Unit 5 Network Security and Management

1. Fundamental Aspects of Network Security

To establish a secure and robust network, engineers and operators must guarantee five major security functionalities. These pillars ensure that data is safe, accessible, and protected from malicious intent.

1. **Availability/Reliability:** Data and services must be accessible to legitimate users whenever they need them. This is achieved through highly available servers (often mirrored across geographical locations), redundant hardware components, and automatic protection switching mechanisms.
2. **Confidentiality:** This guarantees that private information remains private. Third parties, hackers, or unauthorized internal staff cannot access the network infrastructure, read transmitted data, or breach databases.
3. **Integrity:** Protection of the data systems against unauthorized changes. This ensures data is not altered, tampered with, or corrupted during transmission or storage.
4. **Authentication:** The process of login and user authorization. Before a user or device can access the network, they must prove who they are.
5. **Liability, Non-Repudiability:** Any access to the network and databases can be protocolled and logged. A user cannot deny having performed an action because the system has secure proof of their identity and actions.

2. Quality of Service (QoS) and Network Performance

Availability and performance are strongly related to the **Quality of Service (QoS)**. QoS is dependent on various parameters. Based on the ITU-T guidelines, the following technical parameters must be considered during network planning:

- **Data Throughput (Speed):** The speed of the access network.
- **Congestion:** Bottlenecks occurring in the backbone network.
- **End-to-End Delay (Latency):** The time it takes for data to travel from source to destination.
- **Delay-Variation (Jitter):** Fluctuations in the delay of packet delivery.
- **Packet Loss:** Loss of information during transmission.

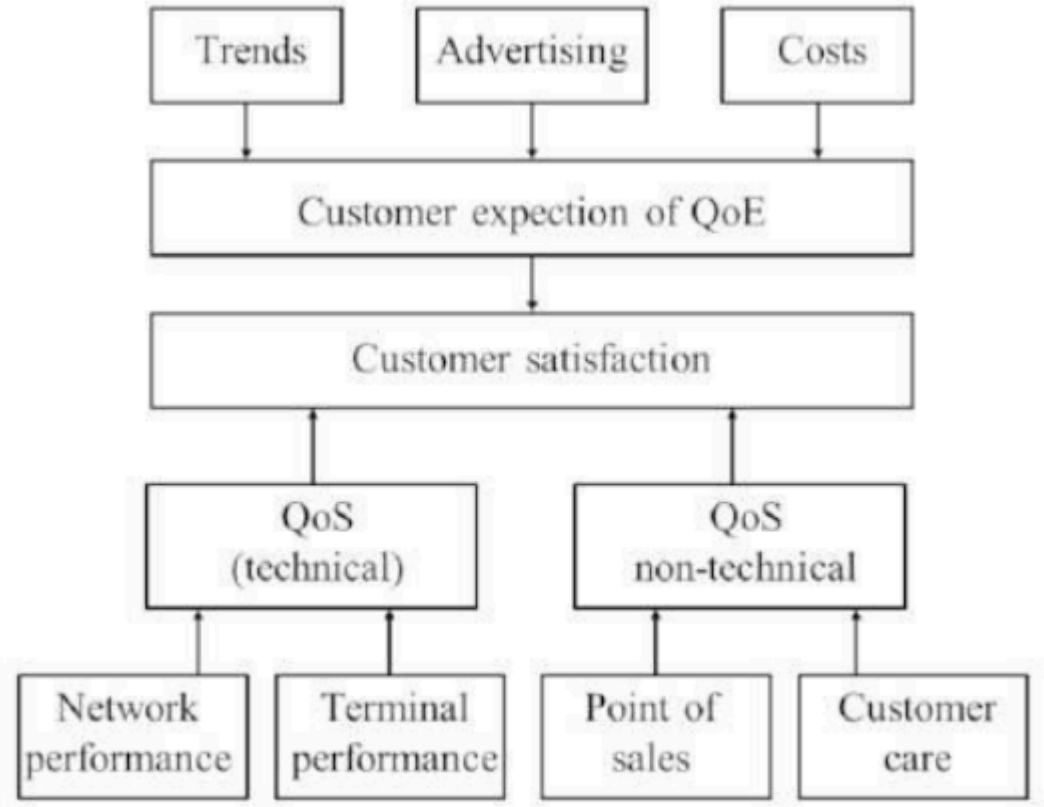


Figure 82 ITU-T QoS guidelines

These technical parameters directly influence the **Quality of Experience (QoE)**, which is the subjective performance from the user's point of view.

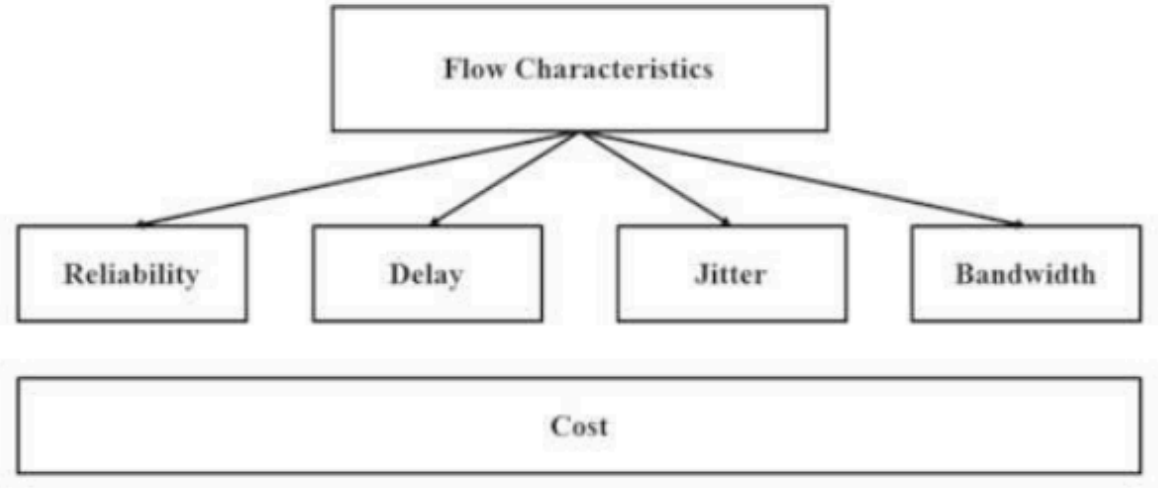


Figure 83 A subset of technical QoS parameters

2.1 Calculating Availability and Reliability

Availability (A) is the fundamental and most critical parameter for QoS. It is defined as:

$$A = \frac{MTBF}{MTBF + MTTR}$$

- **MTBF (Mean Time Between Failures):** The average continuous operating time before a failure.
- **MTTR (Mean Time To Repair):** The average time taken to fix the failure.

