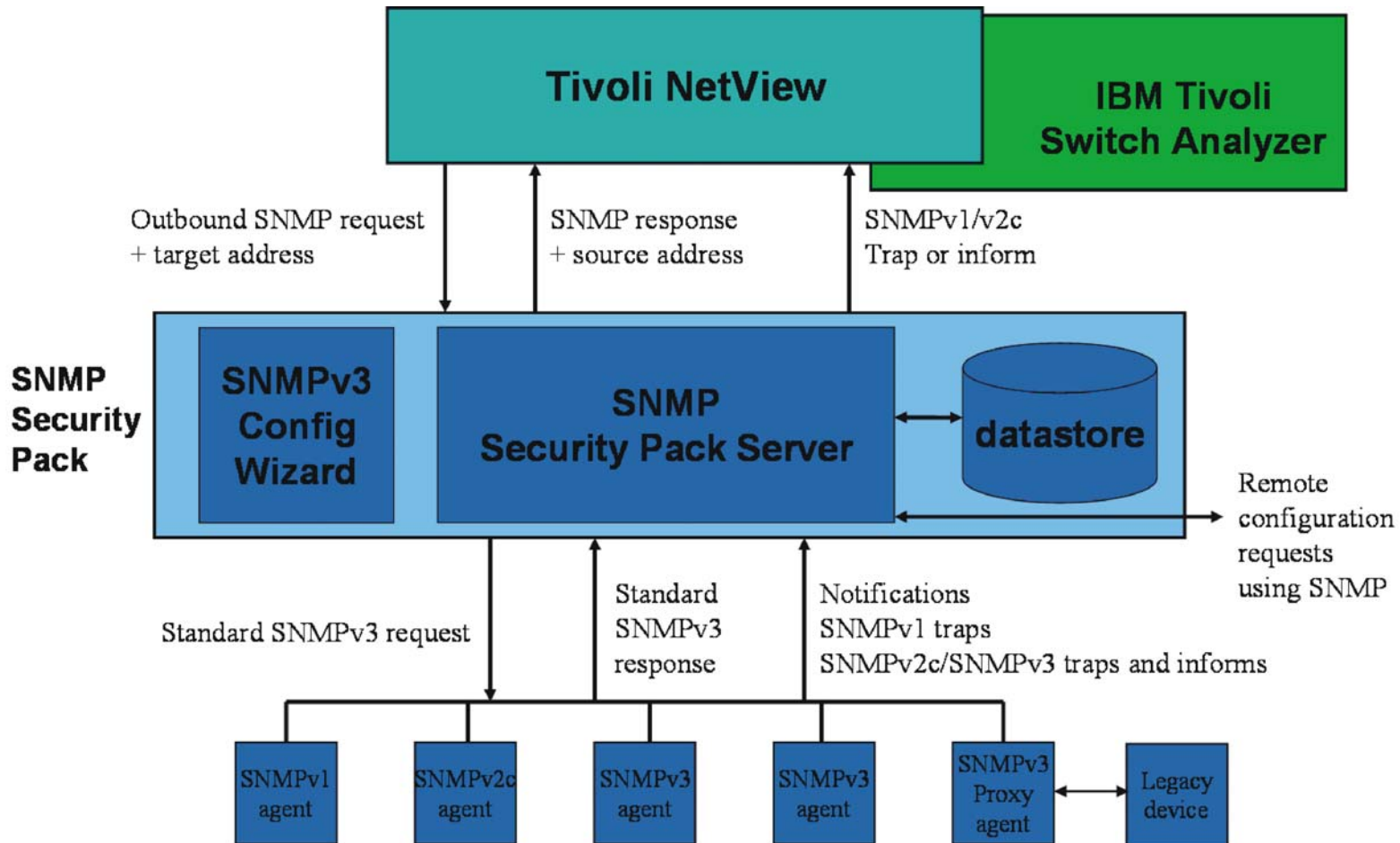
SNScan -

www.foundstone.com/knowledge/free_tools.html

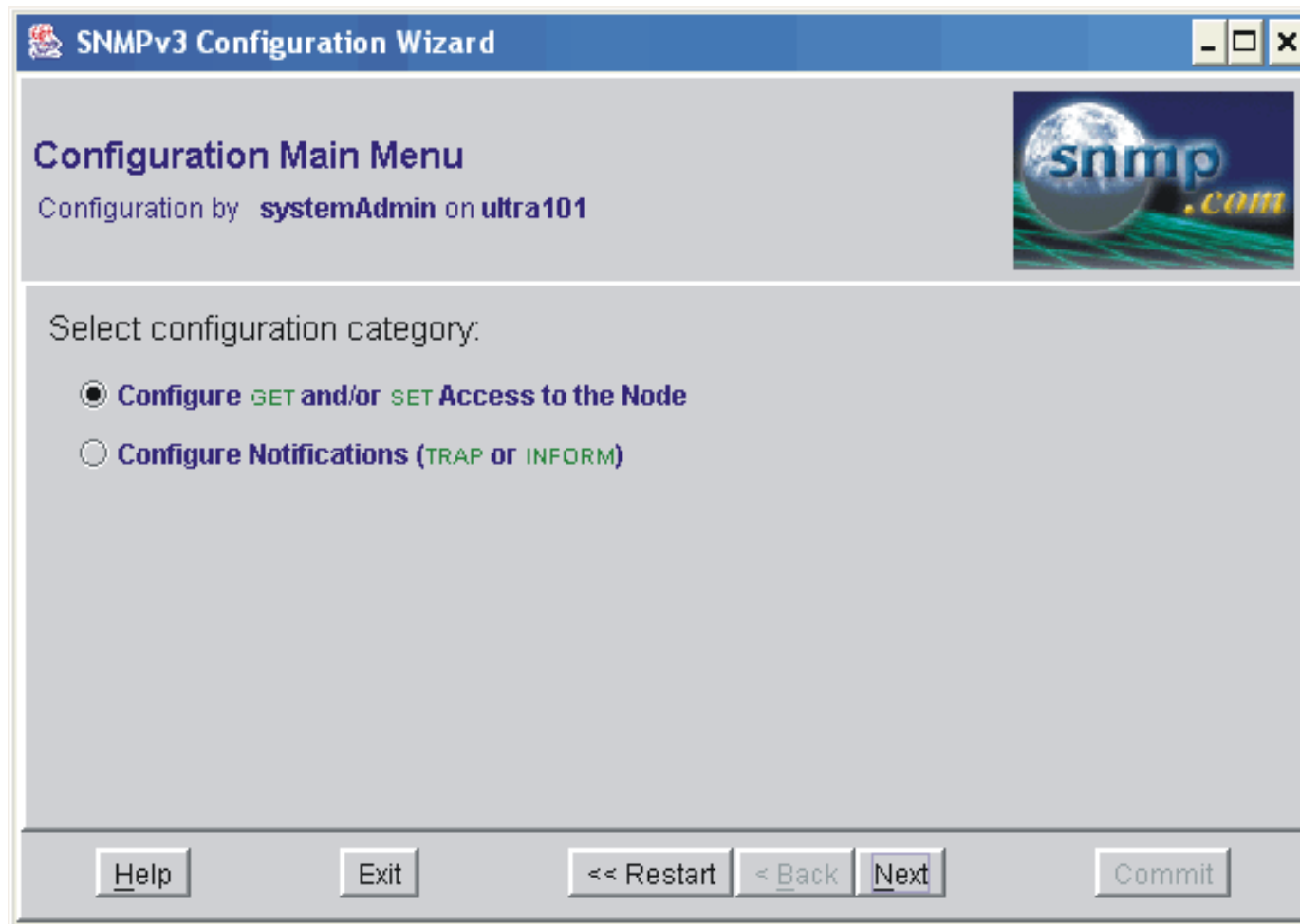
System audits



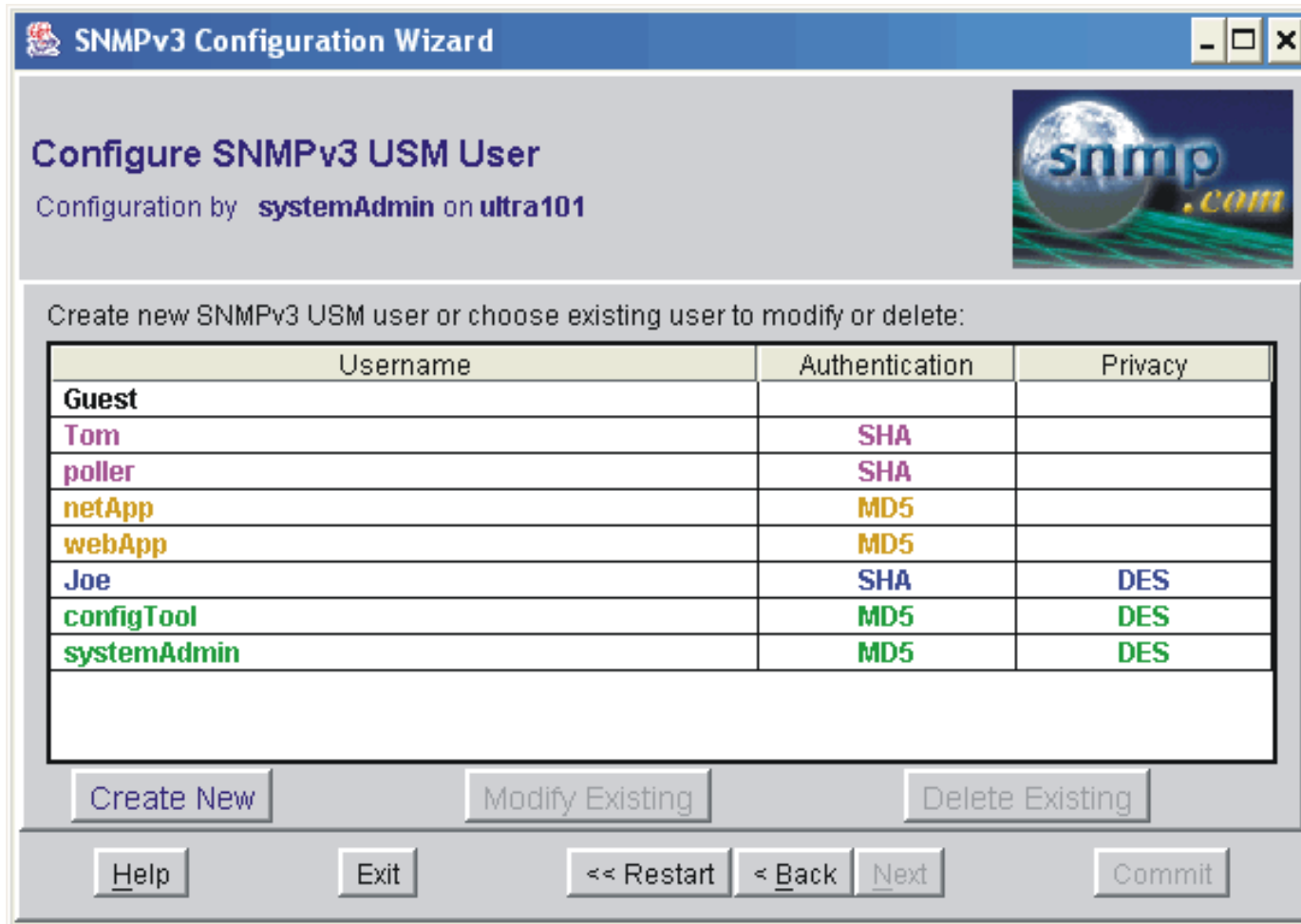
SNMPv3: IBM Support



SNMPv3: Configuration Wizard



SNMPv3: Add User Support



SNMPv3 Configuration Wizard

Configure SNMPv3 USM User
Configuration by **systemAdmin** on **ultra101**

Create new SNMPv3 USM user or choose existing user to modify or delete:

| Username | Authentication | Privacy |
|--------------------|----------------|------------|
| Guest | | |
| Tom | SHA | |
| poller | SHA | |
| netApp | MD5 | |
| webApp | MD5 | |
| Joe | SHA | DES |
| configTool | MD5 | DES |
| systemAdmin | MD5 | DES |

