
Secure Standards-Based Internetwork Management via SNMPv3

***Presented to the East Tennessee Chapter of
InfraGard on December 9, 2004***

Jeff Case

SNMP Research, Inc

+1 865 573 1434

case@snmp.com

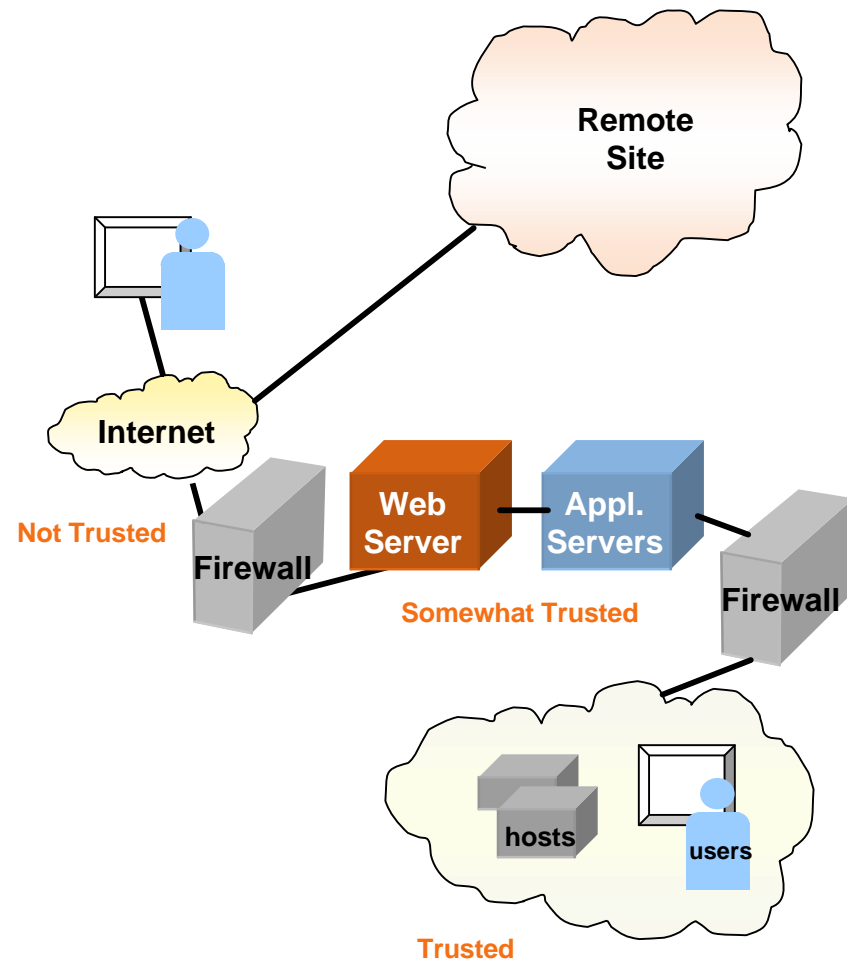
Topics

- ◆ Enterprise security landscape
- ◆ Introduction to secure SNMPv3
- ◆ Elements of a complete solution
- ◆ Future Directions
- ◆ Summary

Enterprise Security Landscape

Multiple Management Zones

- ◆ Good perimeter security reduces risk within the Enterprise
- ◆ Need to manage elements outside the trusted zone
- ◆ Need to manage across “less trusted” zones
- ◆ DMZ’s represent systems and network components that are both high risk and high value



Critical Resources at Risk: Firewalls are good, but not enough

- ◆ Managing using SNMPv1 / SNMPv2c outside firewalls is not usually recommended
 - ◆ Need secure configuration changes (SNMP sets)
 - ◆ Secure SNMPv3 is the standards-based solution
 - ◆ Systems inside “trusted” perimeter still vulnerable to
 - Internal threats
 - “Backdoor” access (e.g., dial-up modem, handheld devices) bypasses firewall-based security
 - ◆ Moving security enforcement as close as possible to individual systems helps address these issues
-

Internet Management and SNMPv3

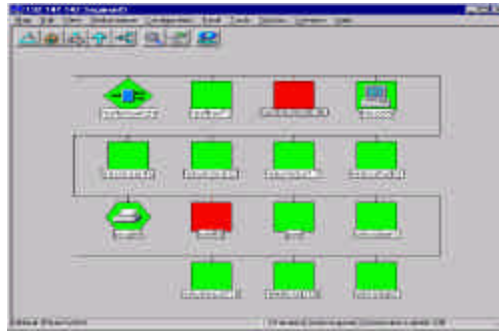
◆ Desired Solution

- Manage using familiar tools and procedures
 - Manage using existing complementary applications
 - Manage using appropriate SNMP level
 - SNMPv1 and SNMPv2c for monitoring older devices in trusted environments
 - SNMPv3 for managing critical systems in less trusted regions
 - SNMPv3 for managing remote sites through less trusted regions
 - SNMPv3 for all configuration operations
 - Common repository for security configuration data
-

Secure SNMPv3

SNMP in One Slide

Manager



- ✓ Common organization structure for management information (SMI)
- ✓ One naming space for all management "objects" (MIB)
- ✓ Communications Protocol (SNMP)

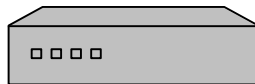
Requests

Get
Set

Responses

Notifications

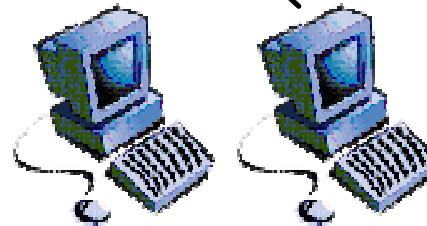
Agents



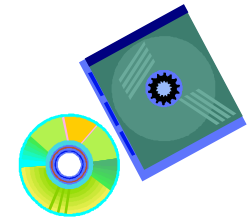
**Networking
Equipment**



Servers



PCs



**Software
Applications**

Standards-based Manager-to-Agent Security

- ◆ The overall goal is to harden today's management systems by incorporating protection mechanisms that match the potential level of threat with multiple levels of rings of protection/trust
- ◆ Today's heightened threat level requires heightened protection mechanisms

Standards-based Manager-to-Agent Security

- ◆ **SNMPv1:** **1988 – present**
 - Plaintext community string, e.g., “public”
 - no Authentication / no Privacy

