**VISION INSTITUTE OF MANAGEMENT**

**COMPUTER NETWORK SECURITY**

**BCA 3rd YEAR/6th SEM**

**UNIT 5(NETWORK MANAGEMENT SECURITY)**

**What is Network Security Management?**

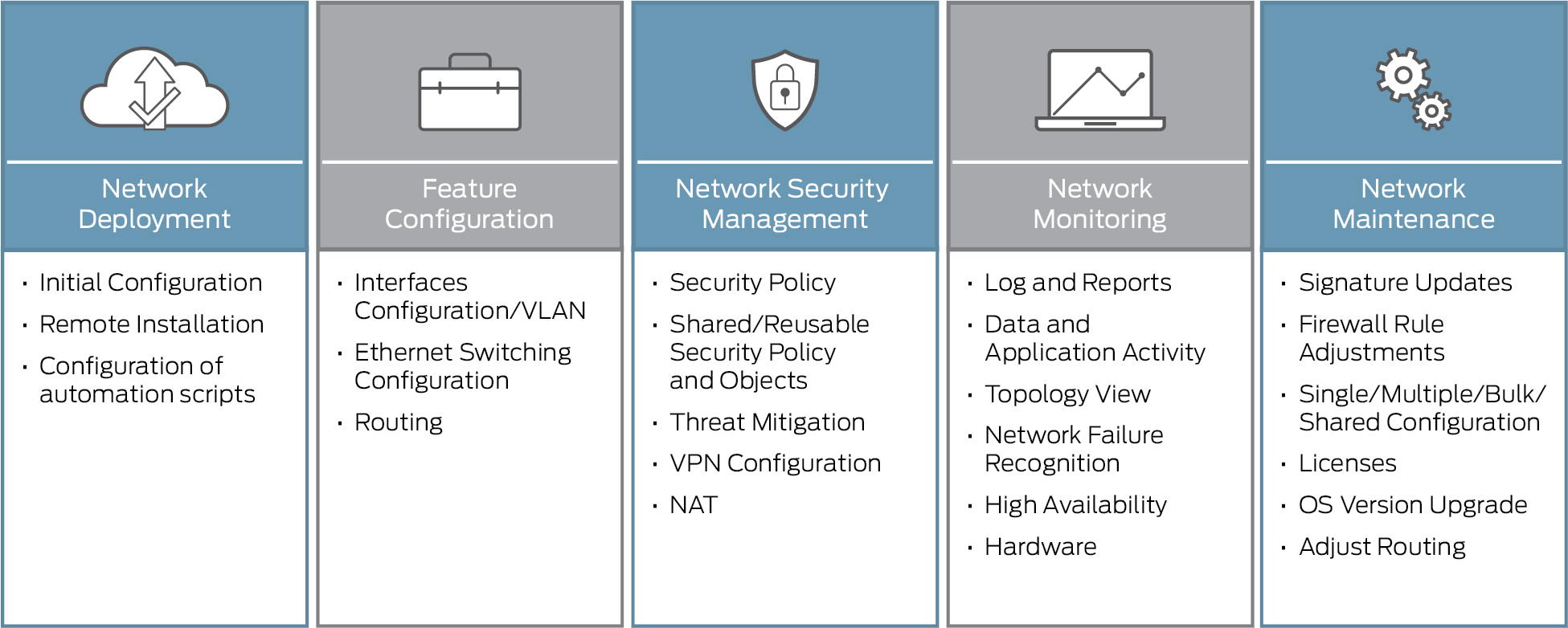
Network security management allows an administrator to manage a network consisting of physical and virtual firewalls from one central location. Administrators need network security management solutions to get a high level of visibility into network behaviour, automate device configuration, enforce global policies, view firewall traffic, generate reports, and provide a single management interface for physical and virtual systems.

Problems Network Security Management Address

In today’s complex network architecture and constantly changing threat environment, it is challenging for IT staff to maintain an effective security posture. Security administrative tasks include supporting an ever-expanding matrix of users, devices, locations, and applications; adhering to compliance; enabling new services; optimizing performance; ensuring access controls and security mechanisms; and troubleshooting on demand. Any misconfiguration can make the network vulnerable to sophisticated threats and regulatory noncompliance.

To confront these challenges, network administrators need to consistently deploy security policies across their network. However, the network infrastructure might have thousands of firewall policies that have accumulated over the years. Often these rules are cluttered, duplicated, outdated, or conflict with new rules, inadvertently affecting a network’s performance and security.

The following illustration depicts a scenario from a typical enterprise, where the IT department needs to address network security management:



Network security management helps reduce manual tasks and human errors by simplifying administration with security policy and workflow tools through a centralized management interface.

