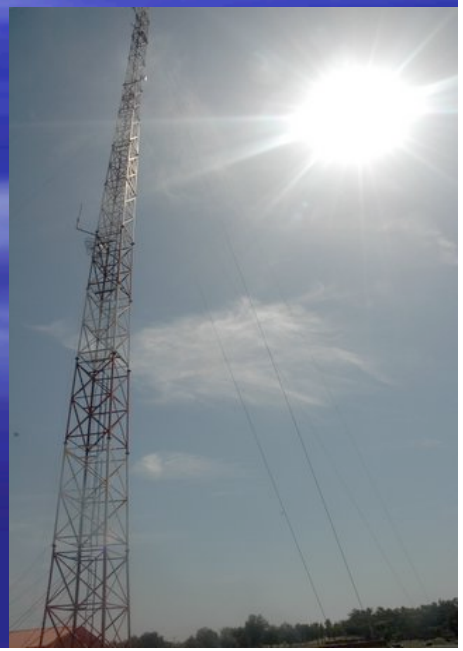
Designing, Developing and Implementing a University Network: Wired and Wireless Infrastructure in a Rural Environment“

Prof. Muhammadou Kah
&
Mr. Folorunso Aliu



OUTLINE

- Introduction
  - PART A
    - Tutorial #1: Gathering Requirements
    - **Tutorial # 2: Analyzing the Network**
    - **Tutorial # 3: Logical Network Design**
    - **Tutorial** Evolution of Wired & Wireless Networks
    - Wired & Wireless LAN in the Enterprise
    - LAN Design Paradigm
    - Wired Local Area Networks **# 4: Physical Network Design**
    - **Unit 5: Designing a Small Network**
    - **Tutorial # 6: Large Network Case Studies**
  - PARTB

OUTLINE –Cont'd

- PARTB
  - Evolution of Wired & Wireless Networks
  - Wired & Wireless LAN in the Enterprise
  - LAN Design Paradigm
  - Wired Local Area Networks
  - Design Considerations in Wireless Local Area Networks
    - Speed/Standards Coverage (How far the signal reaches)
    - Density (How many clients can connect concurrently)
    - Security Issues
    - Standards (802.11, 802.1x etc)
    - Authentication/Access
    - Authorization
    - Encryption
  - RF planning/Management
- Design, Developing and Implementing Wired/Wireless Networks – AAUN Case Study
- Summary
- **Implementing and Managing Networks**

NETWORK DESIGN 101

Tutorial #1: Gathering Requirements

- Here we outline a formal five-phase approach to network design.
- This phased process covers the majority of areas that must be considered in most networking analysis and design projects.
- Topics
  - 1 - The Network Design Process
  - 2 - Business Requirements
  - 3 - User Requirements
  - 4 - Application Requirements
  - 5 - Computing Platform Requirements
  - 6 - Network Requirements
  - 7 - Developing a Requirements Specification Document

Tutorial # 2: Analyzing the Network

- Analysis is the second phase of the network design process. The lessons of the unit focus on the Traffic Specification and Requirements Specification elements of this process, and explain general concepts of network performance and traffic.

- Topics

1 - Review of Internetworking Devices

2 - Network Performance Concepts

3 - Estimating Traffic Volumes and Patterns

4 - Taking Baseline Measurements of LAN Traffic

5 - Developing a Traffic Specification Document

Tutorial # 3: Logical Network Design

- Here we focus on the Logical Design phase.
- Each topic focuses on a different technological design consideration, such as physical media characteristics, wide-area performance, network management, security, and Transmission Control Protocol/Internet Protocol (TCP/IP) addressing flexibility.

- Topics:
  1 - Overview of the Logical Design Phase
  2 - Physical Layer Considerations
  3 - Internetworking Device Considerations
  4 - Optimizing WAN Performance
  5 - Network Management with SNMP and RMON
  6 - TCP/IP Addressing Considerations
  7 - Security Considerations
  8 - Firewall Considerations
  9 - Developing a Logical Design Document

Tutorial # 4: Physical Network Design

- This unit provides an overview of transmission media basics, including a look at structured wiring systems, cable characteristics, wireless LANs, and installation.

- Topics
  - 1 - Overview of a Structured Cable Plant
  - 2 - Copper Cables
  - 3 - Fiber Optic Cable
  - 4 - Wireless LANs
  - 5 - Developing a Physical Design Document

Unit 5: Designing a Small Network

- The lessons in this unit apply the network design process as we gather requirements, analyze, and design a small network for an imaginary company.

- Lessons
  Lesson 1 - Requirements Gathering and Analysis
  Lesson 2 - Logical Design
  Lesson 3 - Physical Design
  Lesson 4 - Project Summary and Project Schedule

Tutorial # 6: Large Network Case Studies

- In this tutorial, we broaden our perspective to consider more general goals, such as:
  - (a) network availability
  - (b) performance and
  - (c) Internet connectivity.

- Tutorial
  - 1 - Designing for Internet Connectivity
  - 2 - Designing for Performance: Gigabit Ethernet
  - 3 - Designing for Performance: ATM
  - 4 - A Three-Stage ATM Migration
  - 5 - Converged Networks
  - 6 - Designing for Availability

Tutorial #1 1: Gathering Requirements

- Here we outline a formal five-phase approach to network design.
- This phased process covers the majority of areas that must be considered in most networking analysis and design projects.
- It can be used by an outside consultant or an internal Information Services (IS) group.
- This network development process, as presented here, is very methodical.
- This level of detail helps ensure that the designer gathers all necessary information, considers all options, and keeps all key players well informed.
- Experienced network developers have found that this approach is essential to keep large projects on track.
- However, although there are many benefits to following a formal process, not every project requires such a detailed approach.
- Once you understand the reasons and methods of this process, you can modify it to fit the size and scope of most projects.

1 - The Network Development Process

Introduction

- Here we introduces the five-phase network analysis and design process that we will follow throughout this tutorial, and shows how it is similar to the phased development approach commonly used in software development and engineering.
- We will discuss why a formal process can prevent many of the most common problems in any technical design work, then describe how each phase of the network development process forms a logical sequence of events referred to as the systems development life cycle (SDLC).

1 - The Network Development Process

The Case for Formality

- As with any technical discipline, a process needs to be followed when designing a network that fills a particular business need.
- Rather than a bureaucratic burden that interferes with the "real work" of network building, a good formal development process makes the developer's work simpler, more productive, and more satisfying.

- Time pressure is a fact of life, and many technical professionals are continually tempted to skip a formal design and "get right to work."
- However, even the simplest development process can help a network avoid the following problems:

a) Failure to meet requirements--If you do not find out what the requirements actually are, it is impossible to create a network that meets them.

b) "Creeping" requirements--Specification additions and changes can disastrously increase the amount of time, effort, and money spent on a project. All change requests must be clearly documented, communicated, and evaluated.

c) Missed deadlines and budget overruns--Haphazard projects almost always take longer and cost more than well-planned ones, often because work must be redone. Also, when you "shoot from the hip," it is easy to miss cost-saving opportunities.

d) Dissatisfied end users--Regardless of how good a network appears, it is a failure if it does not satisfy those who must use it.

e) Dissatisfied management--A haphazard and unprofessional development project can hurt your credibility and create ill will among decision makers.

- A formal process does not have to be burdensome, or any more complex than necessary.
- A development process is like a construction blueprint. Large office buildings require many complex drawings and schedules, but even a tool shed should start with a simple sketch.
- Therefore, a small network project may only require a process as simple as documenting the initial requirements, implementing the solution, and documenting the resulting changes in the network.
- Larger and more complex jobs often require a formal, highly documented process.

The Systems Development Life Cycle

- The process of creating a new system, or changing an existing system, is called a life cycle. During this cycle, a new network or feature is planned, implemented, and maintained. The process begins anew with each change. This cycle is very similar to the SDLC long used by software engineers and system analysts.
- Although no single life cycle perfectly describes all development projects, two general life cycle patterns have been identified by software engineers:
    a) the waterfall cycle and
    b) the spiral cycle.

One of these life cycles describes every network development project to some extent.

Waterfall Cycle

The waterfall life cycle is defined by distinct stages. Different waterfall-based processes have different names for the stages, but they all tend to follow these five general steps, in order:

1. Analyze
2. Design
3. Build
4. Test
5. Deploy

This life cycle is called a waterfall, because work "flows down" from one stage into the next, as shown on the Waterfall Cycle Diagram. After the system is deployed, the life cycle begins again for the next update.

Waterfall Cycle

When a development process follows the waterfall model, each stage must be completed before the next stage can begin. Returning to a previous stage is often not permissible. In this case, changes that are not possible during the current development cycle are scheduled to be part of the next. When returning to an earlier stage is permissible, there are usually repercussions. The completion date is often extended as a result, and significant budget overruns are common.

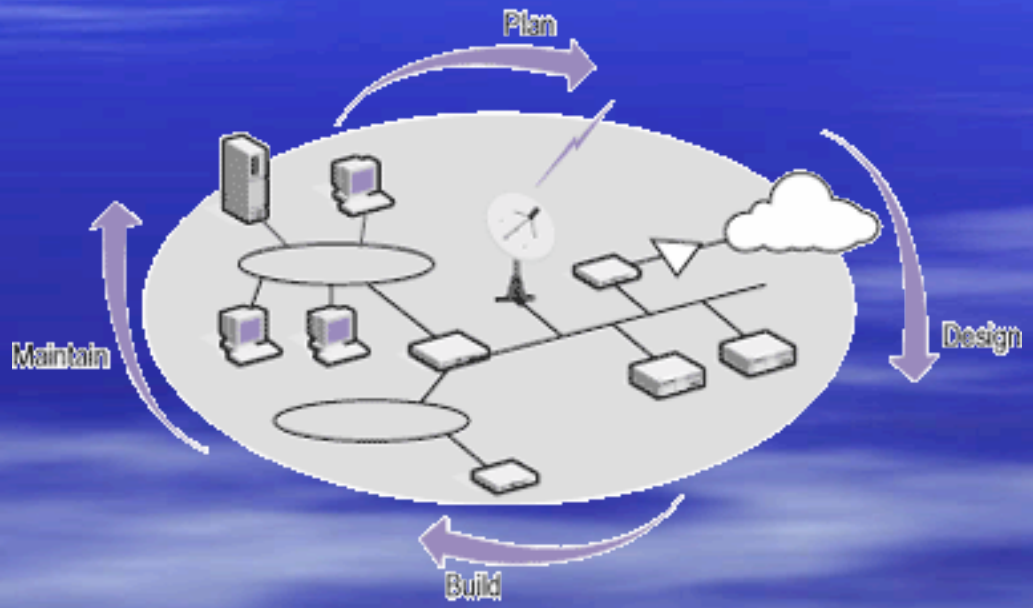
The major advantage of the waterfall cycle is that all planning is done in the early stages. All system stakeholders know exactly what is expected and what stage the process is currently in. Completion dates can be determined at an early stage, and coordination is simplified.

Although the rigidity of the waterfall is appealing to many developers (who can use it as a shield against users who suggest late project changes), it can be cumbersome for any but the smallest projects. In addition, because the requirements of a project often change before the project has been completed, the rigidity of the waterfall cycle can lead to development setbacks.

Spiral Cycle

The spiral cycle, or whirlpool cycle, is a variation of the waterfall cycle. It is a more recent approach, meant to overcome some of the limitations of the waterfall cycle. This cycle is often used in multiple-version software development projects; however, some of its principles can be applied to network development as well.

The guiding principle behind the spiral cycle is change management. Unlike the waterfall cycle, the spiral cycle can adapt quickly to new requirements. This is accomplished by looping through all stages several times, producing a limited version of the project each time, as shown on the Spiral Cycle Diagram.



