Plan

Introduction to Plan

In the Plan phase, you assess your readiness to support a proposed solution. Planning continues the needs analysis begun in the Prepare phase, with the goal of producing a high-level project plan and the initial site survey.

Before You Begin

Understand the features and functions of collaboration applications. Start with the Planning Concepts and the System Release Notes.

When You Are Done

You have defined and created the following:

- A comprehensive list of components and applications that match the requirements
- A project plan based on those requirements including a proposed, high-level design

Major Concepts and Tasks in This Process

- Planning Concepts
- Planning Tasks

Planning Concepts

This topic presents planning concepts. It is assumed that your network is a converged network that combines voice, data, and video and that you have decided on one of network types discussed in the Internetwork Design Guide. Also, review the information contained in the Market Descriptions topic.

The primary planning considerations that drive the planning stage are:

- Types of deployment, whether it is a new installation or migration to new installation with existing equipment
- Application availability based on your networking needs for multimedia and voice, security, redundancy, and fault tolerance
- Costs associated with your needs

Your goal is to minimize costs while delivering service that does not compromise established availability and performance requirements. These issues are essentially at odds. Any increase in availability and performance must generally be reflected as an increase in cost. As a result, carefully weigh the relative importance of resource availability, performance constraints, variables, and overall cost.

Note The concepts discussed in this topic are meant to be a high-level overview of considerations and not meant to be a definitive set of rules.

Deployment Types

The deployment types to consider are as follows:

- New installation
  - Greenfield—Completely new installation of the Cisco Collaboration system, using no existing equipment.
  - Legacy—New installation of the Cisco Collaboration system combined with existing legacy equipment, such as TDM PBXs and third-party adjuncts, which may require long-term co-existence and integration or eventual migration to the new installation.
  - Brownfield—Existing Cisco Collaboration system, which requires an upgrade and migration from a previous system release to the current system release.
- Single-Stage Upgrade
  - Using existing hardware—All components in the network start at the base release set and all components can be upgraded to the target release set within a single maintenance window.
  - Using new hardware (flash-cut or shrink-and-grow)—A parallel network should be built using new hardware and prestaged with configuration to support the existing production network.
- Multistage System Upgrade
  - Using existing hardware (hybrid system)—The components in individual sites can be upgraded from the base release set to the target release set in stages, during separate maintenance windows.
- Multisite Migration with Independent Site Upgrade
  - Using a hybrid network with interworking release sets—Components are upgraded on a site-by-site basis during separate maintenance windows. At the completion of each maintenance window, a hybrid network exists within the multiple sites that have:

- Components that are operating on the base release set, or
- Components that are operating on the target release set, or
- Components that are a hybrid system

Cost of Ownership

Information system budgets can run into millions of dollars. As large organizations increasingly rely on electronic data for managing business activities, the associated costs of computing resources continue to rise. With this in mind, include the following in your basic network plan:

- Environmental consideration—Include the location of hosts, servers, terminals, and other end nodes; the projected traffic for the environment; and the projected costs for delivering different service levels.
- Performance constraints—Consider network reliability, traffic throughput, and host and client computer speeds. For example, network interface cards and hard drive access speeds
- Internetworking variables—Include the network topology, line capacities, packet flow assignments, redundancy and fault tolerance factors, backward compatibility (coexistence and interoperability), and security.

Redundancy

Redundancy is critical considering the number of vital business applications running on the network. If you have a distributed network with several access layers to remote offices, and you have a failure from the distribution layer to the core without redundancy, you have loss of network service for many people. If you have redundancy in the distribution layer and the core, you can potentially lose one or more circuits without disturbing service to any particular group of users. Depending on the application, you may also need some redundancy from the access layer to the distribution layer.

Because of redundancy, if you drop a link at any one point in the network, every remote group or user still has a path to get back to the core. Even if you cut off the connection from one of the distribution switches back to the core, you still have access to the core for every user.

For more information on redundancy planning, see the Redundancy and Load Sharing Design Guide.

Capacity and QoS

Capacity and QoS are major considerations in a converged network and effect one another. QoS prevents applications from using more than a fair share of bandwidth and degrading the performance of other applications. At the WAN interface, QoS allocates expensive wide area capacity among applications.