The **Non-Availability (Unavailability)**, denoted as N or , is:

$$N = 1 - A = \frac{MTTR}{MTBF + MTTR}$$

In network operations, reliability is tracked rigorously. Any second where the bit error rate exceeds 0.1% is classified as a **Severely Errored Second (SES)** and is counted as an outage time.

2.2 Serial vs. Parallel Systems (Redundancy)

Understanding how network components are connected helps in calculating total network reliability.

- **Serial Connections:** If systems are connected in a series, the overall availability is the product of all individual availabilities:

  $$A_{ttal} = A_1 \cdot A_2 \cdot A_3 \cdot \ldots \cdot A_n$$

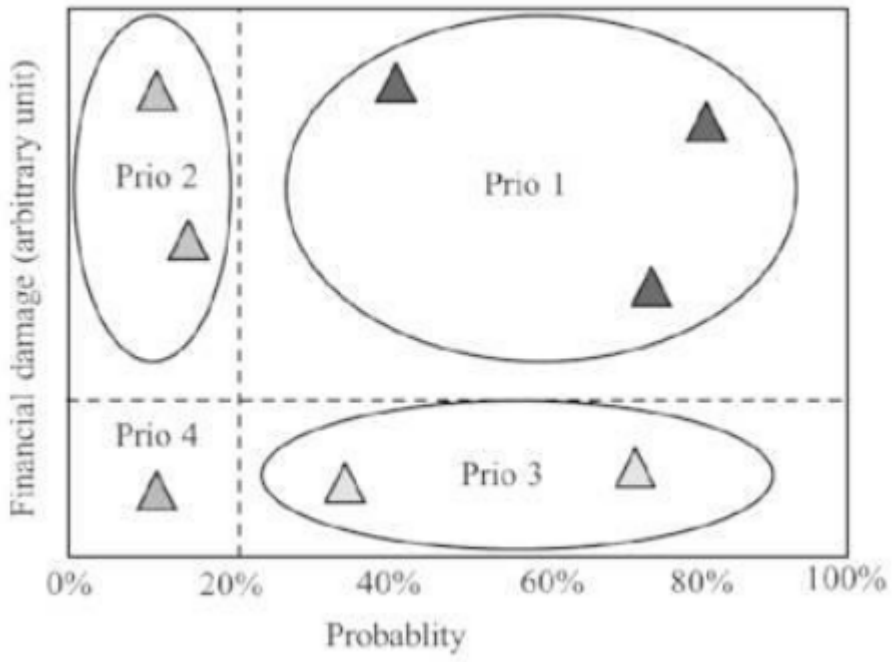
  Since A is always less than 1, the total availability becomes smaller. The chain is only as strong as its weakest link.
- **Parallel Connections (Redundancy):** If systems are connected in parallel (acting as backups to one another), the overall *unavailability* is the product of their individual unavailabilities:

  $$N_{ttal} = N_1 \cdot N_2 \cdot N_3 \cdot \ldots \cdot N_n$$

  Since N is a very small number, multiplying them results in an incredibly small total unavailability, massively boosting the overall availability. Real-world examples include redundant UPS (uninterruptible power supplies) and backup optical fiber transmission paths.

2.3 Risk Analysis

Corporate network security involves rigorous risk analysis to protect business-critical systems:



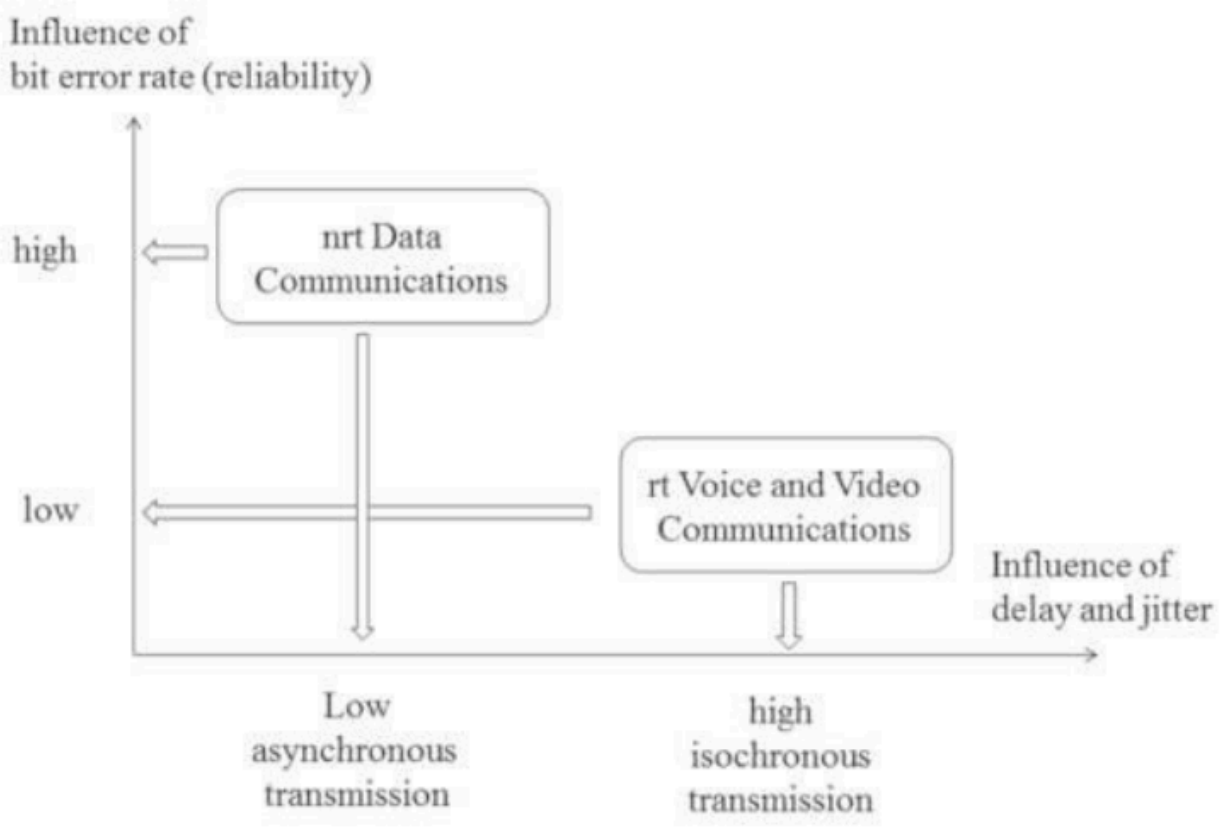
IT departments must calculate:

- The probability of a risk occurring (P_i).
- The expected downtime or outage time (T_i).
- The resulting financial damage ($_i$).