Spiral Cycle

By building a subset of the eventual features in each iteration of the network design, its users get an opportunity to provide feedback on the project before it is finished. Their feedback is then incorporated into the next iteration of the spiral. With each iteration, new features are incorporated and prior problems are fixed.

Although the spiral life cycle handles changing requirements much better than the waterfall cycle, it also has significant limitations. Because there is no way to guess what new features may be requested, it is difficult to estimate the total eventual cost and release date. In addition, major features that require longer development times are difficult to implement. Most importantly, when following a spiral development life cycle, it is very easy to fall into a never-ending series of upgrades.

The Network Design Process

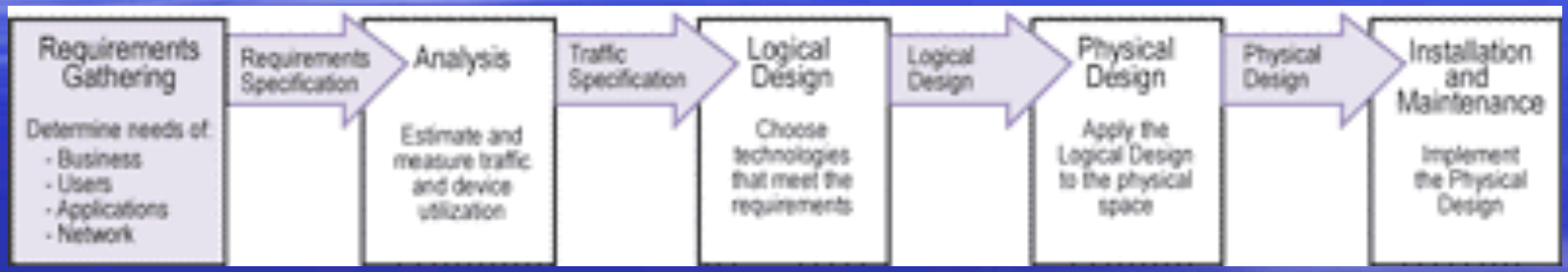
The waterfall and spiral cycles do not perfectly describe all network development projects, and a single project may change from one cycle to another. For example, a waterfall model may describe the process of designing and launching a new network, while a spiral model might better describe its ongoing updates and maintenance.

The network development process describes the general tasks that must be accomplished when developing a network. However, each project has its own unique needs that may require a different process with different tasks.

Process Phases

The phases of a process break a large project down into understandable, manageable pieces. If you think of a project as a long list of tasks, these phases are simply task categories. In other words, each phase includes certain jobs that must be performed to prepare the project to move to the next phase. The life cycle of a typical network development project consists of the following phases, as illustrated on the Network Design Process Diagram:

1. Requirements Gathering
2. Analysis of the Existing Network
3. Logical Design (also referred to as Conceptual Design)
4. Physical Design (also referred to as Final Design)
5. Installation and Maintenance



Network Design Process

This process can apply to either a waterfall or spiral SDLC. In other words, the process only defines the phases of a life cycle. The decision whether to complete each phase before starting another (waterfall), or work through several iterations of the process in one life cycle (spiral), is up to an organization.

Deliverables

You can also think of a project in terms of what it is trying to produce--its "deliverable." For example, if someone asks, "What is the project's deliverable?" you could answer, "a network." However, to get to the final goal of a functioning network, the development team must produce many supporting products, such as design documents, estimates, or reports. Each phase produces its own deliverables that become the input to the next phase.

Like the invisible foundation of a building, these deliverables form a strong structure that strengthens the overall design. Therefore, all documentation that records your design assumptions, technical alternatives, customer information, and management approval should be retained for easy access and future reference.

As you work through this course, it is important to remember that not all projects require all of these phases or deliverables. Smaller projects may skip some phases, or combine them. Once you understand the reason for each phase, task, and deliverable, you can decide how much of this formal process is necessary for each of your development projects.

The Network Development Process

- **Phase 1: Requirements Gathering**

This is the most crucial phase in the development process, because requirements provide the target your network design must hit. However, although requirements analysis is fundamental to the network design, it is often overlooked or ignored because it is one of the most difficult phases of the overall design process.

Gathering requirements means talking to users, managers, and other network personnel, then summarizing and interpreting the results. Often, it means resolving conflicting needs and desires among user groups. However, network personnel are often distanced from the users, and do not have a clear idea of what they want or need.

Requirements analysis is time-consuming, and it may appear to produce no immediate results. On the contrary, requirements analysis helps the designer to better understand how the new network should perform. Therefore, Requirements Gathering produces immediate payoffs in:

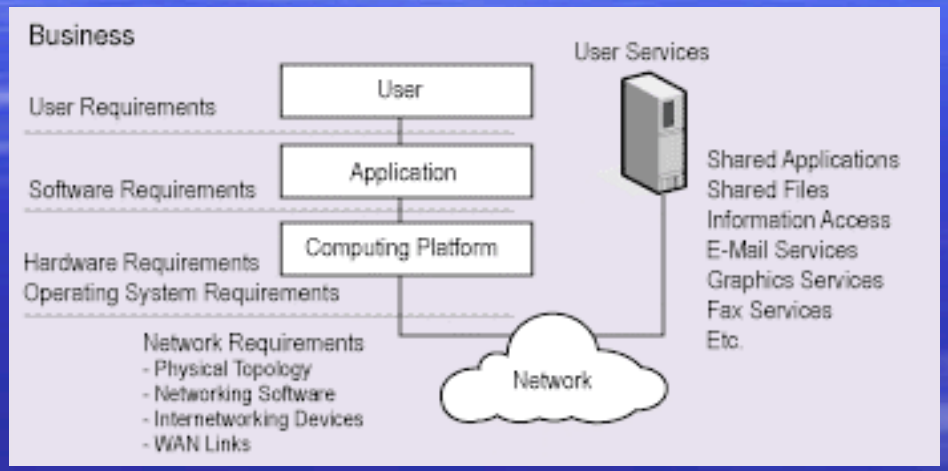
- Better view of current network
- Objective decision-making
- Ability to plan for network migration
- Ability to deliver appropriate resources to all users

Requirements for All Types of Needs

Just as different types of users have different networking needs, each aspect of the organization has its own requirements. In this course, we discuss the need to gather requirements for:

- **The business or organization as a whole**
- **Users**
- **Applications**
- **Computing platforms**
- **The network itself, and the network staff**

The Areas of Requirements Diagram shows these in a layered format with the associated services and requirements at each layer.



Areas of Requirements

The Requirements Gathering process is a series of steps. We begin by gathering requirements from upper management or the owners of the business. Next, we work with the user community, gathering the network requirements for supporting the users, their applications, and the base of installed computing equipment. The network itself is the last consideration; we gather all other requirements before considering the network or network technologies.

Qualities of Good Requirements

- The concept of "garbage in, garbage out" applies to requirements Gathering.
- Good results depend on gathering good requirements that are both user- and business-centered, as well as detailed and specific.
- It is common for network professionals to base a network design solely on a particular technology, service, or vendor (typically ones the designer has the most experience with). However, this makes as much sense as designing a house without knowing anything about the people who will live there.
  A network is not an end in itself; it is a highly customized tool that helps people do their work. Thus, designers must deliberately postpone any technical decision-making, and focus instead on discovering what factors make a real difference to users. Do they have enough storage space? Do their applications perform well? Are people waiting too long for print jobs? Is the security system understandable and usable? Do any network problems really get in their way? A network designer must provide the customer with the proper equipment design to match the specific business.
- Network designers cannot be expected to understand the jobs of system users. However, users often assume that certain "essential" features will be part of a network, even though they never explicitly ask for them.
- The Requirements Gathering phase is a chance to define, as precisely as possible, what users want and need. Detailed requirements make it more likely the final network will satisfy its users. Specific requirements help guard against "scope creep," the process of gradually adding requirements until a project becomes unrecognizable.
- Good Requirements Gathering techniques will not only help individuals do their work, but will also improve the overall productivity of the organization, providing a competitive edge in the marketplace.

- ***Looking to the Future***

  The Requirements Gathering process must consider both the current and future needs of the organization. Without proper planning for future growth, it will be difficult to expand the network later.

- ***Deliverable: Requirements Specification Document***

  The network designer must formally record the requirements in a Requirements Specification document that describes exactly what the organization and users need from the network. This document should not propose solutions or designs (that will come later); instead the Requirements Specification should clearly and specifically summarize the needs and desires of the organization and users.

  After the Requirements Specification document has been written, management and network designers should formally agree that it is correct. In other words, the responsible stakeholders must all sign off on the requirements. At this point, the requirements document becomes an agreement between the development team and management. Management agrees that the requirements document describes the system they want; the network developers agree to deliver that system.

  After the Requirements Specification document has been formally accepted, the development process can move forward to the next phase. However, although formal requirements documents are vitally important, they are not written in stone. Things change, new factors arise, and the key players should always be willing to renegotiate the network requirements. However, a formal requirements process helps makes it clear to everyone that there is always a price (in time, money, or features) for any requirements changes.

Phase 2: Analysis of the Existing Document

When a network design project upgrades or enhances an existing network, it is essential to analyze the existing network architecture and performance. The Analysis phase complements the Requirements Gathering phase; requirements show you where you need to be, and analysis tells you where you currently are.

The effectiveness of a new network design depends on whether the current computing infrastructure can support the new requirements. The existing network installation and its supporting systems may be an asset to the new development, or a liability. Therefore, after the Requirements Specification has been written, but before the design process begins, the development team must thoroughly analyze the existing network and any other resources the new network may depend on.

A thorough analysis should gather both qualitative information (such as user estimates of storage and traffic) and quantitative data (such as traffic measurements and network management statistics). A Traffic Specification Document is created during this phase of the design, and is considered a formal deliverable before proceeding to the Logical Design Phase.

Deliverable: Traffic Specification Document

The network Analysis phase should produce deliverables such as:

- Logical diagram of the current topology
- Estimated traffic volumes and patterns that describe the network capacity required for each application, each network segment, and the network as a whole
- Detailed statistics, baseline measurements, and any other direct measurements that describe the network's current level of performance
- A report on the quality of service provided by suppliers of Internet connections or wide area network (WAN) links
- A list of design constraints, such as the need to use existing cabling or devices

Phase 3: Logical Design

- The Logical Design describes what the network must do, and how it must perform, to meet the requirements.
- A Logical Design specifies how data flows through a network, not where particular network elements are physically located (that comes in the next phase).
- The designer creates a logical network structure based on the Requirements Specification and results of the network analysis.
- If the current hardware or software cannot meet the needs of the new network, they must be upgraded. If current systems can be reused, the new design can integrate them.
- If not, the team can find new systems, and test them to confirm they meet the requirements.

Deliverable: Logical Design

- A Logical Design identifies the services, equipment, network architecture, and addressing structure necessary to create a network that satisfies its requirements. This phase should produce a Logical Design document that includes:
  a) Logical network diagrams
  b) Addressing strategy
  c) Security scheme
  d) Specification of hardware components, software, WAN links, and general services
  e) Specification of new hires or training for the network staff
  f) Initial cost estimates for hardware, software, services, personnel, and training

Phase 4: Physical Design

- The Physical Design shows how to make the Logical Design work in the real world.
- In this phase, the network designer creates a detailed specification of the hardware, software, links, services, and cabling necessary to implement the Logical Design.