 - ◆ **SNMPv2c:** **1995 – present**
 - Plaintext community string, e.g., “public”
 - no Authentication / no Privacy

 - ◆ **SNMPv3:** **1998 – present**
 - Strong Authentication, Weak Privacy

 - ◆ **SNMPv3 ESO:** **2003 – present**
(Extended Security Options)
 - Strong Authentication, Strong Privacy
-

Standards-based Manager-to-Agent Security

◆ SNMPv3

- Since 1998
- Promoted to IETF Full Standard in 2002
- Authentication:
 - None
 - Strong (HMAC-MD5-96)
 - Stronger (HMAC-SHA-96)
- Privacy
 - None
 - Weak (Single DES 56 bit)

New Features of SNMPv3

- ◆ **New features inherited from SNMPv2, plus**
 - **Security**
 - **Administration**

Features of SNMPv3:

Security and Administration

◆ Authentication

- User-based strong authentication of messages
- MD5 or SHA in private key model with localized keys
- More than good enough for virtually all applications today

◆ Privacy

- Protect management and configuration data from unauthorized disclosure
 - Encrypt SNMP payload for confidentiality
 - Private key model with localized keys
 - Standard specifies DES (56-bit) but is extensible for stronger cryptography
 - Standard is extensible for stronger cryptography
-

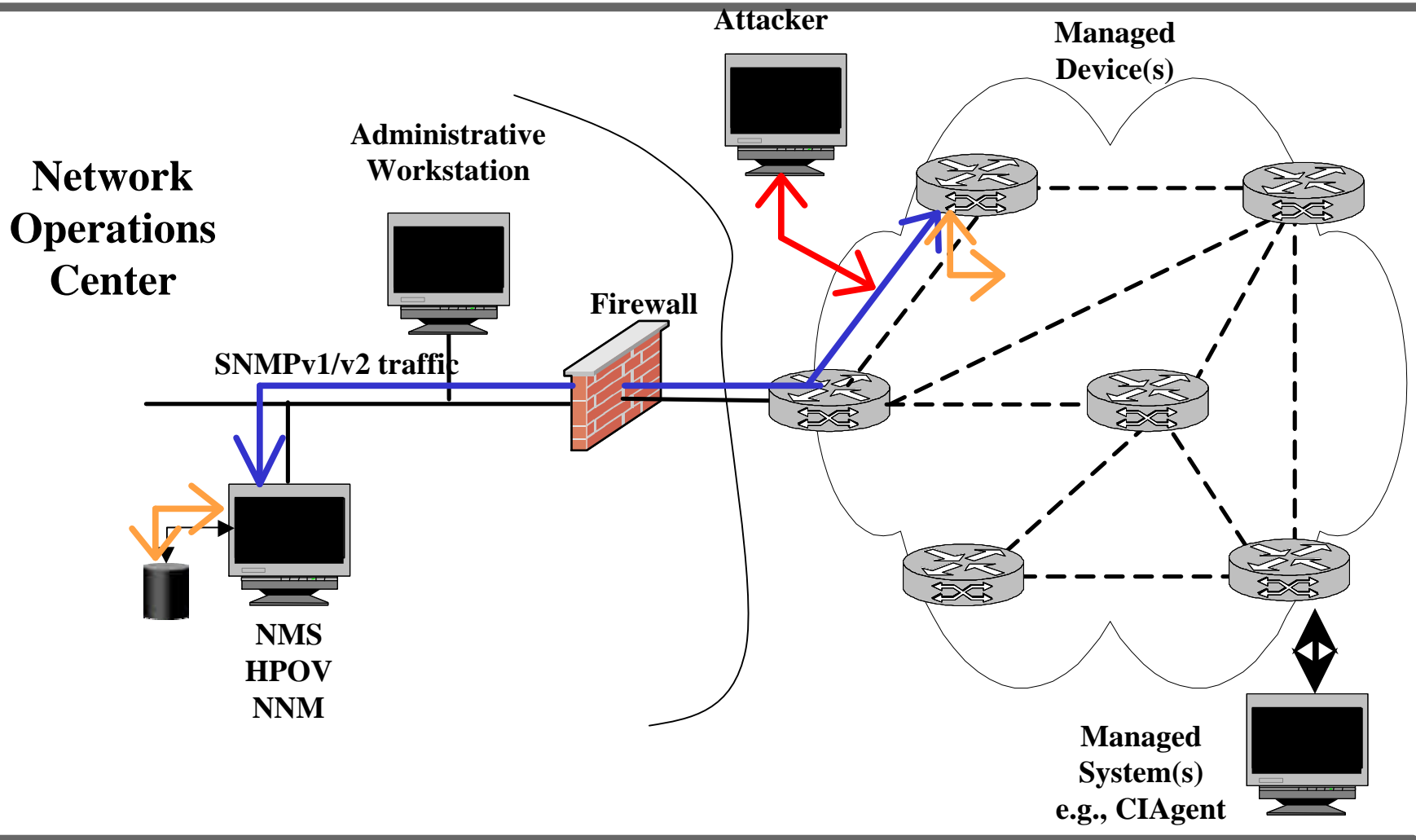
Features of SNMPv3: Security and Administration (Continued)

- ◆ **Authorization and View-Based Access Control**
 - **Authorization:** What functions permitted (read, write, notify)
 - **Access Control:** Restrictions on what data may be read / written, potentially very finely grained
 - **Based on groups of SNMPv3 “users”**
 - An SNMPv3 user might be a system, person, or role
 - Separation of people and policies
 - The management application determines how its “users” (operators) map to SNMPv3 “users”
 - ◆ **Administrative framework to support the above**
-

