TOP DOWN NETWORK DESIGN METHODOLOGY

INTRODUCTION

Networking professionals have the ability to create networks that are so complex that when problems arise they can't be solved using the same sort of thinking that was used to create the networks.

A network created with this complexity often doesn't perform well as expected i.e.

- It doesn't scale as the need for growth arises (as it almost always does),
- It doesn't match a customer's requirements.

A solution to this problem is to use a streamlined, systematic methodology in which the network or upgrade is designed in a top-down approach.

Good network design must recognize that a customer's requirements embody many business and technical goals, including requirements for availability, scalability, affordability, security, and manageability. Many customers also want to specify a required level of network performance, often called a *service level*. To meet these needs, difficult network design choices and tradeoffs must be made when designing the logical network before any physical devices or media are selected.

Definition of Top-down network design

Top-down network design is a methodology for designing networks that begins at the upper layers of the OSI reference model before moving to the lower layers. The top-down methodology focuses on applications, sessions, and data transport before the selection of routers, switches, and media that operate at the lower layers.

The top-down network design process includes:

- Exploring organizational and group structures to find the people for whom the network will provide services
- And from whom the designer should get valuable information to make the design succeed.

Network design should be a complete process that matches business needs to deliver a system that will maximize an organization's success. E.g. In the LAN area it is more than just buying a few devices.

OBJECTIVES OF NETWORK DESIGN

To help one design networks that meet a customer's business and technical goals In terms of functionality, capacity, performance, availability, scalability, affordability, security, and manageability.

Where to Begin

- Analyze business and technical goals first.
- Explore divisional and group structures to find out who the network serves and where they reside.
- Determine what applications will run on the network and how those applications behave on a network
- Focus on Layer 7 and above first

Using a Structured Network Design Process

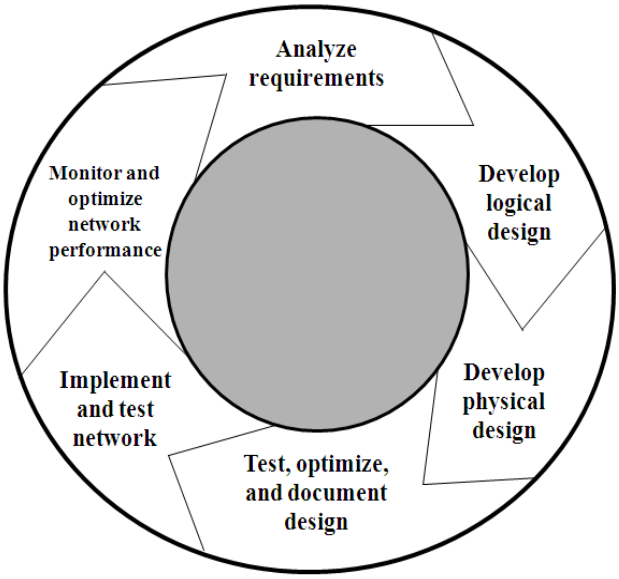
Top-down network design is a discipline that grew out of the success of structured software programming and structured systems analysis. The main goal of structured systems analysis is to more accurately represent users' needs, which unfortunately often are ignored or misrepresented. Another goal is to make the project manageable by dividing it into modules that can be more easily maintained and changed.

- A focus should be placed on understanding data flow, data types, and processes that access or change the data.
- A focus is placed on understanding the location and needs of user communities that access or use the resources of the network.
- Characterizing the existing system, new user requirements, and a structure for the future system.
- A logical model is developed before the physical model.
- Specifications are derived from the requirements gathered at the beginning of the top-down sequence

Difference between the Logical model and the physical Model

- The logical model represents the basic building blocks, divided by function, and the structure of the system.
- The physical model represents devices and specific technologies and implementations.

TOP DOWN NETWORK DESIGN STEPS



PHASE 1: – ANALYZING REQUIREMENTS

In this phase, the network analyst interviews users and technical personnel to gain an understanding of the business and technical goals for a new or enhanced system. The task of characterizing the existing network, including the logical and physical topology and network performance, follows. The last step in this phase is to analyze current and future network traffic, including traffic flow and load, protocol behavior, and quality of service (QoS) requirements.

- Analyze business goals and constraints
- Analyze technical goals and tradeoffs
- Characterize the existing network
- Characterize network traffic

a) *Analyzing Business goals and Constraints*

Business goals

Understanding your customer's business goals and constraints is a critical aspect of network design. Armed with a thorough analysis of your customer's business objectives, you can propose a network design that will meet with your customer's needs.

It is tempting to overlook the step of analyzing business goals, because analyzing such technical goals as capacity, performance, security, and so on is more interesting to many network engineers. It is important to analyze business goals so as to match them with the customer's business objectives.

- ***What to do before meeting the client***

Before meeting with your customer to discuss business goals for the network design project, it is a good idea to research your client's business. Be keen to:-

- Find out what industry the client is in.
- Learn something about the client's market, suppliers, products, services, and competitive advantages.

With the knowledge of your customer's business and its external relations, you can position technologies and products to help strengthen the customer's status in the customer's own industry.

- ***Meeting the customer***

- Ask them to explain the organizational structure of the company. Your final internetwork design will probably reflect the corporate structure, so it is a good idea to gain an understanding of how the company is structured in departments, lines of business, vendors, partners, and field or remote offices.
- Understanding the corporate structure will help you locate major user communities and characterize traffic flow.
- Understanding the corporate structure will also help you recognize the management hierarchy.