3. Traffic Management: Delay, Jitter, and Protocols

Networks carry different types of traffic, which react differently to network imperfections:

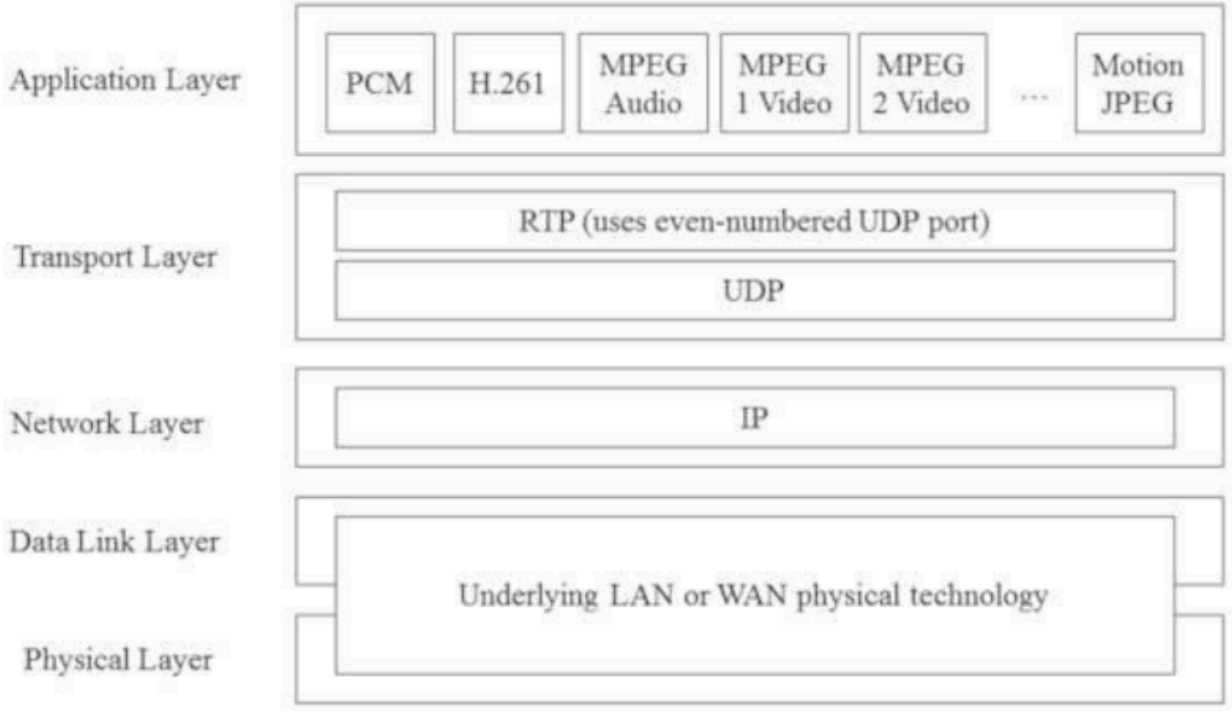
- **rt (Real-Time) Services:** e.g., Voice and Video. Highly sensitive to delay and jitter, but can tolerate some bit errors.
- **nrt (Non-Real-Time) Services:** e.g., Email and Data files. Highly sensitive to bit errors, but insensitive to delay and jitter.



3.1 Real-Time Transport Protocol (RTP) and SIP

Because IP packets take unpredictable routes, delay variation (jitter) occurs. A **playout buffer** is used at the receiver to smooth this out.

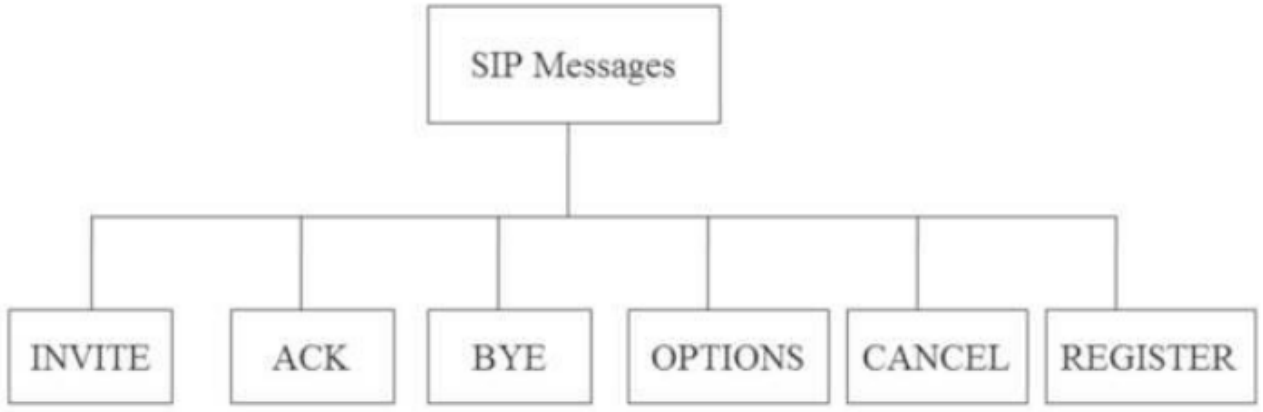
Standard protocols like TCP (causes too much delay due to retransmissions) and UDP (lacks timestamps) are inadequate for real-time traffic. Instead, the **Real-time Transport Protocol (RTP)** is used.



RTP Features:

- **Timestamps:** Indicate delay and help synchronize audio/video.
- **Sequence Numbers:** Guarantee the correct order of playout and detect packet loss.
- **SSRC/CSRC:** Identifies the source of the real-time application.

RTP is managed by **RTCP (Real-time Transport Control Protocol)**, which shares statistics on quality. To establish and manage these multimedia sessions, the **Session Initiation Protocol (SIP)** is used (using messages like INVITE, OPTIONS, BYE).



3.2 Scheduling and Traffic Shaping

To manage congestion, routers use scheduling and shaping:

- **Queuing/Scheduling:**
  - **FIFO:** First in, first out. No prioritization.
  - **Priority Queuing:** High-priority traffic goes first, which can starve low-priority traffic.
  - **Weighted Fair Queuing:** Assigns a certain number of available channels to different priorities for fair handling.
- **Traffic Shaping:**
  - **Leaky Bucket:** Traffic leaks out at a constant rate, ensuring smooth transmission.
  - **Token Bucket:** Uses "tokens" to allow fair transmission, accommodating bursts of data.

