Introduction to Internetwork Design
Overview

As network designers, we rarely get the opportunity to come into a network and build it from the ground up. What we are normally faced with in the course of our careers is a network that has been built like a remodeled house around a rapidly growing family. What began as a rather modest network made up of bridges and a Core router with links to the Internet and perhaps a remote site or two, has become a patched spectrum of devices and protocols, cables and legacy systems.

It is therefore our job to revisit the network design and look for ways to make it better. Perhaps the network requires support for new services such as Voice over IP (VoIP), Quality of Service (QoS), or gigabit Ethernet. Maybe the company has been acquired and needs to be integrated into the corporate infrastructure while considering security, accessibility, and scalability. In all of these cases, it should be our goal to leave the network better than we found it, creating a design that is functional, that performs well under today's load and that scales to suit tomorrow's bandwidth requirements for applications and services. The design must meet user requirements, in other words, while still being at or under budget.

In this chapter we will discuss how to define and set goals for the overall network design. You will learn to spot key issues that will help you in drawing out the design requirements, and you will gather some facts about solid network design methodology.

Design Goals

Networks vary in size and topology, and you never quite know what to expect when you accept a new position or consulting assignment. The wiring closets may be neat and clean, with exceptional cable management and labeling, or you may feel as though you have just walked into the world's largest bowl of Category 5 spaghetti. One thing you can always count on, however, is that a network of any size must make sense to someone. If you are very lucky, that “someone” will be available to help you quickly uncover the network “gotchas” that are unique to each environment. More than likely, you will not be so lucky. You will need a good methodology to help you sort out the issues of the current design.

The best thing to do when you find yourself in an undocumented, unruly bowl of spaghetti is to bear in mind that there are key goals every network
Introduction to Internetwork Design

architect must follow. A network must be functional for the current applications and number of users it supports. It must also be scalable, to allow for expansion for tomorrow's needs, and adaptable to the applications it may have to handle. A network must also be manageable so that faults can be quickly spotted, isolated, and resolved, preferably before the user realizes that something is wrong. All of these things, however, could easily be built into a network if money was no object, but you must also make the design cost-effective. If you design the Taj Mahal network for a company that has budget enough for an efficiency apartment, then you have not served the customer well.

To recap, here are the design goals we will discuss in greater detail:

- Functionality
- Scalability
- Adaptability
- Manageability
- Cost-effectiveness

Functionality

As we stated earlier, somewhere in the middle of every network is a person who knows exactly how to fix whatever goes wrong. That individual may be the one who created the layers of network cabling and equipment, or he may be the one who has just been there so long that he knows the common problems and where they are most likely to happen. To that person, the network is functional. To management, however, it may be a cause for lost sleep.

A truly functional network must provide a certain level of service, as determined by the customer, to a community of users. The defined level of services may vary from network to network. For example, a college or university might have the following, depending on each department's needs.

- Accounting must be able to reach the financial database in the main building.
- The Math department should easily be able to upload computer-based tests to a server in the Sciences hall.

In its early days, the enterprise network existed to make a user's life easier. Files and resources could be shared and some research databases became available over a very primitive Internet—at least, primitive by
today’s standards. As the Internet evolved, the network became a faster way for users to get work accomplished, talk with other users around the world, or simply have fun. Businesses in the 1990s discovered the fertile ground of e-commerce, and many “dot-coms” were born. Now that the network spells recreation, productivity, and profit to everyone from the end-user to the carriers, it is your job to create a design that will be truly functional within the guidelines and budget of the customer.

Scalability

Companies tend to grow over time both in personnel and in space. The key to a good network design should be the ability to scale that network—in other words, to grow the network without having it become a patchwork of upgrades that address only a current need or situation. If you design a network taking in only today’s requirements, you will fall short of this goal. It is up to you to ask questions about projections for the company’s growth over 2, 5, or even 10 years and then design a percentage above that. Make recommendations based on what you may have seen or designed at other similar businesses, and based upon what you learn through this guide.

Once you have the corporate vision of the future understood, it is crucial to get a user’s perspective. Users are normally looking at a short-term fix to a long-term problem. For example, support personnel want user complaints of slowness to stop. They want to end the trouble tickets they are logging about client timeouts when trying to reach a server. A good design not only fixes the current problems but also is flexible enough to allow future growth.

Adaptability

Keep the future in mind when designing a network. That is not to say that it is wrong to choose a familiar technology such as Fast Ethernet; rather, you should build a design that does not limit customers’ ability to change technologies when they find that they simply cannot live without Asynchronous Transfer Mode (ATM). A good network is adaptable enough to allow growth in new directions when and where they become applicable.

Some of the questions to ask when considering adaptability:

- Are the selected routers capable of handling a wide range of routing technologies?
Introduction to Internetwork Design

- Is there support for a multiprotocol environment if this is applicable to the network?
- What is the long-range vision for the company as far as growth, staff additions, acquisitions, and moves?
- How flexible is the Access layer design for moves, adds, and changes?