Buttons: Create New, Modify Existing, Delete Existing, Help, Exit, << Restart, < Back, Next, Commit

SNMPv3: Add Policies

The screenshot displays the Simple PolicyPro application window. The main menu includes File, Edit, Reset, Wizards, and Help. Below the menu are tabs for Build Policies, Distribute Policies, History Log, and Administration. The left sidebar contains a 'Policy Tips' section with five steps:

- Step 1. Define User**
Define SNMPv3 USM Users and/or SNMPv1 and SNMPv2c Communities to configure on managed devices.
- Step 2. Define Group**
Define security groups and the read/write access available to group members.
- Step 3. Assign User to Group**
Assign SNMPv3 Users and SNMPv1 and SNMPv2c Communities to a security group.
- Step 4. Define Notification Target**
Define destinations for agent traps and informs.
- Step 5. Define Policy**
Build a configuration policy by selecting one or more security groups and the members and notification targets associated with the security group(s).

The main content area is titled 'Configuration Policies' and contains the following text:

A configuration policy defines the management access available to agents configured with that policy.

Use the buttons below to define a new policy or modify or delete an existing policy.

Click the Distribute Policies tab above to select and distribute policies to agents.

Below this text is a section titled 'Existing Policies' containing a tree view of policies:

- Policy: NetworkApps
 - SNMPv3 User-based Access
 - SNMPv3 User: netStats
 - SNMPv3 User: poller
 - Community-based Access
 - Notification Configurations
- Policy: coreNetwork
- Policy: FileServers
- Policy: WebServers

At the bottom of the 'Existing Policies' section are three buttons: Define New Policy, Modify Policy, and Delete Policy.

SNMPv3 Distribute Policies

Simple PolicyPro

File Edit Reset Wizards Help

Build Policies **Distribute Policies** History Log Administration

Distribute Policies to Agents - Step 1

Step 1 - Select Agents

Select Agents for Management by hand selecting from the device list, selecting a predefined Agent List, or use the Selection Wizard for advanced selection criteria. You may choose a finer selection by toggling the Select box.

Load Device List **NT_Boxes**

| All Devices | | Agents To Be Configured | | |
|-------------------------------------|-----------------|-------------------------|--|--|
| Select | Address | Device Name | | |
| <input checked="" type="checkbox"/> | 192.147.142.14 | fileserver | | |
| <input checked="" type="checkbox"/> | 192.147.142.185 | shownt2 | | |
| <input checked="" type="checkbox"/> | 192.147.142.188 | freebsd | | |
| <input checked="" type="checkbox"/> | 192.147.142.193 | snowball | | |
| <input checked="" type="checkbox"/> | 192.147.142.199 | support2nt | | |
| <input checked="" type="checkbox"/> | 192.147.142.217 | nortelswitch | | |
| <input checked="" type="checkbox"/> | 192.147.142.218 | warthog | | |
| <input type="checkbox"/> | 192.147.142.224 | supportxp | | |
| <input type="checkbox"/> | 192.147.142.254 | trapsink | | |
| <input type="checkbox"/> | 192.147.142.250 | seymour250 | | |
| <input type="checkbox"/> | 192.147.142.255 | shownt3 | | |
| <input type="checkbox"/> | 192.147.142.264 | weasel | | |
| <input type="checkbox"/> | 192.147.142.267 | cisco2500 | | |
| <input type="checkbox"/> | 192.147.142.268 | bagel | | |

Buttons: Add >, Add All >>, Remove <, Remove All <<, Selection Wizard, Selection 1, Selection 2, Selection 3, Selection 4, Add New Device, Save Device List, Cancel, Back, Next

