This chapter covers the following subjects:

- Cisco Architectures for the Enterprise
- Prepare, Plan, Design, Implement, Operate, and Optimize Phases
- Identifying Customer Requirements
- Characterizing the Existing Network
- Designing the Network Topology and Solutions

CHAPTER 1

Network Design Methodology

Networks can become complex and difficult to manage. Network architectures and design methodologies help you manage the complexities of networks. This chapter provides an overview of Cisco's architectures for the enterprise and the Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) network life cycle. This chapter also describes the six network life cycle phases and steps in design methodology.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz helps you identify your strengths and deficiencies in this chapter's topics.

The ten-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you determine how to spend your limited study time.

Table 1-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 1-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
Cisco Architectures for the Enterprise	1, 2, 3, 4
Prepare, Plan, Design, Implement, Operate, and Optimize Phases	5, 6
Identifying Customer Requirements	9, 10
Characterizing the Existing Network	7
Designing the Network Topology and Solutions	8

1. Which are the three Cisco network architectures for the enterprise?
   a. Hierarchical
   b. Borderless
   c. Integrated
   d. Data center/virtualization
   e. OSI model
   f. Collaboration
2. Which technology forces affect decisions for the enterprise network?
   a. Removal of borders
   b. Virtualization
   c. Growth of applications
   d. 10GigEthernet
   e. Regulation
   f. ROI
   g. Competitiveness
3. Network resiliency and control occurs in which layer of the borderless network architecture?
   a. Policy and Control
   b. Borderless Network Services
   c. Borderless User Services
   d. Connection Management
4. Presence occurs in which collaboration architecture layer?
   a. Communication and Collaboration
   b. Collaboration Services
   c. Infrastructure
   d. Media Services
5. Which of the following is the correct order of the six phases of PPDIOO?
   a. Prepare, Plan, Design, Implement, Operate, Optimize
   b. Plan, Prepare, Design, Implement, Operate, Optimize
   c. Prepare, Plan, Design, Implement, Optimize, Operate
   d. Plan, Prepare, Design, Implement, Optimize, Operate

6. The PPDIOO design methodology includes which steps? (Select all that apply.)

   a. Identify customer requirements.
   b. Design the network topology.
   c. Characterize the network.
   d. Optimize the network.
   e. Operate the network.
   f. Implement the network.
   g. Prepare and plan.

7. What are the three primary sources of information in a network audit?

   a. CIO, network manager, network engineer
   b. Network manager, management software, CDP
   c. Network discovery, CDP, SNMP
   d. Existing documentation, management software, new management tools

8. Which design solution states that a design must start from the application layer and finish in the physical layer?

   a. OSI model
   b. PPDIOO
   c. Hierarchical architecture
   d. Top-down

9. Budget and personnel limitations are examples of what?

   a. Organization requirements
   b. Organization constraints
   c. Technical goals
   d. Technical constraints

10. Improving network response time and reliability are examples of what?

    a. Organization requirements
    b. Organization constraints
    c. Technical goals
    d. Technical constraints

Foundation Topics

With the complexities of networks, it is necessary to use architectures and methodologies in network design to support business goals. The Cisco Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) network life cycle defines a continuous cycle of phases in a network's life. Each phase includes key steps in successful network planning, design, implementation, and operation. The top-down design approach to network design adapts the network infrastructure to the network applications' needs.

Cisco Architectures for the Enterprise

With the constant evolution of networks, Cisco keeps updating its enterprise architectures and frameworks. Business drivers can affect network architecture and technology forces that affect business.

Business forces affecting decisions for the enterprise network include the following:

Key Topic

- **Return on investment:** Companies expect a return (be it cost savings or increased productivity) on its investments of network infrastructure. The solutions need to use technology to work within a business solution.
- **Regulation:** Companies need to meet industry regulations; for example, the Health Insurance Portability and Accountability Act (HIPAA) for the health insurance industry and Payment Card Industry Data Security Standard (PCI DSS) for the credit card industry.
- **Competitiveness:** To maintain a competitive edge, companies need to use technology to make them more competitive than other businesses.

The technology forces affecting decisions for the enterprise network are

- **Removal of borders:** Traditional network boundaries have been removed. Access to network resources need to be enabled from branch offices, teleworkers, home offices, mobile devices, customers, and partner networks.
- **Virtualization:** Allows for the maximization of efficiencies through the reduction of hardware, power consumption, heating and cooling costs, facilities space, and management effort. Virtualization and its benefits are a key goal for almost all organization. It has gained popularity by industry leaders such as VMware.
- **Growth of applications:** Customers continue to ask for new products, service offerings, improved customer service, greater security, and customization flexibility—all at a lower cost.

IT optimization areas are divided into three groups:

- Data center
- Network
- Applications

Each group has its own experts, budget, and challenges.

Cisco has created an interwoven framework to create three architectures for each group that provides for optimization at an individual level and the integration with other areas:

- Borderless networks architecture
- Collaboration architecture
- Data center/virtualization architecture

These three architectures are shown in Figure 1-1 and are covered in more detail in the following sections.

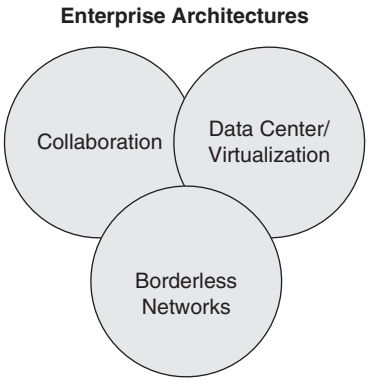

Figure 1-1 *Cisco Enterprise Architectures*

Borderless Networks Architecture

Cisco Borderless Network Architecture is a next-generation solution that enables connectivity to anyone and anything, anywhere, and at any time. The connectivity needs to be secure, reliable, and seamless. The borderless architecture optimizes both business and network performance.