- One of your primary goals in the early stages of a network design project should be to determine who the decision-makers are. Who will have the authority to accept or reject your network design proposal?
- Ask your customer to state an overall goal of the network design project. Explain that you want a short, business-oriented statement that highlights the business purpose of the new network.
- Find out:-
  - Why is the customer embarking on this new network design project?
  - How do they intend to use the network?
  - How will the new network help them achieve their objectives

- After discussing the overall business goals of the network design project, ask your customer:-
  - To help you understand their criteria for success.
  - What goals must be met for the customer to be satisfied? Sometimes success is based on operational costs savings because the new network allows employees to be more productive. Sometimes success is based on the ability to increase revenue or build partnerships with other companies.
  - Make sure you know up-front how "success" is defined by executives, managers, end users, network engineers, and any other stakeholders.
  - Also, determine whether the customer's definition of success will change as yearly fiscal goals change.

➢ **In addition to determining the criteria for success, ascertain the consequences of failure e.g.**

- What will happen if the network design project fails or if the network, once installed, does not perform to specification?
- How visible is the project to upper-level management?
- Will the success (or possible failure) of the project be visible to executives?
- To what extent could unforeseen behavior of the new network disrupt business operations? In general, gather enough information to feel comfortable that you understand the extent and visibility of the network design project.
- You should try to get an overall view of whether the new network is critical to the business's mission.

➢ **Identify the scope of a network design project**

- One of the first steps in starting a network design project is to determine its scope. Some of the most common network design projects these days are small in scope - for example, projects to allow a few people in a sales office to access the enterprise network via a VPN.
- On the other hand, some design projects are large in scope. Ask your customer to help you understand if the design is for a single network segment, a set of LANs, a set of WAN or remote-access networks, or the entire enterprise network.
- Also ask your customer if the design is for a new network or a modification to an existing one.
- Explain to your customer any concerns you have about the scope of the project, including technical and business concerns.
- Help your customer match the schedules of their projects to the scope
- Make sure your customers tell you everything they can about the network and the design project.
- You may want to poke around outside the stated scope of the project; just to make sure nothing essential has been omitted. Double-check that you have gathered all the requirements and that you have accurate information about sites, links, and devices. If the project addresses network security, make sure you know about all external links, including dial-in access.

➢ **Identifying a Customer's Network Applications**

After identifying the customer's business goals and scope of the project, it is now time to focus on the real reason why the networks exist: applications. The identification of your customer's applications should include both current applications and new applications.

➢ **Typical Network Design Business Goals**

With the changes in business strategies and networking discussed above here are some business goals

- Increase revenue and profit
- Increase market share
- Expand into new markets
- Increase competitive advantages over companies in the same market
- Reduce operational costs
- Increase employee productivity
- Shorten product-development cycles

- Use just-in-time manufacturing
- Plan around component shortages
- Offer new customer services
- Offer better customer support
- Open the network to key constituents (prospects, investors, customers, business partners, suppliers, and employees)
- Build relationships and information accessibility to a new level, as a basis for the network organizational model
- Avoid business disruption caused by network security problems and natural and unnatural disasters
- Modernize outdated technologies
- Reduce telecommunications and network costs, including overhead associated with separate networks for voice, data, and video

➢ **Business Goals Checklist**

- You can use the following checklist to determine if you have addressed your client's business-oriented objectives and concerns. If you can't gather every piece of data mentioned in the checklist, make sure you document what is missing in case it becomes critical, but don't stall the project to gather every last detail.
- But if real-world constraints, such as uncooperative network design customers, budget cuts, and time constraints, hamper your ability to follow the methodology precisely, just follow it as much as you can. In general, the methodology still works even if some data is missing after you do your analysis.

Checklist

- I have researched the customer's industry and competition.
- I understand the customer's corporate structure.
- I have compiled a list of the customer's business goals, starting with one overall business goal that explains the primary purpose of the network design project.
- The customer has identified any mission-critical operations.
- I understand the customer's criteria for success and the ramifications of failure.
- I understand the scope of the network design project.
- I have identified the customer's network applications (using the Network Applications chart).
- The customer has explained policies regarding approved vendors, protocols, or platforms.
- The customer has explained any policies regarding open versus proprietary solutions.
- The customer has explained any policies regarding distributed authority for network design and implementation.
- I know the budget for this project.
- I know the schedule for this project, including the final due date and major milestones, and I believe it is practical.
- I have a good understanding of the technical expertise of my clients and any relevant internal or external staff.
- I have discussed a staff-education plan with the customer.
- I am aware of any office politics that might affect the network design.

Business Constraints

Having analyzed the business goals it is important to analyze any business constraints that may affect the network design

➢ ***Politics and Policies***

- In the case of office politics, your best bet is to listen rather than talk. Your goal is to learn about any hidden agendas, turf wars, biases, group relations, or history behind the project that could cause it to fail. In some cases, a similar project was already tried and didn't work.
- You should determine if this has happened in your case and, if it has, the reasons why the project failed or never had a chance to come to fruition.
- Pay attention to personnel issues that could affect the project. Which manager or managers started the project and how much do they have at stake? Are there any managers, network engineers, or users who want the project to fail for any reason?
- Find out who your advocates and opponents are. In some cases, no matter how technically sound your network design is, there will be people who have a negative reaction to it.
- Be sure to find out if your project will cause any jobs to be eliminated. Some network design projects involve automating tasks that were once done by highly paid workers. These workers will obviously have reasons to want the project to fail.

- **Budgetary and Staffing Constraints**
  - Your network design must fit the customer's budget. The budget should include allocations for equipment purchases, software licenses, maintenance and support agreements, testing, training, and staffing. The budget might also include consulting fees (including your fees) and outsourcing expenses.
  - Throughout the project, work with your customer to identify requirements for new personnel, such as additional network managers. Point out the need for personnel training, which will affect the budget for the project.
  - Analyze the abilities of the networking staff. How many in-house experts are there? Should you recommend any training or outsourcing for network operations and management? The technologies and protocols that you recommend will depend on the abilities of internal staff.