SNMPv3: Define MIB Views

The screenshot displays the Simple PolicyPro application window. The main menu includes File, Edit, Reset, Wizards, and Help. Below the menu are tabs for Build Policies, Distribute Policies, History Log, and Administration. A sub-menu is open, showing Define User, Define Group, Assign User to Group, Define Notification Target, and Define Policy. The Define Policy tab is active, displaying the Configuration Policies section. This section contains instructions on how to define a configuration policy and a list of existing policies. The existing policies are listed in a tree view under the 'Policy: NetworkApps' folder, including SNMPv3 User-based Access (with sub-items for netStats and poller), Community-based Access, and Notification Configurations. Other policies listed are coreNetwork, FileServers, and WebServers. At the bottom of the window are buttons for Define New Policy, Modify Policy, and Delete Policy.

Simple PolicyPro

File Edit Reset Wizards Help

Build Policies Distribute Policies History Log Administration

Policy Tips

Build Configuration Policy to distribute to agents:

Step 1. Define User
Define SNMPv3 USM Users and/or SNMPv1 and SNMPv2c Communities to configure on managed devices.

Step 2. Define Group
Define security groups and the read/write access available to group members.

Step 3. Assign User to Group
Assign SNMPv3 Users and SNMPv1 and SNMPv2c Communities to a security group.

Step 4. Define Notification Target
Define destinations for agent traps and informs.

Step 5. Define Policy
Build a configuration policy by selecting one or more security groups and the members and notification targets associated with the security group(s).

Configuration Policies

A configuration policy defines the management access available to agents configured with that policy.

Use the buttons below to define a new policy or modify or delete an existing policy.
Click the Distribute Policies tab above to select and distribute policies to agents.

Existing Policies

- Policy: NetworkApps
 - SNMPv3 User-based Access
 - SNMPv3 User: netStats
 - SNMPv3 User: poller
 - Community-based Access
 - Notification Configurations
- Policy: coreNetwork
- Policy: FileServers
- Policy: WebServers

Define New Policy Modify Policy Delete Policy

SNMPv3: Summary

SNMP3 has significant enhancements

Security necessary as network boundaries fade

Additional control and direction of critical information

Coexistence assured using proxy services

Complexity may impede rollout

Failed security audits are driving corporate rollout



SNMPv3: References

Blumenthal, U., Hiem, N., Wignen, B., Key Derivation for Network Management Applications, IEEE Network Magazine 11(3) May/June 1997

www.simple-times.org Information on SNMPv3
eee.nwc.com Technical articles on SNMPv3
www.ietf.org RFC's and working groups
www.snmp.cs.utwente.nl University tracking of SNMPv3 work
www.snmp.com General information on SNMP

W. Stallings: SNMP, SNMPv2, SNMPv3 and RMON1 and 2, Addison-Wesley, 1999 (ISBN 0-201-48534-6)

M.T. Rose: The Simple Book, Prentice Hall, 1994

J. Case: Management with SNMP and SNMPv3: A Survival Guide, John Wiley & Sons, Inc

D. Zeltsserman: A Practical Guide to SNMPv3 and Network Management Prentice Hall Professional Technical Reference

SNMPv3: References

- RFC 2570 Introduction to Version 3**
- RFC 2571 SNMPv3 Architecture**
- RFC 2572 Message Processing and
Dispatching for SNMPv3**
- RFC 2573 SNMP Applications**
- RFC 2574 User-based Security
Module for SNMPv3**
- RFC 2575 View-based Access Control
Model for SNMPv3**
- RFC 2676 Coexistence between
Version 1, Version 2 and Version 3**
- RFC 2742 Definitions of Managed
Objects for Extensible SNMP Agents**
- RFC 2962 An SNMP Application Level
Gateway for Payload Address Translation**



धन्यवाद

Hind Hindi

多謝

Traditional Chinese

ขอบคุณ

Thai

Спасибо

Russian

Gracias

Spanish

Thank You

English

شكراً

Arabic

Obrigado

Brazilian Portuguese

Grazie

Italian

多谢

Simplified Chinese

Danke

German

Merci

French

நன்றி

Tami Tamil

ありがとうございました

Japanese

감사합니다

Korean