Lantech™
Pioneering Industrial and IP Networks

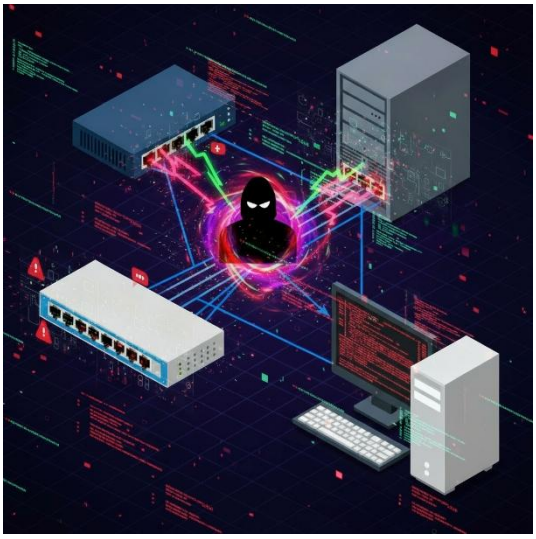
White Paper

SNMPv3:

Modern Network Security Standard

Version1.0
Oct, 2025

Common Challenges in Network Management



Organizations face critical security gaps when using earlier SNMP versions:

- Sensitive configuration data could be intercepted or modified during transmission, causing device failures or outages.
- SNMPv1 and v2c transmit all management information in plaintext, making it vulnerable to packet sniffing and spoofing attacks.
- Limited access control leads to poor user differentiation and insufficient security segmentation.

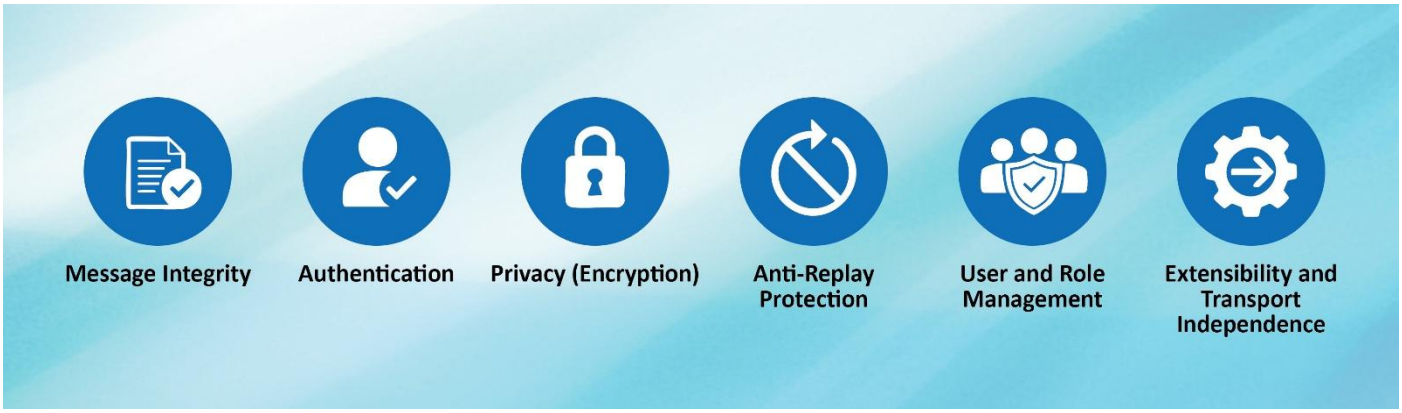
As the number of connected systems in industrial and critical infrastructure grows, secure and flexible remote management has become essential. SNMPv3 was specifically developed to address these challenges.

Table 1: Comparison of SNMP Versions (v1, v2c, and v3)

	SNMPv1	SNMPv2c	SNMPv3
Setup Ease	Easy to set up	Easy to set up	Hard to set up
Efficiency	Less efficient	Less efficient	More efficient
Counter Bits	Supports 32-bit counters	Supports 64-bit counters	Supports 64-bit counters with security
Security	Plain-text community string	Improved error handling and SET commands	Adds encryption and authentication
Packet Types	Get-Request Get-Next-Request Set Request Get Response	Get-Request Get-Bulk-Request Get-Next-Request Set Request Inform-Response SNMP v2 Trap	Basic functions like v1 & v2 New packet types for SNMPv3

Core Security Mechanisms in SNMPv3

SNMPv3 represents a major evolution in network management security, introducing multiple layers of protection that jointly ensure confidentiality, integrity, and authentication across management traffic. Unlike SNMPv1/v2c, which transmitted plain text and lacked access control, SNMPv3 integrates modern cryptographic principles to prevent tampering or unauthorized access.