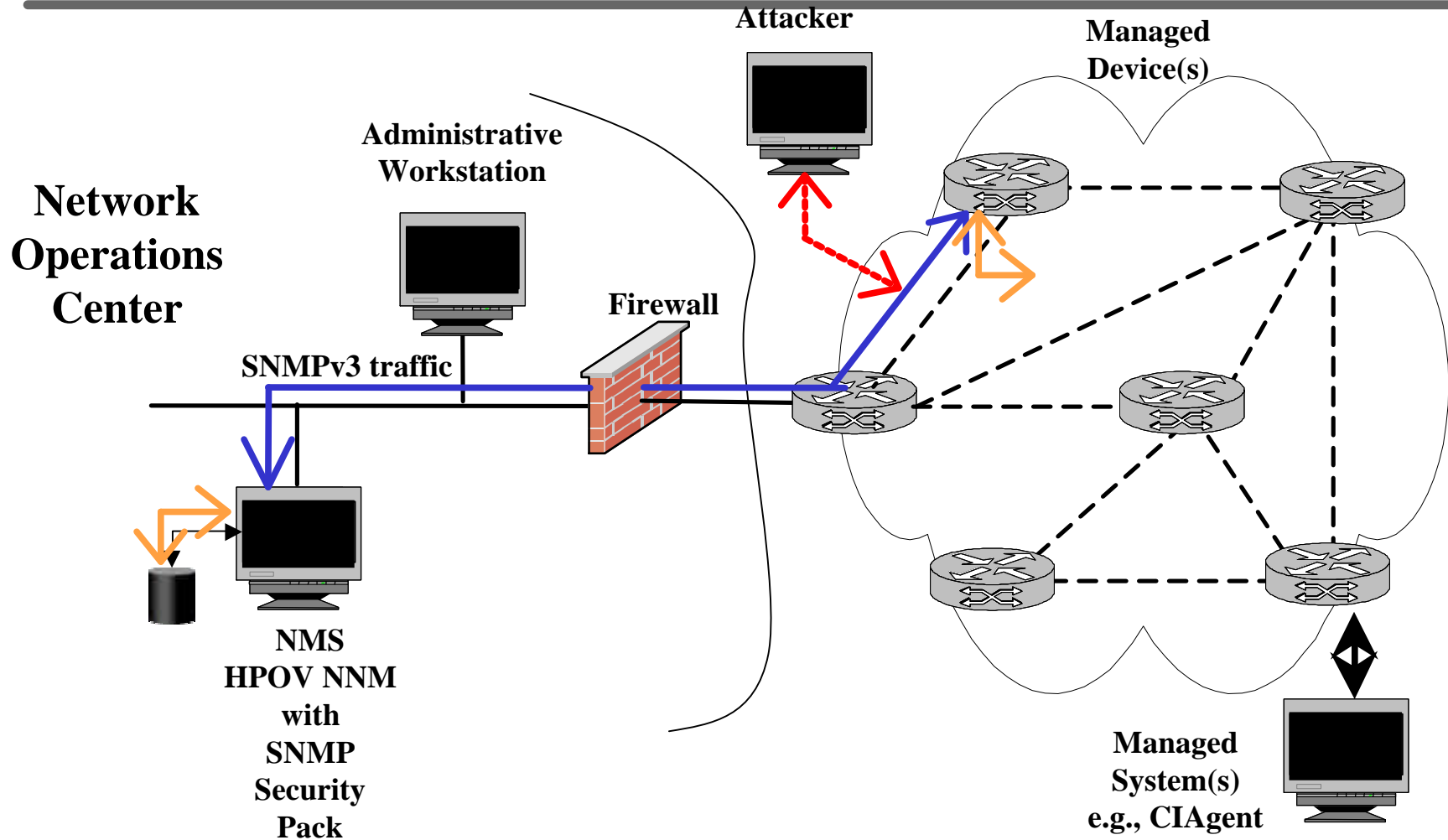
SNMPv3 Administrative Framework

- ◆ All of this configuration information is stored in Management Information Base (MIB) tables
 - ◆ Remotely configurable via SNMP operations
 - ◆ Standard supports remote configuration of:
 - Users including key management
 - Groups
 - Views
 - Community strings for SNMPv1 & SNMPv2c, if any
 - Notification destinations
 - Source-side notification filtering
-

SNMPv1/SNMPv2c Not Secure



Secure SNMPv3



Elements of a Complete Solution

Elements of a Complete Solution

- ◆ **Secure agents**
- ◆ **Secure management applications**
- ◆ **Administrative policies**
- ◆ **Configuration management of users, keys, etc**
- ◆ **Coexist with legacy systems**

