



# HP Software Forum

THINGS CHANGE. BE READY.

JUNE 19 – 23, 2006

MIAMI BEACH, FLORIDA



OpenView Forum  
ADVOCACY • COMMUNITY • EDUCATION

Title: New Technologies in Standards-Based Internetwork Management

Session #: 327

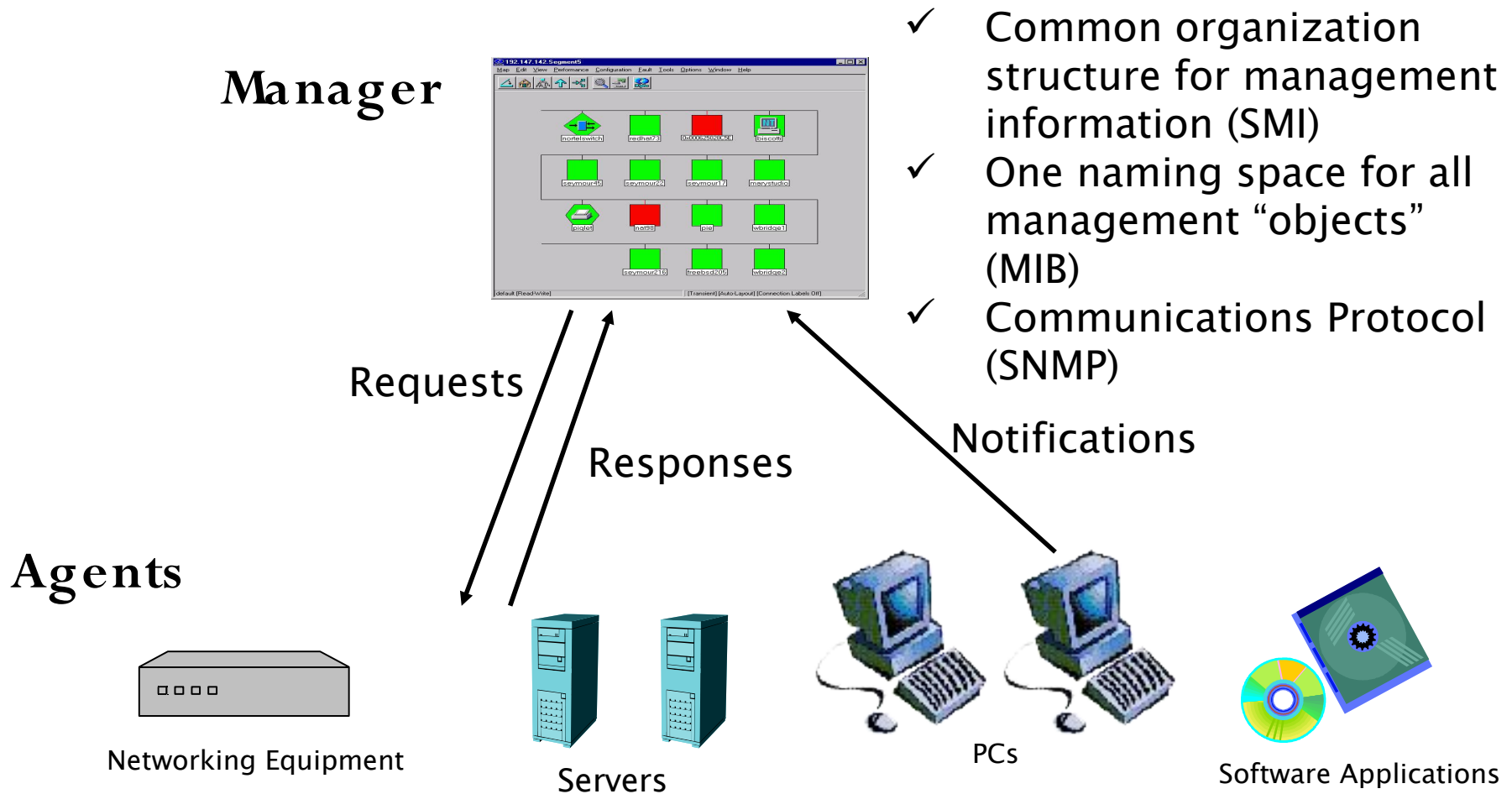
Speaker: Jeffrey D. Case, Ph.D.

Company: SNMP Research

# Topics

- Introduction
- Current State-of-the-Art: SNMPv3
- Future Directions -- 4 Initiatives
  - Ease of use
  - Enhanced Security for Manager-to-Agent Communications (SNMPv3 ESO)
  - Protocol Enhancements (SNMPv3 APO)
  - XML-based modeling and transport of management information (XML SNMP)
- Conclusions

# SNMP in One Slide





# Secure SNMPv3

# 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

# 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
  - DES or AES
  - Standard is extensible for stronger cryptography