Deliverable: Physical Design

- Physical Design outputs guide the equipment procurement and installation, thus the Physical Design document must be as specific and detailed as possible, often including:
  a) Physical network diagrams and to-scale wiring plans
  b) Detailed lists of equipment and parts
  c) Cost estimates for hardware, software, and installation labor
  d) Installation schedule that specifies the time and duration of physical or service disruptions
  e) Post-installation testing plan
  f) User training plan

Phase 5: Installation and Maintenance

Installation

- A smooth installation is the reward for thorough work in the first four phases. When network developers are disciplined enough to invest real effort in the earlier phases, they find that they have already solved or prevented many common installation problems.
- Of course, the main output of the Installation phase is the network itself. However, a good installation should also produce:
  - a) **Updated diagrams** (**logical** and physical) that include all last-minute changes
  - b) **Cabling**, **connections**, and **devices** that are clearly labeled
  - c) Any **notes or documents** that can simplify later **maintenance or troubleshooting**, such as test results or new traffic measurements

- Any necessary hardware or software must be purchased and tested before installation can proceed.
- In a broader sense, any resources the network needs before its final deployment should also be arranged.
- New employees, consulting services, training, and service contracts are all resources that may need to be in place.
- The procurement of these resources should always occur before installation begins in earnest.
- If a vital system cannot be procured and tested prior to installation, a complete or partial redesign may be necessary.
- Although painful, it is better to deal with it before the network staff has already dismantled sections of the existing network.
- The objective of the whole design process is to answer questions, make decisions, and discover problems before the Installation phase begins.
- However, nobody is perfect, and the best plans cannot always prevent unexpected problems.
- Therefore, it is important that the designer participate in the network's installation.

Maintenance

- After the network has been installed, the network staff shifts its focus to getting input from the user community and monitoring the network itself for potential problems.
- As each set of additional requirements arises, the network life cycle repeats.

Tutorial #2 – University/Business Requirements

Introduction

- As we all know, a network is a tool that helps people do work.
- Like any user, a University or an organization is an entity with its own **needs**, **problems**, and **plans for the future**.
- Therefore, in the first part of the requirements gathering process, we focus on the needs of the University or business as a whole.
- Just as a network can influence the productivity of an individual user, a network can also contribute to the success or **failure of an organization**.

- **Key Point**
  Designing a network without requirements is like starting a trip without a destination.

Requirements from the Organization's Perspective

- To gather business requirements for a network, you must first understand the nature of the organization that will use it.
- Each network is **a unique**, **customized solution**. Therefore, we must make design choices that are best for each individual type of organization.
- If you are employed by the University or Organization, you probably already understand its **objectives** and **business needs**. This puts you in a better position to **match network requirements** to the organization strategy.
- If you are an independent consultant, it will be more difficult to create a **network design that fits the strategic intent of the University or the organization**.
- You can begin your research through World Wide Web (Web) site analysis, then conduct detailed interviews with management and key personnel.
- Knowing the **strategic nature of the organization** will help determine some of the **general network requirements**, such as **security**, **redundancy**, and **reliability**.

- Whether you work from the inside or outside, you must still gather the same detailed organization requirements for all projects. These include:
    a) Key players
    b) Major milestones
    c) Funding levels
    d) Type of university or business activity
    e) Estimated growth
    f) Reliability and availability
    g) Security
    h) Web site and Internet connectivity
    i) Remote access

Key Players

- **Human contacts are not part of the technical network requirements**. However, before you can begin gathering the technical requirements, you **must know who to ask**.
- To identify the key players and key groups in the organization, an organization chart is a good place to start.
- As you gather requirements, you will start at the top of the organizational structure and work your way down. In general, you will work with two types of key players:
  a) **Information sources can explain organization strategies, long-term plans, and other general business requirements.**
  b) **Decision makers will approve the overall network design, or establish funding levels.**

- Occasionally, a key information source may also be a decision maker. However, **it is common to gather information and requirements** from some people, and seek approval from others.
- **Communication** is a critical component to the success of **the analysis, design, and implementation of a network**.
- As an outside consultant, or member of an internal Management Information Services (MIS) staff or IT or ICT department, you **must establish contacts with the appropriate levels of management** and **technical staff before beginning the Requirements Gathering phase**.
- As you make these contacts, **learn which of these key players will oversee the network design process**.
- Then, work within the **existing reporting structure to keep these decision makers well informed**, using the methods (*telephone, electronic mail [e-mail], etc*.) that each one prefers.

Major Milestones

- **Timing** is a key factor in any network implementation. The **most common time constraint is a completion deadline.**
- However, the organization may have other important requirements, such as a **particular start date**, **limited period of downtime during installation**, or **particular activity the project must not disrupt.**
- Large-scale projects **require a project plan** to **track project activities**, **key players**, and **required dates**.
- Like the network design itself, a project plan begins as a general outline that you refine as you work.
- At the beginning, **establish dates for the major project phases**, and **add details as you gather more information**.

Funding Levels

- **Cost**, both for **implementation** and **ongoing maintenance**, is **a major constraint in the design of a network.**
- At least one key player (such as an MIS/ICT/IT director or VC's /President's of University or VP for Finance & Admin or MD etc.) will have the authority to determine the amount of money that can be spent on the project.
- Because funding is **a management issue**, **the organization management must be intimately involved in the network design process.** How?
- When **summarizing costs and features for management**, **consider both recurring** and **nonrecurring costs**.
- The **Funding Considerations Table lists cost categories that you should consider when reviewing costs** for:

(a)network design

(b)Implementation

(c) and ongoing maintenance and support.

Funding Considerations

Cost Factor	Nonrecurring Costs	Recurring Costs
Networking Hardware	×	
Networking Software	×	
UPS & Generators	×	
RAID	×	
Virus Protection	×	×
Applications	×	×
Network Utilities	×	
Diagnostic Equipment	×	
Telecom Line Charges	×	×
Personnel		×
Maintenance		×
Energy (ex. Diesel Fuel)	×	×
Training	×	×

Type of Business Activity

- A network is a tool that helps people perform their work. Thus, **before you can design the right tool**, you must understand the work it must do.
    a) For example, 50 University Staff using word processors will strain a network much less than 50 architects using computer-aided design (CAD) systems.

Estimated Growth

- A good network is scalable; it can expand as the company grows.
- Therefore, to know **how much scalability a network needs**, **you must have some estimate of how much your organization plans to grow.**
- You can estimate growth by:
  - a) **the number of new employees your organization plans to hire over the next three to five years**,
  - b) or **by the estimated increase in the amount of network traffic.**
- An estimate of new hires is easier to get, but is also less precise. **If possible, it is best to combine hiring rate** with **estimates of increased application traffic**.
- We also need to know:
  - a) **where the growth is expected. Will your organization open remote locations in the near future?**
  - b) **Does your organization plan to implement or expand a Web site?**
  - c) **Location of network nodes is a key requirement that will also drive the design of the network.**
- Forecasting future growth can have an impact on the network design, as well the applications and underlying software and hardware systems.

Reliability and Availability

- To determine your organization's need for network reliability and availability, simply ask, "What will happen if the network goes down?"
- To some organizations, occasional network downtime is only a minor nuisance. To others, such situations can cause serious damage, including:
    a) Lost productivity because of idle employees
    b) Lost revenue caused by business going elsewhere
    c) The direct expense of support needed to get the local area network (LAN) running again
- Most LANs provide 99+ percent availability; however, this may not be enough for some organizations. In a 24 x 7 business (a business open 24 hours per day, 7 days per week), even 97 or 98 percent availability means that the network is down approximately 30 to 45 minutes per day.
- What happens to a bank if its network of automatic teller machines is down for 45 minutes on a Friday afternoon? What happens to an online stock brokerage if its network fails for 30 minutes during a period of frantic market activity?

Security

- Security requirements also vary from organization to organization. Many businesses have only modest security needs, usually to protect customer or student information or financial records.
- However, some organizations require extremely high security, such as government agencies or companies conducting top-secret development work. This type of organization might require high levels of security clearances for employees, and strict procedures to control information entering or leaving the facility.
- However, even purely private-sector companies are becoming more security-conscious, because security breaches can affect organizations in unusual and subtle ways.
- Even high-security organizations may not need the same level of security for all of its activities. A firm may have high security requirements for certain types of information, while other information is considered public domain. Therefore, network designers should note the security requirements of each type of application and data.

Web Site and Internet Connectivity

- E-commerce is becoming a mainstay of business; the question is not whether to use the Web, but how.
- While retail merchants continue to find new ways to make money directly from the Web, other types of businesses are finding new ways to use the Web to enhance and streamline their existing business processes.
- A corporate Web site or intranet **adds its own layer of business requirements to a network design**, whether the company builds the site on its own network or uses the hosting services of an Internet Service Provider (ISP).
- To design a network with the **right levels of reliability**, **availability**, and **security**, **you must fully understand the details of an organization's Internet business strategy**.

Remote Access

- The proliferation of LANs is making a profound impact on the way organizations do business. Not only do users expect to have computers at their desks, they expect remote network connectivity as well.
- The need, and desire, to work anywhere and at any time is creating the need for secure and reliable remote LAN access.
- Remote access allows users to function as full network peers from distant locations, such as a customer's office, employee's home, or a hotel or airport.
- In addition to file transfers and e-mail access, print service and other special LAN applications are essential for telecommuters, traveling professionals, and field service or delivery personnel.

Output: Business Requirements List

- As you interview key management players about the overall business requirements, capture this information in some form that you can use throughout the design process.
- Every business is different, so the format of this information will vary from project to project.
- However, most business requirements documents should address the items we have discussed in this lesson:

Key Players

a) Names of information sources

b) Names of decision makers

c) Contact information (addresses, numbers, and preferred contact methods)

Milestones

- Required project start or end dates
- Availability of key players (upcoming vacations or business travel)

Tactical versus Strategic Information

- Request management list specific functions that are required in the system.
- Reasons to consider specific features on the new design are:
    a) improve productivity,
    b) competitive advantage, and
    c) reduce operation costs.

Tutorial # 3 - User Requirements

Introduction

- In our earlier discussions, the importance of gathering requirements **from the point of view of the organization as a whole.**
- In this part of the requirements Analysis phase, we gather network requirements **from the users' perspective.**
- At this point in the Requirements Gathering process, we are interested in general things, such as:
    a) **overall usage patterns**
    b) **common problems**
    c) **rough traffic estimates, and**
    d) **subjective perceptions of service quality**
- We want to **identify potential trouble spots**, and **we want users to suggest features that can help them be more productive**.
- We will **not decide how to fulfill these requests until later phases of the design process**; at this point we are only gathering information.
- However, **it is important to gather good, clear information, because these broad impressions will guide the exact measurements we will make during the network Analysis phase.**

Key Point

User perceptions are often subjective and imprecise, but contain important design information.