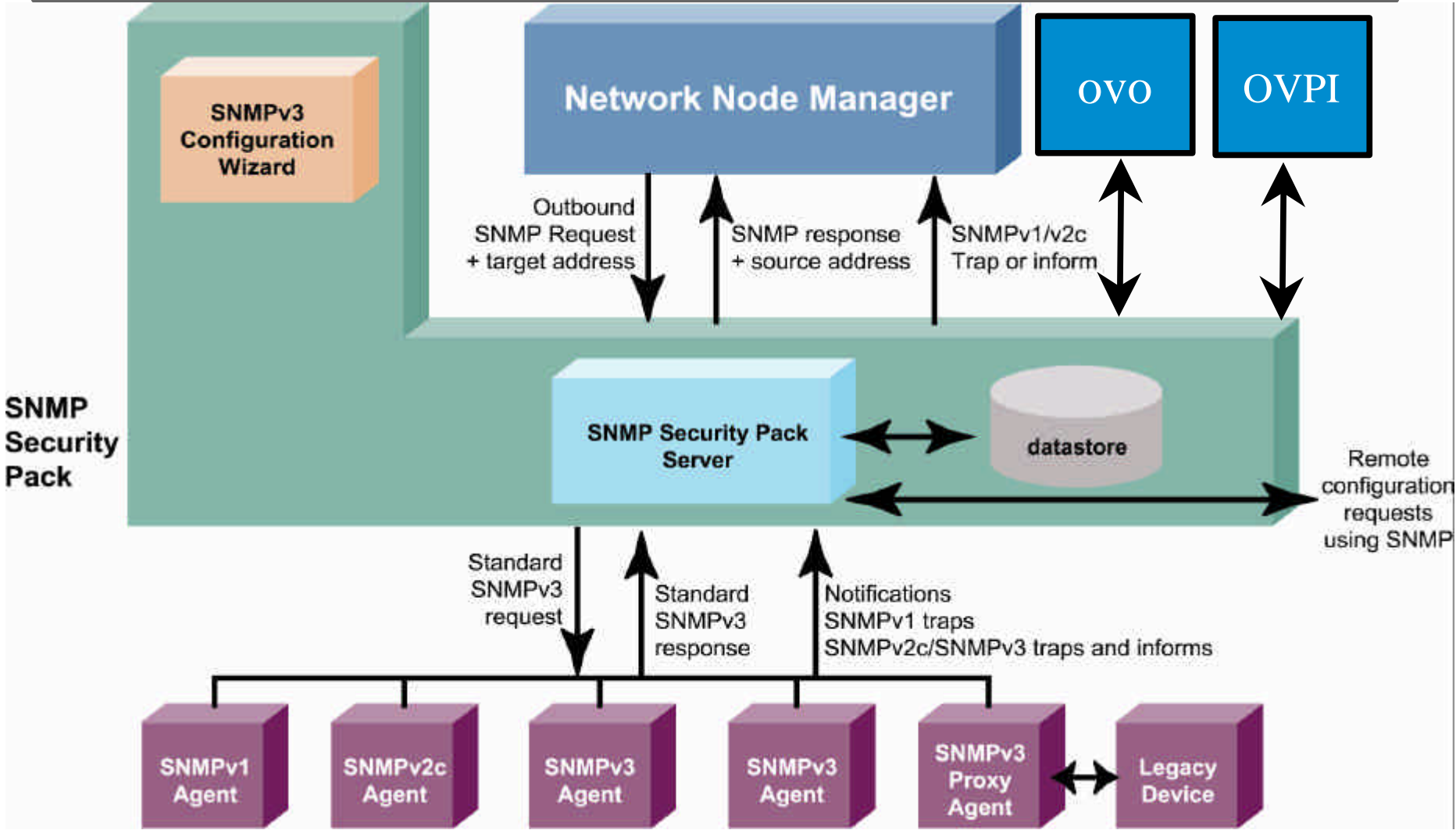
Secure Agents

- ◆ **SNMPv3 agents available on most**
 - Networking devices
 - Open operating systems
 - Real-time operating systems
- ◆ **For integrated network and system management, smart agents based on SNMPv3 are available**
 - Support common SNMPV3 administrative framework
 - Network monitoring
 - Host resource monitoring
 - File system monitoring
 - Critical application monitoring
 - Log file monitoring
 - Service monitoring

Secure Management Applications

- ◆ Management platforms and applications that communicate securely with agents via SNMPv3, e.g., HP OpenView Network Node Manager (NNM) with SNMP Security Pack
 - ◆ After initial configuration, NNM functions work transparently
 - ◆ Partner applications which use NNM SNMP stack will also work transparently
 - ◆ Partner applications which use their own SNMP stack may also route SNMP communications through SNMP Security Pack
-

NNM with



Administrative Policies

- ◆ **Parts of an enterprise security policy include:**
 - Who can see what?
 - Who can change what?
 - How are “users” defined?
 - What level of authentication?
 - What level of encryption?
 - How often are keys changed?
 - Who can change security configurations?
 - How are configurations changed/audited?

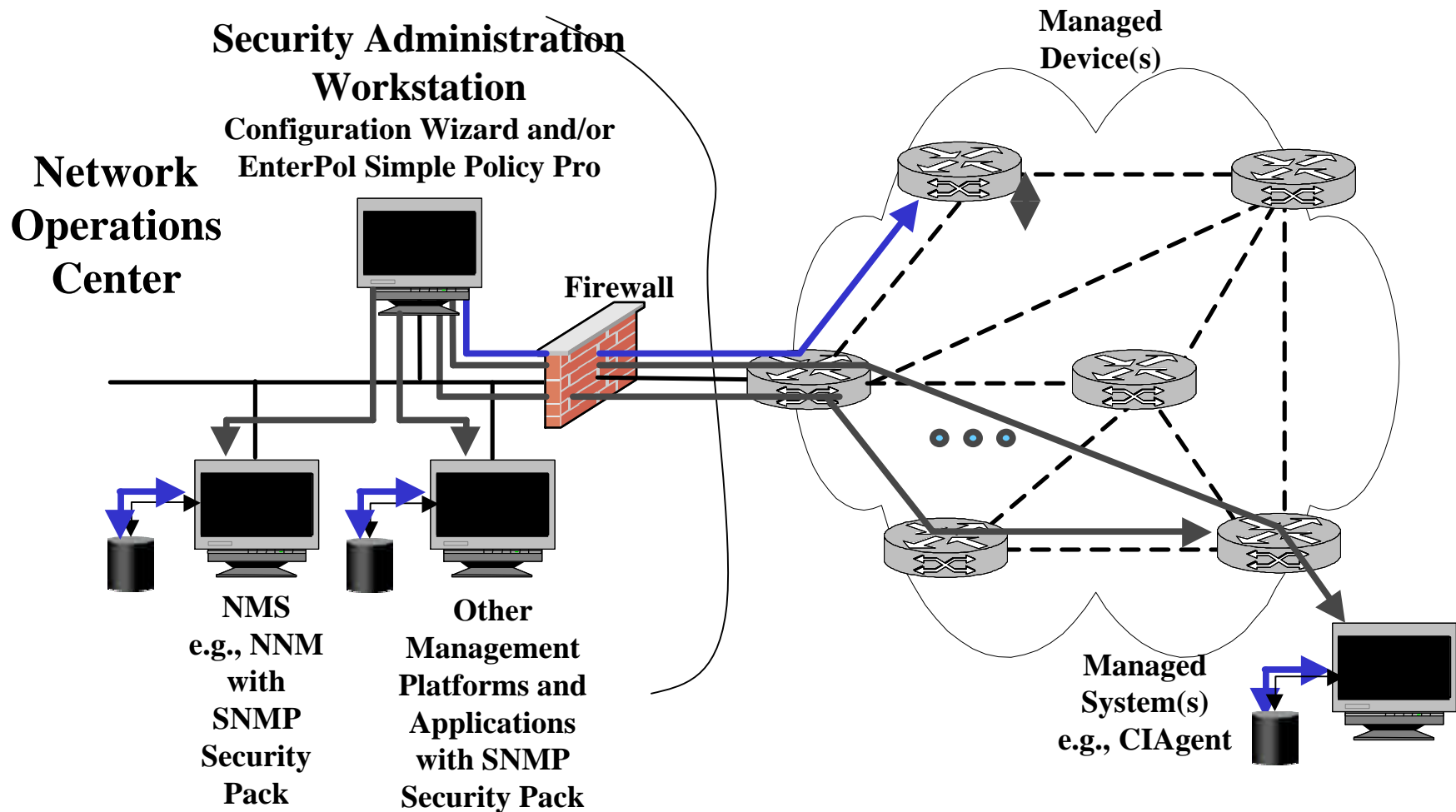
Configuration Management Issues

- ◆ **Users, keys, notifications, etc. must be configured on both managers and agents**
- ◆ **Keys are generated from pass-phrases and localized, pass-phrases not stored on managed devices**
- ◆ **Keys need to be changed periodically**
- ◆ **Configuration must be updated in a timely manner (e.g., deny rights to a terminated employee)**
- ◆ **Configuration needs to be done remotely from a security management station, using a secure and private method**