Network security management can reduce risk across the network and protect data by leveraging the information on threats, network vulnerabilities and their criticality, evaluating potential options to block an attack, and providing intelligence for decision support.

Policy administration is improved by unifying common policy tasks within a single interface, automating policy change workflow, including compliance audits and the management of multiple firewall vendors. This simplified and automated security policy management enables IT teams to save time, avoid manual errors, and reduce risk.

**How Does Network Security Management Work?**

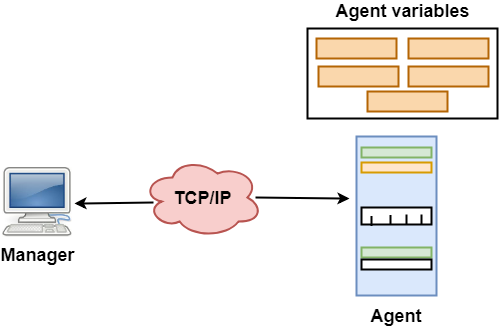
Network security management provides complete visibility into the network and generates data for assets (asset groupings and classifications), firewalls, applications, ports, protocols, VPNs, NAT, and security policies and vendor devices. This information drills into the details for individual devices and is analysed. The data is translated into intelligence that decrypts security transactions into manageable, actionable information in the form of policy creation. Updated policies are distributed to enforcement points (firewalls), ensuring network protection.

# Simple Network Management Protocol (SNMP)

If an organization has 1000 of devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.

**Simple Network Management Protocol (SNMP) –**

SNMP is an application layer protocol which uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults and sometimes even used to configure remote devices.



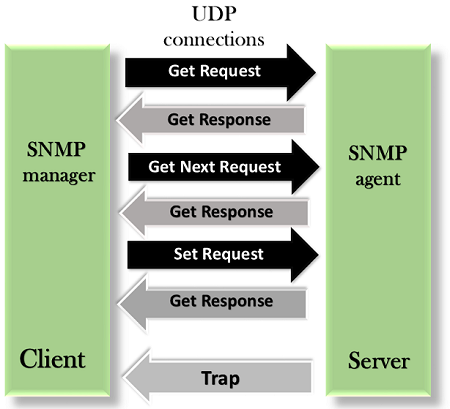
* SNMP has two components Manager and agent.
* The manager is a host that controls and monitors a set of agents such as routers.
* It is an application layer protocol in which a few manager stations can handle a set of agents.
* The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.
* It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways.

**SNMP components –**

There are 3 components of SNMP:

1. **SNMP Manager –**  
   It is a centralised system used to monitor network. It is also known as Network Management Station (NMS).
2. **SNMP agent –**  
   It is a software management software module installed on a managed device. Managed devices can be network devices like PC, router, switches, servers etc.
3. **Management Information Base –**  
   MIB consists of information of resources that are to be managed. These information is organised hierarchically. It consists of objects instances which are essentially variables.

**SNMP messages –**



Different variables are:

1. **GetRequest –**  
   SNMP manager sends this message to request data from SNMP agent. It is simply used to retrieve data from SNMP agent. In response to this, SNMP agent responds with requested value through response message.
2. **GetNextRequest –**  
   This message can be sent to discover what data is available on a SNMP agent. The SNMP manager can request for data continuously until no more data is left. In this way, SNMP manager can take knowledge of all the available data on SNMP agent.
3. **GetBulkRequest –**  
   This message is used to retrieve large data at once by the SNMP manager from SNMP agent. It is introduced in SNMPv2c.
4. **SetRequest –**  
   It is used by SNMP manager to set the value of an object instance on the SNMP agent.
5. **Response –**  
   It is a message send from agent upon a request from manager. When sent in response to Get messages, it will contain the data requested. When sent in response to Set message, it will contain the newly set value as confirmation that the value has been set.
6. **Trap –**  
   These are the message send by the agent without being requested by the manager. It is sent when a fault has occurred.
7. **InformRequest –**  
   It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is same as trap but adds an acknowledgement that trap doesn’t provide.

**SNMP security levels –**

It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely:

1. **noAuthNoPriv –**  
   This (no authentication, no privacy) security level uses community string for authentication and no encryption for privacy.
2. **authNopriv –** This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.
3. **authPriv –** This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses DES-56 algorithm.

**SNMP versions –**

There are 3 versions of SNMP:

1. **SNMPv1 –**  
   It uses community strings for authentication and use UDP only.
2. **SNMPv2c –**  
   It uses community strings for authentication. It uses UDP but can be configured to use TCP.
3. **SNMPv3 –**  
   It uses Hash based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, conclusion is the higher the version of SNMP, more secure it will be.