1. Message Integrity

To guarantee that network management data remains unaltered during transmission, SNMPv3 uses cryptographic checksums (HMAC) to verify packet integrity.

- The receiving device recomputes and compares message digests to detect corruption or tampering.
- This integrity check ensures that malicious intermediaries cannot inject or modify SNMP commands without detection.

2. Authentication

SNMPv3 employs user-level authentication based on HMAC-MD5-96 or HMAC-SHA-96 algorithms, ensuring that the message truly originates from a legitimate administrator.

- Each SNMPv3 entity is assigned authentication keys, preventing identity spoofing.
- Devices must synchronize authentication protocols to avoid mismatched message validation.

3. Privacy (Encryption)

Encryption safeguards against packet sniffing or eavesdropping.

- Initially, DES-CBC was used, but AES became the modern standard for higher security strength.
- Only the Protocol Data Unit (PDU) portion of a message is encrypted, allowing intermediate systems to process routing and version headers as needed.
- This structure balances performance and confidentiality across large-scale systems.

4. Anti-Replay Protection

SNMPv3 includes a time-based synchronization mechanism to block replay attacks — where an attacker

captures a valid request and re-sends it later.

- Every message includes a timestamp and an engine boot count.
- Devices maintain an acceptance window, rejecting outdated or duplicated messages.
- This is especially important in distributed or redundant systems where clock skew can occur.

5. User and Role Management

SNMPv3 supports flexible user management for large networks.

- Administrators can add, remove, or modify user profiles and assign unique security levels (noAuthNoPriv, authNoPriv, authPriv).
- USM (User-based Security Model) handles these accounts, while VACM (View-based Access Control Model) complements it with fine-grained access restrictions.
- This design enables role-based management, where engineers can be assigned authority based on departmental, functional, or geographic boundaries.

6. Extensibility and Transport Independence

SNMPv3 mechanisms are protocol-agnostic, operating independently of the underlying transport (TCP, UDP, etc.).

- They can integrate with Transport Security Model (TSM) using TLS/DTLS, strengthening security for both connection-oriented and connectionless networks.
- USM also supports future cryptographic upgrades, ensuring ongoing compatibility with emerging standards such as AES-256 or SHA-2 families.

SNMPv3 Security Models

SNMPv3 relies on three complementary security models :

1. **User-based Security Model (USM - RFC 3414)**

   Provides authentication and privacy at the user level. Administrators can select from multiple security levels (noAuthNoPriv, authNoPriv, authPriv) according to policy needs.

2. **View-based Access Control Model (VACM - RFC 3415)**

   Defines granular access rights by grouping users and defining MIB "views." Supports role-based control ensuring only authorized users can view or modify specific data objects.

3. **Transport Security Model (TSM - RFC 5591)**

   Integrates TLS and DTLS for secure transport-layer encryption, enabling authentication through X.509 certificates and improving performance with session resumption capabilities.

Together, these models deliver end-to-end protection across network management operations, fitting the strictest requirements of finance, transportation, and industrial environments.

Lantech OS5: Full SNMPv3 Support Across All Models

Lantech's OS5 platform provides full, native SNMPv3 implementation:

- **All models under OS5** include complete SNMPv3 feature sets — USM, VACM, and TSM — as standard.
- **No license required**: SNMPv3 functions are built into the regular firmware.
- **Easy configuration**: Both CLI and Web UI interfaces allow users to enable authentication, encryption, and access control efficiently.

Whether managing large transportation systems, smart infrastructure, or rugged industrial networks, Lantech OS5 ensures secure, standards-compliant network visibility and control through seamless SNMPv3 functionality.

Learn more about Lantech OS5 switches:

https://www.lantechcom.tw/global/eng/software-OS5.html

About Lantech

Lantech Communications Global, Inc. is an IRIS & ITxPT certified manufacturer of Ethernet products focused on the transportation markets, bus, train, trackside, ITS, smart city and many more applications. Our range of onboard EN50155 & E-Marked Ethernet switches & wireless/ LTE routers offer cutting edge design and functionality. We continue to work with our key customers in creating further enhancements & developments in on board passenger information, video security, trackside data communications by providing rugged 10GbE, PoE managed Ethernet switches, LTE/Wi-Fi routers in line with ITxPT and E-Marked certifications for various applications and critical solutions.