# Features of SNMPv3: Security and Administration (Continued)

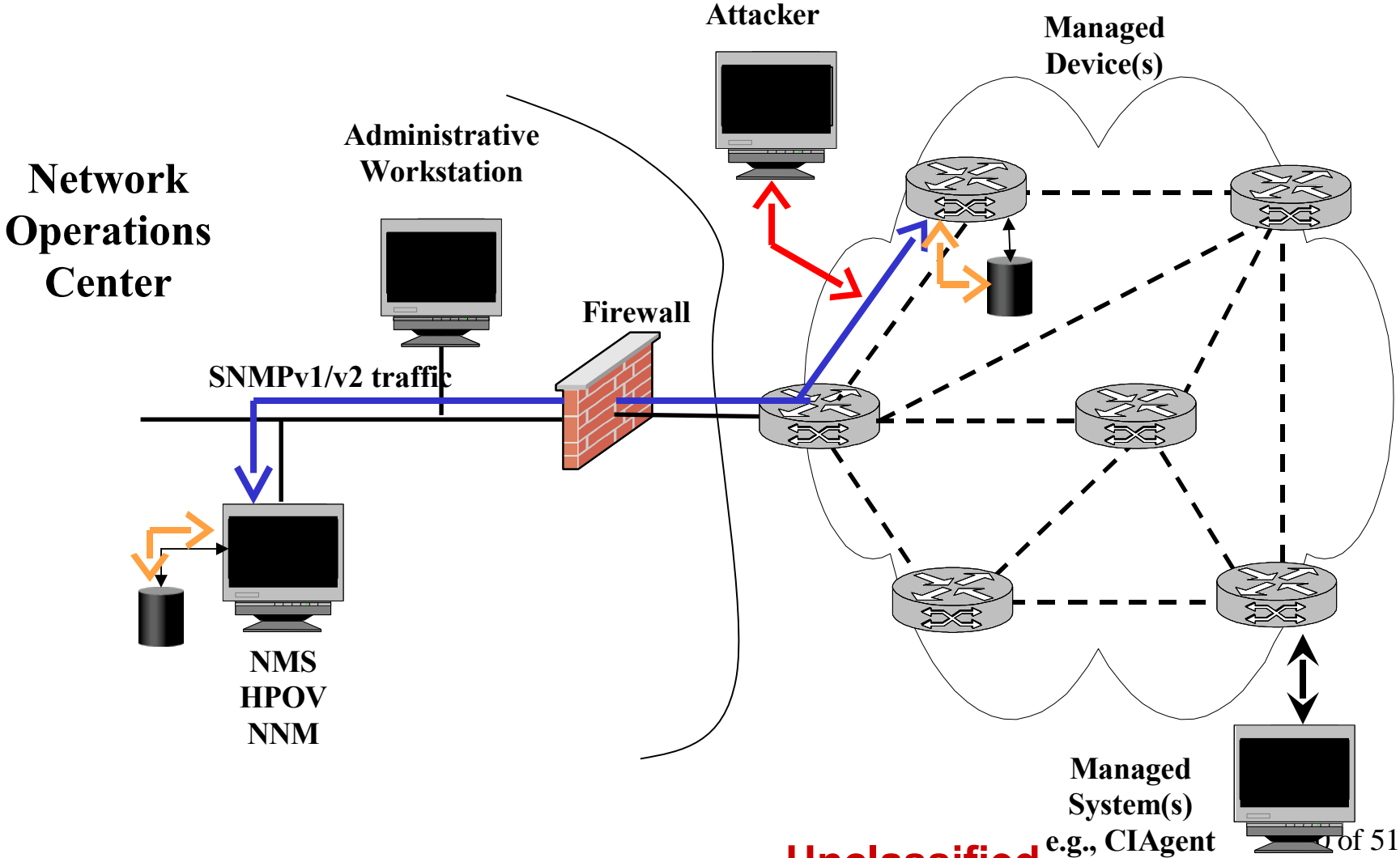
- **Authorization and View-Based Access Control**
  - Authorization: What functions permitted (read, write, notify)
  - Access Control: Restrictions on what data may be read / written, potentially very fined grained
  - Based on groups of SNMPv3 “users”
    - An SNMPv3 user might be a system, person, 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