The Users' Perspective

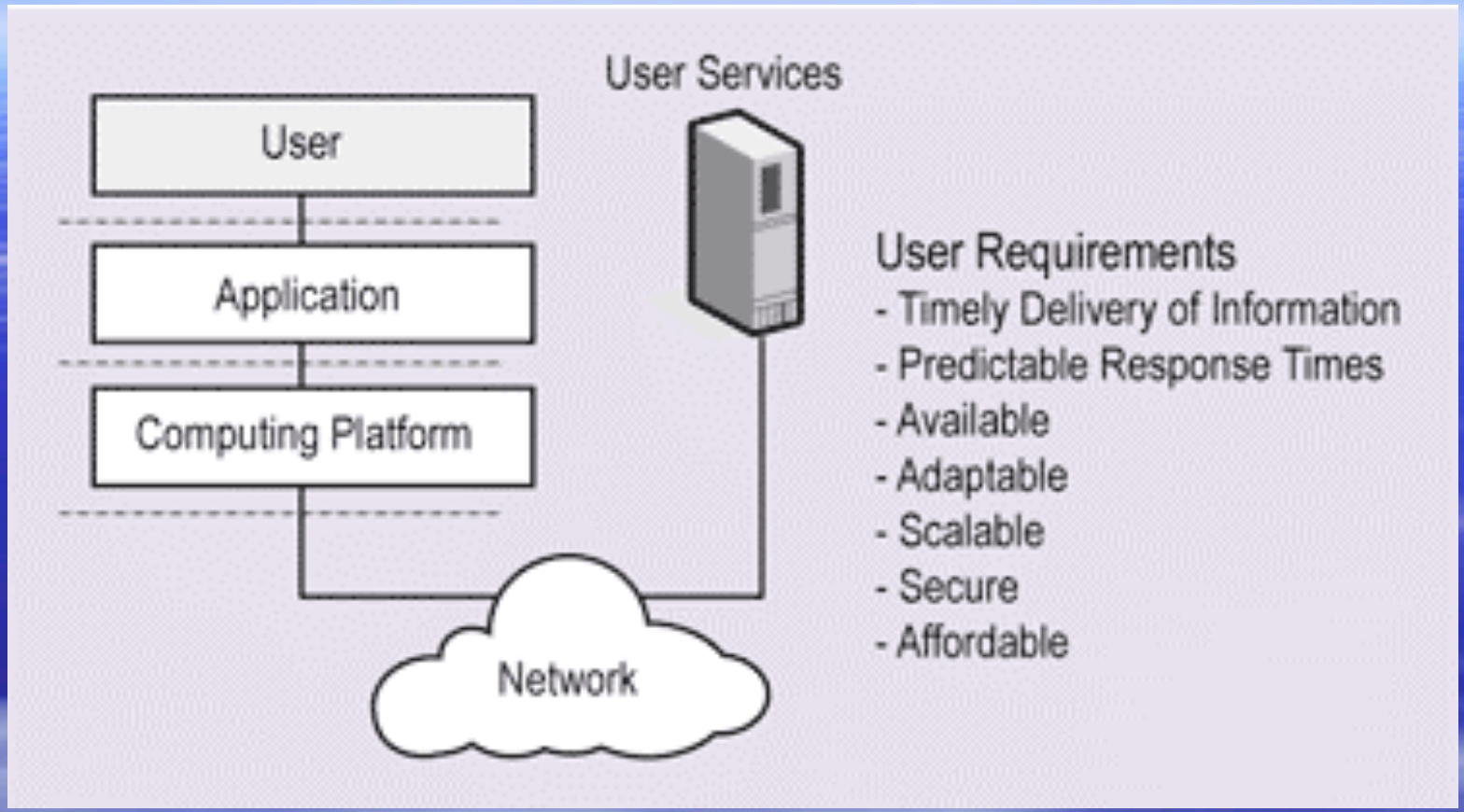
- To **design a network that meets users' needs**, we **must find out what network services or functions are important for users to get their work done**.
- These services **may or may not need a network**. Some user services are provided by **local applications that only need the user's computer and attached peripherals.**
- Other services **need network connectivity provided by a workgroup server, corporate mainframe, or Web server**.
- In many cases, a number of alternatives may provide the service needed by a user.
- The **process of gathering user requirements** is also complicated by the fact that **users rarely state their requirements in a technically precise way**. For example, commonly heard user requirements are:

  a) **"It takes too long to load files from the server."**
  b) **"I can't print to the color printer from my desktop."**
  c) **"The network seems to constantly be down."**
  d) **"If we ever lost these files, the company would be out of business!"**

- As a network designer, it is up to you to make the connection between user requirements, stated in common language, and network attributes.
  - ✓ **For example, "The network seems to constantly be down" identifies a problem with reliability and availability.**
- User-stated requirements are also subjective and variable, depending on the user's environment.
- However, at this stage, all input should be noted; eventually, you can use these subjective clues to guide more precise measurements.
  - ✓ **For example, if one department frequently complains of slow response times, but the other does not, that is a clue to investigate further.**

Common User Concerns

- User-level requirements, which impact applications, computing platforms, and ultimately the network, include factors such as the following, shown on the User Requirements Diagram:
  a) **Timely delivery of information**
  b) **Predictable response times**
  c) **Available**
  d) **Adaptable**
  e) **Scalable**
  f) **Securable**
  g) **Affordable**



User Requirements

Tutorial # 4 - Application Requirements

Introduction

- Each type of **software application** has its **own needs for network services**. Therefore, **determining the application requirements is the next step in the Requirements Gathering process.**
- In general, this step describes the kind of work people will perform on a network. For example:
  a) Will the network support standard office activities, such as word processing or
  b) accounting? Publishing or imaging? Video or audio production? Engineering or architecture? Software development? Manufacturing or industrial process control?
- The business activity of an organization strongly influences its network design, because each type of work has its own requirements for **applications**, **computing platforms**, and **network communications**.
- As you gather application requirements, **it is also important to note whether the same kind of activity occurs across the entire network, or whether different groups of users perform different types of work.**
  - ✓ **For example, a manufacturing plant may have completely different needs on the factory floor and the front office.**
- **Key Point**
  User and application requirements are closely related.

Typical Application Requirements

- When gathering information about an organization's **applications**, consider the following factors:
  a) Application type and location
  b) Usage of applications
  c) Growth
  d) Reliability and availability needs
  e) Network response needs

Tutorial # 5 - Computing Platform Requirements

Introduction

- Computing platform requirements are the next requirements to be gathered during this information gathering phase of the network design process.
- There are several reasons why it is important to understand the current level of an organization's computing hardware.
  - a) **First, the Requirements Gathering process can help determine the true causes of problems. Users often blame the network for slow performance; however, the quality of desktop computer microprocessors, memory, or input/output (I/O) bus can also degrade the performance of a user's system.**
  - b) **Second, inadequate components can also degrade the performance of network servers. Network performance bottlenecks are often caused by overworked servers.**
  - c) **Third, while a network redesign may provide an opportunity to upgrade servers or desktop systems, it is more likely that an organization's installed base of hardware can be a powerful constraint on a network design.**
    - ✓ **For example, plans for Fast Ethernet can quickly evaporate if it means replacing 2,000 10-megabits per second (Mbps) network interface cards (NICs).**

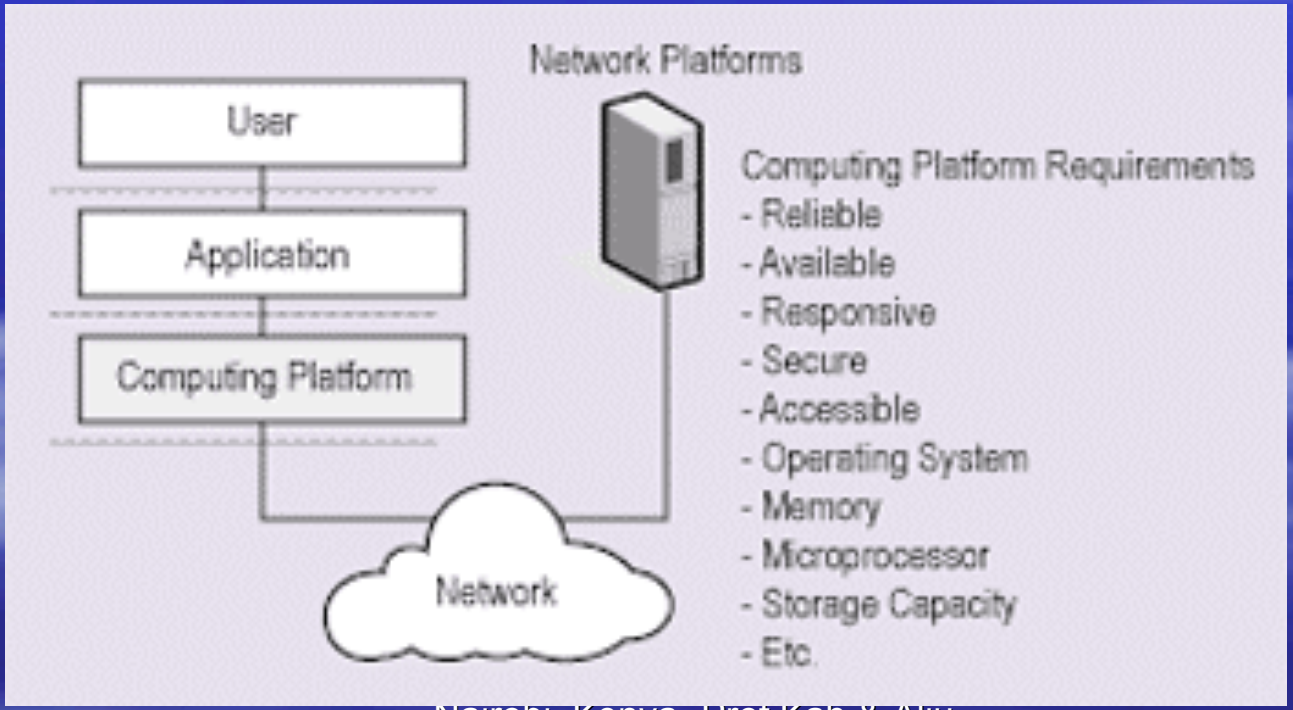
Key Point

The performance of individual computers is a key factor in overall network performance.

Types of Computing Platforms

- Networks include a wide variety of computing hardware. In general, computing platforms fall into three categories:
  a) PC's
     -Desktop
     -Server
  b) Workstations
     -Desktop
     -Server
  c) Midrange
  d) Mainframe
  e) Etc….

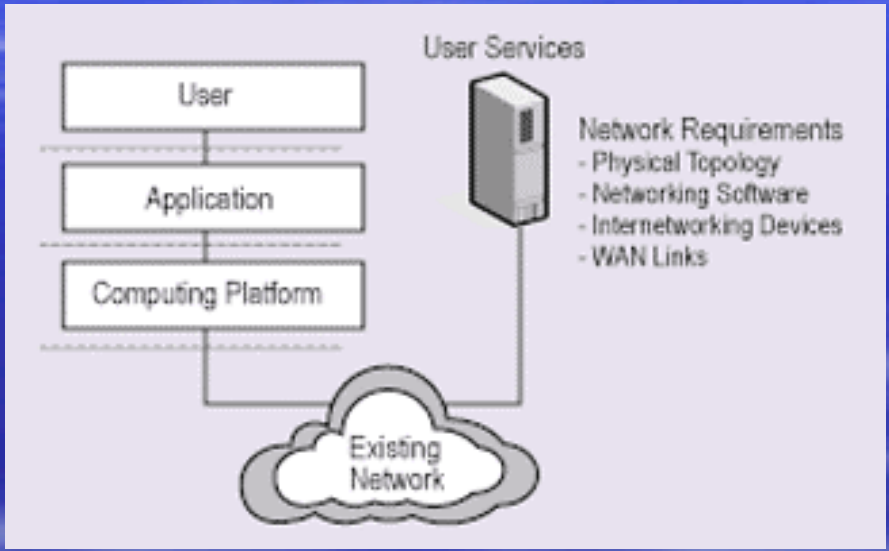
- Because both **the hardware characteristics and software** of each type of computer **have implications for the network design, the Requirements Gathering process must collect detailed information about every computer that will connect to the network**.
- The Computing Platforms Requirements Diagram illustrates where this process fits within the overall Requirements Gathering process.



Tutorial# 6 - Network Requirement

Introduction

Finally, we consider the requirements of the network itself, as well as the network staff that must maintain it. The Network Requirements Diagram demonstrates some of the network-specific consideration



Network Requirements

In this part of the Requirements Gathering phase, we examine the existing network to understand its current topologies, performance, and software. We also consider other broad requirements that should be reflected in the new network design.

Key Point

Network requirements describe the basic desirable qualities of a network.