As shown in Figure 1-2, the Cisco borderless network architecture blueprint consists of four major blocks:

- **Policy and Control:** Policies are applied to all users and devices across the architecture.
- **Network Services:** These services include resiliency and control. Cisco EnergyWise and Medianet provide capabilities to borderless networks.
- **User Services:** These services include mobility, performance, and security.
- **Connection Management:** This block delivers secure access anytime and anywhere, regardless of how the network is accessed.

Collaboration Architecture

Cisco's collaboration architecture is composed of three layers:

- **Communication and Collaboration Applications:** This layer contains conferencing, customer care, enterprise social software, IP communications, messaging, mobile applications, and TelePresence.

- **Collaboration Services:** This layer contains services that support the collaboration applications: presence, location, session management, contact management, client frameworks, tagging, and policy and security management.
- **Infrastructure:** This layer is responsible for allowing collaboration anytime, from anywhere, on any device. It includes virtual machines, the network, and storage.

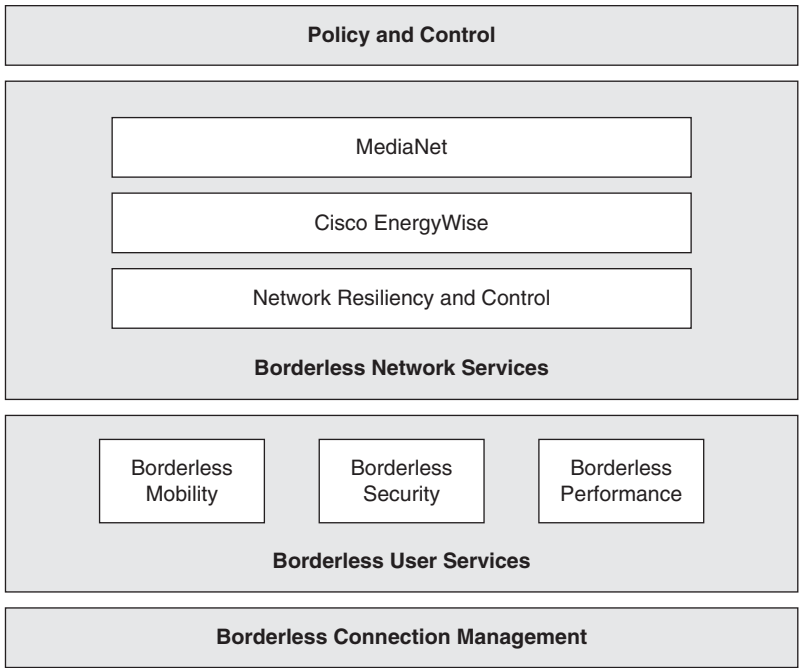

Figure 1-2 *Borderless Architecture*

Data Center/Virtualization Architecture

Cisco's data center/virtualization architecture is built upon Cisco Data Center 3.0. It comprises a comprehensive set of virtualization technologies and services that bring the network, computing, storage, and virtualization platforms together. Figure 1-3 shows the architecture framework for data centers.

Data center architecture and design is covered in Chapter 4, "Data Center Design."

Table 1-2 lists the benefits of Cisco network architectures.

Table 1-2 *Benefits of Cisco Network Architectures*

Benefit	Description
Functionality	Supports organizational requirements
Scalability	Supports growth and expansion of organizational tasks
Availability	Provides services reliability, anywhere and anytime

Table 1-2 *Benefits of Cisco Network Architectures*

Benefit	Description
Performance	Provides responsiveness, throughput, and utilization on a per-application basis
Manageability	Provides control, performance monitoring, and fault detection
Efficiency	Provides network services and infrastructure with a reasonable operational costs and appropriate capital investment

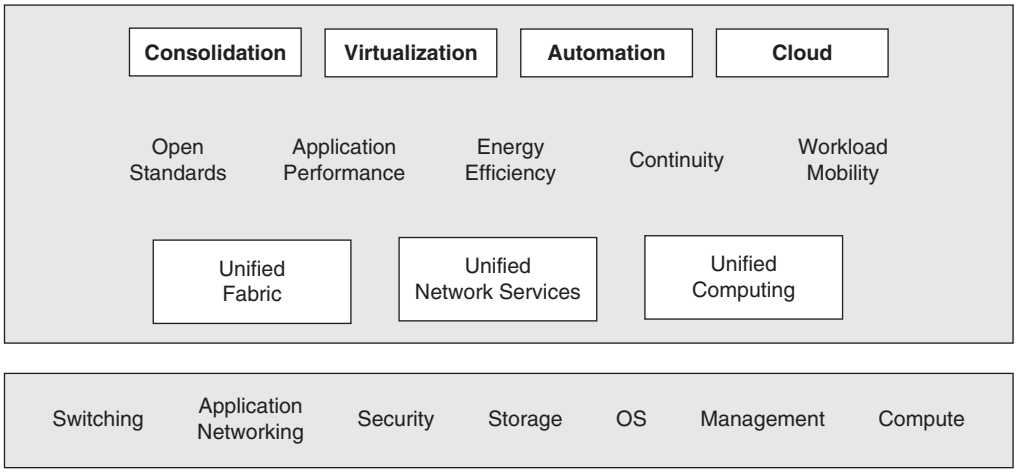

Figure 1-3 *Data Center Architecture Framework*

Prepare, Plan, Design, Implement, Operate, and Optimize Phases

Key Topic

Cisco has formalized a network's life cycle into six phases: Prepare, Plan, Design, Implement, Operate, and Optimize. These phases are collectively known as PPDIOO. The PPDIOO life cycle provides four main benefits:

- It lowers the total cost of ownership by validating technology requirements and planning for infrastructure changes and resource requirements.
- It increases network availability by producing a sound network design and validating the network operation.
- It improves business agility by establishing business requirements and technology strategies.
- It speeds access to applications and services by improving availability, reliability, security, scalability, and performance.