Acquisitions are particularly important considerations when choosing the network design and the devices supporting that design. When a company acquires another company, there may be legacy protocols and network equipment to be integrated into the existing design. It is important that the overall design be able to support the addition of the acquired network with as little disruption as possible to both sets of users. Failure to plan for such scenarios can mean inability to integrate a legacy network or extended network downtime for large segments in the future.

When you take the time to discuss these and other issues with the support staff and users of a network, many headaches associated with major changes can be avoided later.

Manageability

A network should be designed in such a way as to allow for monitoring and management using standard management protocols, such as simple network management protocol (SNMP) and remote network monitoring (RMON), without the tools becoming a part of the problem. Even if a company is not currently using any form of network management, it is important to take this into account for several reasons:

- For future growth
- To avoid redesign
- To add value to the design

First, if the company or user base does continue to grow, the likelihood is that the network will also grow, expanding beyond the level at which the current support staff are accustomed to serving. Network management would allow for more rapid fault isolation and resolution. Secondly, when the company realizes a need for network management, the ability should already have been considered in their new network design so that they don’t have to revisit the issue later. Finally, the entire spectrum of network management adds value to a network design by providing a way to avoid problems and to quickly assess and resolve them when they do occur.
Chapter 1

If a company has not already considered network management, they have the ability to do so when reviewing the design. If they had considered it but were not ready to implement it, the optimal locations of probes, network management stations (NMS), or analyzers can be shown on the final design. In this manner, the plan is already in place when they are ready. Chances are the subject is already part of the “big picture” for the customer. Usually, when a network redesign has become necessary, a network has experienced many problems that could have been easily spotted through good network management.

Another choice to consider is whether to use centralized or distributed network management. Traditional network management generally uses one network management system that receives all traps, or network management events and messages, that are generated anywhere in the network. This can create problems in many instances, since additional traffic is constantly being fed into an already busy network. Distributed network management, as illustrated in Figure 1-1, places less of a burden on the network by keeping the traffic local between probes or sending devices and their designated SNMP server. Periodic updates are sent from the remote NMS to the “lead” NMS.

As Figure 1-1 shows, it is best to implement distributed network management with periodic updates sent to a Manager-of-Managers (MoM)—where possible—rather than have multiple devices polling more devices across an already congested link. This might mean having RMON probes reporting to...
Introduction to Internetwork Design

a central NMS, or it might mean further dividing the workload to include a NMS at each remote location, with RMON probes reporting to that station and updates flowing at scheduled intervals back to the main NMS. This is the design shown in Figure 1-1. Each RMON probe reports to a local NMS. That NMS reports to the MOM. Traffic is kept local most of the time.

This goal takes you outside the routing and switching area into the entire picture of the customer network. A good network is rarely about having the fastest, most expensive equipment. A good network is usually a result of an excellent eye for details, such as network management and related devices.

Cost-Effectiveness

The best design in the world is worthless if your client cannot afford it. For example, a small business may only have the budget for a basic network, supporting a small number of users and applications. Later, the Core router may need to be upgraded, but if the wiring closets are ready, the cabling is not outdated, and the users are being served adequately, the upgrade should be an easy one. Creation of a good architecture sometimes means taking the requirements and finding the best solution with the least compromise, all within the budget. When you do this, you will earn the trust and loyalty of your customer.

TIP: Creation of a good architecture means taking the requirements and finding the solution of least compromise—within the budget!

Design Issues

There is almost always a trade-off in any network design. Some of the factors to keep in mind are fixed costs, recurring costs, and projected longevity of the network design. The network may currently be going through a major upgrade every five years. Even though you have considered the scalability and adaptability of the design, there is still the reality of technological
changes that will, at some juncture, mean upgrading certain devices, interface cards, or wiring. If we were to see the issues as an equation, it might look like this:

\[(X + \frac{Yn}{n} = r)\]

Fixed costs \((X)\) are a one-time major outlay of funds that can seem to be a great burden if looked at solely on the initial impact. Add this to your recurring costs.

Recurring costs \((Y)\) can be something like the monthly cost of the circuit from the service provider or the costs for administration of the systems. Multiply that cost by the number \((n)\) of billing periods in the entire projected lifecycle—in this case, 60 months.

Divide the entire cost over the life of the project by the number of billing periods in the lifecycle \((n)\). This should yield a resulting monthly cost over the life of the project.

Let’s suppose that the fixed costs of a given project are $1,000,000 in equipment, wiring, and installation services. The anticipated lifecycle is 60 months. Recurring costs are $2,500 per month for circuits and $7,500 per month for network management from a consultant. Your equation would be as follows:

\[\$1,000,000 + \frac{($10,000 \times 60)}{60} = \$26,666.66\]

This figure is usually a more digestible sum to the finance department than an initial outlay of 1 million dollars followed by monthly bills totaling at least 10,000 for the next 5 years (assuming no increases in fees).