Types of Network Requirements

- Just as users and applications have their own requirements, the network itself (and the network staff) has its own set of needs that must be considered in the network design. Some of these are:
  a) LAN functions
  b) Physical topologies
  c) Performance
  d) Networking software
  e) Security
  f) Economy and cost control
  g) Metropolitan area network (MAN) / WAN options

LAN Functions

- When evaluating a LAN, whether it is the initial implementation of a LAN or an existing LAN, there are many factors to consider.

- A good starting point is to summarize the functions necessary for the LAN to meet the particular organizational needs.

- A matrix, such as the LAN Function Matrix, can help you determine what functions are most important for individual portions of the LAN. For example, an engineering department that contains highly sensitive information may place a higher value on security and redundancy than other parts of the organization.

- To use such a matrix, you would use the requirements (business, users, applications, and platforms) you have already gathered. Based on that information, you can then rate the overall priority of each function.

Function	Segment X Rate Value (1-10)	Segment Y Rate Value (1-10)	Segment Z Rate Value (1-10)
File Services			
Print Services			
E-Mail Services			
Maintenance			
Reliability			
Security			
Management			
Scalability			
Redundancy			
Fault Tolerance			
Application Compatibility			
Wide Area Compatibility			
Backup Capabilities			
Performance			
Fax Services			

LAN Function Matrix

- Your application may require high-speed file transfer capabilities.
- Your environment may be distributed or centralized, or inter-networked or not--or maybe in the future it will need one of these features.
- You may need quick and constant access to the Internet, or the Internet may be the only feasible wide area alternative.
- If these decisions are not self-evident, the matrix is a way to resolve them.
- A matrix like this can also improve communication between **the network design team and key players in an organization**

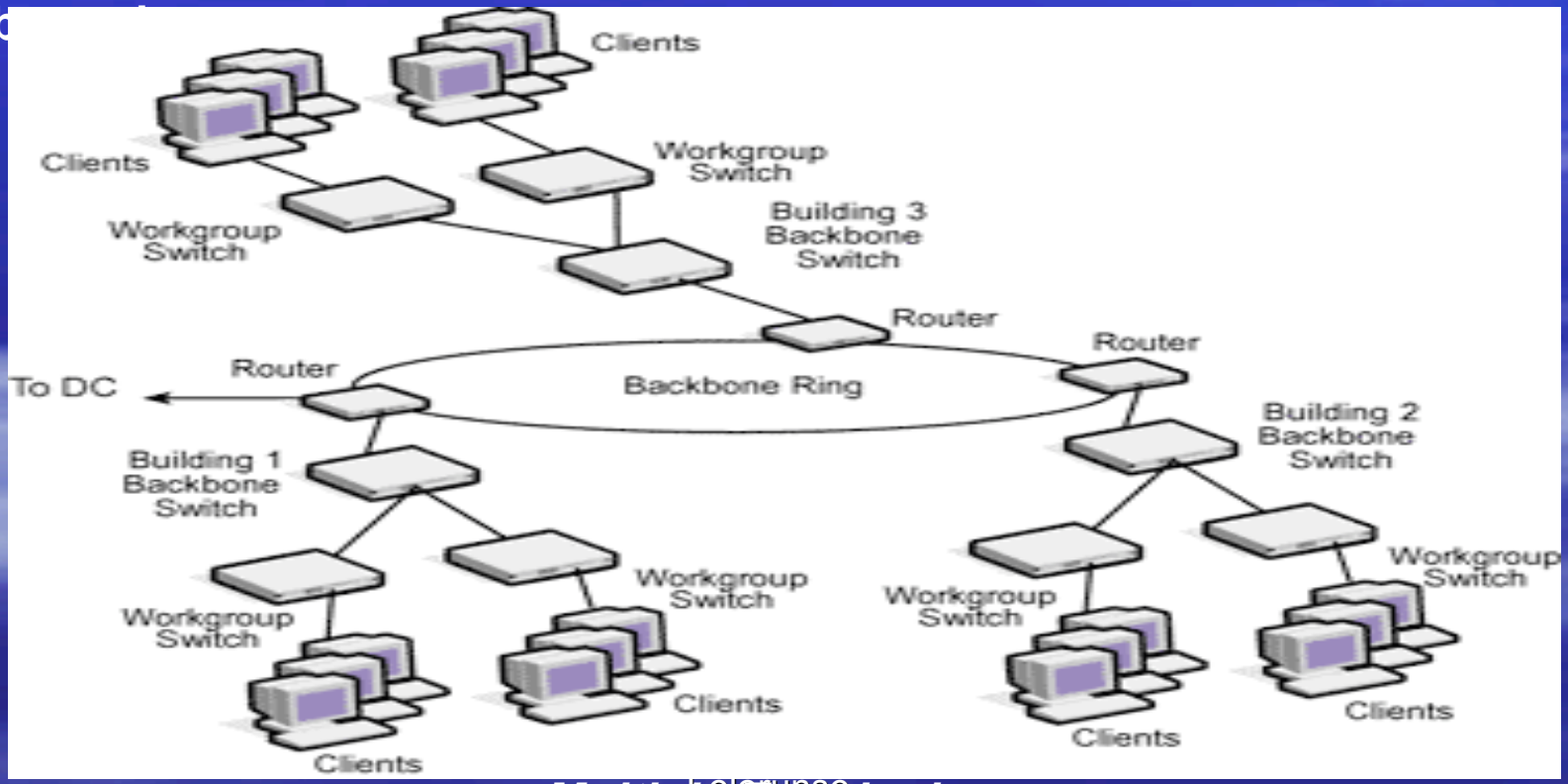
Physical Topologies

•Understanding the current LAN and WAN topologies **will provide insight into the current operation and potential modifications or upgrades that may be required.**

•Networks are physically configured in many different ways, and a single network typically consists of multiple topologies.

•Most organizations will have a diagram of the existing network, that can provide some initial insight into its logical structure.

•The **Multiple Topologies Diagram shows a switched Ethernet network consisting of three separate locations connected by means of a MAN backb**



Multiple Topologies

Performance

•Several performance metrics should be considered during the requirements Analysis process, including:

a) Capacity and response time

b) Availability

c) Recoverability

•These requirements are not always important to the user in the initial installation of a network; however, they should always be considered by the designer.

Capacity and Response Time

• Knowing the type of traffic the network will support will assist in understanding your LAN.

• If users **have provided estimates of their average transaction or file transfer sizes, as well as the number of times they access particular applications or resources, you can use these figures in simple calculations to estimate current and future network bandwidth requirements.**

✓As a general rule of thumb, most Token Ring LANs running at 4 Mbps, or Ethernet LANs running at 10 Mbps, can easily handle 20 to 25 users. Response time is not a problem in typical file transfer applications, but becomes critical in transaction-driven systems.

- If performance is not a specified design criterion, using general rules of thumb or rough estimations may be sufficient.

- If your design criteria are more precise, you can use network design tools to model the behavior of a LAN under a given load. These tools can give you an accurate picture of a LAN's performance, given a certain number of users, applications, and telecommunications links.

- Some tools include application profiles that provide estimates for traffic for specific applications. They may also have user libraries that contain performance profiles for various pieces of equipment, such as bridges and routers.

- These can be plugged into the model without doing a lot of research, and provide reasonable estimates of **device throughput and latency**. Many networking products have built-in capabilities to determine CPU utilization against network traffic.

- Purchasing separate design tools is expensive. However, if you **need an engineered network with high reliability, the cost of failure far outweighs that of the tool.**

Availability

The importance of availability affects the choice of the following:

- **LAN topology**
- **Server hardware--You may need redundant features, such as redundant power supplies and hard drives, or even redundant servers.**
- **Mass storage, such as a redundant array of inexpensive disks (RAID)**
- **Uninterruptible power supply (UPS)--What kind of supply is needed, and how long must the system provide power? Which components must use the UPS?**
- **Network operating system (NOS) selection and backup methodology--Do you need disk and/or server mirroring and/or duplexing?**
- **Vendors--When requirements are high, a company's reputation, product track record, and support quality become critical issues.**

Recoverability

The **information stored on servers or a key individual's hard drive is the lifeblood of your organization. Losing mission-critical information can be devastating.** Therefore, **keeping data properly backed up is a key element of a network's recoverability**.

• Before you can develop backup policies and choose technologies, you must assess the overall risk to the organization, and determine the relative importance of various types of data. In other words, not all data is mission-critical.

• And, of your mission-critical data, you must decide how frequently to back it up; some data changes by the minute, while other data can be archived once a year.

At a minimum, your recovery plan should include:

- A backup procedure that copies all files on a regular basis (the frequency depends on the business and data). Many media options exist, including digital audio tape (DAT) which has a storage capability of many gigabytes.
- Secure on-site storage that can protect backup media in the event of a small fire, flood, or other natural disaster. Usually, a small fireproof safe or storage box is adequate.
- Secure off-site storage to preserve backups even after the total destruction of the original building. Some organizations offer services that frequently replicate data at a secure storage facility. In the event of total failure or disaster, operations can be quickly moved to an alternate site.

• Good backup and archival procedures are only the beginning. An organization-wide disaster prevention and recovery policy should be developed, if one is not already in place.

Networking Software

There are several categories of networking software that should be considered, along with the desktop and server applications software mentioned earlier. These include:

a) **NOS**
b) Backup management and archiving
c) Network management

Networking Operating Systems (NOSs)

There are at least six NOSs commonly encountered in computer networks, some of these are intended for large-scale networks, others for specialized or small-scale networks.
The six primary NOSs found in networks today are:

- ✓ **Novell's NetWare and IntranetWare**
- ✓ **Microsoft's NT / 2000**
- ✓ **Banyan Vines**
- ✓ **UNIX / Linux**
- ✓ **AppleTalk**
- ✓ **LANtastic**

Backup Management and Archiving

Automatic backup software makes it simple and painless to perform regular full and incremental backups of all servers. The whole process occurs in the background, usually in the evenings, and takes anywhere from one to several hours, depending on the speed of the network.

Virus Protection

Virus prevention software is essential, because a single virus can infect an entire network within minutes. Excellent applications are available; however, all virus prevention programs are blind to new viruses that use new and unknown techniques. Therefore, any virus protection plan must emphasize user education and procedures that reduce the chance that users will introduce a virus in the first place

.

Network Management

In most networks, remote management of networking components is essential. Fortunately, there are many software and hardware solutions that support the Simple Network Management Protocol (SNMP). When documenting your requirements for a network management system, there are **two major factors** to consider:

Tasks-- The type of jobs you want the network management system to perform

Modes of operation--The degree of control you want to maintain over the system, or the amount of automation you require

Before we discuss these factors, let us briefly review the basics of SNMP network management systems.