# SNMPv3 with Security and Administration

# Introduction

Secure management is available with SNMPv3, the ``Full Standard,'' IETF-recommended version of the Internet-Standard Management Framework. This technology provides commercial-grade security and the ease of administration, which includes authentication, authorization, access control, and privacy.

The secure management of SNMPv3 is an important enabling technology for safe configuration and control operations. SNMPv3 provides security with authentication and privacy, and its administration offers logical contexts, view-based access control, and remote configuration. This technology is available for networks, systems, applications, manager-to-manager communications, and proxy management of legacy systems.

SNMPv3 is derived from and builds upon both the original Internet-Standard Management Framework (SNMPv1) and the second Internet-Standard Management Framework (SNMPv2c). All versions (SNMPv1, SNMPv2c, and SNMPv3) of the Internet-Standard Management Framework share the same basic structure and components. Furthermore, all versions of the specifications of the Internet-Standard Management Framework follow the same architecture.

## **SNMPv3 Features**

Many SNMP products remain fundamentally the same under SNMPv3, but are enhanced by the following new features:

**Security**

* Authentication
* Privacy

**Administration**

* Authorization and access control
* Logical contexts
* Naming of entities, identities, and information
* People and policies
* Usernames and key management
* Notification destinations and proxy relationships
* Remote configuration via SNMP operations

## **Additional SNMPv3 Features (from v2)**

The following features are incorporated from the SNMPv2 Framework by reference.

|  |  |
| --- | --- |
| **Feature** | **Example** |
| Expanded data types | 64-bit counters |
| Improved efficiency and performance | get-bulk operator |
| Confirmed event notifications | inform operator |
| Richer error handling | errors and exceptions |
| Improved sets | row creation/deletion |
| Fine tuned data definition language | SMI, textual conventions, conformance statements, and agent capabilities |

# Security Threats and SNMPv3 Protection

Secure management with SNMPv3 protects against four threats:

|  |  |
| --- | --- |
| **Threat** | **SNMPv3 Protection** |
| **Masquerade** | Verifies the identify of the message's origin by checking the integrity of the data. |
| **Modification of Information** | Thwarts accidental or intentional alterations of in-transit messages by checking the integrity of the data, including a time stamp. |
| **Message Stream Modification** | Thwarts replay attacks by checking message stream integrity, including a time stamp. |
| **Disclosure** | Prevents eavesdropping by protocol analyzers, etc., by using encryption. |
| **Unauthorized Access** | Verifies operator authorization and protects critical data from intentional and/or accidental corruption by using an access control table (part of policy-based management). |

**Security Mechanisms**

User-based Authentication Mechanism is based on the following:

* MD5 message digest algorithm in HMAC
  + Directly provides data integrity checks
  + Indirectly provides data origin authentication
  + Uses private key known by sender and receiver
  + 16-byte key
  + 128-bit digest (truncates to 96 bits)
* SHA, an optional alternative algorithm
* Loosely synchronized monotonically increasing time indicator values defend against certain message stream modification attacks

User-based Privacy Mechanism is based on the following:

* Data Encryption Standard (DES) Cipher Block Chaining (CBC) mode
  + Provides data confidentiality
  + Uses encryption
  + Subject to export and use restrictions in many jurisdictions
* Uses 16-byte key (56-bit DES key, 8-byte DES initialization vector) known by sender and receiver
* Multiple levels of compliances with respect to DES due to problems associated with international use
* Triple Data Encryption Standard (Triple DES)
* Advanced Encryption Standard (128, 192, and 256, bit keys)

**Configuration**

SNMPv3 provides the following configuration possibilities. (Note: availability depends on export restrictions.)

* No authentication and no privacy (noAuthNoPriv) - usually for monitoring
* Authentication and no privacy (authNoPriv) - usually for control
* Authentication and privacy (authPriv) - usually for downloading secrets

The network administrator has the potential to configure the protection level on a transaction-by-transaction basis. Criteria to consider when choosing configuration options are system resources and level of protection.

**SNMPv3 Architecture**

The specifications of the Internet-Standard Management Framework are based on a modular architecture. This framework is more than just a protocol for moving data. The framework consists of

* A data definition language,
* Definitions of management information (the Management Information Base, or MIB),
* A protocol definition, and
* Security and administration.

The framework was structured with a protocol-independent data definition language and Management Information Base, along with a MIB-independent protocol. The SNMPv3 Framework builds and extends these architectural principles by

* Building on these four basic architectural components, in some cases incorporating them from the SNMPv2 Framework by reference, and by
* Using these same layering principles in the definition of new capabilities in the security and administration portion of the architecture.

Those who are familiar with the architecture of the SNMPv1 Management Framework and the SNMPv2 Management Framework find many familiar concepts in the architecture of the SNMPv3 Management Framework. However, in some cases, the terminology may be somewhat different.