- **Project Scheduling**
  - You should review with your customer is the timeframe for the network design project.
  - When is the final due date is and what are the intermediate and major milestones? In most cases, management of the project schedule is the customer's obligation, not yours, but you should ask the customer to give you a copy of the schedule and to keep you informed.

b) *Analyze technical goals and tradeoffs*

We look at techniques for analyzing a customer's technical goals for a new network design or network upgrade. Analyzing your customer's technical goals can help you confidently recommend technologies that will perform to your customer's expectations.
Typical goals include:-

1. Scalability

It refers to how much growth a network design must support. For many enterprise network design customers, scalability is a primary goal. Many large companies add users, applications, additional sites, and external network connections at a rapid rate. The network design you propose to a customer should be able to adapt to increases in network usage and scope.

- **Planning for Expansion**

Your customer should be able to help you understand how much the network will expand in the next year and in the next two years. (Ask your customer to analyze goals for growth in the next 5 years also, but be aware that not many companies have a clear 5-year vision.)
You can use the following list of questions to analyze your customer's short-term goals for expansion:

- How many more sites will be added in the next year? The next 2 years?
- How extensive will the networks be at each new site?
- How many more users will access the corporate internetwork in the next year? The next 2 years?
- How many more servers will be added to the internetwork in the next year? The next 2 years?

- **Expanding Access to Data**

Many companies have centralized servers residing on server farms located on building or campus backbone networks. In addition, corporations increasingly implement intranets that enable employees to access centralized World Wide Web servers using Internet Protocol (IP) technologies.
At some companies, employees can access intranet web servers to arrange business travel, search online phone directories, order equipment, and attend distance learning training classes.

- **Constraints on Scalability**

- When analyzing a customer's scalability goals, it is important to keep in mind that there are impediments to scalability inherent in networking technologies.
- Selecting technologies that can meet a customer's scalability goals is a complex process with significant ramifications if not done correctly. For example, selecting a flat network topology with Layer 2 switches can cause problems as the number of users scales, especially if the users' applications or network protocols send numerous broadcast frames. (Switches forward broadcast frames to all connected segments.)

2. Availability

Availability refers to the amount of time a network is available to users and is often a critical goal for network design customers. Availability can be expressed as a percent uptime per year, month, week, day, or hour, compared to the total time in that period.

Network design customers don't use the word availability in everyday English and have a tendency to think it means more than it does. In general, availability means how much time the network is operational. Availability is linked to reliability, but has a more specific meaning (percent uptime) than reliability. Reliability refers to a variety of issues, including accuracy, error rates, stability, and the amount of time between failures.

Availability can be expressed as a percent uptime per year, month, week, day, or hour, compared to the total time in that period For example:

- 24/7 operation
- Network is up for 165 hours in the 168-hour week
- Availability is 98.21%

Different applications may require different levels
Some enterprises may want 99.999% or "Five Nines" availability

Availability can also be expressed as a mean time between failure (MTBF) and mean time to repair (MTTR)
Availability = MTBF/(MTBF + MTTR) For example:

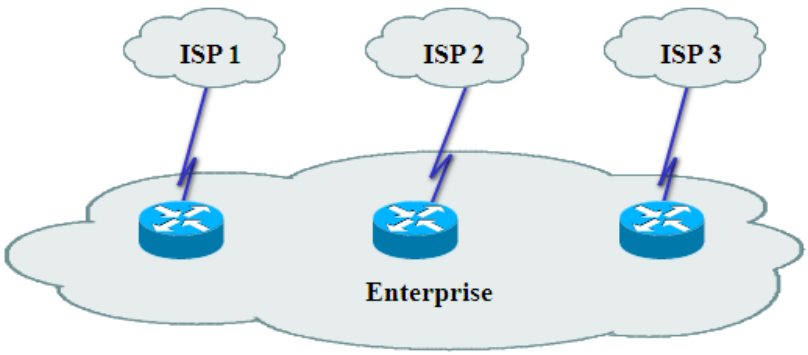
- The network should not fail more than once every 4,000 hours (166 days) and it should be fixed within one hour
  4,000/4,001 = 99.98% availability

➢ **Availability Downtime in Minutes**

	Per Hour	Per Day	Per Week	Per Year
99.999%	.0006	.01	.10	5
99.98%	.012	.29	2	105
99.95%	.03	.72	5	263
99.90%	.06	1.44	10	526
99.70%	.18	4.32	30	1577

99.70% availability sounds pretty good, but it could mean that the network is down for 0.18 minutes every hour. This is 11 seconds. If those 11 seconds were spread out over the hour, nobody would notice possibly. But if there were some bug, for example, that caused the network to fail for 11 seconds every hour on the hour, people would notice. Users these days are very impatient.
Notice that 99.70% availability also could mean one catastrophic problem caused the network to be down for 1577 minutes all at once. That's 26 hours. If it were on a Saturday and the network was never down for the rest of the year, that might actually be OK. So, you have to consider time frames with percent availability numbers.

99.999% Availability May Require Triple Redundancy



Can the customer afford this?

In the event of failure of the primary router, the secondary becomes the primary and still has a backup. Fix the previous primary and have it become the tertiary.

This helps with maintenance too. Pull out the tertiary and upgrade it. The primary still has a backup. After extensive testing, put the tertiary back in as the primary. Pull out the original primary and upgrade it. Put it back as the secondary. Finally pull out the original secondary and upgrade it.