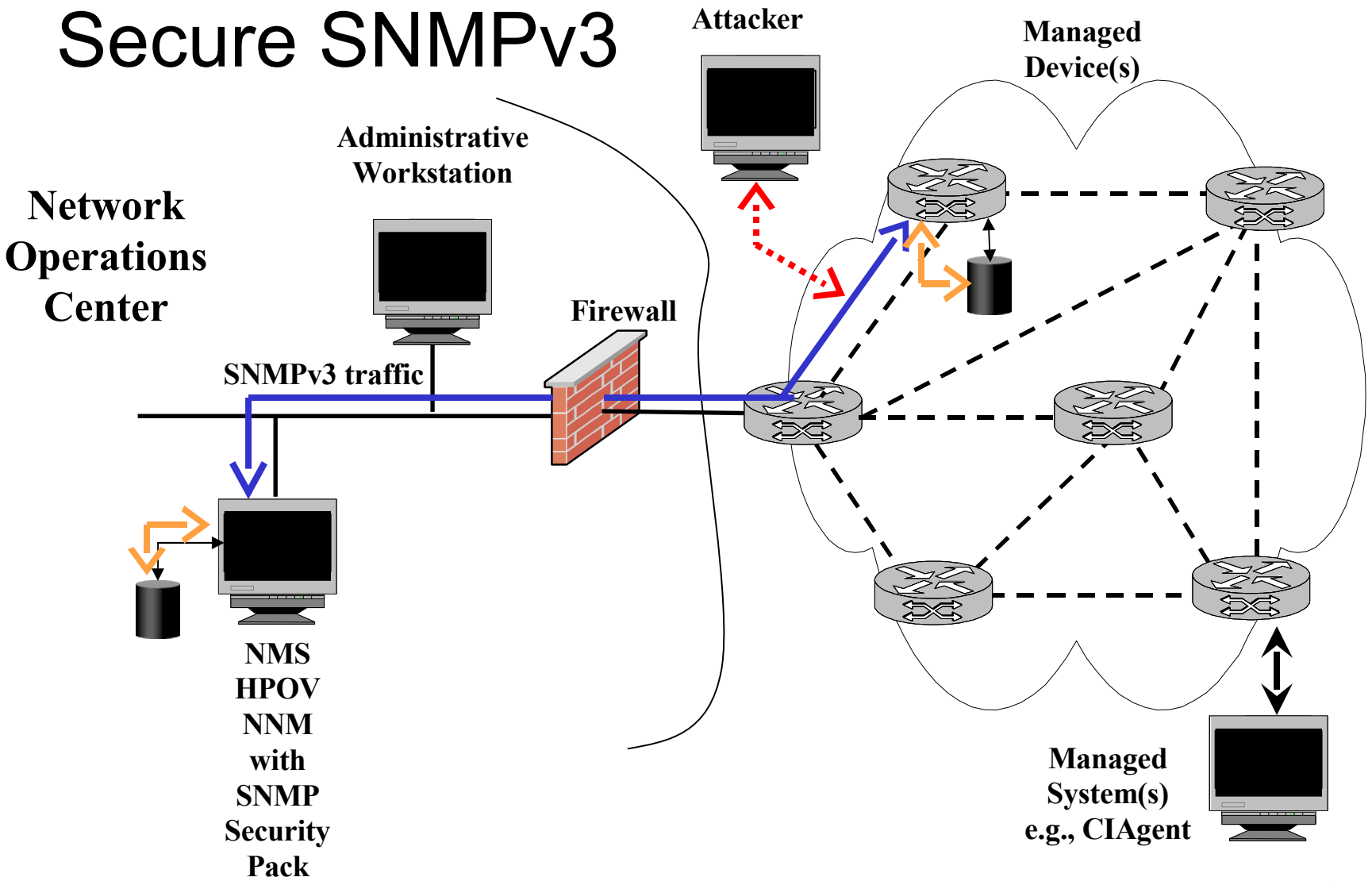
# SNMPv1/SNMPv2c **Not** Secure



**Unclassified**



# Secure SNMPv3



# “Distributed SNMP Security Pack for HP OpenView” Solution

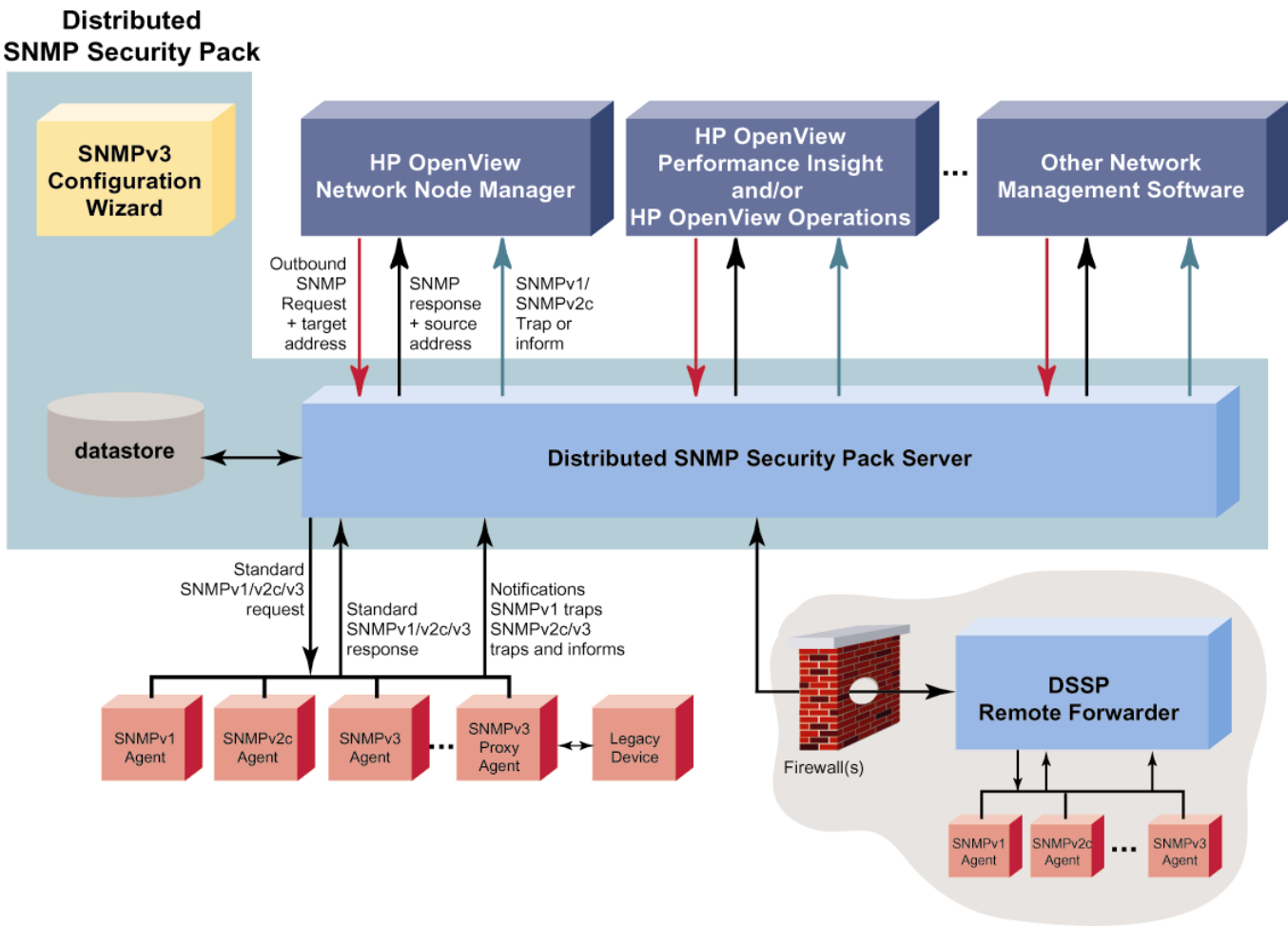
- Standards-Based Security Solution with NNM
- Integration was jointly developed by HP and SNMP Research
- Maps outbound SNMPv1/SNMPv2c requests to SNMPv3 requests sent to target agent
- Converts responses from agent into SNMPv1/SNMPv2c, and provides additional information on source address
- Receives notifications (traps and informs) and passes to NNM, OVPI, OVO, etc.

# “Distributed SNMP Security Pack for HP OpenView” Solution

- Includes security configuration datastore
- Includes SNMPv3 Configuration Wizard
- Now available from SNMP Research, soon to also be available from HP
- Also available with Remote Forwarder



# Distributed SNMP Security Pack





# 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

There is still more to be done

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.
- We need to make this technology easier
  - For vendors to implement and
  - Users to deploy and use

# 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
  - Ease-of-Use Initiative: Configuration aids, MIBGuide, etc
  - DSSP: Distributed SNMP Security Pack for management through firewalls
- Technology Initiatives
  - Extended Security Options (ESO Initiative)
  - Advanced Protocol Operations (APO Initiative)
  - XML-Based Internet Management (XML SNMP Initiative)