3.3 Integrated Services (IntServ) vs. Differentiated Services (DiffServ)

- **IntServ:** Reserves a dedicated channel end-to-end (like a telephone circuit) using RSVP. It provides great QoS but struggles with **scalability** over large internetworks.

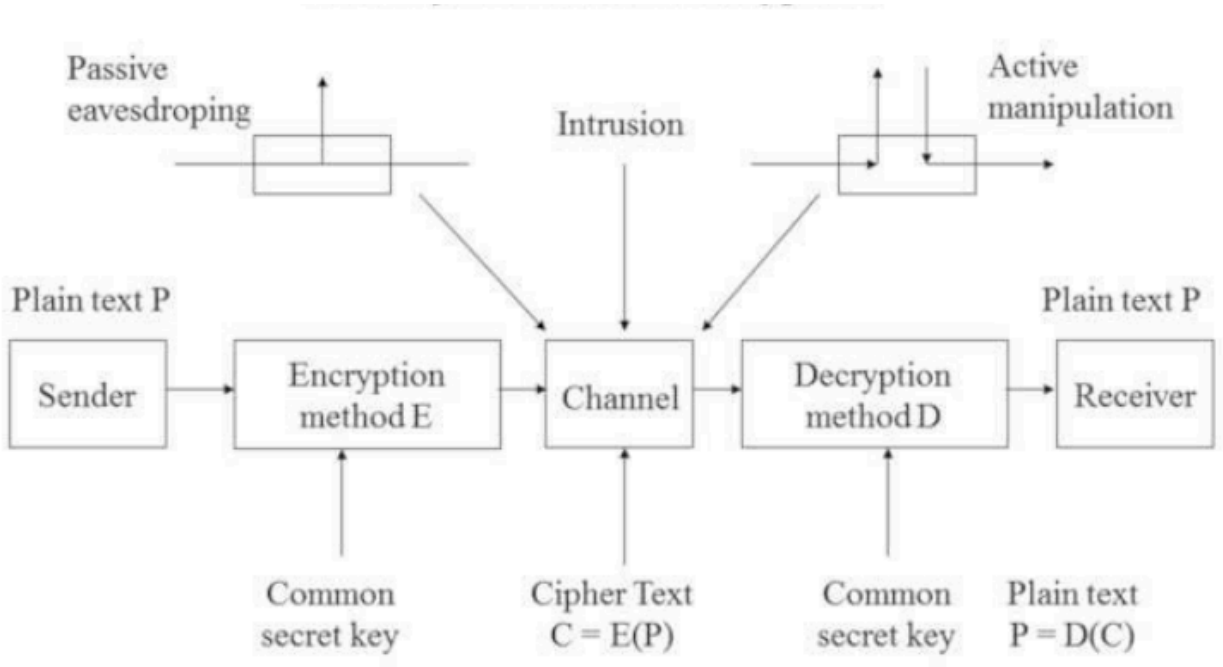
- **DiffServ:** Solves scalability by categorizing traffic into classes per-hop rather than reserving end-to-end paths. It uses **Per-Hop Behaviors (PHB)**:
  - **EF PHB (Expedited Forwarding):** Low loss, low latency, ensured bandwidth (Premium).
  - **AF PHB (Assured Forwarding):** Prioritized as long as it doesn't exceed its traffic profile.
  - **Default PHB:** Best-effort traffic.

4. Cryptography: Symmetrical and Asymmetrical Encryption

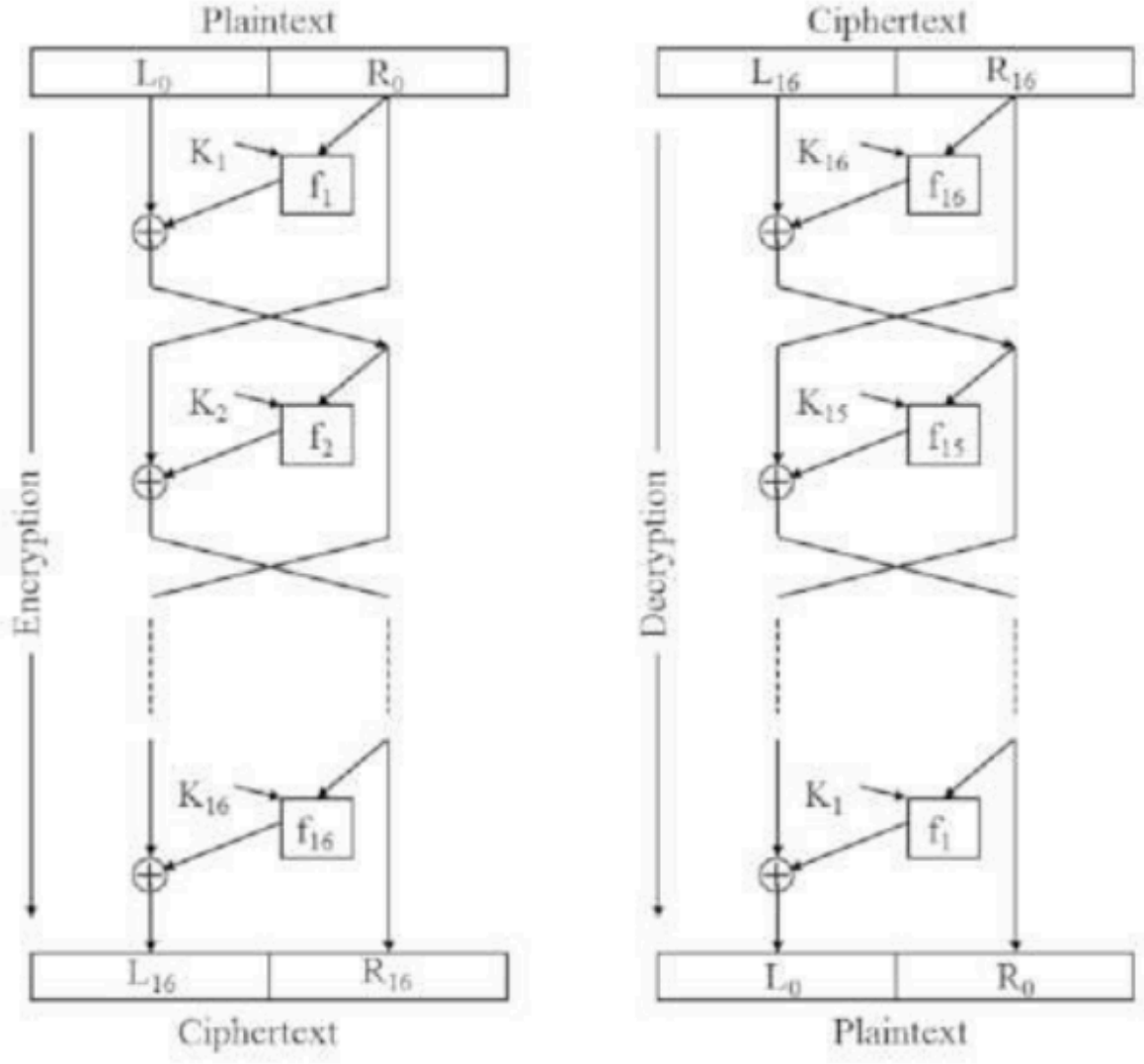
Cryptography conceals secret information to ensure confidentiality, authenticity, and integrity.