SNMPv3 Remote Administration

- ◆ Need to configure manager platforms and agents in accordance with enterprise policies
- ◆ Can do it with “vi” or “edit” but really need something more friendly and powerful
- ◆ Security dependent on correct configurations
- ◆ Wizard and/or policy-based tools
- ◆ Configurable agents
- ◆ Configurable managers

SNMPv3 Remote Administration



Configuration Management Applications

- ◆ **Configuration Management applications are very helpful to reduce complexity and human error**
 - **One agent at a time “wizard” application**
 - **Included with the standards-based security solution for NNM, i.e., the SNMP Security Pack for HP OpenView NNM**
 - **Policy-based, multiple-target distribution application**
 - **Available separately**

SNMPv3 Configuration Wizard



The image shows a screenshot of a Windows-style window titled "SNMPv3 Configuration Wizard". The window has a blue title bar with standard minimize, maximize, and close buttons. The main content area is titled "Security Configurations" and contains the following text: "Configuration by systemAdmin on ultra101" and "SNMPv3 USM User to Create netReporter". To the right of this text is a logo for "snmp.com" featuring a globe. Below this, the instruction "Select the maximum security level for this SNMPv3 USM user:" is followed by three radio button options: "No Authentication or Privacy (noAuthNoPriv)", "Authentication without Privacy (authNoPriv)", and "Authentication with Privacy (authPriv) (recommended)". The "recommended" option is selected. At the bottom of the window, there is a row of buttons: "Help", "Exit", "<< Restart", "< Back", "Next", and "Commit".

SNMPv3 Configuration Wizard

Security Configurations

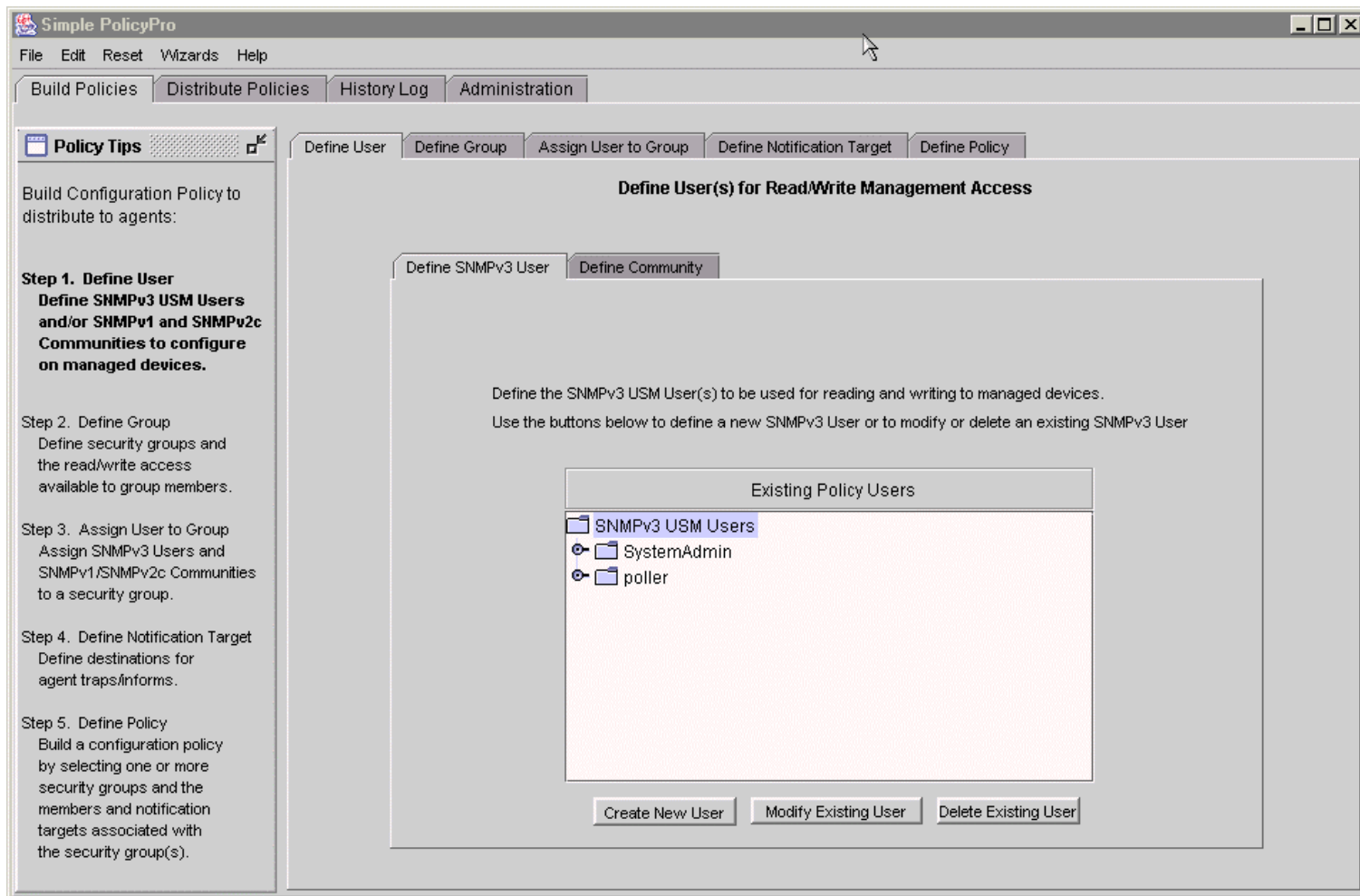
Configuration by **systemAdmin** on **ultra101**
SNMPv3 USM User to Create **netReporter**

Select the maximum security level for this SNMPv3 USM user:

- No Authentication or Privacy (**noAuthNoPriv**)
- Authentication without Privacy (**authNoPriv**)
- Authentication with Privacy (authPriv) (recommended)**

Help Exit << Restart < Back Next Commit

Policy-based SNMP Configuration Management



Coexist with Legacy Systems

- ◆ **Multilingual environments:**
 - Some management agents will not support SNMPv3
 - Most agents that support SNMPv3 also support SNMPv1 & SNMPv2c
 - Cannot upgrade all agents at once
 - ◆ **SNMP Security Pack is multi-lingual, so fully supports a heterogeneous SNMPv1 / SNMPv2c / SNMPv3 agent environment**
 - Old agent, old packet, old rules, old response
 - New agent, new packet, new rules, new response
 - ◆ **Properly handle SNMPv1 traps**
 - ◆ **Properly handle SNMPv2c traps and informs**
-

Product and Technology Initiatives

Where are we?