These benefits are realized by the actions listed in Tables 1-3 through 1-6.

Table 1-3 *Actions That Lower the Cost of Ownership*

Actions That Lower the Cost of Ownership
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 the network and the staff that supports it
Reducing operating expenses by improving the efficiency of operation processes and tools

Table 1-4 *Actions That Increase Network Availability*

Actions That Increase Network Availability
Assessing the state of the network and its ability to support the proposed design
Specifying the correct set of hardware and software releases and keeping them current
Producing a sound operations design and validating network operation
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

Table 1-5 *Actions That Improve Business Agility*

Actions That Improve Business Agility
Establishing business requirements and technology strategies
Readying sites to support the system that will be implemented
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

Table 1-6 *Actions That Accelerate Access to Applications and Services*

Actions That Accelerate Access to Applications and Services
Accessing 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 that run on it
Managing and resolving problems that affect the system and keeping software applications current

Figure 1-4 shows the PPDIOO network life cycle.

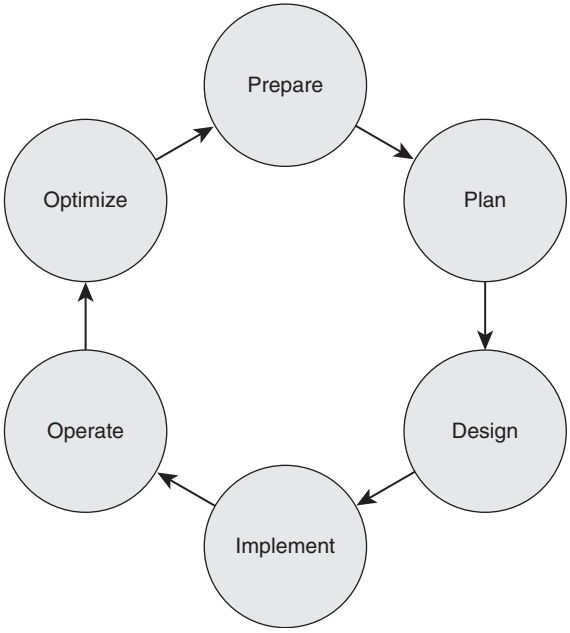

Figure 1-4 *Cisco PPDIOO Network Life Cycle*

The following sections discuss the PPDIOO phases in detail.

Prepare Phase

The Prepare phase establishes organization and business requirements, develops a network strategy, and proposes a high-level conceptual architecture to support the strategy. Technologies that support the architecture are identified. This phase creates a business case to establish a financial justification for a network strategy.

Plan Phase

The Plan phase identifies the network requirements based on goals, facilities, and user needs. This phase characterizes sites and assesses the network, performs a gap analysis against best-practice architectures, and looks at the operational environment. A project plan is developed to manage the tasks, responsible parties, milestones, and resources to do the design and implementation. The project plan aligns with the scope, cost, and resource parameters established with the original business requirements. This project plan is followed (and updated) during all phases of the cycle.

Design Phase

The network design is developed based on the technical and business requirements obtained from the previous phases. The network design specification is a comprehensive detailed design that meets current business and technical requirements. It provides high availability, reliability, security, scalability, and performance. The design includes network diagrams and an equipment list. The project plan is updated with more granular information for implementation. After the Design phase is approved, the Implement phase begins.

Implement Phase

New equipment is installed and configured, according to design specifications, in the Implement phase. New devices replace or augment the existing infrastructure. The project plan is followed during this phase. Planned network changes should be communicated in change control meetings, with necessary approvals to proceed. Each step in the implementation should includes a description, detailed implementation guidelines, estimated time to implement, rollback steps in case of a failure, and any additional reference information. As changes are implemented they are also tested before moving to the Operate phase.

Operate Phase

The Operate phase maintains the network's day-to-day operational health. Operations include managing and monitoring network components, routing maintenance, managing upgrades, managing performance, and identifying and correcting network faults. This phase is the design's final test. During operation, network management stations should monitor the network's general health and generate traps when certain thresholds are reached. Fault detection, correction, and performance monitoring events provide initial data for the optimize phase.

Optimize Phase

The Optimize phase involves proactive network management by identifying and resolving issues before they affect the network. The Optimize phase may create a modified network design if too many network problems arise, to improve performance issues, or to resolve application issues. The requirement for a modified network design leads to the network life cycle beginning.

Summary of PPDIOO Phases

Table 1-7 summarizes the PPDIOO phases.