Availability can also be expressed as a mean time between failure (MTBF) and mean time to repair (MTTR)
Availability = MTBF/(MTBF + MTTR) For example:

- The network should not fail more than once every 4,000 hours (166 days) and it should be fixed within one hour
- 4,000/4,001 = 99.98% availability

➢ **Specifying Availability Requirements**

- You should encourage your customers to specify availability requirements with precision. Consider the difference between an uptime of 99.70 percent and an uptime of 99.95 percent. An uptime of 99.70 percent means the network is down 30 minutes per week, which is not acceptable to many customers.
- An uptime of 99.95 percent means the network is down 5 minutes per week, which may be acceptable, depending on the type of business. Availability requirements should be specified with at least two digits following the decimal point.
- It is also important to specify a timeframe with percent uptime requirements. Go back to the example of 99.70 percent uptime, which equated to 30 minutes of downtime per week. A downtime of 30 minutes in the middle of a working day is probably not acceptable. But a downtime of 30 minutes every Saturday evening for regularly scheduled maintenance might be fine.

➢ **The Cost of Downtime**

- In general, a customer's goal for availability is to keep mission-critical applications running smoothly, with little or no downtime. A method to help you, the network designer, and your customer understand availability requirements is to specify a cost of downtime. For each critical application, document how much money the company loses per hour of downtime. (For some applications, such as order processing, specifying money lost per minute might have more impact.)
- If network operations will be outsourced to a third-party network management firm, explaining the cost of downtime can help the firm understand the criticality of applications to a business's mission.
- Specifying the cost of downtime can also help clarify whether in-service upgrades or triple redundancy must be supported.

3. Network Performance

Common performance factors include:-

a) Capacity (bandwidth): The data-carrying capability of a circuit or network, usually measured in bits per second (bps)

b) Throughput: Quantity of error-free data successfully transferred between nodes per unit of time, usually seconds

- Throughput is defined as the quantity of error-free data that is transmitted per unit of time. Throughput is often defined for a specific connection or session, but in some cases the total throughput of a network is specified.
- Novices consistently misuse the words throughput and bandwidth. Remember, bandwidth means capacity and is generally fixed.
- Throughput is an assessment of the amount of data that can be transmitted per unit of time. Can vary depending on network performance characteristics and how the measurements are made. Bandwidth is a given.

Why is throughput not the same as bandwidth?

- Theoretically, throughput should increase as offered load increases, up to a maximum of the full capacity of the network.
- However, network throughput depends on the access method (for example, token passing or carrier sensing), the load on the network, and the error rate.

Bandwidth Vs. Throughput

Bandwidth and throughput are not the same thing
Bandwidth is the data carrying capacity of a circuit

- Usually specified in bits per second

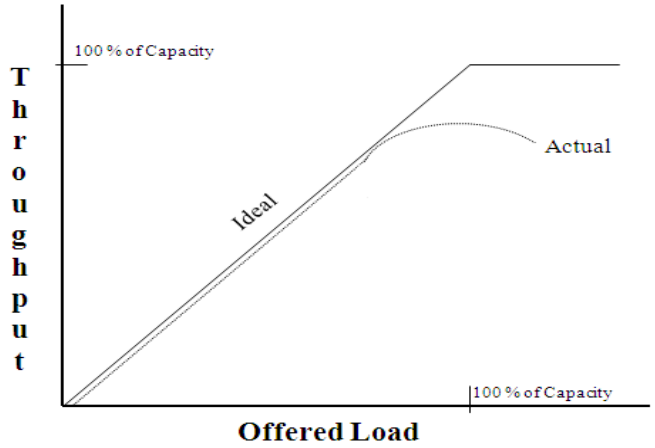
Throughput is the quantity of error free data transmitted per unit of time

- Measured in bps, Bps, or packets per second (pps)

Throughput Vs. Goodput

- You need to decide what you mean by throughput
- Are you referring to bytes per second, regardless of whether the bytes are user data bytes or packet header bytes
  - Or are you concerned with application-layer throughput of user bytes, sometimes called "goodput"
    - In that case, you have to consider that bandwidth is being "wasted" by the headers in every packet

Bandwidth, Throughput, Load



Other Factors that Affect Throughput

- The size of packets
- Inter-frame gaps between packets
- Packets-per-second ratings of devices that forward packets
- Client speed (CPU, memory, and HD access speeds)
- Server speed (CPU, memory, and HD access speeds)
- Network design
- Protocols
- Distance
- Errors
- Time of day, etc., etc., etc.

c) Utilization: The percent of total available capacity in use

d) Optimum utilization: Maximum average utilization before the network is considered Saturated

e) Offered load: Sum of all the data all network nodes have ready to send at a particular time

- Delay (latency) and delay variation
- Response time

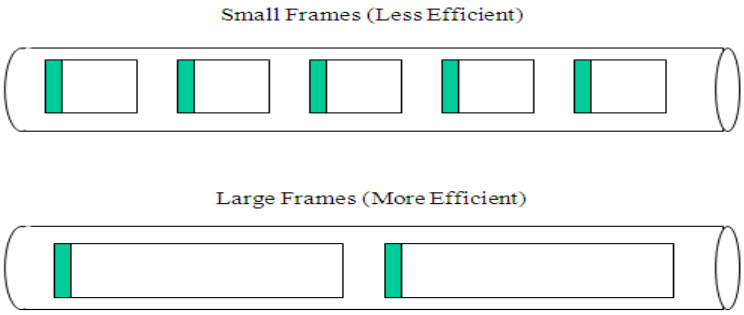
f) Accuracy: The amount of useful traffic that is correctly transmitted, relative to total traffic. Typical causes of data errors include:-

- Power surges or spikes, impedance mismatch problems, poor physical connections, failing devices, and noise caused by electrical machinery. Sometimes software bugs can cause data errors also.
- Frames that have an error must be retransmitted, which has a negative effect on throughput.
- The overall goal for accuracy is that the data received at the destination must be the same as the data sent by the source.

g) Efficiency: An analysis of how much effort is required to produce a certain amount of data throughput

- How much overhead is required to deliver an amount of data?
- How large can packets be?
  - Larger better for efficiency (and goodput)
  - But too large means too much data is lost if a packet is damaged