4.1 Symmetrical Encryption

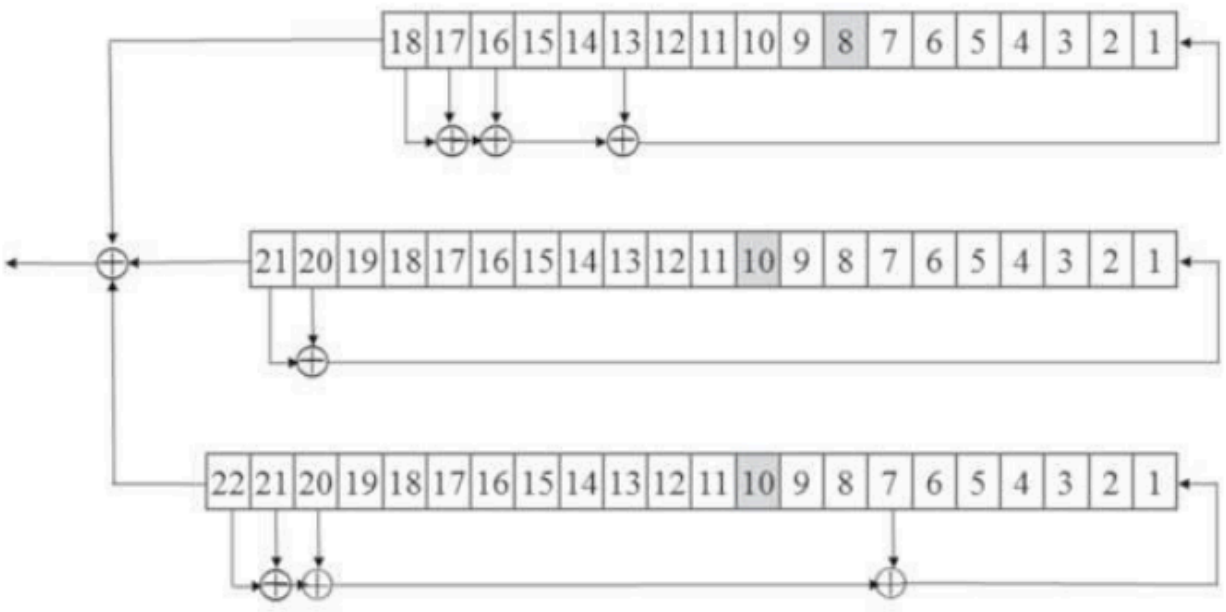
Both sender and receiver use the **same secret key** for encryption and decryption.



- **Classical Ciphers:** e.g., Caesar Cipher (shifting the alphabet). Easily cracked via statistical frequency analysis.
- **Modern Block Ciphers:** Process data in fixed blocks using boolean logic (AND, OR, XOR).
  - **DES (Data Encryption Standard):** Uses a 64-bit block and 56-bit key through a 16-step **Feistel network**.
  - **3DES:** Cascades DES three times to defeat brute-force attacks.
  - **AES (Advanced Encryption Standard):** Replaced DES. Uses 128, 192, or 256-bit keys and provides high security.



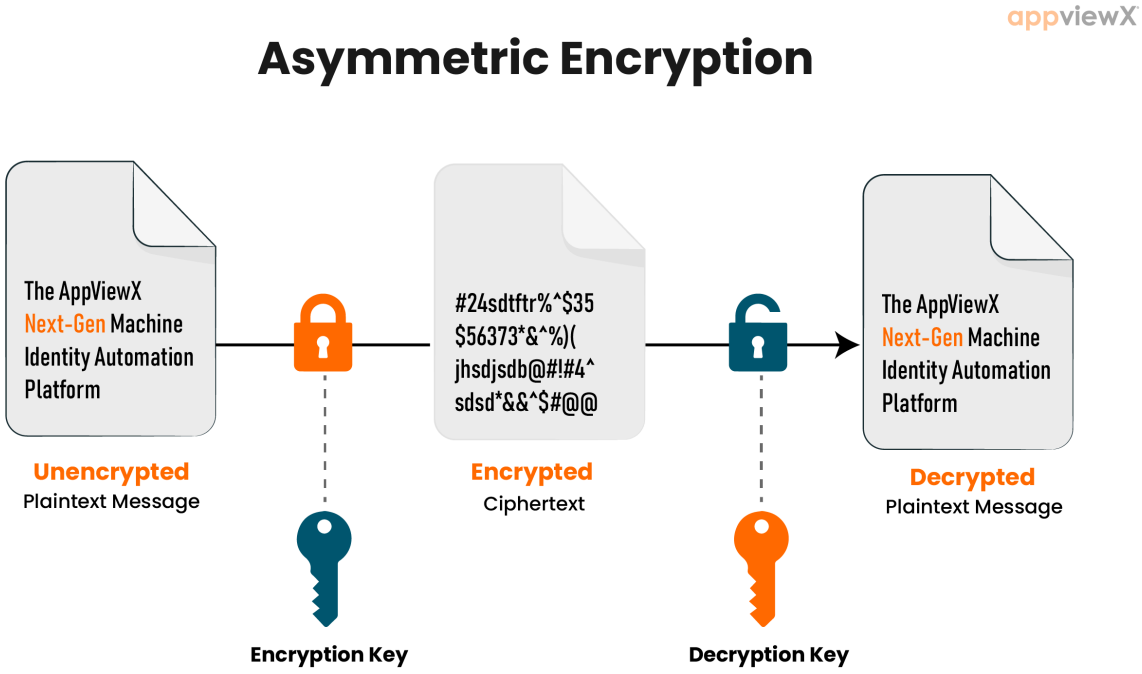
- **Stream Ciphers:** Encrypt plaintext bits continuously with a pseudo-random key stream.
  - **A5/1:** Used in GSM mobile networks. Uses linear feedback shift registers (LFSR) to generate a pseudo-random key stream that is XORed with the payload data burst.



The Main Problem: Symmetrical encryption is fast, but securely exchanging the shared secret key between the sender and receiver is very difficult (Key Distribution Problem).