# Ease of Use Initiative

Security Configuration  
Tools, MIBGuide, etc

# Configuration Management Issues

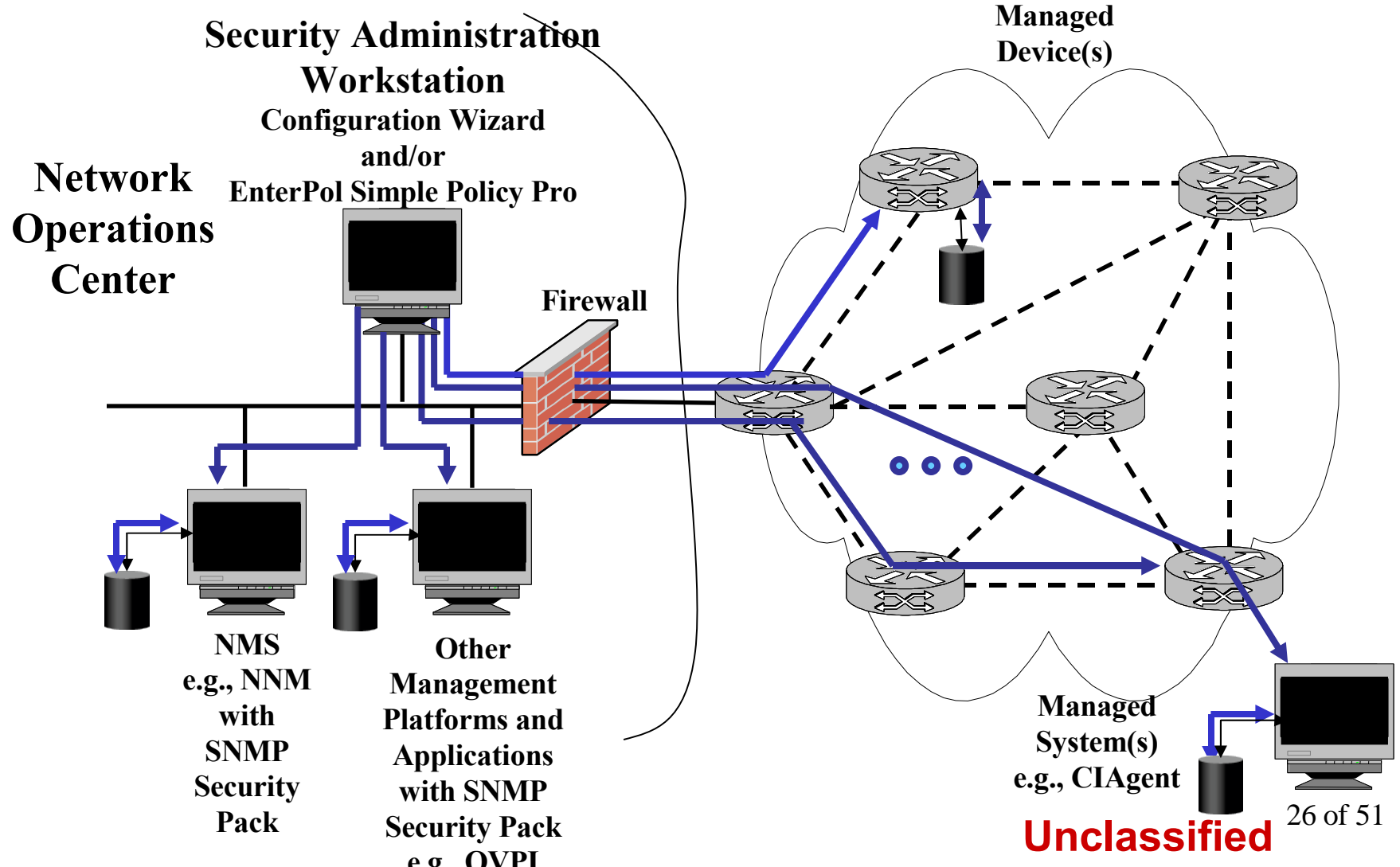
- Users, keys, notifications, etc. must be configured on both managers and agents
- Keys are generated from pass-phrases and localized, pass-phrases not stored on managed devices
- Keys need to be changed periodically
- Configuration must be updated in a timely manner (e.g., deny rights to a terminated 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

**SNMPv3 Configuration Wizard**

**Security Configurations**

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

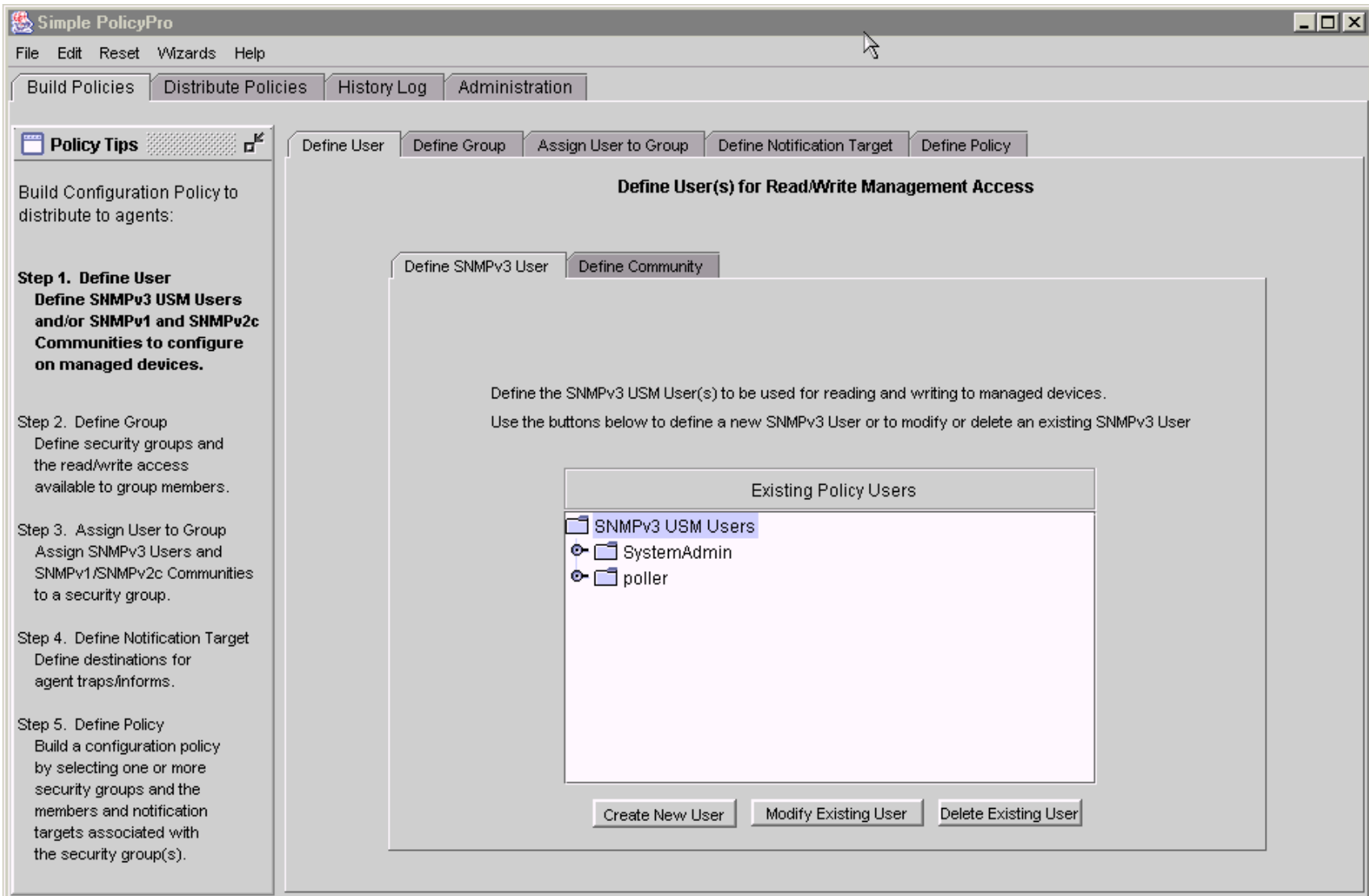


Select the maximum security level for this SNMPv3 USM user:

- 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



The screenshot shows the Simple PolicyPro application window. The main menu includes File, Edit, Reset, Wizards, and Help. The interface is divided into several sections:

- Navigation Tabs:** Build Policies, Distribute Policies, History Log, Administration.
- Sub-Steps:** Define User, Define Group, Assign User to Group, Define Notification Target, Define Policy.
- Current Step:** Define User(s) for Read/Write Management Access.
- Sub-Steps for Current Step:** Define SNMPv3 User, Define Community.

**Policy Tips Panel (Left):**

**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/SNMPv2c Communities to a security group.

Step 4. Define Notification Target  
Define destinations for agent traps/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).

**Main Content Area:**

**Define User(s) for Read/Write Management Access**

Define the SNMPv3 USM User(s) to be used for reading and writing to managed devices.  
Use the buttons below to define a new SNMPv3 User or to modify or delete an existing SNMPv3 User

**Existing Policy Users**

- SNMPv3 USM Users
  - SystemAdmin
  - poller

**Buttons:** Create New User, Modify Existing User, Delete Existing User

# MIBGuide

- Comprehensive toolset to design and develop multi-protocol accessible agents using a graphical Integrated Development Environment (IDE).
- Ease-of-use
  - Ease the burden of creating MIB documents and developing, testing, and deploying agents.
- Productivity tool
- Quality improvement by design not inspection

# Secure Manager-to-Agent Communications Initiative

Extended Security Options  
(SNMPv3 ESO)

# SNMPv3 ESO: Extended Security Options

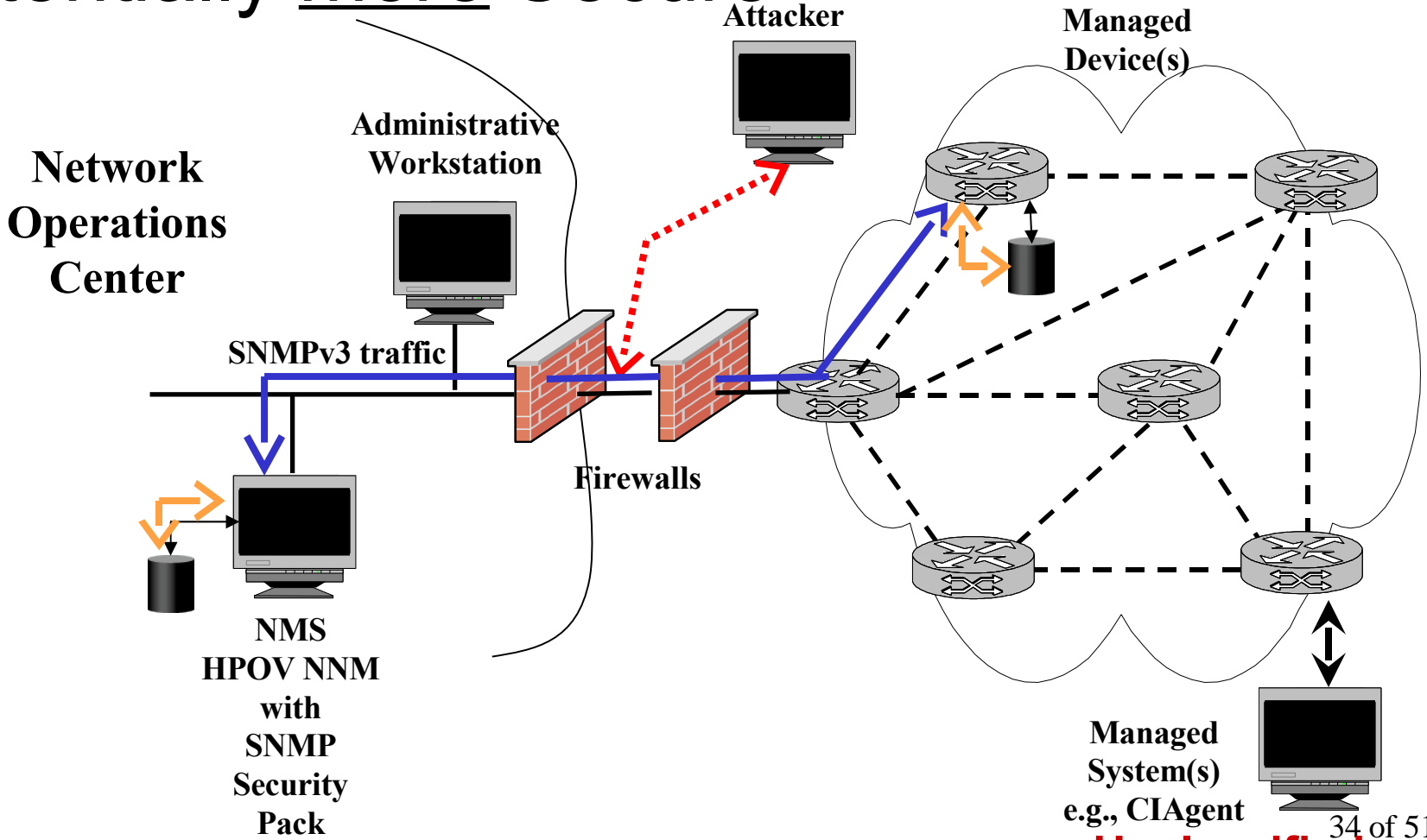
- SNMPv3 framework designed to be extensible and allow additional security models including new
  - Authentication algorithms and mechanisms
  - Privacy algorithms and mechanisms
- ESO uses this to add two new strong privacy algorithms
  - Advanced Encryption Standard (AES) in 128 bit CBC mode
  - Triple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