How many packets can be sent in one bunch without an acknowledgment**?**



h) Response Time:- Refers to the amount of time between a request for some network service and a response to the request

- Response Time
  - A function of the application and the equipment the application is running on, not just the network
  - Most users expect to see something on the screen in 100 to 200 milliseconds

i) Delay:- Refers to the time between a frame being ready for transmission from a node and delivery of the frame elsewhere in the network

- Propagation delay
  - A signal travels in a cable at about 2/3 the speed of light in a vacuum
- Transmission delay (also known as serialization delay)
  - Time to put digital data onto a transmission line
    For example, it takes about 5 ms to output a 1,024 byte packet on a 1.544 Mbps T1 line
- Packet-switching delay
- Queuing delay

j) Delay Variation

- The amount of time average delay varies its also known as jitter
  - Voice, video, and audio are intolerant of delay variation
  - So forget everything we said about maximizing packet sizes
- There are always tradeoffs
- Efficiency for high-volume applications versus low and non-varying delay for multimedia

4. Security

- Focus on requirements first
- Detailed security planning later (Chapter 8)
- Identify network assets
  - Including their value and the expected cost associated with losing them due to a security problem
  - These include hardware, software, applications, data, intellectual property, company reputation and company reputation
- Analyze security risks which may arise such as:-
  - Hacked network devices
  - Data can be intercepted, analyzed, altered, or deleted
  - User passwords can be compromised
  - Device configurations can be changed
  - Reconnaissance attacks
  - Denial-of-service attacks

5. Manageability

Network management functions include:-

- **Fault management:** Detecting, isolating, and correcting problems; reporting problems to end users and managers; tracking trends related to problems
- **Configuration management:** Controlling, operating, identifying, and collecting data from managed devices
- **Accounting management:** Accounting of network usage to allocate costs to network users and/or plan for changes in capacity requirements
- **Performance management:** Analyzing traffic and application behavior to optimize a network, meet service-level agreements, and plan for expansion

- **Security management :**Monitoring and testing security and protection policies, maintaining and distributing passwords and other authentication and authorization information, managing encryption keys, and auditing adherence to security policies

What to consider in manageability

- Select internetworking equipment that is easy to configure, operate, maintain, and manage.
- Select a network design that is easy to understand and troubleshoot.
- Develop good network documentation that can help reduce troubleshooting time.
- Select network applications and protocols that are easy to use so that users can support themselves to some extent

6. Usability

It refers to the ease of use with which network users can access the network and services Networks should make users' jobs easier

- Some design decisions will have a negative affect on usability:
  - Strict security, for example

7. Adaptability

- A good network design should adapt to new technologies and changes. Changes can come in the form of new protocols, new business practices, new fiscal goals, new legislation, and a myriad of other possibilities.
- When designing a network, you should try to avoid incorporating any elements that For example, some countries have enacted environmental laws that require a reduction in the number of employees driving to work. To meet the legal requirement to reduce automobile emissions, companies need their remote-access designs to be flexible enough to adapt to increasing numbers of employees working at home.
- The adaptability of a network affects its availability. For example, some networks must operate in environments that change drastically from day to night or from winter to summer. Changes in temperature can affect the behavior of electronic components of a network.
- A network that cannot adapt cannot offer good availability.
- A flexible network design can also adapt to changing traffic patterns and QoS requirements.

8. Affordability

- The final technical goal this chapter covers is affordability which is sometimes called cost-effectiveness. Most customers have a goal for affordability, although sometimes other goals such as performance and availability are more important. Affordability is partly a business goal and a technical goal.
- For a network design to be affordable, it should carry the maximum amount of traffic for a given financial cost. Financial costs include nonrecurring equipment costs and recurring network operation costs.
- As mentioned in Chapter 1, you should be aware of your customer's budget so that you can recommend solutions that are affordable.

- **Making Network Design tradeoffs**

- Despite what politicians tell us in their manifestos during an election, in the real world meeting goals requires making tradeoffs. We look at some typical network design tradeoffs in organizations today.
- To meet high expectations for availability, redundant components are often necessary, which raises the cost of a network implementation. To meet rigorous performance requirements, high-cost circuits and equipment are required. To enforce strict security policies, expensive monitoring might be required and users must forgo some ease of use.
- To implement a scalable network, availability might suffer, because a scalable network is always in flux as new users and sites are added. Implementing good throughput for one application might cause delay problems for another application. Lack of qualified personnel might suggest the need for expensive training or the need to drop certain features.
- One cause of network problems can be inadequate staffing and reduced training due to overzealous cost cutting. The tradeoff with cutting costs might be a network that isn't robust or has substandard performance until the problem is recognized, which often takes a year or two. If the in-house network staff was cut, outsourcing might become a necessity, which could end up being more costly than it would have been to keep the in house staff.
- The network design process is usually progressive. This means that legacy equipment must coexist with new equipment. Your design might not be as elegant as you would like because you might need for it to support old devices and old applications.

- If the new network is not being introduced at the same time as new applications, the design must provide compatibility with old applications. Also, be aware that insufficient bandwidth in parts of the network, where the bandwidth cannot be increased due to technical or business constraints, must be resolved by other means.
- To help you analyze tradeoffs, ask your customer to identify a single driving network design goal.
- This goal can be the same overall business goal for the network design project.
- In addition, ask your customer to prioritize the rest of the goals. Prioritizing will help the customer get through the process of making tradeoffs.
- Ask customers to add up how much they want to spend on scalability, availability, network performance, security, manageability, usability, adaptability, and affordability. For example, a customer could make the following selections:
- The network design that you develop must take these tradeoffs into consideration.