- ◆ **Now that SNMPv3 is at Full Standard, are we done yet?**
 - Not yet
 - More to be done
- ◆ **There are still unmet needs in the area of standards-based Internet management**

It is still too hard to do right

The Problem

- ◆ It continues to be unnecessarily expensive to develop, deploy, use, and support secure heterogeneous multi-vendor internets consisting of networked devices, systems, applications, and services.

In The Beginning ...

- ◆ **15 years ago, we had**
 - **Monitoring via proprietary CLI “show” commands**
 - **Configuration and control via proprietary CLI commands**
 - **No programmatic interface, difficult to write scripts, no “expect”**
 - **The definition, implementation, and deployment of the SNMP-based Internet Standard Management Framework made an order-of-magnitude advancement in the state-of-the-art for Internet monitoring**

... and Today

- ◆ **Standards-based monitoring is now a solved problem for the most part -- now in pervasive and continuous use**
 - ◆ **The Internet Standard Management Framework based on SNMPv1 was an instant success that continued to grow**
 - ◆ **SNMPv2 was a disaster**
 - ◆ **SNMPv3 caught on slowly but is now in demand**
 - **The need for security**
 - **September 11, 2001 but not limited to USA**
 - **Unrelated CERT advisory on SNMPv1 in February 2002**
 - **Government Sector: Strong acceptance growth**
 - **Private Sector: Public company audits/scrutiny/regulatory environment**
-

... and Today

- ◆ For a variety of good reasons and poor excuses the frameworks have not been as widely exploited for configuration and control operations as they have been for monitoring operations
 - ◆ For the configuration and control of many products, we are still stuck where we were 10 to 15 years ago:
 - Proprietary CLI
 - No programmatic interface → difficult-to-write scripts
 - Little change control rigor
 - Poor interoperability within a vendor, none between
-

The Goal

- ◆ We need to make order-of-magnitude advances in the state-of-the-art for configuration and control operations similar to those made for monitoring over the past 15 years ...
- ◆ ... with an increased level of seamlessness between monitoring and configuration / control

The Approach

- ◆ **Execution:** Implement and deploy the technology standards we have today
- ◆ **Extension:** Evolve and improve the technology

Product Initiatives

- ◆ **We are always working on new product initiatives**
 - **Ease-of-Use Initiatives:**
 - MIBGuide
 - Configuration aids
 - Etc
 - **DSSP: Distributed SNMP Security Pack for management through firewalls**
 - ◆ **We continue to work on improving our existing products**
-

Technology Initiatives

- ◆ **We continue to work on extending the specifications for management**
 - **Extended Security Options (ESO Initiative)**
 - **Advanced Protocol Operations (APO Initiative)**
 - **XML-Based Internet Management (XML SNMP Initiative)**
 - **SMI enhancements (SMI-DS2 Initiative)**

The Internet Standard Management Frameworks

Generation	SMI	Protocol Operations	Security	Instrumentation
SNMPv1	SMIv1	SNMPv1	Little/None	The MIB
SNMPv2	SMIv2	SNMPv2	Disaster → Little/None	The MIB
SNMPv3	SMIv2	SNMPv2	User-based Security Model (USM) and View-based Access Control Model (VACM)	The MIB
SNMPv3 extensions	SMI-DS2	APO Initiative	ESO Initiative	The MIB