Bandwidth and QoS requirements are easy to figure in a multilayered design because the traffic flow is fairly predictable. You can also have end-to-end QoS in a multilayered design. End-to-end QoS is critical when you have real-time applications, such as a voice conversation or video presentation, and you have non-real time applications that can interfere with the real-time applications. For example, if the real-time and non-real time applications arrive at the same layer at the same time, the network must pass the real-time packets first, as well as keep latency and jitter low. QoS end-to-end is the answer.

Consider Call Admission Control (CAC) as an alternative to QoS. CAC limits the amount of traffic allowed onto the network at the ingress point. Because you know that the network will be congested at various times during the day, you can disallow more traffic by using CAC. Also consider using traffic-shaping techniques using traffic-shaping devices. A combination of QoS, CAC, and traffic shaping provides optimal performance for applications on a converged network.

Managing link speed mismatches is the last element of traffic management. The mismatches, called chokepoints or bottlenecks, are a basic design issue whenever a large capacity link generates traffic destined for a low capacity link. To avoid the mismatches, carefully analyze the traffic and the device capabilities, then upgrade the interface (if needed) and apply a combination of CAC and QoS.

For more information on QoS, see the Enterprise QoS Solution Reference Network Design Guide.

Security

Cisco recommends multiple layers of security technologies to prevent a single configuration error from jeopardizing the security of the network. Cisco also recommends operational processes that ensure prompt application of software patches, timely installation of new security technologies, and performance of regular security audits and assessments.

As you begin to design your network, rank the importance of your network assets and services by considering these factors:

- What keeps you in business?
- How do you make money?
- Does loss of data or privacy equal lost money?
- What about regulatory compliance?
- How do you protect your critical data?
- Where does voice fit?

Then consider the potential threats to your business, which may include

- Toll fraud
- Eavesdropping
- Address spoofing
- Fake caller identity
- Media tampering
- Denial of service
- SPAM, SPIT (SPAM over IP telephony), and SPIM (SPAM over Instant Messaging)

In addition to the operational processes, review and consider advanced security technologies. Security technologies can be categorized as follows:

- Network security
  - Virtual LANs (VLANs)
  - Access control lists (ACLs)

  - Stateful firewalls with protocol aware inspection
  - Virtual Private Networks (VPNs)
  - QoS
  - Dynamic Address Resolution Protocol (ARP) inspection
  - Dynamic Host Configuration Protocol (DHCP) snooping
  - Port security
  - Network intrusion prevention
- Host security
  - Cisco Security Agent
  - Third-party antivirus software
  - Host-based firewalls
  - Hardened operating systems
- User authentication, authorization, and accounting security
  - Phone image authentication
  - Multilevel administration privileges
  - Call detail reporting

For more information about Cisco end-to-end security designs, see the Cisco SAFE guidelines at http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_safe.html. For more details about Cisco integrated network security solutions, see the following resources:

- Security Products and Solutions
- Secure Unified Communications
- Cisco Support Community for Security

Planning Tasks

The following overview shows the high-level tasks of the planning process:

Determine Your Business Requirements

Two important factors that drive your business requirements are:

- Size of your business. For more information, see Market Descriptions
- Requirements for installation and upgrade. For more information, see:
  - Install and Configure System Components

Review the Deployment Models, on page 7 topic for more details.

Collecting Requirements

The following are suggested methods to use in gathering information to plan your network:

- Assess User Requirements—Users want applications to be available on demand in the network. The chief components of application availability are response time, throughput, and reliability. You can assess user requirements as follows:
  - Develop community profiles of what different user groups require. Although many users have roughly the same requirements of an electronic mail system, engineering groups using Windows terminals and Sun workstations in an NFS environment have different needs from PC users sharing print servers in a finance department.
  - Build a baseline for implementing an internetwork by interviewing groups, forming focus groups, or using surveys. Some groups may require access to common servers, while others may want to allow external access to specific internal computing resources. Formal surveys can be used to get a statistically valid reading of user sentiment about a particular service level or proposed internetworking architecture.
  - Conduct a test involving representative users in a lab environment. This is most applicable when evaluating response time requirements. As an example, you may set up working systems and have users perform normal remote host activities from the lab network. By evaluating user reactions to variations in host responsiveness, you can create benchmark thresholds for acceptable performance.
- Identify Functionality Requirements—After you understand your internetworking requirements, you can select the specific functionality that fits your environment, such as the level of application availability and the implementation costs for that availability. Also consider fault tolerance and redundancy.

Use Planning Tools and Templates

This topic includes planning tools and links to documents that provide guidelines for designing and configuring your Cisco Collaboration Systems. It also includes information on quoting and ordering Cisco Collaboration Systems products.