c) *Characterize existing network*

- Purpose of examining a customer's existing network
  - To better judge how to meet expectations for network scalability, performance, and availability.
  - Examining the existing network includes
  - learning about the topology and physical structure
  - Assessing the network's performance.
- Purpose of understanding of the existing network's structure, uses, and behavior:
  - determine whether a customer's design goals are realistic
  - Document any bottlenecks or network performance problems, and identify internetworking devices and links that will need to be replaced because the number of ports or capacity is insufficient for the new design.
  - Identify performance problems and select solutions to solve problems
  - Develop a baseline for future measurements of performance
  - Ensure interoperability between the existing and anticipated networks

- **Characterizing the infrastructure of a network means**

Develop a set of network maps and know the location of major internetworking devices and network segments.
It also includes:-

- Documenting the names and addresses of major devices and segments
- Identifying methods for addressing and naming
- The types and lengths of physical cabling
- Investigating architectural and environmental constraints
- Learning the location of major hosts, interconnection devices, and network segments is a start to developing an understanding of traffic flow.
- Coupled with data on the performance characteristics of network segments, it gives insight into user concentrations and the level of traffic that a network design must support. The goal is to obtain a map or set of maps of the existing network

- **Characterize the logical topology of the network and the physical components.**

- The logical topology illustrates the architecture of the network, which can be hierarchical or flat, structured or unstructured, layered or not,
- The logical topology also describes geometric shape (eg: star, ring, bus, hub, spoke, or mesh).

- **Characterizing Network Addressing and Naming**
  - Characterizing the logical infrastructure of a network involves documenting any strategies your customer has for network addressing and naming.
  - Drawing of detailed network maps, include the names of major sites, routers, network segments and servers

  - Need to also investigate the network layer addresses the customer uses. Customer's addressing scheme (or lack of any scheme) can influence ability to adapt the network to new design goals. For example, customer might use unregistered IP addresses that will need to be changed or translated before connecting to the Internet, As another example, current IP subnet masking might limit the number of nodes in a LAN or VLAN

- **Characterizing Wiring and Media**
  - Understanding cabling design and wiring of the existing network is important for meeting scalability and availability goals for the new network design.

- Documenting the existing cabling design can help in plan for enhancements and identify any potential problems. Need to document the types of cabling in use, cable distance, number of pairs, distance information important when selecting data link layer technologies based on distance restrictions.
- Within buildings, try to locate telecommunications wiring closets, cross-connect rooms, any laboratories or computer rooms. The type of cabling that is installed between telecommunications closets and in work areas;
- Technologies, such as 100BASE-TX Ethernet, which may require later cabling, so be sure to document the existence of any old cabling that needs to be replaced.

Vertical and horizontal wiring

- Vertical wiring runs between floors.
- Horizontal wiring runs from telecommunications closets to wall plates in cubicles or offices.
- Work-area wiring runs from the wallplate to a workstation in a cubicle or office.
- The cabling from a telecommunications closet to a workstation should be approximately <=100 meters, including the work-area wiring
- Use a time-domain reflectometer (TDR) to verify suspicions of excess distance. (TDR functionality is included in most cable testers.)
- Many network designs are based on the assumption that workstations are no more than 100 meters from the telecommunications closet.

➢ **Checking Architectural and Environmental Constraints**

When investigating cabling, need to pay attention to such environmental issues as the possibility that cabling will run near:-

- Creeks that could flood
- Railway tracks or highways where traffic could jostle cables
- Construction or manufacturing areas where heavy equipment or digging could break cables.

Need to determine if there are any:-

- Legal right-of-way issues that must be dealt with before cabling can be put into place: cross a public street? through property owned by other companies?
- Obstacles blocking the line of sight for line-of-sight technologies
- Within buildings, need to pay attention to architectural issues that could affect the feasibility of implementing the network design.

Typical architectural elements that must be sufficient to support your design:-

- Air conditioning, Heating, Ventilation
- Power
- Protection from electromagnetic interference
- Doors that can lock
- Space for:
- Cabling conduits
- Patch panels
- Equipment racks
- Work areas for technicians installing and troubleshooting equipment

Typical architectural elements that must be sufficient to support your design:-

- Air conditioning, Heating, Ventilation
- Power
- Protection from electromagnetic interference
- Doors that can lock
- Space for:
- Cabling conduits
- Patch panels
- Equipment racks
- Work areas for technicians installing and troubleshooting equipment

A site survey starts with a draft WLAN design. Using a floor plan or blueprint for the site, the designer decides on the initial placement of the wireless access points.

- Can decide where to place access points for initial testing based on some knowledge of
- Where the users will be located,

- Characteristics of the access points' antennas, and
- The location of major obstructions.
- The initial placement of an access point is based on an estimate of the signal loss that will occur between the access point and the users of the access point.

An RF signal traveling through objects of various sorts can be affected by many different problems, including the following:-

- **Reflection**: - causes the signal to bounce back on itself. The signal can interfere with itself in the air and affect the receiver's capability to discriminate between the signal and noise in the environment. Is caused by metal surfaces such as steel girders, scaffolding, shelving units, steel pillars, and metal doors
- **Absorption**: - Some of the electromagnetic energy of the signal can be absorbed by the material in objects through which it passes, resulting in a reduced signal level. Water has significant absorption properties, and objects such as trees or thick wooden structures can have a high water content.
- **Refraction**:-When an RF signal passes from a medium with one density into a medium with another density, the signal can be bent.
- **Diffraction**: - results when a region through which the RF signal can pass easily is adjacent to a region in which reflective obstructions exist.

➢ **Checking the Health of the Existing Internetwork**

- Studying the performance of the existing internetwork gives a baseline measurement from which to measure new network performance.
- Because the performance of existing network segments will affect overall performance, need to study their performance to determine how to meet overall network performance goals.
- By analyzing existing networks, y can also recognize legacy systems that must be incorporated into the new design. Sometimes customers are not aware that older protocols are still running on their internetworks.
- By capturing network traffic as part of your baseline analysis, you can identify which protocols are actually running on the network and not rely on customers' beliefs.
- Developing a Baseline of Network Performance
- One challenging aspect is selecting a sufficient time to do the analysis. If measurements are made over too short a timeframe, temporary errors appear more significant than they are.
- In addition to allocating sufficient time for a baseline analysis, it is also important to find a typical time period to do the analysis.

