# NETWORK DESIGN

Network design methodology

- SONA provides built-in manageability, configuration management, performance monitoring, fault detection, and analysis tools. SONA provides an efficient design with the goal of reducing the total cost of ownership (TCO) and maximizing the company's existing resources when application demands increase.
- The methodology is derived from PPDIOO.

PPDIOO Lifecycle Model

1. Prepare
2. Plan
3. Design
4. Implement
5. Operate
6. Optimize

PPDIOO Life cycle
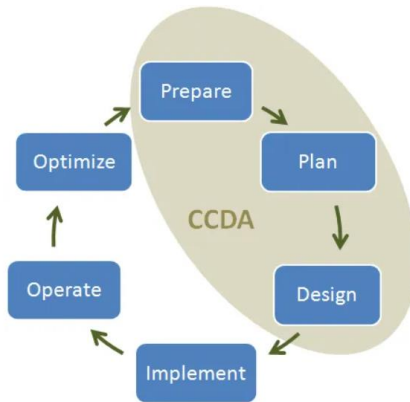
Prepare Phase:
- ➢ This is where you establish the company's requirements and goals.
- ➢ The IT and the network/security infrastructure must always be in line with the company's goals and business requirements.
- ➢ At this stage, a network strategy and high-level architecture to support that strategy is developed.
- ➢ Possible technologies that can support that architecture must be identified.
- ➢ A business case must also be established in order to have a financial justification for the overall network strategy.
- ➢ Representations from the company's board of directors (CIO, COO, etc.) might be involved in this phase.

Plan Phase:

➢ Planning is the most underutilized phase in the PPDIOO process.

➢ This includes identifying the decision- and policy-makers, and determining the fundamental network requirements (who needs what services and when).

➢ The plan phase is where the entire information gathering process is completed, and the network and security requirements are identified, as well as identifying the legislation to which the company or its customers must adhere.

➢ The network security system lifecycle must be analyzed carefully, including the company's needs and risk analysis.

➢ The security policies, guidelines, and processes must be evaluated, along with the security system that is in place or with possible future security system acquisitions, such as the Cisco Adaptive Security Appliances (ASAs).

- ➢ Planning also includes the study of best practices and case studies, and then putting into place the security operations, responses, monitoring, and compliance.

- ➢ The network management processes also must be considered in this phase because they are closely related with the network infrastructure.

- ➢ This includes fault management to detect and correct specific problems; configuration management that helps in establishing a network baseline and in developing a configuration tracking process (for networking appliances and devices); accounting management that keeps track of circuits for billing of services; performance management to monitor the network's effectiveness in delivering packets; and security management.

- ➢ In the plan phase, you will characterize the network and perform an analysis against best-practice architectures, and look at the operational environment overall.

Design Phase:

➢ The next phase involves designing the network according to the company's policies, procedures, business goals, and available budget and technologies.

➢ The design phase also might mean meeting with policy-makers, team leaders, and end-users in the process of gathering and analyzing data, and auditing all key activities.

➢ Results of the design phase are the basis for the approach taken in the next phase, which involves implementation.

➢ The focus of the CCDA blueprint is comprised of the first three PPDIOO phases – prepare, plan, and design – among which the design phase is the most complex.

Implement Phase:

➤ The competitive nature of business, and the rush to market products and services, forces many organizations to skip the first three phases of the PPDIOO lifecycle model and start with the implement phase.

➤ The implement phase involves constructing the network infrastructure with the best affordable technologies based on all the design specifications

➤ The implement phase includes configuration, installment, maintenance, and so on. This is where the new equipment is installed and configured using the command line interface (CLI) or graphical tools (SDM, ASDM, etc.).

➤ Old devices might be replaced with new devices, or some components might be upgraded (memory, operating systems, etc.).

➤ Planned network changes should occur here, and they should be communicated through control channels in meetings and receive the appropriate approvals.

➤ Each step in the implement phase should have a description, detailed implementation guidelines, a time estimate, and instruction steps for falling back to a previous state in case something goes wrong.

Operate Phase:

➢ The operate phase is the final proof that the network design was implemented properly.

➢ Performance monitoring, fault detection, and operational parameters will be confirmed in this phase. This will also provide the data used for the final phase.

➢ This phase involves maintaining the day-to-day operational maintenance and health of the network infrastructure.

➢ This includes managing the network components, monitoring, conducting analysis and creating reports, routine maintenance, managing the upgrades of the systems (hardware, software, of firmware), managing performance, and identifying and correcting any network faults or security incidences.

➢ This final test of the design process involves analyzing the actual operations of the implemented network system.

➢ Network management stations (NMSs) should monitor network health parameters, through SNMP traps (and certain thresholds reached) or other real-time monitoring solutions.

Optimize Phase:

➢ Optimizing involves proactive and aggressive management and control over the network. Problems must be identified quickly so that troubleshooting can take place to assure fault detection.

➢ This phase is crucial because it is often followed by another planning or design session in order to redesign the implementation, which makes these phases all the more important. Much time and money might be invested into the optimize phase if some failures occur in the initial planning and design phases.

➢ Optimization refers to proactive network management, meaning identifying and resolving issues before they move throughout the entire network. The optimize phase might also generate a modified network design if too many problems appear in the implement and operate phases. Sometimes, you might need to go back to the design phase in order to solve those problems and implement new solutions.

Benefits of a Lifecycle Approach

1. Lowering the total cost of network ownership
2. Increasing network availability
3. Improving business agility
4. Speeding access to applications and services

Lowering costs by these actions:

- Identifying and validating technology requirements
- Planning for infrastructure changes and resource requirements
- Developing a sound network design aligned with technical requirements and business goals
- Accelerating successful implementation
- Improving the efficiency of your network and of the staff supporting it
- Reducing operating expenses by improving the efficiency of operational processes and tools

Improves high availability of networks by these actions:

➢ Assessing the network's security state and its capability to support the proposed design

➢ Specifying the correct set of hardware and software releases, and keeping them operational and current

➢ Producing a sound operations design and validating network operations

➢ Staging and testing the proposed system before deployment

➢ Improving staff skills

➢ Proactively monitoring the system and assessing availability trends and alerts

➢ Proactively identifying security breaches and defining remediation plans

Improving business agility by the following actions:

➢ Establishing business requirements and technology strategies

➢ Readying sites to support the system that you want to implement

➢ Integrating technical requirements and business goals into a detailed design and demonstrating that the network is functioning as specified

➢ Expertly installing, configuring, and integrating system components

➢ Continually enhancing performance

Accelerates access to network applications and services by the following actions:

➢ Assessing and improving operational preparedness to support current and planned network technologies and services

➢ Improving service-delivery efficiency and effectiveness by increasing availability, resource capacity, and performance

➢ Improving the availability, reliability, and stability of the network and the applications running on it

➢ Managing and resolving problems affecting your system and keeping software applications current