Table 1-7 *PPDIOO Network Life Cycle Phases*

PPDIOO Phase	Description
Prepare	Establishes organization and business requirements, develops a network strategy, and proposes a high-level architecture
Plan	Identifies the network requirements by characterizing and assessing the network, performing a gap analysis
Design	Provides high availability, reliability, security, scalability, and performance
Implement	Installation and configuration of new equipment
Operate	Day-to-day network operations
Optimize	Proactive network management; modifications to the design

Design Methodology Under PPDIOO

The following sections focus on a design methodology for the first three phases of the PPDIOO methodology. This design methodology has three steps:

Step 1. Identifying customer network requirements

Step 2. Characterizing the existing network

Step 3. Designing the network topology and solutions

In Step 1, decision makers identify requirements, and a conceptual architecture is proposed. This step occurs in the PPDIOO Prepare phase.

In Step 2, the network is assessed, and a gap analysis is performed to determine the infrastructure necessary to meet the requirements. The network is assessed on function, performance, and quality. This step occurs in the PPDIOO Plan phase.

In Step 3, the network topology is designed to meet the requirements and close the network gaps identified in the previous steps. A detailed design document is prepared during this phase. Design solutions include network infrastructure, Voice over IP (VoIP), content networking, and intelligent network services. This set occurs in the PPDIOO Design phase.

Identifying Customer Design Requirements

To obtain customer requirements, you need to not only talk to network engineers, but also talk to business unit personnel and company managers. Networks are designed to support applications; you want to determine the network services that you need to support.

As shown in Figure 1-5, the steps to identify customer requirements are as follows:

Step 1. Identify network applications and services.

Step 2. Define the organizational goals.

Step 3. Define the possible organizational constraints.

Step 4. Define the technical goals.

Step 5. Define the possible technical constraints.

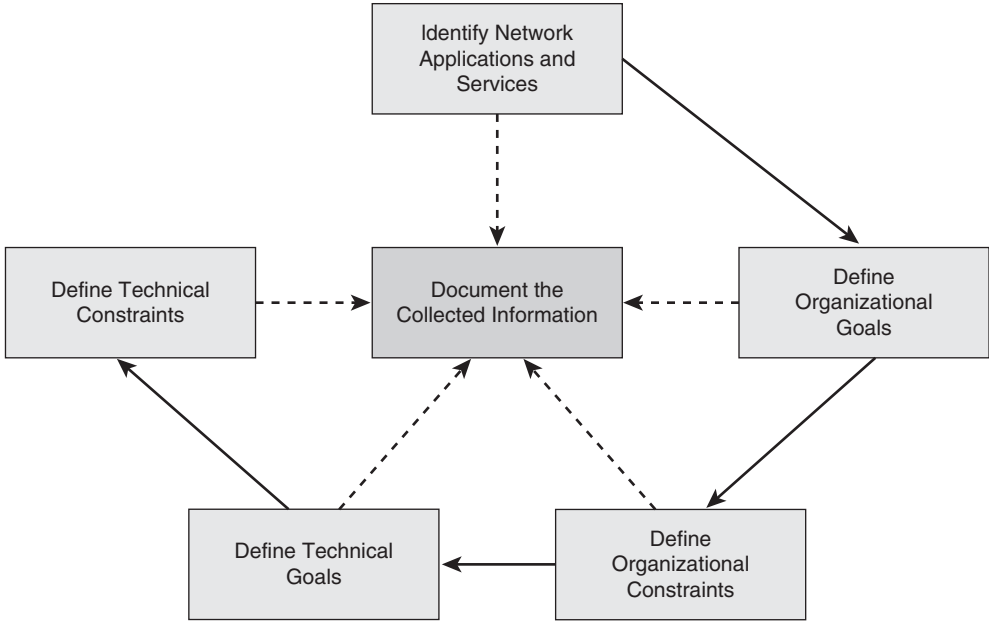

Figure 1-5 *Identifying Customer Requirements*

After you complete these steps, you then analyze the data and develop a network design.

You need to identify current and planned applications and determine the importance of each application. Is email as important as customer support? Is IP telephony being deployed? High-availability and high-bandwidth applications need to be identified for the design to accommodate their network requirements. A table identifying applications should list the following:

- **Planned application types:** Such as email, collaboration, voice, web browsing, file sharing, database
- **Concrete applications:** Such as Outlook, MeetingPlace
- **Business importance:** Labeled as critical, important, or unimportant
- **Comment:** Any additional information critical to the design of the network

Planned infrastructure services should also be gathered. Network services include security, quality of service (QoS), network management, high availability, unified communications, mobility, and virtualization.

For organizational goals, you should identify whether the company's goal is to improve customer support, add new customer services, increase competitiveness, or reduce costs. It might be a combination of these goals, with some of them being more important than others. Some organizational goals are as follows:

- Increase competitiveness
- Reduce costs

- Improve customer support
- Add new customer services

Organizational constraints include budget, personnel, policy, and schedule. The company might limit you to a certain budget or timeframe. The organization might require the project to be completed in an unreasonable timeframe. It might have limited personnel to support the assessment and design efforts, or it might have policy limitations to use certain protocols.

Technical goals support the organization's objectives and the supported applications. Technical goals include the following:

- Improve the network's response-time throughput
- Decrease network failures and downtime (high availability)
- Simplify network management
- Improve network security
- Improve reliability of mission-critical applications
- Modernize outdated technologies (technology refresh)
- Improve the network's scalability

Network design might be constrained by parameters that limit the solution. Legacy applications might still exist that must be supported going forward, and these applications might require a legacy protocol that may limit a design. Technical constraints include the following:

- Existing wiring does not support new technology.
- Bandwidth might not support new applications.
- The network must support exiting legacy equipment.
- Legacy applications must be supported (application compatibility).

Characterizing the Existing Network

Characterizing the network is Step 2 of the design methodology. In this section, you learn to identify a network's major features, tools to analyze existing network traffic, and tools for auditing and monitoring network traffic.