SNMP Network Management Review

A typical SNMP network management system is composed of three main parts, as illustrated on the Manager/Agent Model Diagram:

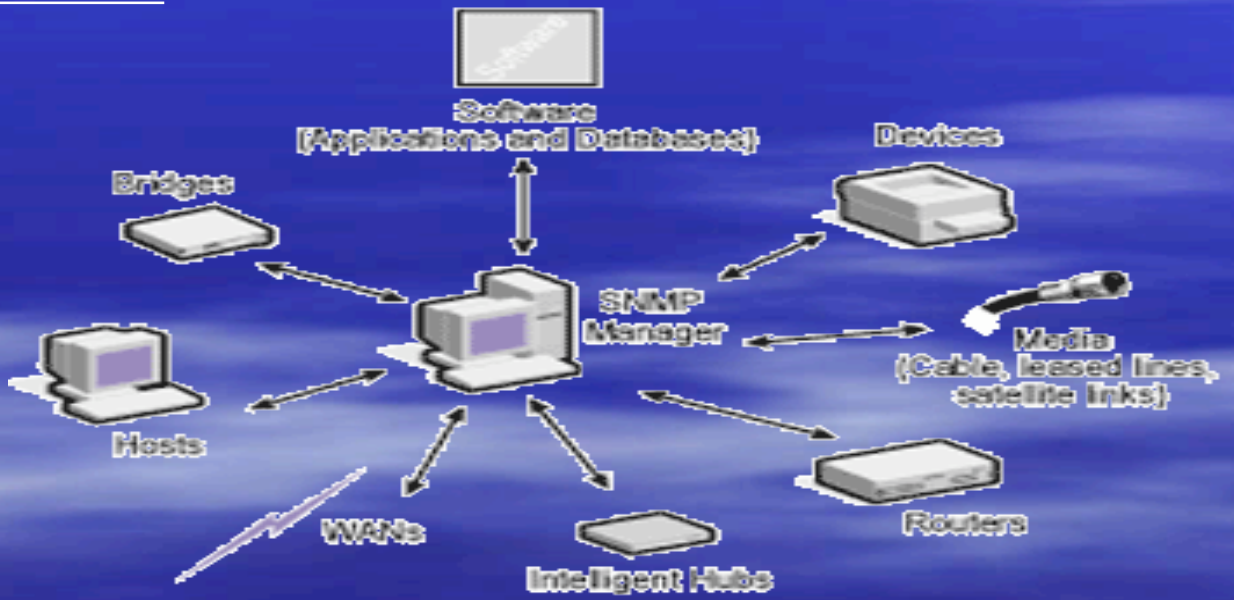
- Individual network elements (devices or resources), including agent software that runs in each managed element
- Network management station (NMS) that runs the management application (manager)
- SNMP used to exchange management information between the NMS and agent

Manager/Agent Model

• The management application (manager), running on the NMS, **provides the interface between the human network administrator and network elements being managed.**

•The manager commands the agent in each **managed element to provide management data**, and **can also adjust network performance by sending agents commands to change the configuration of their managed elements.**

• Vendors have built into *their products, either by means of software or firmware, increased network management functionality*. The Types of Managed Elements Diagram **provides a representative sampling of the different kinds of managed entities that typically exist in today's networks.**



Types of Managed Elements

Network Management Tasks

The Management Task Categories Diagram illustrates some typical functional goals of a network management system. Your network management requirements should specify the relative importance of these tasks to your overall network design.

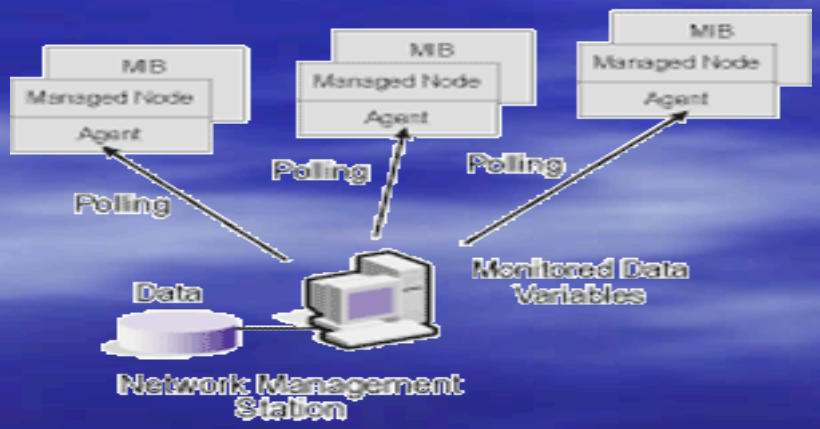
These goals could (and often do) apply to a single network device, such as a router. For example, if we list these categories under the heading of a "managed router," we would have:

- **Fault management--**Monitoring the state of the router's LAN and WAN links
- **Configuration--**Reading and changing the router's routing tables and route costs
- **Accounting--**Gathering statistics on path usage for billing purposes
- **Performance--**Discovering how many datagrams were forwarded and how many were discarded
- **Security--**Changing the valid authentication codes for routing protocols such as Open Shortest Path First (OSPF)

Modes of Operation

Your network management requirements should also specify whether you want to retain complete control over the network, or you want the management system to automate some control activities. Network management can be categorized into three general modes of operation:

• **Passive management--**The manager polls agents to gather information. Data is stored in each managed element's management information base (MIB), and is available upon request. For example, the management station can poll a Traffic Monitor for the status of the current network utilization. The Passive Management Diagram illustrates a network management station polling an agent to collect information about specific data for that device.

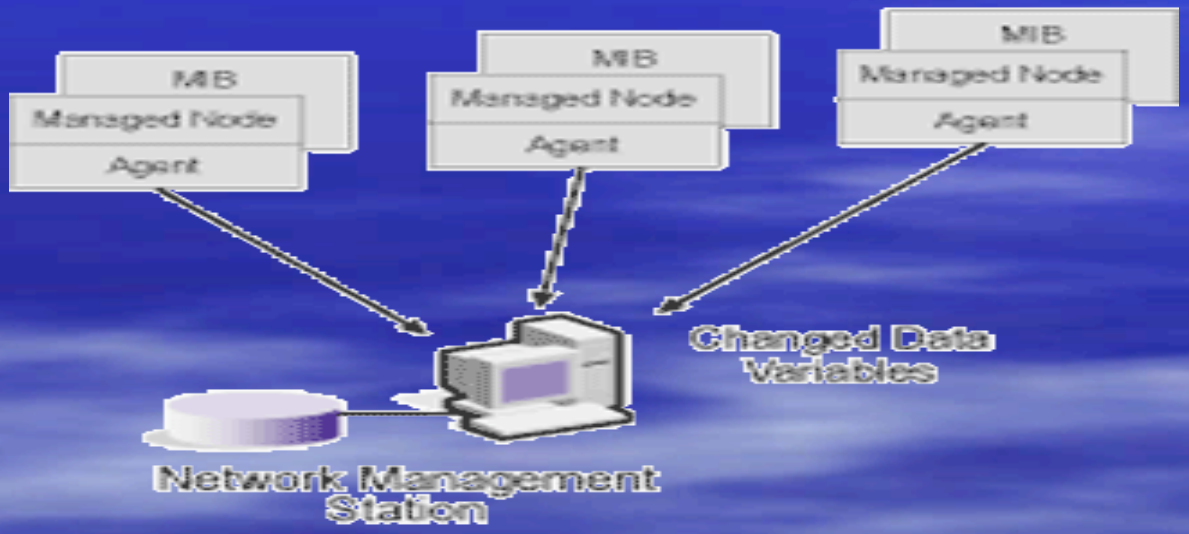


Passive Management

Active management

• The manager changes the characteristics and operating parameters of a managed element.

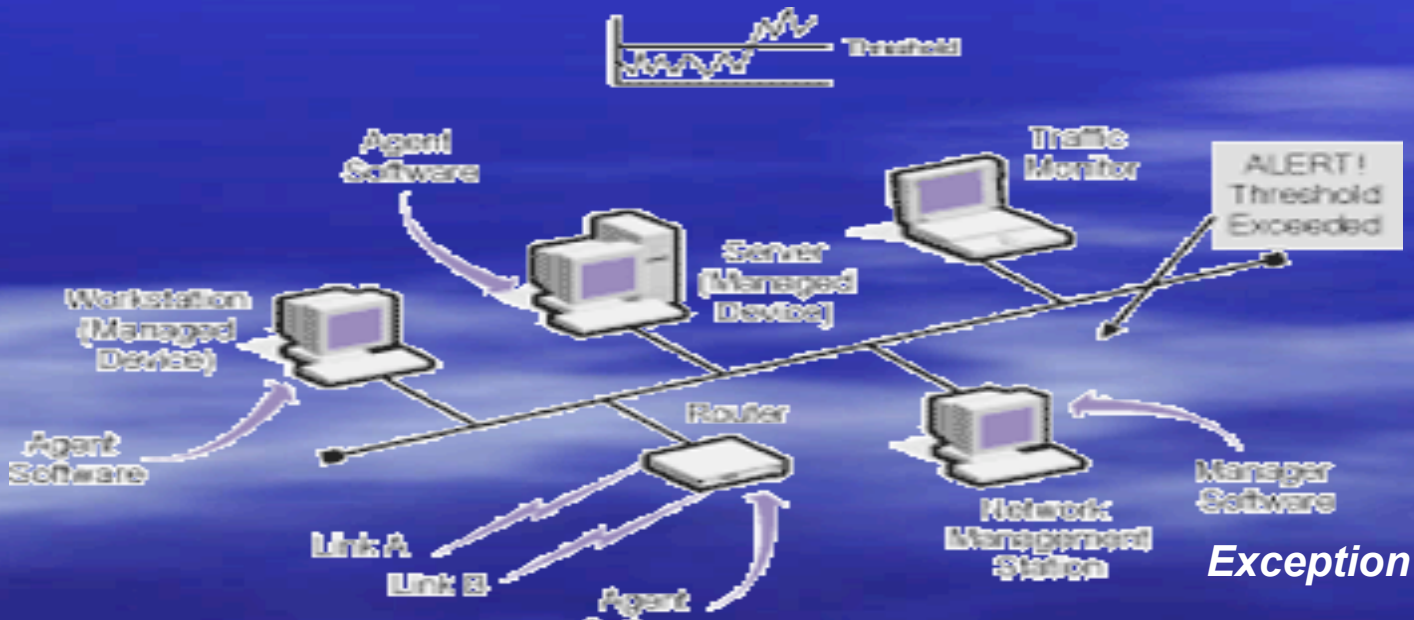
✓**For example, if the managed element is a bridge, the network manager may add additional filtering parameters to the bridge configuration to prevent the bridge from forwarding certain frames to another network segment. The Active Management Diagram illustrates an NMS changing variables on managed nodes**



Active Management

Exception management

- Agents may notify the manager of conditions that require some action.
  - ✓ **For example, an agent process can notify the manager if a previously configured parameter has been exceeded.**
  - ✓**A network administrator can also take a more proactive posture by configuring agents to inform the manager of potential problem areas before they become critical.**
  - ✓**The value of this type of proactive management to the networking support groups' effectiveness and credibility cannot be overstated.**
  - ✓**The Exception Management Diagram illustrates an example of a condition, or exception, that has triggered a network management action.**



Exception Management

Security

•All data flowing through networks, or cached temporarily on network nodes, is at risk. By identifying the points of greatest network vulnerability, steps can be taken to protect and monitor those areas for intrusion.

•Network security involves deploying physical products and operating procedures to protect the integrity, accessibility, and reliability of networks and systems. Modern network security takes basic security concepts into the distributed networking environment.

•The goal of network security is resource protection. A secure network can be defined by the following three attributes

- **Confidentiality**--Data is kept private.
- **Integrity**--Data cannot be changed without authorization.
- **Authenticity**--Data, or information about data (such as a sender's name), cannot be falsified.

Risk Analysis

- Before you can develop a security strategy, you must first describe exactly what systems or data you need to protect.

•**Risk analysis** is the process of identifying the financial worth of network systems and data.

•This analysis must identify these computing systems and data, and estimate the cost to restore the data if it is destroyed, compromised, or corrupted. This cost estimate must go beyond the immediate cash cost, to include factors such as:

a) Business exposure to fraud

a) Loss of competitive advantage

a) Loss of customer confidence

a) Direct impact to financial records data

a) Potential impact to stockholders or officers (loss of confidentiality, personal exposure to fraud, etc.)

The **risk analysis produces the facts that upper management needs to make informed decisions about the organization's overall security priorities.**

•As part of that overall policy, **an external access policy should define how many levels of access challenges, and what kinds of challenges, are appropriate for each type of requested data or system.**

Tutorial # 7 - Developing A Requirements Specification Document

Introduction

• As you approach the end of the Requirements Gathering phase, you should have **collected a large amount of input from representative managers and users.** This **collection of individual requirements, ranging from overall business needs to specific application and user requirements, is a rich source of information; however, it is not very usable as a large collection of individual forms or database entries.**

Key Point

The Requirements Specification summarizes the most important needs of the organization and its users, and reveals conflicts among requirements.