4.2 Asymmetrical Encryption

Uses different keys: a **Public Key** (openly shared to encrypt data) and a **Private Key** (kept strictly secret to decrypt data).



- **RSA:** Relies on the mathematical difficulty of prime number factoring and modulus operations.
- **Diffie-Hellman:** A protocol allowing two parties to securely agree on a common key over an insecure channel by exchanging partial mathematical values.

Asymmetrical encryption solves the key exchange problem but is much slower. Modern systems usually use asymmetrical encryption to securely exchange a symmetrical key, and then use symmetrical encryption for the actual data.

5. Authentication, Hash-Values, and Integrity Checks

Mobile networks (like GSM) authenticate users securely using algorithms stored on the SIM card and the Authentication Center (AuC).

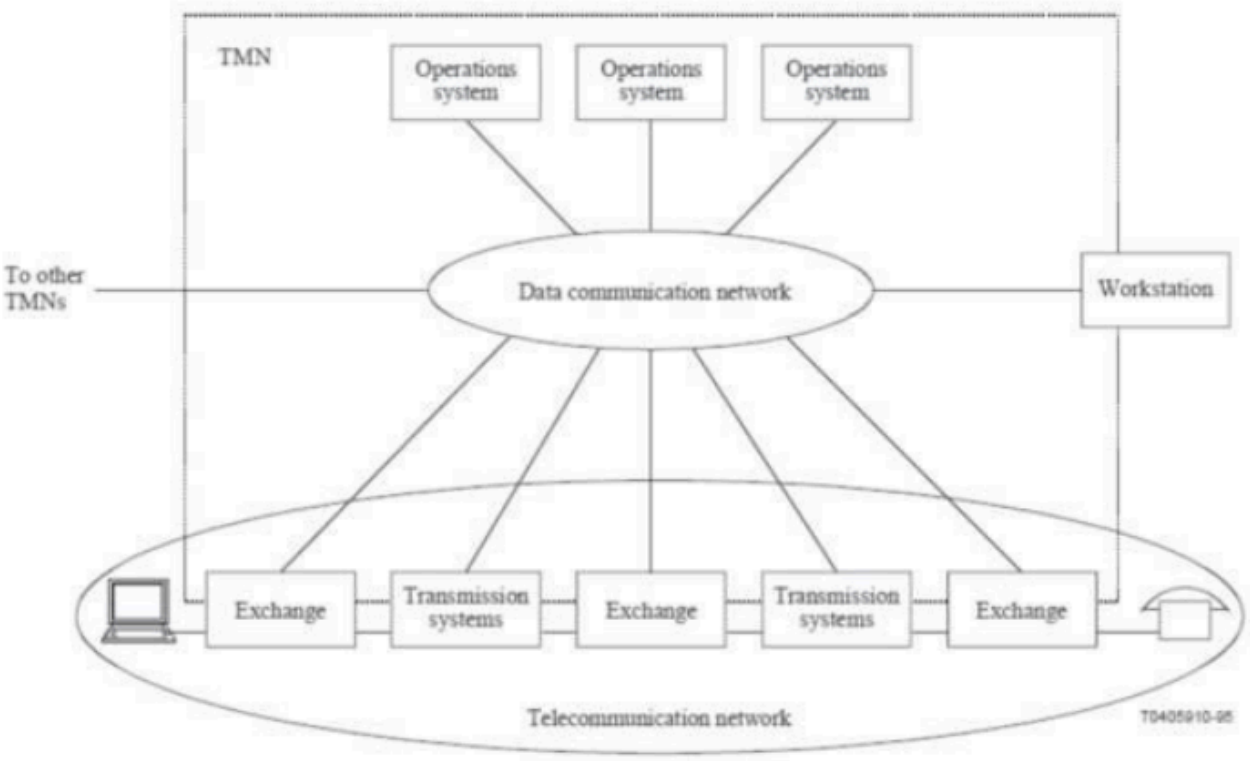
- **Authentication (A8 Algorithm):** The SIM card contains a highly secret 128-bit subscriber key (Ki). The network sends a random number challenge (RAN). The A8 algorithm calculates a session cipher key (K) using Ki and RAN. This K is used for the A5 air-interface encryption.

- **Hash-Value / Integrity (A3 Algorithm):** Simultaneously, the A3 algorithm uses the same Ki and RAN to calculate a 32-bit hash called the **Signed Response (SRES)**. The phone sends the SRES back to the network. If it matches the network's own calculation, the user is authenticated.

6. Telecommunications Management Network (TMN)

TMN is standardized by the ITU-T to manage complex networks (ISDN, ATM, GSM, All-IP). It features four hierarchical layers:

1. **Business Management:** Analyzes trends, handles billing, and manages high-level business aspects.
2. **Service Management:** Handles the definition, administration, and charging of customer services.
3. **Network Management:** Distributes network resources, configures routing, and supervises the global network.
4. **Element Management:** Handles individual network elements (hardware/software maintenance, alarms, backups).