Steps in Gathering Information

When arriving at a site that has an existing network, you need to obtain all the existing documentation. Sometimes no documented information exists. You should be prepared to use tools to obtain information and get access to log in to the network devices to obtain information. Here are the steps for gathering information:

Step 1. Identify all existing organization information and documentation.

Step 2. Perform a network audit that adds detail to the description of the network.

Step 3. Use traffic analysis information to augment information on applications and protocols used.

When gathering exiting documentation, you look for site information such as site names, site addresses, site contacts, site hours of operation, and building and room access. Network infrastructure information includes locations and types of servers and network devices, data center and closet locations, LAN wiring, WAN technologies and circuit speeds, and power used. Logical network information includes IP addressing, routing protocols, network management, and security access lists used. You need to find out whether voice or video is being used on the network.

Network Audit Tools

When performing a network audit, you have three primary sources of information:

- Existing documentation
- Existing network management software tools
- New network auditing tools

After gathering the existing documentation, you must obtain access to the existing management software. The client may already have CiscoWorks tools from which you can obtain hardware models and components and software versions. You can also obtain the existing router and switch configurations.

The network audit should provide the following information:

- Network device list
- Hardware models
- Software versions
- Configuration of network devices
- Auditing tools output information
- Interface speeds
- Link, CPU, and memory utilization
- WAN technology types and carrier information

In small network, you might be able to obtain the required information via a manual assessment. For larger network, a manual assessment might be too time-consuming. Network assessment tools include the following:

- **Manual assessment**
  - Manual commands: Review of device configuration and operation though the use of **show** commands of router configurations, interface loads, and router logs
  - Scripting tools

- **Existing management and auditing tools**
  - CiscoWorks: Maps the network and collects network topology, hardware and software versions, and configurations
  - NetFlow: Provides a view of network traffic flows on a specific network interface.
  - Network-Based Application Recognition (NBAR): Intelligent classification engine.
  - Third-party tools: Such as AirMagnet Survey PRO, BVS Yellowjacket, Redcell Engineering, Netcordia NEtMRI, Netformix, NetQoS, and Pari Networks Assessment Tool
- **Additional tools with emphasis on VoIP, wireless, and security**
  - AirMagnet Analyzer Pro
  - Ekahau Site Survey
  - LANguard Network Security scanner
  - NetIQ Vivinet Assessor
  - neteXpose DNA
  - Cisco Operations Manager
  - Stats Manager
  - Service Statistics Manager
  - ClarusIPC
  - Prognosis

When performing manual auditing on network devices, you can use the following commands to obtain information:

- **show tech-support**
- **show processes cpu** (provides the average CPU utilization information)
- **show version**
- **show processes memory**
- **show log**
- **show interface**
- **show policy-map interface**
- **show running-config** (provides the full router or switch configuration)

Example 1-1 shows the output of a **show version** command. This command shows the operating system version, the router type, the amount of flash and RAM memory, the router uptime, and interface types.

Example 1-1 show version *Command*

```
R2>show version
Cisco IOS Software, 7200 Software (C7200-K91P-M), Version 12.2(25)S9, RELEASE SO
FTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright  1986-2006 by Cisco Systems, Inc.
Compiled Tue 28-Mar-06 23:12 by alnguyen

ROM: ROMMON Emulation Microcode
BOOTLDR: 7200 Software (C7200-K91P-M), Version 12.2(25)S9, RELEASE SOFTWARE (fc1
)

 R2 uptime is 5 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0
x0, BOOT_COUNT 0, BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 7206VXR (NPE400) processor (revision A) with 147456K/16384K bytes of memory.
Processor board ID 4294967295
R7000 CPU at 150Mhz, Implementation 39, Rev 2.1, 256KB L2 Cache
6 slot VXR midplane, Version 2.1

Last reset from power-on

PCI bus mb0_mb1 (Slots 0, 1, 3 and 5) has a capacity of 600 bandwidth points.
Current configuration on bus mb0_mb1 has a total of 200 bandwidth points.
This configuration is within the PCI bus capacity and is supported.
```

```
PCI bus mb2 (Slots 2, 4, 6) has a capacity of 600 bandwidth points.
Current configuration on bus mb2 has a total of 0 bandwidth points
This configuration is within the PCI bus capacity and is supported.

Please refer to the following document "Cisco 7200 Series Port
Adaptor Hardware Configuration Guidelines" on CCO <www.cisco.com>,
for c7200 bandwidth points oversubscription/usage guidelines.


1 FastEthernet interface
8 Serial interfaces
125K bytes of NVRAM.

65536K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2102
```

NetFlow provides extremely granular and accurate traffic measurements and a high-level collection of aggregated traffic. The output of NetFlow information is displayed via the **show ip cache flow** command on routers. Table 1-8 shows a description of the fields for NetFlow output.