# SNMPv3 with ESO: Potentially more Secure



# SNMPv3 ESO Availability (in some countries)

- SNMPv3 ESO available today for:
  - HP OpenView NNM and HP Extensible Agent
  - Other management platforms
  - Some embedded systems (e.g., Marconi ATM switches)
  - Most open systems
  - Other
- Future ESO work
  - Articulation with other systems
    - Radius
    - TACACS+
    - Etc
  - Integrated Security Model for SNMP (ISMS)



# Protocol Enhancements Initiative

## Advanced Protocol Operations (SNMPv3 APO)

# Protocol Evolution

Generation	Protocol Operations	Transport Mappings	Security & Administration
1 <sup>st</sup>	RFC 1157 (1988–1993)		
2 <sup>nd</sup>	RFC 3416 (1993–now)	RFC 3417 (1993–now)	Party-based RFC 1445-47 (1993-1995)
3 <sup>rd</sup>	APO (new work)	XML (new work)	User-based RFC 3410-15 (1998–now)

# Advanced Protocol Operations (APO) Initiative

- 3rd Generation Protocol Operations
  - 1st Generation: RFC 1157
  - 2nd Generation: RFC 1448 → RFC 1905 → RFC 3416
- 2 Levels
  - APO Level 1: Compatible with SMIv2 MIB documents
  - APO Level 2: A superset – requires enhancements to MIB grammar

# Advanced Protocol Operations (APO) Initiative

- APO Level 1: Compatible with SMIv2 MIB docs
  - Aggregate objects formerly inaccessible
    - Row Operations
    - Tabular Operations
  - OID Suppression
  - Improved read operations, e.g., GetBulk scoping, etc
  - Improved write operations, e.g., improved error handling, applications specific error codes, etc

# Data Format: Traditional Way vs New Ways

TblNam.1.C1.R1=val,TblNam.1.C2.R1=val,...,TblNam.1.Cm.R1=val  
TblNam.1.C1.R2=val,TblNam.1.C2.R2=val,...,TblNam.1.Cm.R2=val  
...  
TblNam.1.C1.Rn=val,TblNam.1.C2.Rn=val,...,TblNam.1.Cm.Rn=val

versus (explicit)

or (implicit)

```
TblNam.0={  
  {1={1=val, 2=val, ..., m=val}},  
  {2={1=val, 2=val, ..., m=val}},  
  ...,  
  {n={1=val, 2=val, ..., m=val}}  
}
```

```
TblNam.0={  
  {1={val, val, ..., val}},  
  {2={val, val, ..., val}},  
  ...,  
  {n={val, val, ..., val}}  
}
```