Solution Reference Network Design Documents

Solution Reference Network Design (SRND) documents provide guidelines, recommendations, and best practices for implementing collaboration network solutions. The SRNDs recommended for designing Cisco

Collaboration Systems are available from the: Cisco Collaboration Solutions Design Guidance document or at http://www.cisco.com/go/srnd.

Note Another SRND resource is Enterprise QoS System Reference Network Design.

Ordering Guides

Cisco partners, Cisco sales staff, and Cisco service providers can access Cisco Collaboration Ordering Guides.

Deployment Models

With Cisco Collaboration Systems, you can choose from many deployment options, including cloud computing, hybrid, and on-premises. The following sections provide deployment model examples and information.

Cisco Preferred Architecture and Cisco Validated Designs

Cisco Preferred Architectures and Cisco Validated Designs (CVDs) help you design and deploy powerful, comprehensive, and scalable collaboration architectures with collaboration services, such as Cisco Unified Communications, Video Collaboration, and Contact Center. Cisco Preferred Architectures and CVDs guides provide the framework for systems design based on common use cases or current engineering system priorities. Cisco engineers have tested and documented each CVD to help ensure a faster, more reliable, and more predictable deployment.

- Cisco Preferred Architecture design overviews provide a prescriptive, end-to-end architecture. They also provide an understanding of the individual products and their role in the overall architecture, and basic design best practices and sample Bill of Materials
- CVDs provide detailed design and step-by-step deployment information for collaboration deployments and are based on Preferred Architectures.

For samples of Cisco Preferred Architecture and CVDs, see Cisco Validated Designs for Collaboration.

Tested Deployment Models

Cisco has developed various site models as standard architectures. These models were tested and optimized for maximum efficiency and performance. You can derive your network design by choosing the deployment model that most closely matches your business. Then, add the specific features and applications that meet your business needs.

For information about Collaboration tested deployments and site models for this release, go to Collaboration Test Bed for Collaboration Systems Release 11.0(1).

Cisco Collaboration Systems Solution Reference Network Designs (SRND)

For more guidelines, recommendations, and best practices for implementing Collaborations networking solutions, go to the SRNDs inCisco Collaboration Solutions Design Guidance .

Identify System Components

The Cisco Collaboration Systems Release Compatibility Matrix lists all the components and their versions for a particular release. It is the recommended set of components and specific software versions that have been tested and verified for interoperability within a specific system release. For compatibility information before Collaboration Systems Release 10.5(1), refer to the Compatibility Tool.

See the Install and Configure System Components topics in the Implement chapter for links to information that describe components that are specific to the collaboration system.

Review Compatibility Matrix

The Compatibility Matrix lists all the components and their versions for a particular release. It is the recommended set of components and specific software versions that have been tested and verified for interoperability within a specific system release. For compatibility information before Collaboration Systems Release 10.5, refer to the Compatibility Tool.

Collect and Analyze Data

Using available tools, collect data on the network to assess network readiness. Tasks for data collection and analysis include:

- Perform an infrastructure analysis—Obtain floor plans and campus maps, including utilities and conduit systems, to identify deficiencies in infrastructure.
- Perform a software gap analysis—Do a software gap analysis to address network management tools for the IP network.
- Perform an initial traffic analysis—Collect data on all potential converged infrastructure traffic flows. Use station message detail recording (SMDR) and billing records to determine legacy call volumes. Use network management tools to collect key statistics on your IP data network.

Create High-Level Design

When data is collected and analyzed, record the results in the site survey and high-level design documents.

Preparing for Your System Installation

This topic provides links to documentation for you to review before you install the Cisco Collaboration System. It lists the components in the release set and provides information about the deployment of various components.

For more information, see:

- Cisco Collaboration Systems Release Compatibility Matrix
- Limitations and restrictions

When your installation plans are complete and you are ready to install components, go to Performing Your System Installation.

Note There may be more than one upgrade path available based on the software deployed in your specific environment.

When your upgrade plan is in place and you are ready to upgrade, go to Preparing for Your System Upgrade, on page 9

Preparing for Your System Upgrade

Before the upgrade process, review the following for details about the different collaboration components, upgrade release versions of components involved in the upgrade, and release version compatibility.

- Upgrade Paths
- Compatibility Matrix

When your upgrade plan is in place and you are ready to upgrade, go to Performing a System Upgrade.

Note There may be more than one upgrade path available based on the software deployed in your specific environment.