Table 1-8 *NetFlow Output Description*

Field	Description
Bytes	Number of bytes of memory that are used by the NetFlow cache
Active	Number of active flows
Inactive	Number of flow buffers that are allocated in the NetFlow cache
Added	Number of flows that have been created since the start of the summary
Exporting flows	IP address and User Datagram Protocol (UDP) port number of the workstation to which flows are exported
Flows exported	Total number of flows export and the total number of UDP datagrams
Protocol	IP protocol and well-known port number
Total flows	Number of flows for this protocol since the last time that statistics were cleared
Flows/sec	Average number of flows this protocol per second
Packets/flow	Average number of packets per flow per second
Bytes/pkt	Average number of bytes for this protocol
Packets/sec	Average number of packets for this protocol per second

Network Analysis Tools

To obtain application-level information, the IP packet needs to be further inspected. Cisco devices or dedicated hardware or software analyzers capture packets or use Simple Network Management Protocol (SNMP) to gather specific information. Network analysis tools include the following:

- **Netformx DesignXpert Enterprise:** An integrated desktop tool for discovery, design, configuration, quoting and proposing integrated communications network solutions.
- **CNS NetFlow Collector Engine:** Cisco hardware that gathers every flow in a network segment.
- **Cisco Embedded Resource Manager (ERM):** Allows for granular monitoring on a task basis within the Cisco IOS software. It monitors the internal system resource utilization for specific resources, such as the buffer, memory, and CPU.
- **Third-party tools:** Such as Sniffer, AirMagnet Wifi Analyzer, BVS Yellowjacket 802.11, NetIQ Vivinet Assessor, Netcordia NetMRI, and SolarWinds Orion.

Network Checklist

The following network checklist can be used to determine a network's health status:

- New segments should use switched and not use dated hub/shared technology.
- No WAN links are saturated (no more than 70 percent sustained network utilization).
- The response time is generally less than 100ms (one-tenth of a second); more commonly, less than 2ms in a LAN.
- No segments have more than 20 percent broadcasts or multicast traffic. Broadcasts are sent to all hosts in a network and should be limited. Multicast traffic is sent to a group of hosts but should also be controlled and limited to only those hosts registered to receive it.
- No segments have more than one cyclic redundancy check (CRC) error per million bytes of data.
- On the Ethernet segments, less than 0.1 percent of the packets result in collisions.
- A CPU utilization at or more than 75 percent for a 5-minute interval likely suggests network problems. Normal CPU utilization should be much lower during normal periods.
- The number of output queue drops has not exceeded 100 in an hour on any Cisco router.
- The number of input queue drops has not exceeded 50 in an hour on any Cisco router.
- The number of buffer misses has not exceeded 25 in an hour on any Cisco router.
- The number of ignored packets has not exceeded 10 in an hour on any interface on a Cisco router.

- QoS should be enabled on network devices to allow for prioritization of time-sensitive or bandwidth-sensitive applications.

Table 1-9 summarizes areas in characterizing the network.

Table 1-9 *Characterizing the Network*

Characteristic	Description
Steps in gathering information	**1.** Obtain existing information and documentation **2.** Network audit **3.** Traffic analysis
Primary sources of network audit information	Existing documentation Existing network management software New network management tools

Designing the Network Topology and Solutions

This section describes the top-down approach for network design, reviews pilot and prototype test networks, and describes the components of the design document. As part of the Design phase of the PPDIOO methodology, a top-down approach is used that begins with the organization's requirements before looking at technologies. Network designs are tested using a pilot or prototype network before moving into the Implement phase.

Top-Down Approach

Top-down design just means starting your design from the top layer of the OSI model and working your way down. Top-down design adapts the network and physical infrastructure to the network application's needs. With a top-down approach, network devices and technologies are not selected until the applications' requirements are analyzed. To complete a top-down design, the following is accomplished:

- Analysis of application and organization requirements
- Design from the top of the OSI reference model
  - Define requirements for upper layers (Application, Presentation, Session)
  - Specify infrastructure for lower OSI layers (transport, network, data link, physical)
- Gather additional data on the network

Figure 1-6 shows a top-down structure design process. The design process begins with the applications and moves down to the network. Logical subdivisions are then incorporated with specifics.

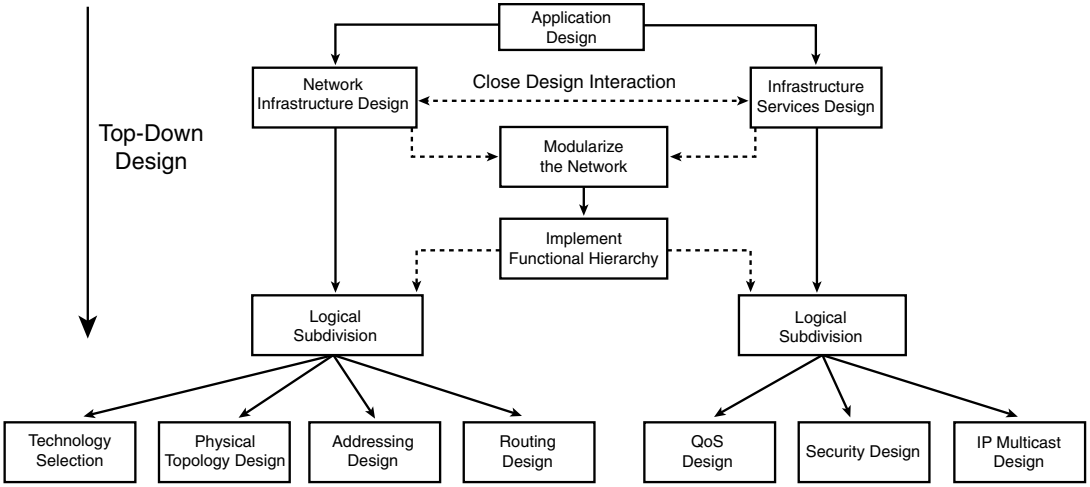

Figure 1-6 *Top-Down Design Process*

Table 1-10 compares the top-down approach to the bottom-up approach to network design.