Extended Security Options: ESO Technology Initiative

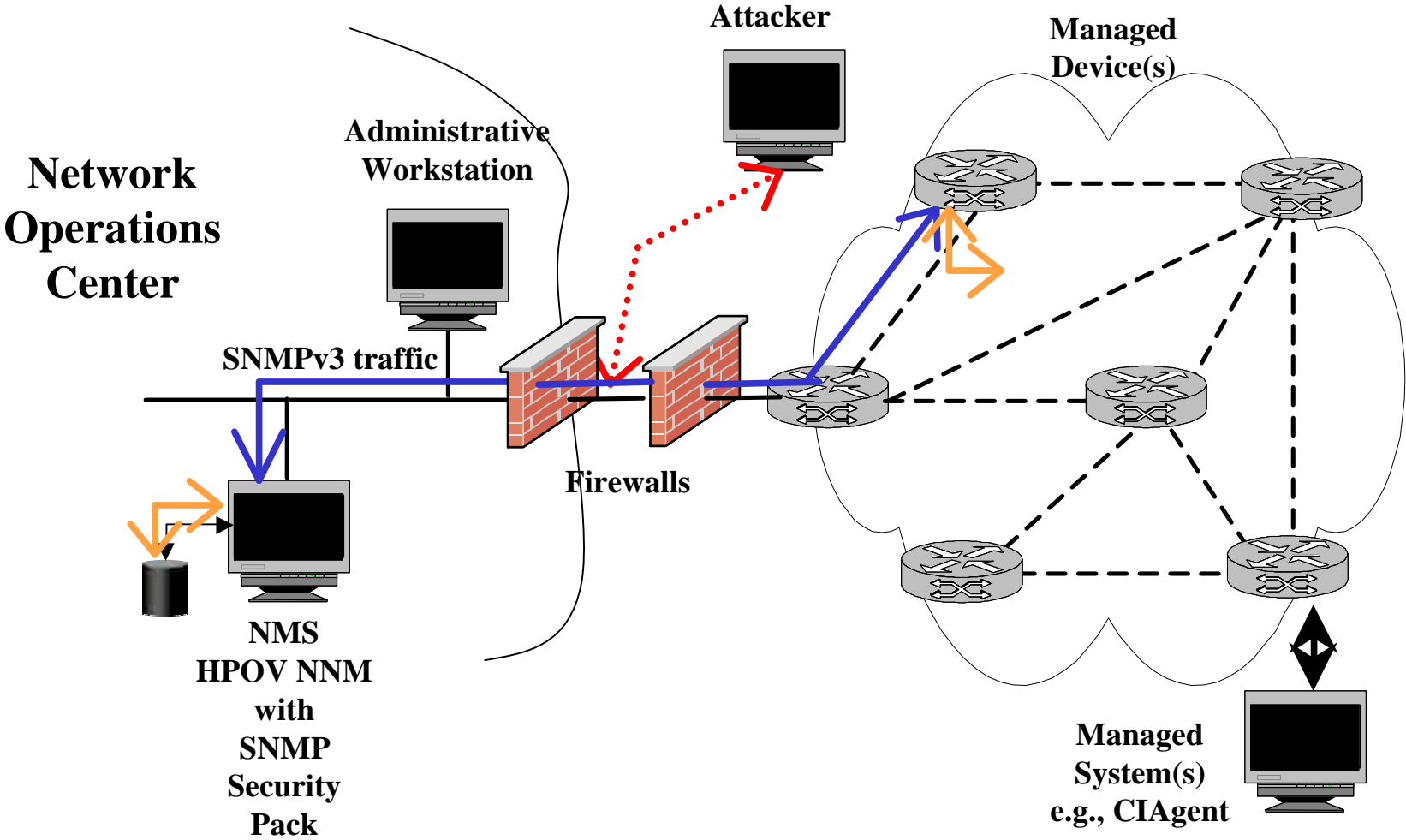
SNMPv3 ESO: Extended Security Options

- ◆ **SNMPv3 framework designed to be extensible and allow additional security models including new**
 - Authentication algorithms and mechanisms
 - Privacy algorithms and mechanisms
- ◆ **ESO uses this to add two new strong privacy algorithms**
 - Advanced Encryption Standard (AES) in 128 bit CFB mode
 - Triple DES (3DES) in 168 bit EDE CBC mode

SNMPv3 with ESO Yields

- ◆ **Multiple authentication options: (Same as before)**
 - None, Strong, Stronger
- ◆ **Multiple privacy options: (Two new ones)**
 - None, Weak, **Strong, Stronger**
- ◆ **Multiple strong authentication algorithms and multiple strong privacy algorithms provide hot standby replacements if one is believed to be compromised**
- ◆ **Reconfigure rather than redeploy**
- ◆ **Available today in some countries**
- ◆ **Additional other future work, e.g., articulation with other systems including Session-based Security Model**

SNMPv3 with ESO: Potentially more Secure



Advanced Protocol Operations: APO Technology Initiative

Advanced Protocol Operations (APO) Initiative

- ◆ 3rd Generation Protocol Operations
 - APO Level 1: Compatible with SMIV2 MIB documents
 - Operations on aggregate objects: Rows and Tables
 - OID Suppression
 - Improved read and write operations
 - APO Level 2: A superset – requires enhancements to MIB grammar such as the SMI-DS initiative
 - All of APO Level 1, plus ... Union, Struct, Array
 - Nesting, e.g., something like this within a table

```
IPAddress struct {
    AddressType  INTEGER,
    AddressValue union {
        IPv4Address  OCTET STRING (SIZE(4)),
        IPv6Address  OCTET STRING (SIZE(16))
    }
}
```

APO Benefits

- ◆ **Suppression of redundant information yields network and processing efficiencies – 2x to 10x not unusual**
 - ◆ **Think in the abstraction that is most natural**
 - **A row is a row, a table is a table**
 - ◆ **Operations on meta-objects easier for some people to understand and code correctly**
 - **Somewhat easier on read operations**
 - **A lot easier on thorny configuration operations**
 - ◆ **XML initiative builds on APO initiatives**
-

XML-Based Internet Management: XML Transport Mapping Technology Initiative)