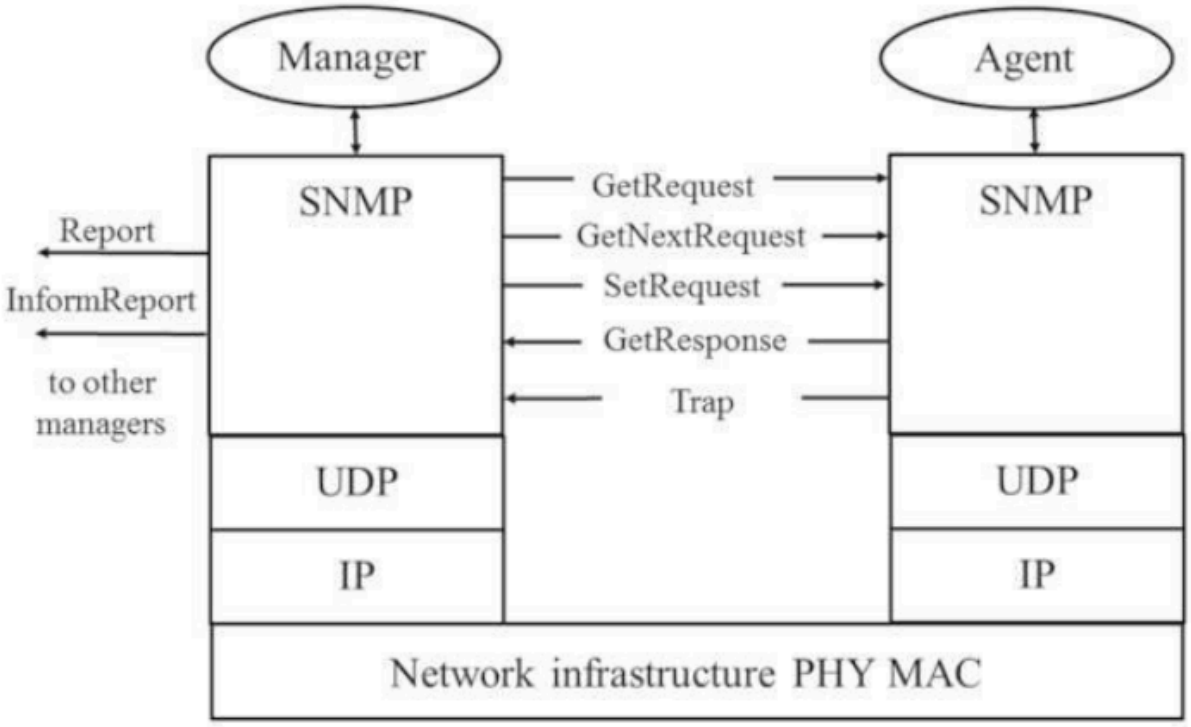


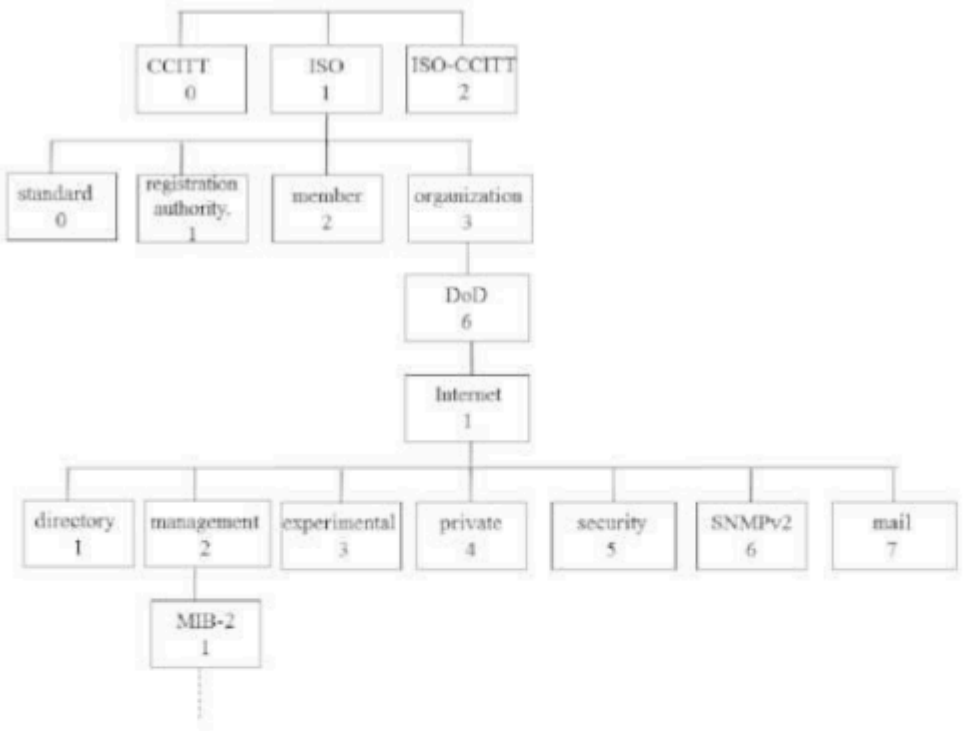
7. Simple Network Management Protocol (SNMP)

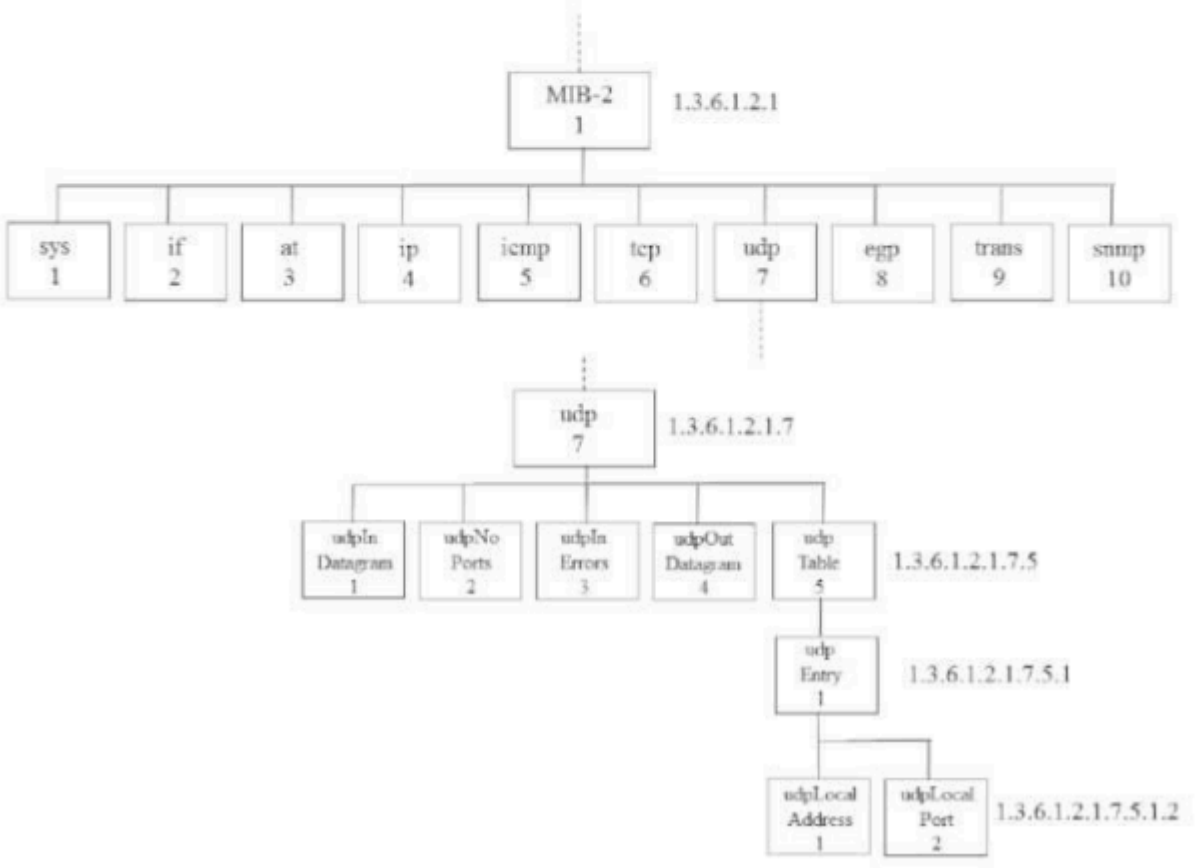
SNMP is the IETF standard for managing IP-based computer networks. It is a Client-Server system:

- **Manager (NMS):** The central monitoring station that requests data.
- **Agent:** Software installed on network elements that gathers data and reports to the Manager.