Components of the Requirements Specification

• The objective of any design document is to provide managers the information they need to make good business decisions. Because managers are usually pressed for time, any design document should be as **short and clear as possible**, while presenting all important information.

• Just as all networks are unique, so are all network design documents. In general, however, **a Requirements Specification should usually include the following major elements:**

- **Executive Overview**
- **Overview of the Requirements Phase & Summary of Requirements Data**
- **Prioritized Requirements List & Approval Section**

Executive Overview

• Begin any network design document with a brief introduction to remind a busy manager of the highlights of the project. An executive overview should include:

- A short description of the project (one or two sentences)
- A list of the phases of the design process
- The project status, including completed phases and the phase in progress

Overview of the Requirements Phase

• Briefly describe the work done in this phase. Name the groups and individuals you contacted, and describe the methods you used to gather information from them (interviews, focus groups, surveys, etc.).
• Provide the total number of interviews, surveys, etc. Also mention any important constraints on the process, such as a requirement for short surveys, or an inability to meet with key people.

Summary of Requirements Data

•Clearly summarize the things you learned from the data. Depending on the data and the information it reveals, you may find it easier to use all words, all drawings, or all numbers.

•However, it is usually effective to use a combination of all three. As you develop your summary, keep these points in mind:

Keep it Simple and Focused

- Respect your manager's busy schedule by getting directly to the point.
- Present the overall pattern of information, without getting deep into details.

•Use simple language and layman-level terms whenever possible; if you must use specialized terms, define them.

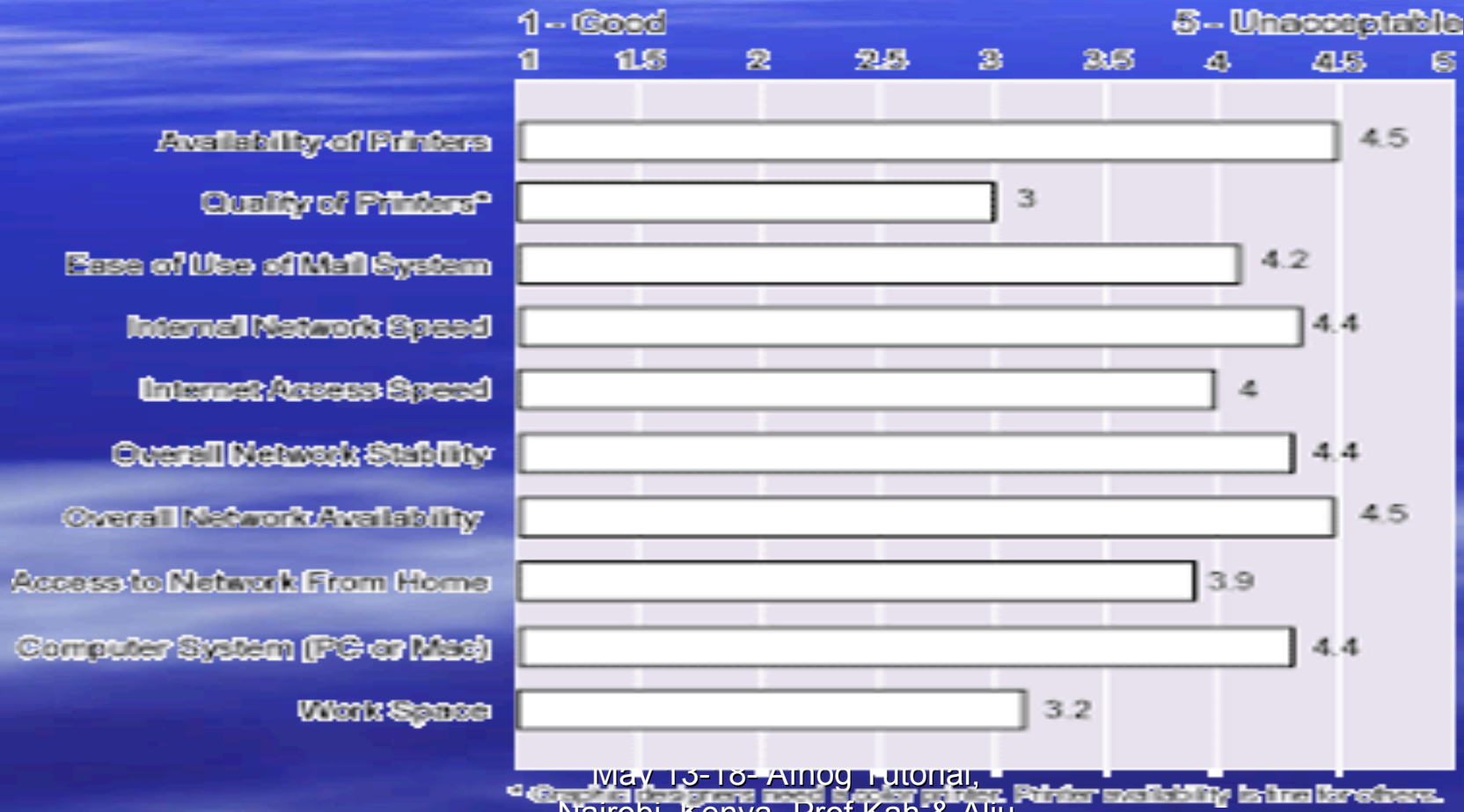
Identify Sources and Priorities

• Clearly show which requirements are business-level needs, user desires, application needs, and so on.

•Note the high-priority requirements and, when appropriate, the source of a requirement. For example, a request for a firewall carries more weight coming from the network administrator than from a salesman.

Use Images Whenever Possible

•To make it easier for your readers to visualize data patterns, present data as graphs or charts instead of tables of numbers. For example, the following table and bar chart present the same data. Which form is easier to understand?



Category	Average Rating 1 = Good 5 = Unacceptable
Availability of Printers	4.5
Quality of Printers	3
Ease of Use of Mail System	4.2
Internal Network Speed	4.4
Internet Access Speed	4
Overall Network Stability	4.4
Overall Network Availability	4.5
Access to Network From Home	3.9
Computer System (PC or Mac)	4.4
Work Space	3.2

Point Out Conflicting Requirements

- It is normal for some requirements to conflict with others.

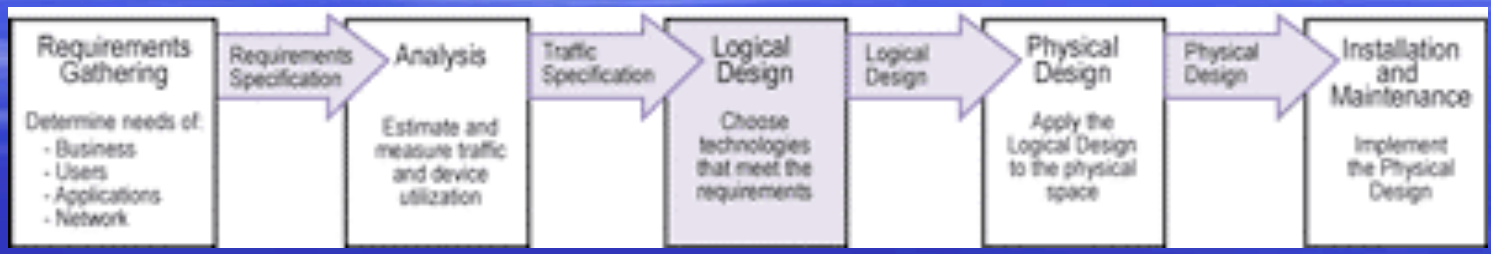
- The Requirements Specification should clearly reveal those conflicts, so that management can decide how to resolve them.

- It is appropriate to suggest a resolution, but the organization's management must set its

Tutorial # 8 ANALYZING THE NETWORK

Overview

Analysis is the second phase of the network design process, as the Network Design Process Diagram illustrates.



Network Design Process

- A Traffic Specification typically includes the following elements that describe the current network:

a) Logical network diagram

a) Inventory of internetworking devices and servers

a) Estimates of local segment and backbone traffic

a) Baseline measurements

1 - Review of Internetworking Devices

Introduction:

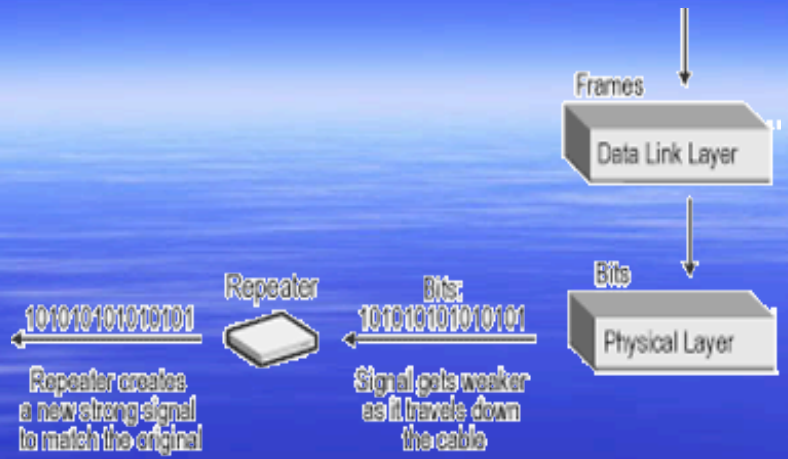
Before we discuss the process of analyzing a network, it is helpful to briefly review the internetworking devices that control the way data travels through a network. This lesson summarizes the most important features, advantages, and disadvantages of repeaters, hubs, bridges, switches, routers, and gateways (protocol converters).

Key Point

A few type of devices can be combined to create a nearly endless variety of internetworking solutions.

Repeaters

Repeaters, working at the Physical Layer, are the simplest type of internetworking device. Repeaters receive a signal (bits) on a local area network (LAN) segment and regenerate the bit pattern to boost the signal and extend the physical length of the segment. Because a repeater operates at the Physical Layer of the OSI model, as illustrated on the Repeater and OSI Model Diagram, the job of a repeater is to repeat bits. If a "1" bit is received on the input port of a repeater, a "1" bit is regenerated, with a stronger signal, at the output of the repeater. If a "0" bit is received on the input port of a repeater, a "0" bit is regenerated at the output of the repeater. A repeater is considered a "no discriminating" device, because all incoming signals are passed on to each connected segment. These devices are also transparent to the sending and receiving (end) devices.



Repeater and OSI Model

Because a repeater reproduces exactly what it receives, bit by bit, it can reproduce errors. However, repeaters are very fast (10 megabits per second [Mbps] for Ethernet) and cause very little delay.

Repeater Advantages

There are several advantages to using repeaters as follows.

- A repeater can connect one segment of a LAN to another, possibly connecting different types of media. For example, a repeater can connect thin Ethernet cables to unshielded twisted pair (UTP) Ethernet cables.

- Repeaters are fast, simple to use, and inexpensive.

- Repeaters can be used to attach "link segments" to extend the overall distance of a network, subject to the Ethernet "5/4/3 rule." This rule states that there can be a maximum of five segments connected by four repeaters with a maximum of three segments containing network nodes.

Repeater Disadvantages

Disadvantages to using repeaters are listed below.

- Because it is only a signal-boosting device, working at the Physical Layer, a repeater cannot connect two different media access types (Data Link protocols) such as Token Ring and Ethernet. It cannot recognize the contents or format of a frame, or convert one type of Data Link header to another.