➢ **Analyzing Network Availability**

- To document availability characteristics of the existing network, gather any statistics that the customer has on the mean time between failure (MTBF) and mean time to repair (MTTR) for the internetwork as a whole and major network segments. Compare these statistics with MTBF and MTTR goals, as established during technical goals analysis:-
- Does the customer expect your new design to increase MTBF and decrease MTTR? Are the customer's goals realistic considering the current state of the network?

➢ **Analyzing Network Utilization**

- Network utilization is a measurement of the amount of bandwidth that is in use during a specific time interval. Commonly specified as a percentage of capacity.
- Different tools use different averaging windows for computing network utilization. Some tools let the user change the window. Using a long interval can be useful for reducing the amount of statistical data that must be analyzed, but granularity is sacrificed.

➢ **Analyzing Network Accuracy**

Network accuracy may be specified as a bit error rate (BER).

- One can use a BER tester (also called a BERT) on serial lines to test the number of damaged bits compared to total bits.
- One can also use Cisco show commands to gain an understanding of errors on a serial interface, which is a more common practice than using a BERT.
- With packet-switched networks, it makes more sense to measure frame (packet) errors because a whole frame is considered bad if a single bit is changed or dropped.
- A protocol analyzer can check the CRC on received frames.

➢ **Analyzing Network Efficiency**

- It is advisable to use maximum frame sizes is a strategy to increase network efficiency. Bandwidth utilization is optimized for efficiency when applications and protocols are configured to send large amounts of data per frame, thus minimizing the number of frames and round-trip delays required for a transaction. The number of frames per transaction can also be minimized if the receiver is configured with a large receive window allowing it to accept multiple frames before it must send an acknowledgment
- The goal is to maximize the number of data bytes compared to the number of bytes in headers and in acknowledgment packets sent by the other end of a conversation. Changing frame and receive window sizes on clients and servers can result in improved efficiency. Increasing the maximum transmission unit (MTU) on router interfaces can also improve efficiency, although doing this is not appropriate on low-bandwidth links that are used for voice or other real-time traffic.

➢ **Analyzing Network Delay and Response Time**

- To verify that performance of a new network design meets a customer's requirements, you need to measure response time between significant network devices before and after a new network design is implemented.
- Response time can be measured using many ways. Using a protocol analyzer, you can look at the amount of time between frames and get a rough estimate of response time at the data link layer, transport layer, and application layer. This is a rough estimate because packet arrival times on an analyzer can only approximate packet arrival times on end stations.
- On a typical workstation, run some representative applications and measure response time for typical operations, such as checking email, sending a file to a server, downloading a web page, updating a sales order, printing a report, and so on.

d) Characterizing Traffic Flow

Characterizing traffic flow involves:-

- Identifying sources and destinations of network traffic
- Analyzing the direction and symmetry of data travelling between sources and destinations.

The flow may depend on the application, and may be:

- bidirectional and symmetric
- Bidirectional and asymmetric.
- unidirectional and asymmetric

➢ **Identifying Major Traffic Sources and Stores**

Need to identify user communities and data stores for existing and new applications

User community

- It refers to a set of workers who use a particular application or set of applications. It can be a corporate department or set of departments.
- It is becoming increasingly necessary to characterize user communities by application and protocol usage rather than by departmental boundary

Major data stores

A data store is an area in a network where application layer data resides, maybe any of:

- Server, server farm, mainframe
- Storage-area network (SAN)
- Tape backup unit
- Digital video library
- Any device or component of an internetwork where large quantities of data are stored.

➢ **Documenting Traffic Flow on the Existing Network**

It involves identifying and characterizing individual traffic flows between traffic sources and stores.

Traffic Flow

An individual network traffic flow can be defined as a protocol and application information transmitted between communicating entities (end system, network, autonomous system) during a single session.

A flow has attributes such as:-

- Direction,
- Symmetry,

- Routing path and routing options,
- Number of packets,
- Number of bytes, and
- Addresses for each end of the flow.

Size of Traffic Flow

The simplest method for characterizing the size of a flow is to measure the number of megabytes per second (MBps) between communicating entities.

Tools to use are:-

- A protocol analyzeror network management systemto record load between important sources and destinations.
- Cisco NetFlow, which collects and measures data as it enters router and switch interfaces, including source and destination IP addresses, source and destination TCP or UDP port numbers, packet and byte counts, etc.

➢ **Characterizing Types of Traffic Flow for New Network Applications**

Network flow can be characterized by its direction and symmetry

- Direction specifies whether data travels in both directions or in just one direction and the path that a flow takes as it travels from source to destination through an internetwork.
- Symmetry describes whether the flow tends to have higher performance or QoS requirements in one direction than the other direction.
- A good technique for characterizing network traffic flow is to classify applications as supporting one of a few well-known flow types:

➢ **Traffic flow types**

1. terminal/host traffic flow

- Usually asymmetric.
- The terminal sends a few characters and the host sends many characters.
- Telnet is an example of an application that generates terminal/host traffic

2. Client/server traffic flow

Servers: powerful computers dedicated to managing disk storage, printers, or other network resources.
Clients: PCs or workstations on which users run applications.

- The flow usually bidirectional and asymmetric.
- Requests (from clients) are typically small frames, except when writing data to the server.
- Responses range from 64 bytes to 1500 bytes or more,

Client/server traffic flow: effect of caching on http traffic

- Flow not always between the web browser and the web server because of caching.
- With caching,
- requests often do not generate network traffic or
- WAN band width utilization is reduced.