- **MIB (Management Information Base):** A distributed virtual database holding all Managed Objects.
- **MIT (Management Information Tree):** Organizes Managed Objects globally using unique identifiers.


Manager
Agent
SNMP
SNMP
GetRequest
GetNextRequest
SetRequest
GetResponse
Trap
Report
InformReport
to other
managers
UDP
UDP
IP
IP
Network infrastructure PHY MAC





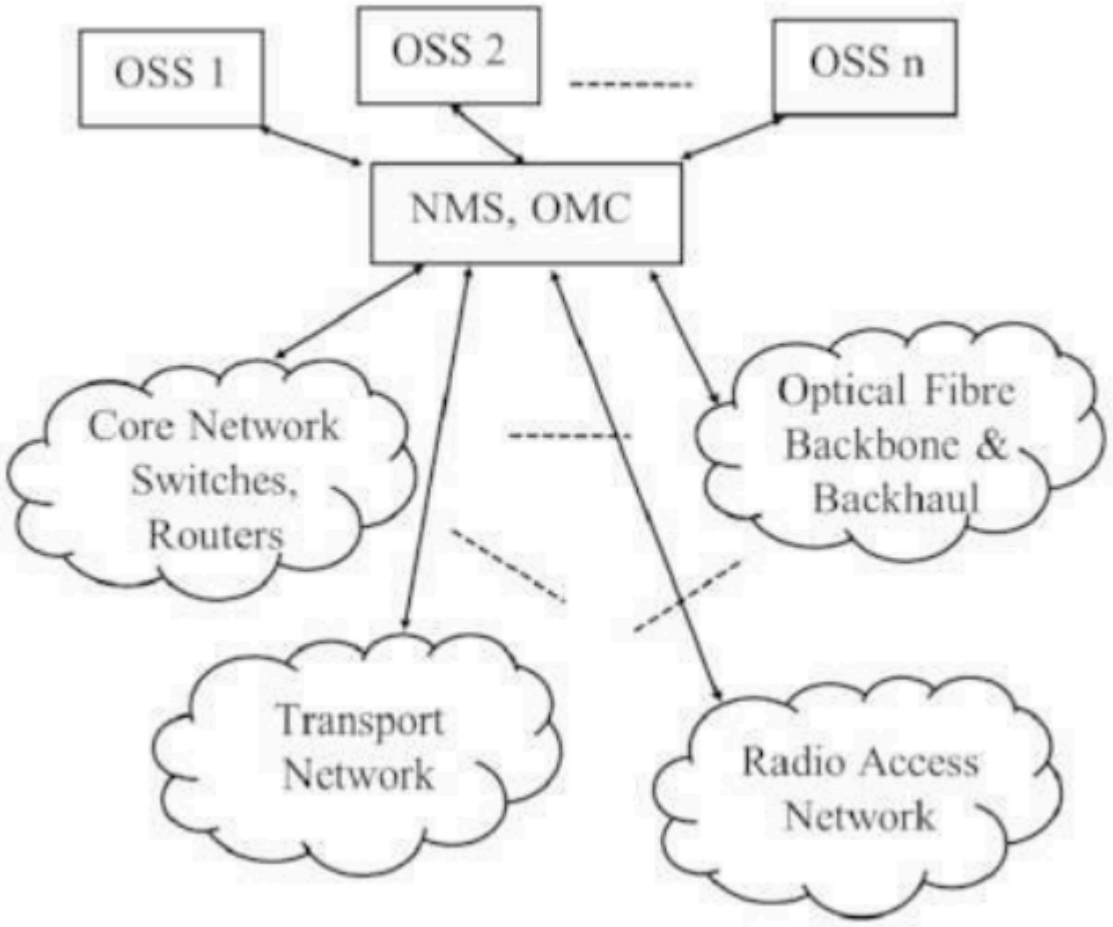
SNMP Operations: The Manager uses `GetRequest` to ask for data and `SetRequest` to change configurations. The Agent responds with `GetResponse`. Critically, if an Agent detects an error, it can send an unprompted `Trap` alarm to the Manager.

8. Functionalities of Network Management (FCAPS)

Network Management Systems (NMS) or Operation Maintenance Centers (OMC) perform five critical tasks:

1. **Configuration Management:** Provisioning new circuits, executing SW-updates, configuring hardware, and documenting assets.
2. **Fault Management:** Recognizing, localizing, and troubleshooting failures. Includes reactive fixes and proactive maintenance.
3. **Performance Management:** Monitoring QoS, congestion, delay, bit error rates, and traffic measurements.
4. **Accounting Management:** Determining the usage of network resources for customer billing.
5. **Security Management:** Protecting management info, handling encryption keys, and stopping fraud or Denial of Service (DoS) attacks.

Network operators manage complex multi-vendor networks. The goal of the NMS is to monitor all these subsystems (Optical backbone, GSM/LTE/5G access, switches) in parallel to prevent outages.



9. Trends and Future Developments

- **Improved Mobile & 6G:** Using beamforming, MU-MIMO, and mmWaves/THz frequencies. **Software Defined Radio (SDR)** and **Network Function Virtualization (NFV)** allow **Network Slicing** to provide tailored QoS for different services (e.g., ultra-reliable low latency for autonomous driving). 6G targets 1 Tbps speeds and 0.1 ms latency.

- **Optical Fibers: FTTH** (Fibre to the Home) and **FTTBS** (Fibre to the Base Station) are expanding to replace copper lines and handle 5G/6G backhaul traffic.
- **Coherent Optical Communications:** Using higher-order modulation (like 256QAM) and DWDM to transmit tens of Terabits per second over a single fiber pair.
- **Deep Space Optical Communications (DSOC):** NASA and ESA are investigating laser communications to replace RF in space, offering smaller footprints and vastly higher data rates.
- **AI & Green IT:** Machine learning and Big Data are being used for intelligent traffic transmission. Meanwhile, Extreme Large Scale Integration is reducing hardware size and power consumption to combat climate change.

Links:

Unit 1 Information Theory and Communication Technologies

Unit 2 Wireless Communication Technologies

Unit 3 Cellular Mobile Networks

Unit 4 Free Space Optical Communications

Unit 5 Network Security and Management

Social Network Analysis

Conversational AI