Table 1-10 *Top-Down Design Compared to Bottom-Up Design*

Design Approach	Benefits	Disadvantages
Top-down	Incorporates the organization's requirements. Provides the big picture. The design meets current and future requirements.	More time-consuming.
Bottom-up	The design is based on previous experience and allows for a quick solution.	May result in inappropriate design. Organizational requirements are not included.

Pilot and Prototype Tests

As soon as the design is complete and before the full implementation, it is a best practice to test the new solution. This testing can be done in one of two ways: prototype or pilot.

A prototype network is a subset of the full design, tested in an isolated environment. The prototype does not connect to the existing network. The benefit of using a prototype is that it allows testing of the network design before it is deployed before affecting a production network. When implementing a new technology such as IPsec, you might want to implement a prototype test before deploying it to the operational network.

A pilot site is an actual "live" location that serves as a test site before the solution is deployed to all locations in an enterprise. A pilot allows real-world problems to be discovered before deploying a network design solution to the rest of the internetwork.

With both a prototype and a pilot, successful testing leads to proving the design and moving forward with implementation. A failure leads to correcting the design and repeating the tests to correct any deficiencies.

Design Document

The design document describes the business requirements; old network architecture; network requirements; and design, plan, and configuration information for the new network. The network architects and analysts use it to document the new network changes, and it serves as documentation for the enterprise. The design document should include the following sections:

- **Introduction** describes the project's purpose and the reasons for the network design.
- **Design Requirements** lists the organization's requirements, constraints, and goals.
- **Existing Network Infrastructure** includes logical (Layer 3) topology diagrams; physical topology diagrams; audit results; network health analysis; routing protocols; a summary of applications; a list of network routers, switches, and other devices; configurations; and a description of issues.
- **Design** contains the specific design information, such as logical and physical topology, IP addressing, routing protocols, and security configurations.
- **Proof of Concept** results from live pilot or prototype testing.
- **Implementation Plan** includes the detailed steps for the network staff to implement the new installation and changes.
- **Appendixes** contains list of exiting network devices, configurations, and additional information used in the design of the network.

Table 1-11 summarizes the contents of the design document.

Table 1-11 *Sections of the Design Document*

Section	Description
Introduction	Purpose and goals of the network design
Design Requirements	Organization requirements and constraints
Existing Network Infrastructure	Contains diagrams, hardware and software versions, and existing configurations
Design	New logical topology, design, and IP addressing
Proof of Concept	Results from pilot or prototype
Implementation Plan	Detailed steps for implementation
Appendixes	Supporting information

The implementation of a network consists of several phases. The each step should contain the following information:

- Description of the step
- Reference to the design document
- Detailed implementation guidelines
- Detailed rollback guidelines
- Estimated time to implement

References and Recommended Reading

Cisco Design Zone. www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html.

Design Zone for Borderless Networks. www.cisco.com/en/US/netsol/ns1063/networking_solutions_program_home.html.

Design Zone for Collaboration. www.cisco.com/en/US/netsol/ns1062/networking_solutions_program_home.html.

Design One for Data Center. www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html

Cisco Data Center. www.cisco.com/en/US/netsol/ns340/ns394/ns224/architecture.html.

Exam Preparation Tasks

Review All Key Topics

Review the most important topics in the chapter, noted with the Key Topics icon in the outer margin of the page. Table 1-12 lists a reference of these key topics and the page numbers on which each is found.

Table 1-12 *Key Topics*

Key Topic Element	Description	Page
List	Forces affecting decisions for the enterprise network	8
List	PPDIOO life cycle four main benefits	11
List	Steps in gathering information	18
Summary	Describes the top-down approach to network design	23

Complete Tables and Lists from Memory

Print a copy of Appendix D, "Memory Tables," (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix E, "Memory Tables Answer Key," also on the CD, includes completed tables and lists to check your work.

Define Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:

PPDIOO, NBAR, NetFlow, policy control, virtualization

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the exam engine on the CD-ROM.

1. List the PPDIOO phases in order.
2. Which business forces affect decisions for the enterprise network?
   - **a.** Removal of borders
   - **b.** Virtualization
   - **c.** Growth of applications
   - **d.** 10GigEthernet
   - **e.** Regulation
   - **f.** ROI
   - **g.** Competitiveness
3. Which design methodology step is important for identifying organizational goals?
   - **a.** Identify customer requirements
   - **b.** Characterize the existing network
   - **c.** Design the network topology and solution
   - **d.** Examine the architecture
   - **e.** Validate the design
   - **f.** Obtain the ROI
4. What needs to be obtained prior to designing the network?
   - **a.** Expected ROI
   - **b.** Organizational and technical goals
   - **c.** Technical constraints
   - **d.** Bill of materials
   - **e.** Existing and new network applications
5. Match each PPDIOO phase with its description.
   - i. Implement
   - ii. Optimize
   - iii. Design
   - iv. Prepare
   - v. Operate
   - vi. Plan

a. Establish requirements

b. Gap analysis

c. Provides high-availability design

d. Installation and configuration

e. Day to day

f. Proactive management

6. Which borderless architecture provides mobility?

a. Policy

b. Network services

c. User services

d. Connection management

e. Control services

7. Which are the three steps in PPDIOO *design* methodology?

a. Reviewing the project cost

b. Designing the network topology and solution

c. Characterizing the network

d. Identifying customer requirements.