# Advanced Protocol Operations (APO) Initiative

- APO Level 2: Akin to the IETF's suspended work on SMI-DS within the SMI-NG WG
  - All of APO Level 1, plus ...
  - Union, Struct, Array, Row, Table
  - Data-type maintenance, i.e., Integer64, Unsigned64
  - Nesting, e.g., something like this within a table

```
– IPAddress struct {
    AddressType    INTEGER,
    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 Modeling and Transport of Management Information Initiative

## XML-based Internet Management (XML SNMP)

# XML Transport Mapping Initiative

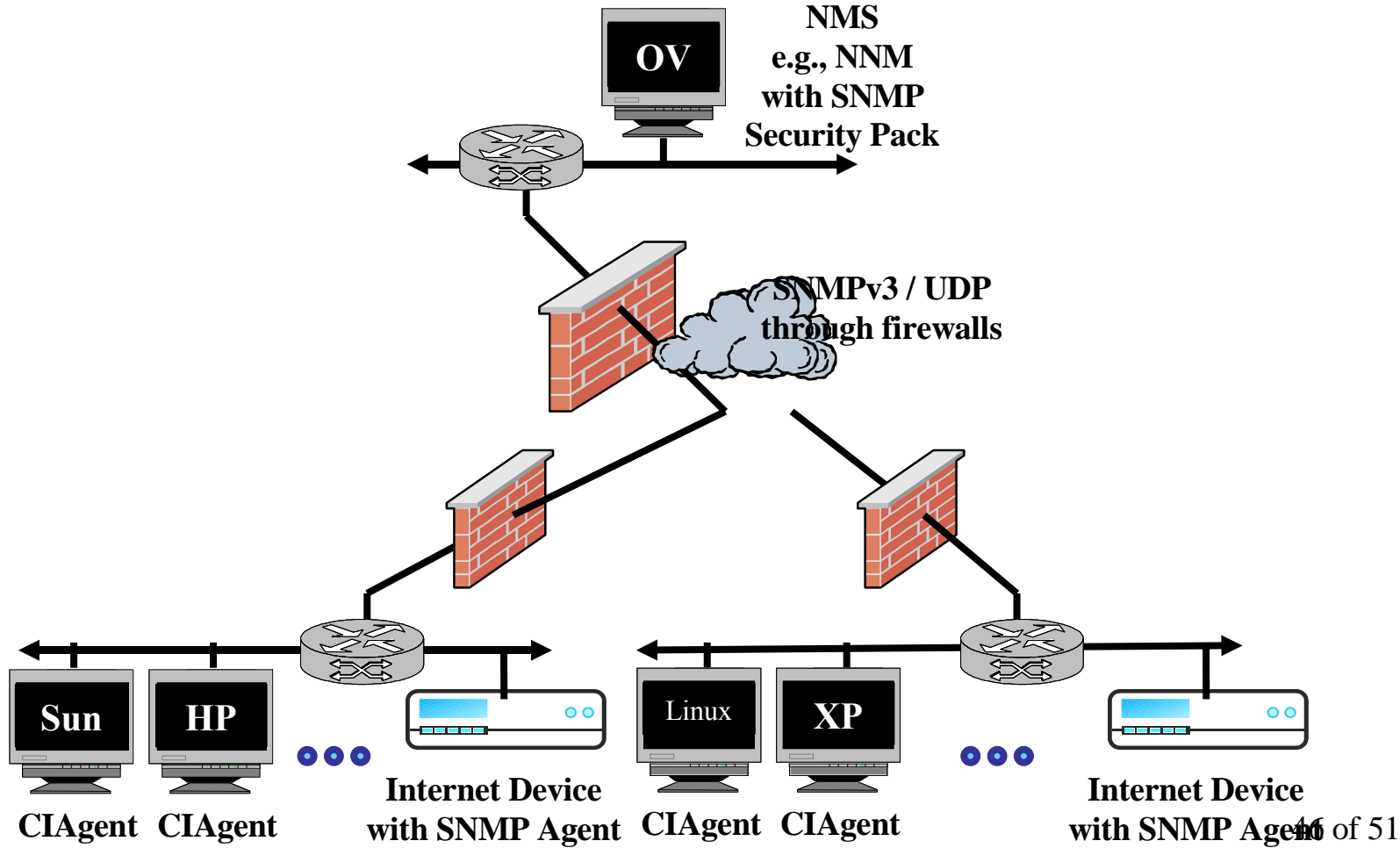
- XML-Based Internet Management means different things to different people
  - XML-ification of proprietary CLI: a factor of 2 incremental improvement
  - XML-ification of standards-based management data: an order-of-magnitude advancement
  - XML transport of entirely new and different data model(s):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

# XML Initiative

- XML-Based Internet Management
- Lacking a catchy marketing name
- Stream over TCP connection
- ASCII rather than compact binary encodings
- Respond to market demand
- Need to be careful not to repeat history:
  - re-solving the solved problem
