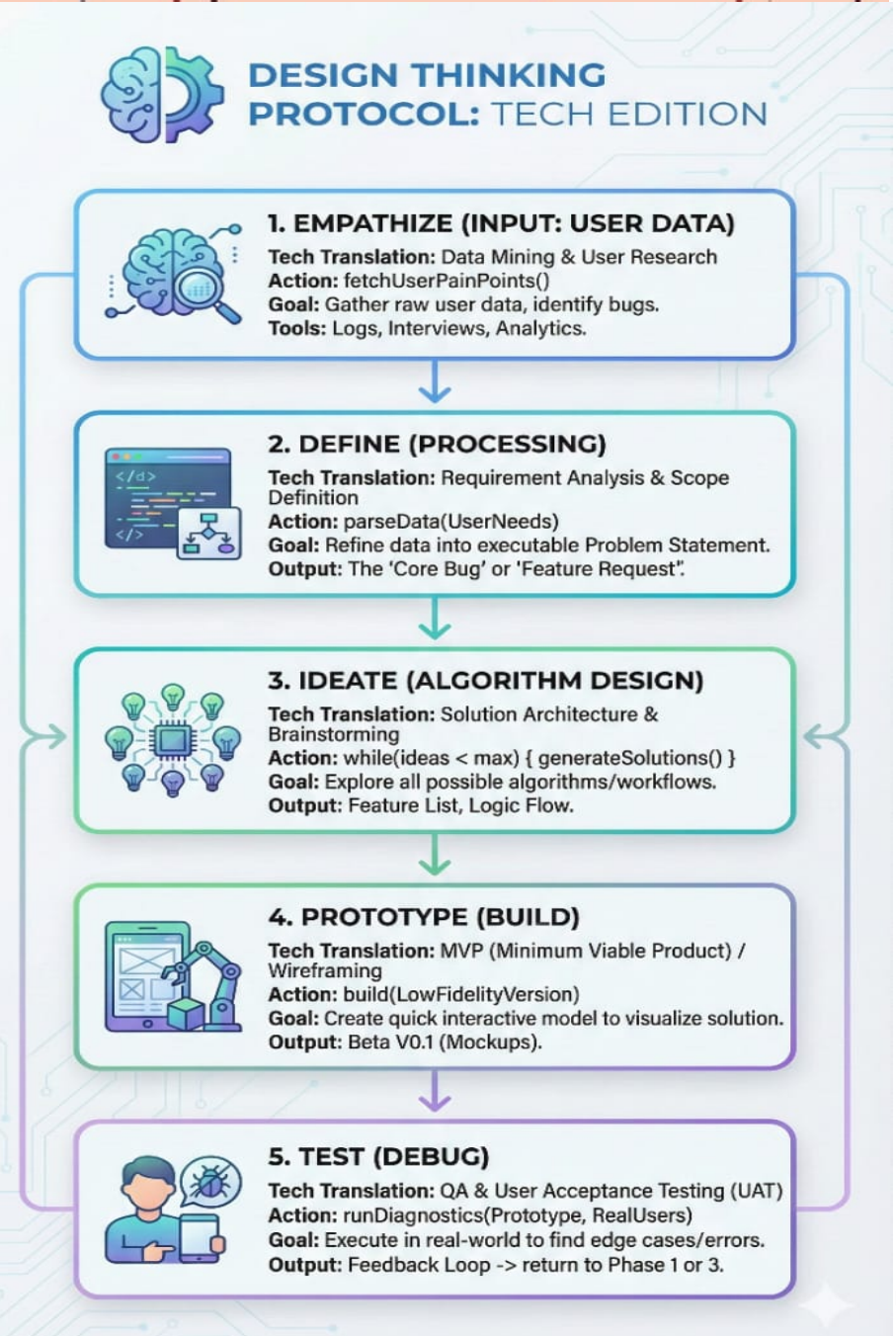
# 23ITT204 - COMPUTER NETWORK

## UNIT 1 - INTRODUCTION AND APPLICATION LAYER

## SNMP




# Introduction to SNMP: The Backbone of Network Management

Discover how a decades-old protocol continues to power network monitoring and management across the globe, keeping critical infrastructure running smoothly 24/7.

# What is SNMP?

SNMP (SimpleNetwork Management Protocol) is an industry-standard protocol for monitoring and managing network devices remotely. Operating at the application layer of the TCP/IP suite, it enables seamless communication between a central management station and agents deployed on network devices.

The protocol supports diverse hardware including routers, switches, servers, printers, and IoT devices. Network administrators use SNMP to query device status, configure settings remotely, and receive real-time alerts (traps) when critical network events occur.

### QueryDeviceStatus

Poll devices for performance metrics, health indicators, and operational data

### Configure Settings

Remotely adjust device parameters and update configurations across the network

### Receive Alerts

Get instant notifications when devices detect faults, threshold breaches, or anomalies

ARCHITECTURE

# SNMP Architecture & Versions

## Core Architecture Components

1

### Manager

The network management station (NMS) that orchestrates monitoring activities by sending requests to agents and processing responses and trap notifications. It provides the central dashboard for administrators.

2

### Agent

Lightweight software running on managed devices that maintains a local Management Information Base (MIB) containing device-specific data. Agents respond to manager queries and send autonomous trap alerts.

3

### MIB

A hierarchical database structure defining all manageable objects with unique Object Identifiers (OIDs). Think of it as a standardized data dictionary that ensures consistent device communication.

## Evolution Across Versions

### SNMP1 (1988)

Original version withbasic monitoring capabilities and community string authentication. Simple but lacked robust security features.

1

2

### SNMP2 (1996)

Enhanced performance with bulk data retrieval operations and improved error handling. Still used community-based security model.

3

### SNMP3 (2004)

Modern standard featuring strong authentication, message encryption, and access control. Addresses enterprise security requirements with user-based security model.

IMPACT

# Why SNMP Matters Today


## Real-Time Visibility

SNMP enables continuous monitoring across enterprise and service provider networks, providing instant fault detection and performance metrics that keep operations running smoothly.

## Universal Compatibility

Standardized MIBs allow seamless management of devices from countless vendors, creating a unified view of heterogeneous network environments without proprietary tools.

## Enterprise-Grade Security

SNMP3's authentication and encryption capabilities address modern cyber threats, making it suitable for securing mission-critical infrastructure in today's threat landscape.

> SNMP's elegant simplicity combined with powerful extensibility keeps it indispensable for managing increasingly complex IP networks, from small offices to global telecommunications infrastructure.