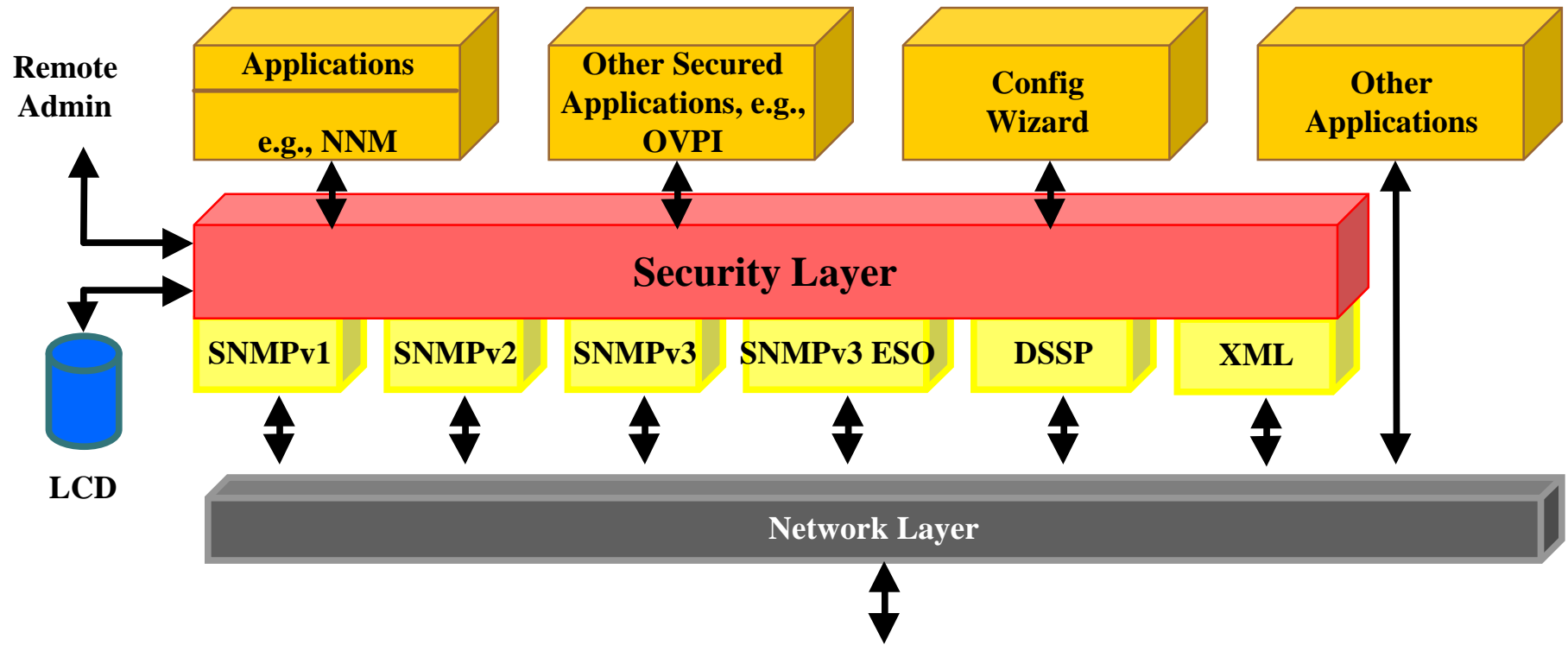
XML Transport Mapping Initiative

- ◆ **XML-Based Internet Management means different things to different people**
 - XML-ification of proprietary CLI: a factor of 2 incremental improvement
 - XML-ification of standards-based management data: an order-of-magnitude advancement
 - XML transport of entirely new and different data model(s): an order of magnitude backwards
 - ... many more ...
- ◆ **These are not mutually exclusive and can coexist**

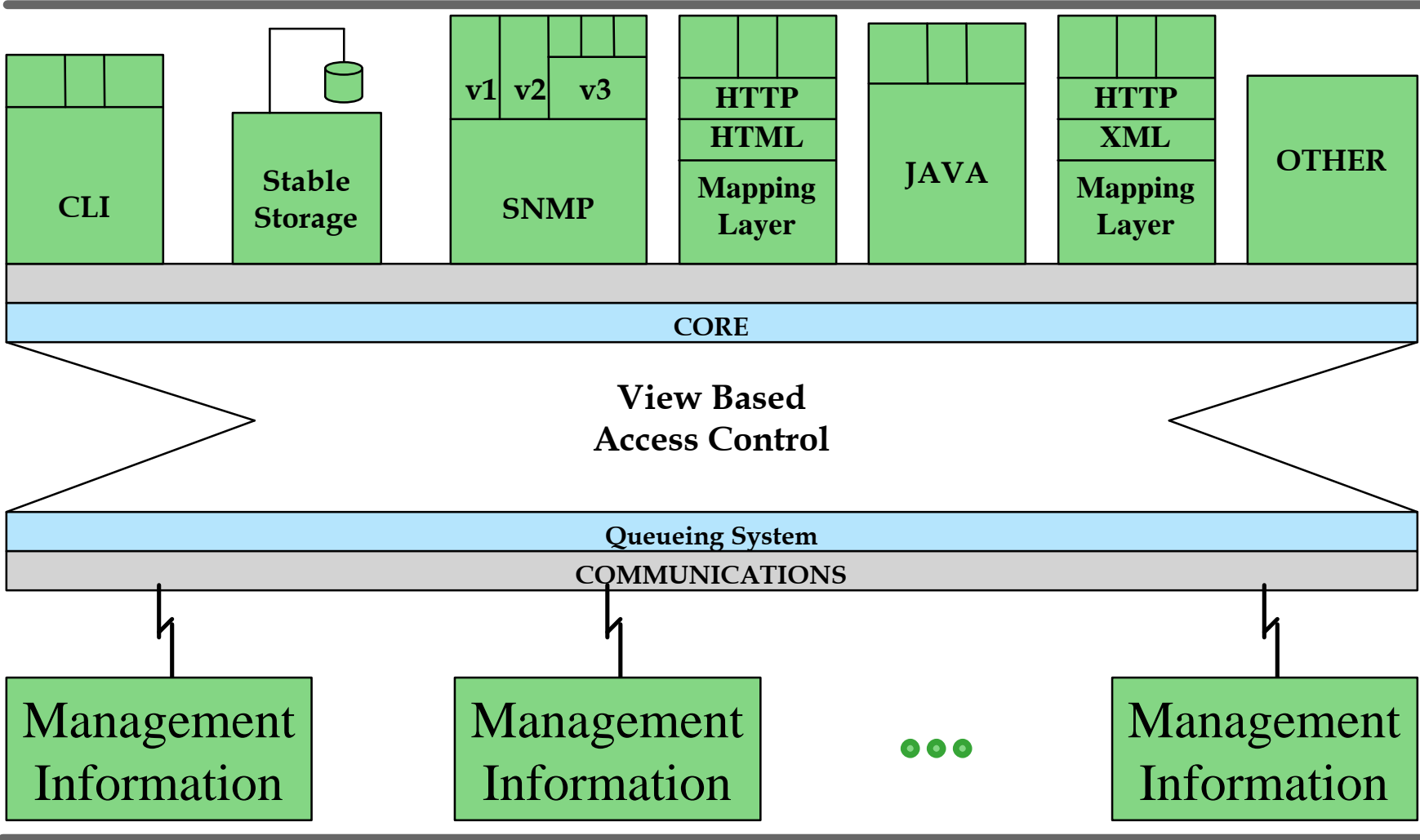
XML Transport Mapping Initiative

- ◆ XML-Based Internet Management
- ◆ Third generation Transport Mapping specification
- ◆ Lacking a catchy marketing name
- ◆ Stream over TCP connection
- ◆ ASCII rather than compact binary encodings
- ◆ Respond to market demand

SNMP Security Pack with XML



Multiprotocol Agent Architecture with XML



Summary

Summary

- ◆ **SNMPv3 adds strong authentication and weak privacy to our arsenal for standards-based Internetwork management**
- ◆ **Follow-on work adds strong privacy**
- ◆ **Much better than SNMPv1 and SNMPv2c**
- ◆ **Standard, available off-the-shelf today**

Summary

- ◆ **Additional work underway in the areas of**
 - **Security enhancements: ESO initiative**
 - **Protocol enhancements: APO initiative**
 - **Transport enhancements: XML initiative**
 - **Ease-of-use enhancements: MIBGuide initiative**
 - **Data language enhancements: SMI-DS initiative**

For More Information

- ◆ ESO: <http://www.snmp.com/protocol/eso.html>
- ◆ APO: <http://www.snmp.com/protocol/apo.html>
- ◆ XML: <http://www.snmp.com/protocol/xml.html>

Dr. Jeff Case
3001 Kimberlin Heights Road
Knoxville, TN 37920
USA
+1 865 573 1434
case@snmp.com