Client/server traffic flow: thin client flow

- The application runs on the central server, or the software is downloaded from server into the client machine for execution.
- Amount of data flow can be substantial. Networks with thin clients should be designed with sufficient capacity and appropriate topology.
- Thin client technology (aka server-based computing): client software or hardware that is designed to be particularly simple. the bulk of data processing occurs on a server.
- An information appliance or computing appliance is a thin client designed to perform a particular set of dedicated tasks.
- Main advantage of the technology is lower support costs. Thin clients provide a lower total cost of ownership (TCO) and a scalable TCO for large enterprises.

3. Peer-to-peer traffic flow

- Flow usually bidirectional and symmetric.
- Communicating entities transmit approximately equal amounts of information. There is no hierarchy. No device stores substantially more data than any other device.

- Examples - In small LAN environments, PCs set up in a peer-to-peer configuration so that everyone can access each other's data and printers. No central server.
- A set of multiuser UNIX hosts where users set up FTP, Telnet, HTTP, and NFS sessions between hosts. Each host acts as both a client and server.

Examples of peer-to-peer traffic flow

- Peer-to-peer applications for downloading music, videos, and software. Each user publishes music or other material and allows other users on the Internet to download the data. It can cause an inordinate amount of traffic
- A video-conference: meeting between business people at remote sites using video-conferencing equipment. All sites have the same QoS requirements.

4. Distributed computing traffic flow

- DC refers to applications that require multiple computing nodes working together to complete a job in a reasonable timeframe by processing data and running algorithms simultaneously. E.g. complex modeling and rendering tasks (the visual effects for movies are often developed in a dc environment.)
- With some distributed computing applications, the task manager sends request to the computing nodes on an infrequent basis, resulting in little traffic flow.
- With other applications, there is frequent communication between the task manager and the computing nodes.
- In some cases, the task manager allocates tasks based on resource availability, which makes predicting flow somewhat difficult.
- Characterizing traffic flow for distributed computing applications might require study the traffic with a protocol analyzer or model potential traffic with a network simulator.

➢ **Traffic Flow in Voice over IP**

In VoIP networks there are two flows.

- The flow associated with transmitting the audio voice
- The flow associated with call setup and teardown.
- The flow for transmitting the digital voice is peer-to-peer
- Call setup and teardown can be characterized as a client/server flow

➢ Documenting Traffic Flow

To document traffic flow, characterize the flow type for each application and list the user communities and data stores that are associated with applications.

➢ **Characterizing Traffic Load**

- It helps in selecting appropriate topologies and technologies to meet a customer's goals.
- Can help design networks with sufficient capacity for local usage and internetwork flows.
- Traffic load estimates are unlikely to be precise because of the many factors involved in characterizing network traffic.
- The goal is simply to avoid a design that has any critical bottlenecks by monitoring application-usage patterns, idle times between packets and sessions, frame sizes and other traffic behavioural patterns for application and system protocols.
- For customers with numerous applications, this level of analysis might not be practical, however. For these customers, you could limit the analysis to the top five or ten applications.

➢ Documenting Application-Usage Patterns

The first step: identify user communities, the number of users in the communities, and the applications the users employ. This step can help you identify the total number of users for each application.

Then document the following:-

- The frequency of application sessions (per day, week, month, ...)
- The length of an average application session
- The number of simultaneous users of an application

Find out the following

- Do the users of the application translate to the number of simultaneous connections?
- Are all applications are used all the time

➢ **Refining Estimates of Traffic Load Caused by Applications**

To refine estimate of application bandwidth requirements:-

- Research the size of data objects sent by applications,
- Overhead caused by protocol layers
- Any additional load caused by application initialization.
- Some applications send much more traffic during initialization than during steady-state operation.

To completely characterize application behaviour, should investigate which protocols an application uses. From the protocols calculate traffic load more precisely by adding the size of protocol headers to the size of data objects.

- **Characterizing Traffic Behavior**

Broadcast/Multicast Behavior

- A broadcast frame: goes to all network stations on a LAN. At the data link layer, and a multicast frame: goes to a subset of stations. Layer 2 internetworking devices, such as switches and bridges, forward broadcast and multicast frames out all ports.
- The forwarding of broadcast and multicast frames can be a scalability problem for large flat (switched or bridged) networks.
- A router does not forward broadcasts or multicasts. All devices on one side of a router are considered part of a single broadcast domain.

Network Efficiency

Frame Size

- Using a frame size that is the maximum supported (MTU) for the medium in use has a positive impact on network performance for bulk applications. The MTU can be configured for some applications.
- In an IP environment, you should avoid increasing the MTU to larger than the maximum supported for the media traversed by the frames, to avoid fragmentation and reassembly of frames. When devices such as end nodes or routers need to fragment and reassemble frames, performance degrades.

Windowing and Flow Control

- **Need to understand windowing and flow control:-** A TCP/IP device, for example, sends segments (packets) of data in quick sequence, without waiting for an acknowledgment, until its send window has been exhausted. A station's send window is based on the recipient's receive window. The recipient states in every TCP packet how much data it is ready to receive. This total can vary from a few bytes up to 65,535 bytes. The recipient's receive window is based on how much memory the receiver has and how quickly it can process received data.
- One can optimize network efficiency by increasing memory and CPU power on end stations, which can result in a larger receive window.

Characterizing QoS Requirements

Analyzing network traffic so far:

- Identifying flows,
- Measure the load for flows, and characterizing traffic behaviour such as broadcast and error recovery behaviour.

Need to also characterize the QoS requirements for applications.

- Some applications continue to work (although slowly) when bandwidth is not sufficient.
- Other applications are inflexible and are rendered useless if a certain level of bandwidth is not available.
- Voice is also inflexible with regard to delay, and is sensitive to packet loss, which results in voice clipping and skips