e. Validating the design

8. Match each infrastructure service with its description.

i. Identity

ii. Mobility

iii. Storage

iv. Compute

v. Security

vi. Voice/collaboration

a. Access from a remote location

b. Improved computational resources

c. Unified messaging

d. AAA, NAC

e. Storage of critical data

f. Secure communications

9. A company location is used to test a new VoIP solution. What is this type of test called?
   a. Prototype
   b. Pilot
   c. Implementation
   d. New
10. An isolated network is created to test a new design. What is this type of test called?
   a. Prototype
   b. Pilot
   c. Implementation
   d. New
11. NBAR, NetFlow, and EtherPeek are examples of what?
   a. Network audit tools
   b. Network analysis tools
   c. SNMP tools
   d. Trending tools
12. Monitoring commands, CiscoWorks, and WhatsUP are examples of what?
   a. Network audit tools
   b. Network analysis tools
   c. SNMP tools
   d. Trending tools
13. Which of the following are technical constraints? (Select all that apply.)
   a. Existing wiring
   b. Existing network circuit bandwidth
   c. Improving the LAN's scalability
   d. Adding redundancy
14. Which of the following are technical goals? (Select all that apply.)
   a. Existing wiring
   b. Existing network circuit bandwidth
   c. Improving the LAN's scalability
   d. Adding redundancy

15. Which of the following are organizational goals? (Select all that apply.)

- **a.** Improving customer support
- **b.** Budget has been established
- **c.** Increasing competitiveness
- **d.** Completion in three months
- **e.** Reducing operational costs
- **f.** Network personnel are busy

16. Which of the following are organizational constraints? (Select all that apply.)

- **a.** Improving customer support
- **b.** Budget has been established
- **c.** Increasing competitiveness
- **d.** Completion in three months
- **e.** Reducing operational costs
- **f.** Network personnel are busy

17. What components are included in the design document? (Select four.)

- **a.** IP addressing scheme
- **b.** Implementation plan
- **c.** List of Layer 2 devices
- **d.** Design requirements
- **e.** Selected routing protocols
- **f.** List of Layer 1 devices

18. Match each design document section with its description.

i. Introduction

ii. Design requirements

iii. Existing Network Infrastructure

iv. Design

v. Proof of Concept

vi. Implementation Plan

vii. Appendix

a. Detailed steps

b. Current diagram and configuration

c. Organizational requirements

d. Goals

e. Pilot

f. New logical topology

g. Supporting information

19. The network health analysis is based on what information?

a. The number of users accessing the Internet

b. The statements made by the CIO

c. Statistics from the existing network

d. The IP addressing scheme

20. While performing a network audit, you encounter a Frame Relay WAN segment running at a sustained rate of 75 percent from 9 a.m. to 5 p.m. What do you recommend?

a. Nothing. The daily 24-hour average rate is still 45 percent.

b. Change from Frame Relay to MPLS.

c. Increase the provisioned WAN bandwidth.

d. Deny VoIP calls from 9 a.m. to 5 a.m.

21. What information is included in the network audit report? (Select all that apply.)

a. Network device list

b. IOS versions

c. Router models

d. Interface speeds

e. WAN utilization

22. Which three tasks are part of characterizing the existing network?

a. Speaking with the CIO

b. Using traffic analysis

c. Automated auditing of the network using tools

d. Collect information

e. Obtaining organizational chart

f. Defining organizational goals

23. Which command provides the average CPU of a Cisco router?

- **a.** **show cpu**
- **b.** **show processes cpu**
- **c.** **show processes memory**
- **d.** **show cpu utilization**
- **e.** **show cpu average**

24. Which parameters can be obtained by the use of a traffic analyzer?

- **a.** Application importance
- **b.** QoS requirements
- **c.** Devices using a specific protocol
- **d.** IP addresses of devices and TCP/UDP port number
- **e.** Average bit rate and packet rate

25. Which commands provide information about individual applications, protocols, or flows? (Choose three.)

- **a.** **show process cpu**
- **b.** **show ip interface**
- **c.** **show ip cache flow**
- **d.** **show ip nbar protocol-discovery**
- **e.** **show process memory**
- **f.** **show interface application**

26. What is used to create the documentation of the existing network?

- **a.** Router **show** commands
- **b.** Network audit, documentation, and traffic analysis tools
- **c.** Audit tools
- **d.** Existing documentation and input from organization

27. What is the sequence for the stages of top-down design?

28. Which are potential scopes for a network design project? (Choose three.)

- **a.** Network layer redundancy
- **b.** Campus upgrade
- **c.** Data link layer redundancy
- **d.** Network redesign
- **e.** WAN upgrade
- **f.** Application upgrade

29. A credit card company network is being designed. Secure transactions are emphasized throughout the initial requirements. Redundant links are required to reduce network outages. What is the order of importance of the following design issues?

- **a.** IP addressing design
- **b.** Physical topology design
- **c.** Network modules
- **d.** Security design

30. Which types of tools are used during the network design process?

- **a.** Network management tools
- **b.** Network trending tools
- **c.** Network modeling tools
- **d.** Network simulation and testing tools
- **e.** Network implementation tools

31. Which four items should be present in the implementation plan?

- **a.** Implementation description
- **b.** Estimated time to implement
- **c.** Reference to design document
- **d.** Rollback procedure
- **e.** Estimated cost of implementation
- **f.** Application profiles

32. A new design uses IPsec for the WAN. Which approach should be used to verify the design?

- **a.** Live network
- **b.** Pilot network
- **c.** Prototype network
- **d.** Cable network
- **e.** Internet network

33. Which three is included in the design document?

- **a.** Design details
- **b.** Design requirements
- **c.** Current cable runs
- **d.** List of Layer 2 devices
- **e.** Implementation plan