Transport
OSI layer transport: UDP/TCP/SSH etc

Remote Operations
offers three distinct functions that complement and perform important services for the Management Operations layer on top: association control, remote, operations support

- **Association control**, deals with how to establish and tear down management sessions—that is, management associations between managers and agents.
- **Remote operations**, support involves the mechanism that is used to wrap and delineate management requests and responses in communication exchanges.
Encoding, finally, entails how management information that constitutes the payload of management operations is “flattened” and encoded in a PDU.

An encoding that is used in conjunction with SNMP is defined in the ASN.1 (Abstract Syntax Notation One) Basic Encoding Rules.

Another encoding is XML.

Management Operations
It provides the actual management primitives: the base operations that are used to manage the network. Management primitives include different types of management requests, responses to those management requests, and events.

Management Services
additional offering to management applications that builds itself on the Management Operations layer. Management services combine the management primitives provided at the Management Operations layer with additional capabilities.

Examples of management services:
- Subscription service: subscribe to specific types of events based on certain filter criteria, such as all events pertaining to a specific port.
- Introspection service that allows management applications to retrieve information about management information and management functions on a managed device, to produce documentation.
- Remote scheduling service that allows management applications to set up a probe that periodically executes a management operation.

Manager-Initiated Interactions: Request and Response
REQUEST
- The type of request being made
- The management information that the request applies to or, alternatively, parameters that carry information needed to carry out the request
- Additional housekeeping information—for example, an identifier for the request and security credentials such as authentication information to verify the identity of the requestor

RESPONSE
- A response code indicating whether the request was successful. In case the request was not successful, a reason should be given.
- The result of the request—for example, the information that was requested.
- Additional housekeeping information, such as the identifier of the original request, to help the manager match the response to the original request that it sent.
Network Management

Information Retrieval: Polling and Polling-Based Management

- Requests for Configuration Information
  - Information about the logical and physical configuration of the device.
  - Changes to configuration information are initiated from the outside of the agent; several advantages to this:
    - Management traffic over the network is reduced.
    - Load that is imposed on the device to respond to such queries is reduced.
    - Performance of the management application is improved.

Polling a managed device for operational data and state information is generally used in scenarios such as the following:

- Device viewing: A remote user wants to obtain a real-time view of a device, requiring a snapshot of the most current information.
- Troubleshooting and diagnostics: Erratic behavior has been observed in the network, and applications need to obtain current data from the device to determine the cause.
- "Hot spot" polling: A particular device is under routine and specific observation; its state information is polled repeatedly over an extended period of time.

- Requests for Operational Data and State Information
  - Operational data and state information generally tend not to be represented in a management application’s database.
  - It must poll it for the current snapshot of operational data and device state.
Information Retrieval: Polling and Polling-Based Management

- Incremental Request (Incremental Operation)
  - Get several pieces of management information, separate requests are sent.

- Bulk Request
  - Get several pieces of management information, on one request.
  - e.g.: all operational data of a line card or "all configuration information"

Historical Information

- Typically performance data such as bandwidth utilization or packet drop rates that are taken at certain intervals in time.
- Collecting and analyzing these snapshots can reveal valuable information for network providers.
Configuration Operations

for example, configuring an interface, enabling or disabling a routing feature, changing access control lists that define firewall rules, or configuring where to send alarm messages.

- Failure Recovery

- Response Size and Request Scoping
  - One small request can result in the return of a substantial amount of Information.
  - The size of the response is typically similar to the size of the request.
  - The response includes a return code that indicates whether the request was successful and perhaps the new setting that is in effect as a result

- Dealing with Configuration Files
  - Preparing a configuration file that contains the configuration that is to take effect
  - Downloading this configuration file on the device
  - Explicitly telling the device to switch over from the current configuration to the new configuration in the new file

Configuration Operations

- Actions

A request is sent to perform the action, and a response is sent that indicates the outcome of the action or any errors that were encountered.
Management Transactions

- Sometimes management applications would like not having to issue a request/response pair for each configuration operation or management action.
- But instead be able to group several commands together and have them execute together as one unit.
- This is often the case when services need to be provisioned over a network.

Example of transaction

```
Begin transaction {
  Operation 1
  Operation 2
  Operation 3
}
End transaction;
```
Agent-Initiated Interactions: Events and Event-Based Management

example, the event message could be an alarm that indicates that the device is overheating or that it has been experiencing a failure.

Event Taxonomy

Notifying managers of many different types of event occurrences. Accordingly, they can be classified into a number of categories. The most common ones are as follows:

- **Alarms**: Unexpected events indicating a condition that typically requires management attention.
- **Configuration-change events**: Events that inform of a configuration change that has taken effect at the device.
- **Threshold-crossing alerts**: Events that inform that a performance-related state variable has exceeded a certain value, pointing to conditions that might require management attention to prevent network and service degradation.

**Logging events**: Events that occur regularly and that are expected to occur during the operation of a network, that indicate what is currently going on in the network. In general, those events do not require an operator’s attention but need to be logged (that is, written to a file or stored in a database) so that they are available for further analysis when needed. Logging events can be related to the following:

- **Operator activity**: These events might be relevant for security purposes and provide trails of any commands that had earlier been directed at network devices.
- **System activity**: These events provide for detailed execution traces. They can be useful in debugging a network but in general are simply turned off.
- **Activity on the network and services**: These events record the occurrence of service-related events, such as the fact that a call was initiated, and can provide data used for accounting.

**Informational events**: Any other kind of event. To be useful, any event includes at least the following information:

- The system from which the event originated.
- A time stamp of when the event occurred. (In some cases, applications receiving the event add a second time stamp to indicate when the event was actually received.)
- The type of event that has occurred.
- Event detail information.
Agent-Initiated Interactions: Events and Event-Based Management

The Case for Event-Based Management (monitoring network)

- Polling based: The manager relies on periodic requests and responses to monitor the state of the network.
- Event based: The manager relies on event messages that the agent sends automatically.

The Case for Event-Based Management

- Number of required communication exchanges for a given task
- Timeliness
- Request-processing capacity on the managed device
- Wastefulness
- Available management bandwidth
- Management application scale

Reliable Events

Management application must be confident that all event occurrences are indeed reported through event messages and that no events are missed.

The following techniques are used to make management events reliable:

- Use a reliable transport protocol over which management events are communicated.
- Add sequence numbers to the event information and provide the capability to replay or retrieve events upon request.
- Require events to be acknowledged.