Another possibility when selling a network design is to consider capital leasing companies. Many smaller or not-for-profit organizations do not have the kind of capital to build the networks that would enable them to grow and be successful. Capital leasing companies can purchase the fixed equipment and lease it to the company for a fee each month. When the lease term ends, the company may then upgrade and start a new lease agreement or may find themselves in a better financial position to purchase equipment outright for the next design.

While financial issues are not always the only hurdle you will encounter in your initial design phase, they are often the most difficult ones to get past, if you are not prepared. There are almost always trade-offs in any network design, usually because the best design is the most expensive design. It is incumbent on you, as the network designer, to find the best possible
solution for the customer with the fewest trade-offs. Don't sacrifice what
you know will be a critical router in the Core for better switches in the
wiring closets, for example.

Design Methodology

There is more to designing a good network than selecting the hardware and
cabling and coming to a viable trade-off between cost and need. After
assessing the requirements, the budget, and the needs of the network, there
is the topology consideration, selection of the naming conventions, and the
decision of how to address the network entities.

A good methodology gives you a foundation on which to start any project.
Cisco recommends a six-step process, shown in Figure 1-2, which is applic-
able to almost any network plan. Steps 1 through 3 are done sequentially
and should only be needed one time, unless the site adopts a new topology
at some point. Steps 4 through 6 form a loop that may be repeated at each
upgrade or design change in the future of the network. We will go through
these steps individually, and then we will dig deeper with some practical
examples in figures to follow.

Step 1: Analyze the Requirements

In this step, many questions will be asked and answered before the overall
picture of the requirements will begin to emerge. Some of those questions
may be as follows:

- How many users exist today?
- Is there a prediction for growth over the target lifecycle?
- What applications are being used in the network?
- Will new applications be deployed in the near future? If so, what are
  the bandwidth requirements of those applications?
- If a network exists today, where are the bottlenecks and the greatest
  number of user complaints?
- Are there any available reporting tools, such as a trouble ticketing
  system, that can be used to gather information?
Based upon the business model, what are the applications or technology that would promote the most business growth (video teleconferencing, VoIP, data mining, point-of-sale systems, or Web servers, for example)?

Are there any new remote sites in the planning stages? If so, what will their bandwidth requirements be? (Will remote clients need to do uploads frequently to a main site server, for example?)

If there are any network management tools in place, are reports from these systems available to show baselines and trends?

As evidenced here, the list of questions is infinite, depending upon the scope of the project. Careful attention must therefore be paid to not only making the business case for the proposed upgrade or redesign, but to planning for future growth and user needs.
Step 2: Develop the Topology
(Internetwork Structure)

In order to design a highly scalable internetwork, the structure of the network must be planned in a hierarchical manner. The Cisco-recommended network design model, the three-tier model, is shown in Figure 1-3. By following this model, you will be able to see the key issues and requirements of each area without becoming overwhelmed by the total network topology and its endless possibilities. These are the three main areas in a network hierarchy.

Core Layer    The Core provides the wide-area links between remote sites and “campus” networks that connect to form a WAN. It is where the enterprise network touches the world. At this layer you will find serial links (T1/T3), Frame Relay, and other WAN protocols and Core services. The network backbone exists in the Core area.

Distribution Layer    At the Distribution layer, the network begins to take on its personality. Here you will find the campus backbone, firewalls/VPN devices, the beginning of the enterprise naming conventions and number schemes, and the type of network formed, whether Fast Ethernet, FDDI, or ATM. The Distribution layer typically extends the network to the wiring closets.

Access Layer    The users enter the network at the Access layer via Fast Ethernet, Ethernet, or Token Ring. The hosts attach to the network in order to reach local and remote applications and network services.
Step 3: Define Naming Conventions and Addressing Strategy

Selecting a good naming convention is more than a way to assign hostnames and to establish a way of communicating with devices (other than by network address); it is a smart way to easily recognize the location and application of a given host. In Figure 1-4, we see an example of what might be a typical campus environment.

For instance, let’s assume we have a mixture of Unix and Windows NT servers in the Math department’s second-floor server room. To quickly assess a problem with a given Web server running FreeBSD, it is best that the name reflect something unique about the host. Observe the following examples:

<table>
<thead>
<tr>
<th>Good Choice</th>
<th>Poor Choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA2UN4WEB</td>
<td>abacus</td>
</tr>
<tr>
<td>2MATHWEB4</td>
<td>webboy</td>
</tr>
</tbody>
</table>

In the first example, MA reflects the building or department, 2 represents the floor, UN represents the operating system in use, and WEB represents the applications. A network manager could quickly determine that Web server 4 in the Math department’s second-floor server room was unresponsive. The manager could further deploy a network technician along with the Unix system administrator for that server room. The poor choice,
abacus, may reflect that the unit is in the Math department, but nothing else about the host is revealed. A network technician would have a harder time tracking down the device, perhaps having to resort to knowing the subnet associated with the Math department, in order to track down the offending device.