  - while not solving the unsolved problems and
  - creating new problems
- Avoid political wars

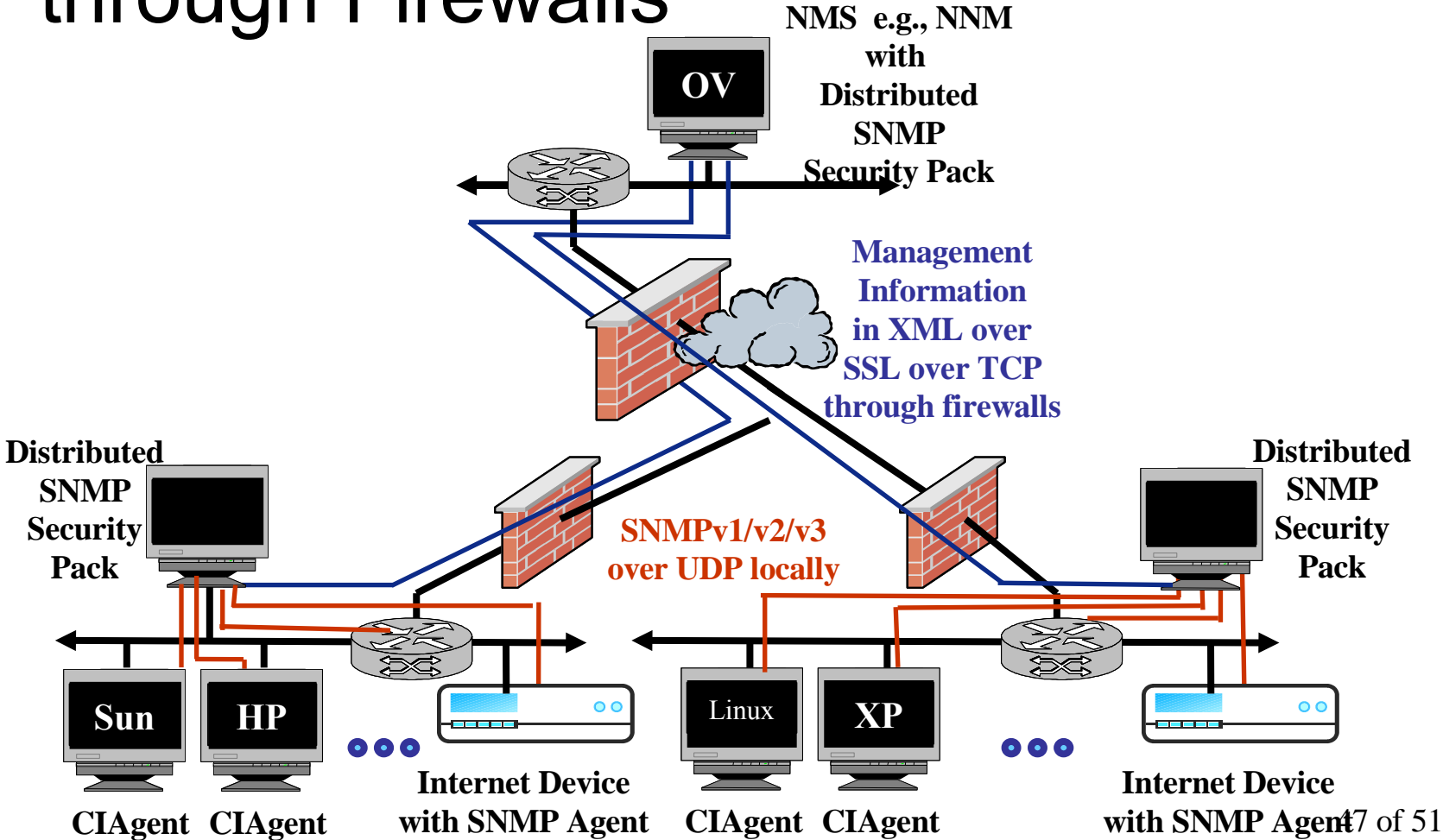


# SNMPv3 over UDP through Firewalls

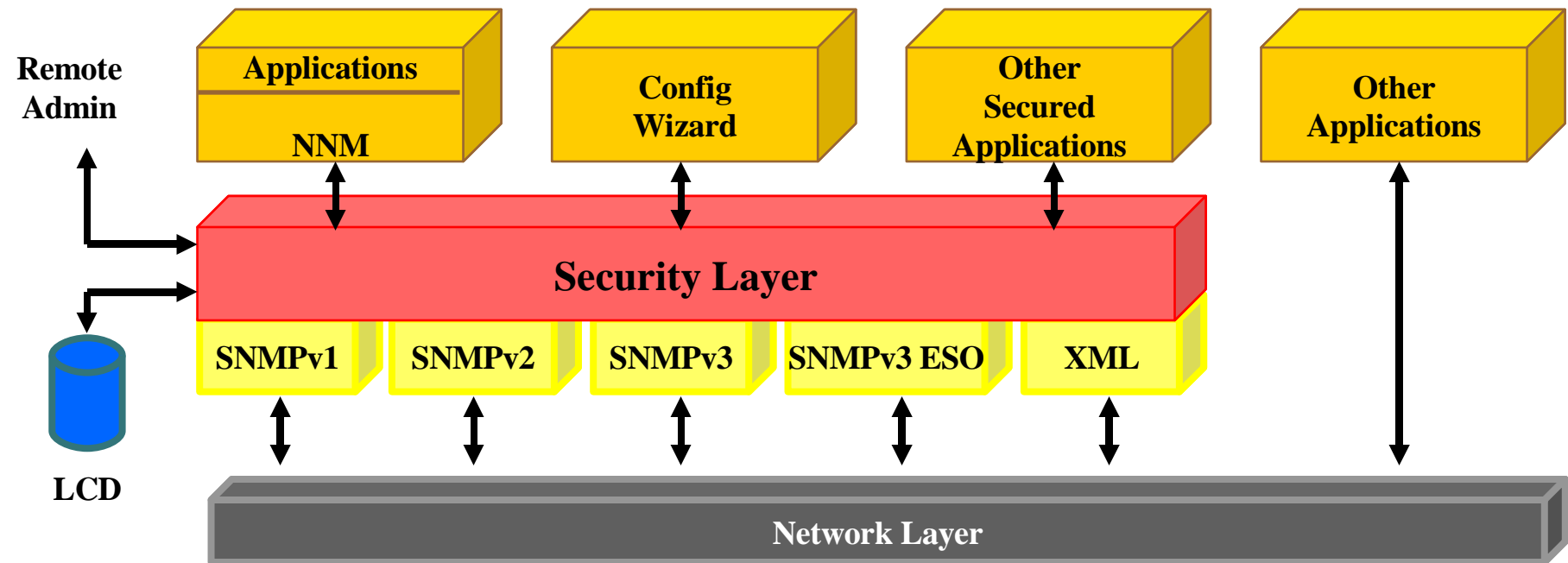




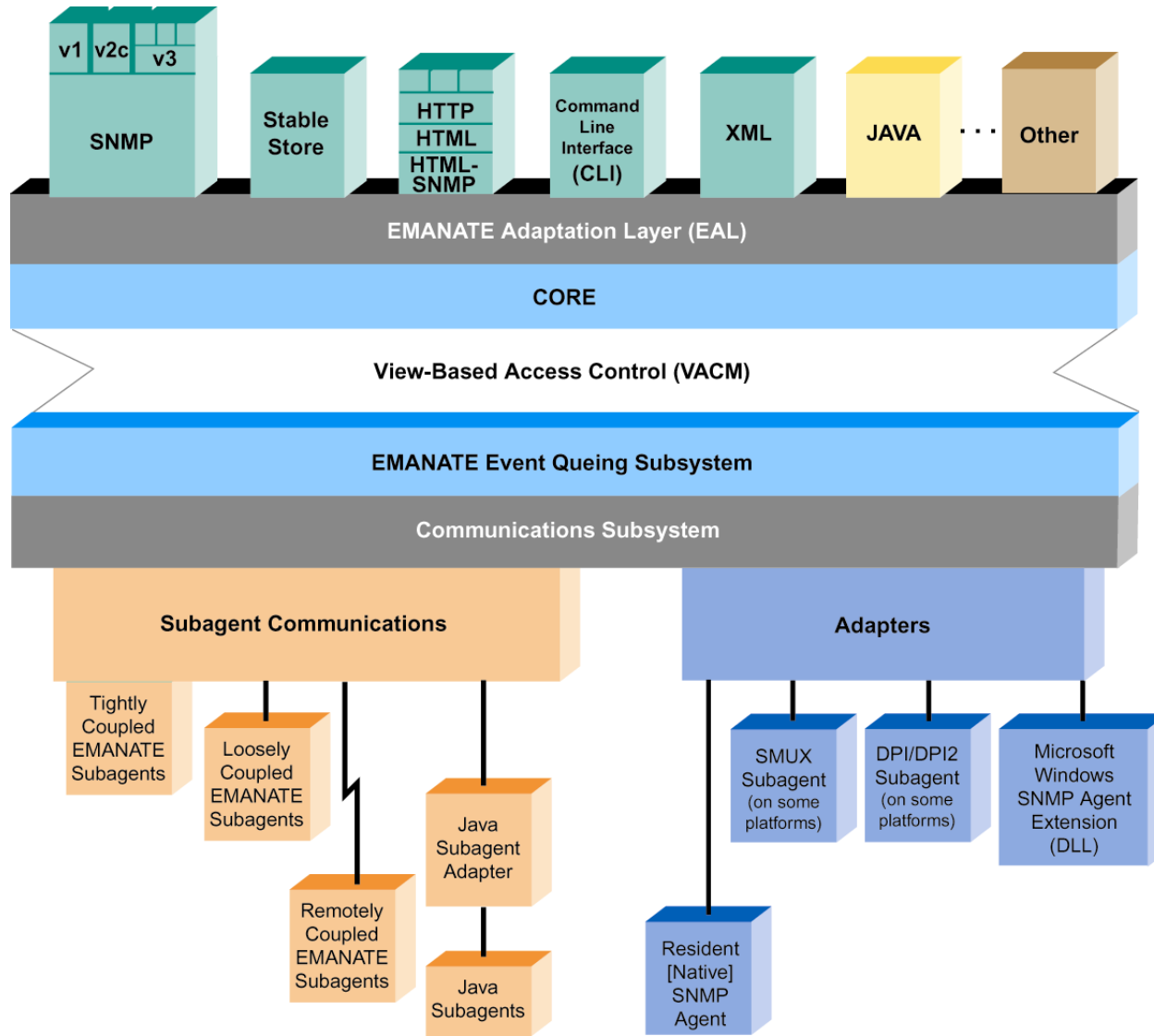
# Management Traffic in XML tunnel through Firewalls



# NNM with SNMP Security Pack and XML



# Multiprotocol Agent Architecture with XML



# Summary

- SNMP Security Pack is a pragmatic solution for adding secure SNMPv3 capability to NNM
  - After security credentials have been configured, operation using Security Pack is transparent to NNM functions
  - Includes “SNMPv3 Configuration Wizard” application for configuration of agents
  - Supported on HP-UX, Solaris, and Windows
- Additional work underway
  - Security enhancements: ESO initiative
  - Protocol enhancements: APO initiative
  - Transport enhancements: XML initiative
  - Ease-of-use enhancements: MIBGuide initiative

# For More Information

- Exhibit Area
- Session 325: Wednesday, June 21, 8:30-9:30
  - Standards-based Secure Management of Networks, Systems, Applications and Services using SNMPv3 and HP OpenView
- 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](mailto:case@snmp.com)