In the second example, again we have clues that this is Web server 4 on the math department’s second floor. The poor choice merely reflects a possible Web server that only the system administrator would recognize.

A good addressing strategy goes hand-in-hand with good naming convention choices. With a good addressing scheme, the groundwork is laid for future growth of the network as well as for good network performance. Network areas should be contiguous, that is, the network should be able to grow in a consecutive block of addresses, even if the block is further subnetted. This simplifies route summarization and routing protocol convergence.

**Step 4: Provision the Hardware**

There is a lot more to “provisioning the hardware” than just going with whatever is the latest and greatest technology. Many factors have to be taken into consideration when deciding upon the hardware and software to be purchased. You will take into account:

- **Cost**
- **Footprint**
- **Upgrade path**
- **Manageability**
- **Training**
- **Interface types and port density**
- **Memory, CPU, and bus requirements**
- **HVAC/facility requirements**

**Cost**  Initial and recurring costs to provision and maintain the hardware and software are always something to be considered in any design plan.

**Footprint**  Is there enough rack space in the computer room or lab? How much rack space will the equipment require? Will the hardware acquired for the new project overflow your area?
Upgrade Path  How often are upgrades released for the product, and what is the procedure for obtaining the upgrades? Will each software upgrade also require a memory upgrade? Will entire line cards need to be replaced to upgrade firmware on a piece of equipment? Part of a good overall design should include answers to the questions normally asked either during the install phase or during the operational phase.

Manageability  If the site uses network management, are the devices manageable? What version of SNMP are they compliant with? Even a UPS can be managed with SNMP, so if this is an important matter in the selection of equipment or software, be sure to document the answers to these and any other questions on manageability.

Training of Personnel  Very important! If you are proposing a design that requires the retraining of all of the network personnel, that also must be taken into account when budgeting. If the design is truly the best solution, find a way to soften the blow by agreeing to package deals or free training from the reseller or vendor.

Interface Types and Port Density  Part of the equipment selection is to define the site needs such as number of serial ports (and type) for current and future needs, density required to support the LANs connecting to the equipment, and growth needs. It would be unwise to purchase a five-slot router that will be fully loaded as soon as it is deployed. Leave room for planning.

Memory/CPU/Bus Requirements  To support the proposed configuration, purchase RAM in proportions recommended by the vendor. These can usually be found on the Web sites of various manufacturers. In the router realm, CPU power and bus speeds are usually specific to the model.

HVAC/Facility Requirements  It is also good practice to run the design by the facilities personnel once the details of the equipment to be ordered are documented. Have the data sheets ready that specify heat output, voltage, and amperage as well as temperature and humidity ranges for a given device. This permits factors such as cooling, humidity control, and power requirements to be addressed before the equipment is purchased.
Step 5: Deploy Cisco IOS Features

During the design process, there will be some idea of the types of traffic that will pass through the network devices—Internet Protocol (IP), Internet Packet Exchange (IPX), and Systems Network Architecture (SNA), for example—and as the process goes on, more granularity will be added. Will access lists be employed on the router? If so, what type, and what is the desired outcome? There may also be features such as QoS or Border Gateway Protocol (BGP) communities that are important in the overall traffic management in the design. It is also at this stage that other products may be taken into consideration: firewalls, RADIUS or TACACS+ servers, encryption devices, and configuration management stations. All of these are factors in the final design.

Step 6: Implement, Monitor, and Maintain the Network

Congratulations! Your design has been built, accepted, and is ready for deployment. Whenever possible you will build the network in a lab or demo environment prior to actual deployment into a production network. This step helps to avoid unnecessary downtime and general headaches when the network upgrade takes place. It is a good time to work out the bugs in the plan, to explain each step to the network personnel, and to fine-tune any last-minute requirements that may have been overlooked.

Summary

In this chapter we discovered how to determine and set goals for the network design process and the components that went into those goals. We then covered key design issues common to almost any network structure. Finally, we discussed a design methodology that helps set the course for most network design and redesign projects. You should now have the basic tools to help you get underway with the case studies in this book as well as with “real-life” projects you may be ready to undertake.

In Chapter 2, “Hierarchical Design Model,” we’ll take a closer look at the three-tier model, at each individual layer, and at the variations and benefits of the model, as well as how to begin using it to build Cisco networks.
Bibliography


Cisco Internetwork Design, Cisco Press, 2000, Matthew H. Birkner, Editor