- As internetworking devices for Ethernet LANs, repeaters are feasible only for relatively small LANs (less than 100 nodes), confined to a small geographical area such as one or two floors of an office building. A repeater should not be used to connect heavily used LANs, because it cannot isolate traffic between LAN segments. Because each bit is copied to the attached segments, all data passes through a repeater in both directions. Therefore, if we connect multiple LAN segments using a repeater, we may experience performance problems, because total network traffic will increase.

- The Ethernet specification allows no more than four repeater regenerations of a signal. This may constrain large topologies.

When to Use Repeaters

The main function of a repeater is to extend the physical distance of a LAN segment. Repeaters are not normally used to add more devices to a network, only to extend the distance a workstation or group of workstations can be located from other parts of a network.

Repeater Considerations

When analyzing repeaters in an existing network, note the following factors:

- Latency
- Cable type (s) supported
- Network management capabilities

Hubs

Hubs are Physical Layer devices that logically function as a shared bus, or a multiport repeater. All devices connected to a hub belong to the same collision domain, because every device connected to a hub receives frames transmitted by any other device on that hub. They are mainly a convenient way to implement multiple repeaters on twisted pair cable.

Hub Advantage

Using hubs offers several advantages as follows:

- Hubs are inexpensive, and can be used very widely to connect individual devices. Hubs create a simple star topology in which all cables run into the hub. Problems can be solved in the wiring closet, which saves time chasing after cabling problems or changing wiring patterns.
- A network can be designed so that all traffic flows through one or more hubs. This makes it easier to manage traffic flow, avoid bottlenecks, and provide security.
- The technologies that can be included in a high-performance hub seem almost limitless, and most hubs support multiple LAN and wide area network (WAN) protocols. Although this might seem to complicate matters, most network administrators prefer to manage multiple technologies in a single box, rather than in a nonintegrated network.
- As a network grows and more hub ports are needed to connect additional nodes or a server, it is simple to add additional hubs. Many hubs allow one of the hub ports to be used to connect a device or another hub. A switch is normally mounted under this uplink port, to enable either device connectivity or hub connectivity. The Ethernet Hub-to-Hub Connectivity Diagram illustrates this principle.

Hub Disadvantages

Some disadvantages of hubs are listed below.

- As the center of a star topology, a faulty central hub can cause the entire LAN to fail, or break the network into isolated sections. This failure can also happen if power to the hub is lost.

- The Ethernet specification allows no more than four repeater regenerations of a signal. A hub is a multiple-port repeater, so it automatically counts as the first regeneration. This may constrain large topologies.

- A network connected by simple hubs is one large collision domain. As more users share the same collision domain, performance gradually decreases until it is unacceptable. In other words, the bandwidth shared by all devices in the broadcast network will no longer be adequate. When this happens, Ethernet switches are often used to increase performance.

Hub Considerations

When analyzing hubs in an existing network, note the following factors:

- Redundancy features
- LAN topology support
- Port-switching capabilities
- Segment-switching capabilities
- Migration capabilities
- Network management capabilities

Bridges

Bridges operate at the media access control (MAC) sub layer of the OSI Data Link Layer. They listen to all traffic on their connected network segments, examine each destination network interface card (NIC) address, and use an internal table of addresses to decide whether to forward a frame to the rest of the network.

Bridge Advantages

There are several advantages to using bridges.

- One of the primary benefits of a bridge is to isolate traffic between LAN segments that have nodes that only occasionally send traffic across the bridge. Bridges divide a network into separate collision domains, because they use NIC addresses to filter or forward traffic between different network segments. This segmentation provides a larger share of the available bandwidth to each end station in each smaller collision domain. For example, a bridge could isolate the traffic of diverse departments such as engineering and accounting, giving each department more effective bandwidth.

- Bridges are simple to install. To use advanced bridging features, such as custom filters, a minimal amount of configuration is required. The presence of a bridge is transparent to users from the instant it is first installed, and bridges adapt automatically to network changes. Bridge-based internetworks can be modified and reconfigured very easily.

- Bridges can connect networks running different high-level protocols, without requiring additional software. They operate at the Data Link Layer of the OSI model; network managers do not need to know in advance which high-level protocols will be used.

- Some protocols are simply unroutable, such as Digital Equipment Corporation's (DEC's) Local Area Transport (DEC-LAT) terminal communications protocol, IBM's Systems Network Architecture (SNA), and network basic input/output system (NetBIOS)/NetBios Enhanced User Interface (NETBEUI). Unroutable protocols must be bridged.

- Bridges form logically single networks. All interconnected network segments have the same network identifier; we can move end stations without configuring new network addresses for them.

- When traffic on a LAN starts to cause performance problems, bridges allow us to reduce the load by segmenting the network, reducing the number of nodes in each collision domain. Bridges can also control traffic between segments and the network backbone.

- Bridges can connect two different LAN technologies, such as Ethernet and Token Ring. This type of bridge performs MAC layer conversion between 802.3 and 802.5 formats. These translating bridges operate at the LLC sublayer as well as the MAC sublayer.

Bridge Disadvantages

Several disadvantages of using bridges are presented below.

- There is a limit to the size of bridge-based networks. Each time a frame traverses a bridge it is delayed as the bridge software reads the source and destination addresses, checks its address database, and determines whether to forward the frame to each port. If the frame crosses many bridges, this frame latency may cause the destination station to time out and request retransmission. This would result in an unnecessary duplication of frame transmissions. As the network grows, so must the bridge's address table. This would also increase the delay of frames traversing the bridge.

- While network segments attached to a bridge belong to different collision domains, they all belong to the same broadcast domain. This is because bridges allow broadcast frames to flood the network. Bridges themselves also create broadcast traffic that congests the network, as they attempt to resolve unknown destination NIC addresses.

- Bridges cannot prevent broadcast storms that may occur when certain broadcast protocols cause frames to be flooded to every port. If there is a malfunction or an incorrectly configured parameter, these traffic spikes can be severe enough to disable the entire network.

- Bridges cannot take simultaneous advantage of redundant paths in a network. They cannot load-split over network segments.

- Bridges do not provide significant support for fault isolation or other distributed network management capabilities. Networks become harder to manage and maintain as their size and complexity increase. Because bridges form a single logical network, fault isolation in very large bridged networks may become extremely difficult. Bridge-based internetworks may require extra attention from network administrators to track what is running on the network and where.

- Bridges cannot convert protocols above the Data Link Layer.

Bridge Considerations

When analyzing bridges in an existing network, consider the following factors:

- What you get in the base
- configurationHardware upgrade costs
- Software upgrade costs
- LAN architectures supported (Ethernet, Token Ring,etc.)
- Remote access support for WAN bridges
- Network management capabilities
- Performance (frames per second)

Switches

A switch is a device that consists of many high-speed ports connecting either LAN segments or individual devices on a port-by-port basis. Many types of switches exist, each supporting different speeds and LAN types such as Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), and Asynchronous Transfer Mode (ATM). Unlike a bridge, which shares the LAN bandwidth among all of its ports, a switch dedicates the entire LAN media bandwidth (such as 10-Mbps Ethernet) to each port-to-port frame transmission. In this way, a switch multiplies the amount of effective network bandwidth

Switch Advantages

Switches offer several advantages as described below. .

- Switches segment a network into smaller collision domains, providing a larger share of the available bandwidth to each end station. Their protocol transparency allows them to be installed in networks running multiple protocols with little or no software configuration.
- Switches also form logically single networks. Administrative overhead is very low for switches, simplifying adds, moves, and changes.
- Switches are totally transparent to end stations. They use existing cabling, repeaters/hubs, and end station adapters without expensive hardware upgrades.
- The use of Application-Specific Integrated Circuit (ASIC) technology allows a switch to provide greater performance at a lower cost per port than a traditional bridge. A switch can simultaneously forward frames at wire speed across multiple port pairs.
- Switching technology allows bandwidth to be scaled in both shared and dedicated LAN segments, and can alleviate traffic bottlenecks between LANs. Switching products are available for Ethernet, Fast Ethernet, FDDI, Token Ring, and ATM technologies.
- A switch provides a high level of performance for a significantly lower cost per port than a router. Router prices can be as high as ten times the cost per port as an Ethernet switch. A switch is easier to configure, manage, and troubleshoot than a router, because more of a switch's functionality is built into hardware.

Switch Considerations

When analyzing switches in an existing network, consider the following factors:

- Reliability and redundancy
- Performance (frames per second)
- Congestion control
- Bridging options
- Broadcast control
- Network management options

Routers

- A router operates at the Network Layer of the OSI reference model, distinguishing between Network Layer protocols and making intelligent packet-forwarding decisions based on each packet's network address.
- As Network Layer devices, routers are protocol dependent. They can interconnect networks that have the same communications architecture, but possibly different lower level architectures.
- Routers are general-purpose devices that can segment a network into separate broadcast domains, and provide security, control, and redundancy between individual broadcast domains.
- Routers use specialized routing protocols to maintain and exchange network path information in their internal routing tables. Depending on the protocol in use, these tables can allow routers to flexibly choose routing paths based on distance, speed, quality of service, or other factors.
- A router can also provide firewall service and economical WAN access. Routers are essentially software devices. They process complex protocol suites, sometimes many suites, using powerful processors and memory. High-end routers are expensive, and it is too expensive to connect individual devices to them. Thus, high-end routers are used as backbone devices and interconnectivity devices.

Router Advantages

Routers offer several advantages as presented below.

- Like a switch, a router provides users with seamless communication between individual LAN segments. Unlike a switch, a router determines the logical boundaries between groups of network segments. A router provides a firewall service, because it forwards only traffic specifically addressed to go across the router. This eliminates the possibility of broadcast storm propagation, the transmission of frames from unsupported protocols, and the transmission of frames destined for unknown networks across the router. Routers keep potentially disastrous events local to the area in which they occur, preventing them from spreading across the corporate network.
- The enhanced intelligence of a router allows it to support redundant network paths, and select the best forwarding path based on several factors in addition to the destination MAC address. This increased intelligence can also result in enhanced data security, improved bandwidth utilization, and more control over network operations.
- Routers are the only internetworking devices that can provide efficient WAN access. Because routers do not forward broadcast traffic, they help control the traffic load on small, expensive WAN pipes. Routers offer access to a wide variety of WAN technologies, allowing network managers to select the best economic value for their networking needs. Router-based techniques such as data compression, traffic prioritization, and packet spoofing also help make efficient use of WAN bandwidth
- Routers can flexibly integrate disparate Data Link Layer technologies, such as Ethernet, Fast Ethernet, Token Ring, FDDI, and ATM. They can also consolidate legacy IBM mainframe networks with personal computer (PC)-based networks through the use of Data Link Switching (DLSw).

Routers also have several disadvantages as follows.

- The additional software processing performed by a router Router Disadvantages
  can increase packet latency, reducing the router's performance when compared to simpler switch architecture.
- To be "routable," an architecture must have a Network Layer. Not all do; those protocols must be bridged. "Unroutable" protocols include DEC-LAT terminal communications protocol, IBM's SNA, and NetBIOS/NETBEUI.

When to Use Routers

1. Routers are needed when network applications require limiting broadcast traffic, support for redundant paths, intelligent packet forwarding, or WAN access. If the application requires only increased bandwidth to ease a traffic bottleneck, a switch is likely the better choice. The technology choices appropriate for a specific workgroup, department, or building backbone depend upon the organization's business and technical requirements.
2. One of the functions of a router is to provide traffic isolation to help diagnose problems. Because each port of a router is a separate sub network, broadcast traffic is not forwarded across the router. The definition of network boundaries makes it easier for a network manager to provide redundancy and isolate problems resulting from broadcast storms, misconfigurations, chatty hosts, and equipment failures.
3. Another important benefit of routers is their ability to support mesh network topologies that provide active redundant paths. Unlike switches and bridges, which require a loop-free topology, routing protocols impose no constraints on network topologies, even on those that contain redundant paths and active loops. In addition, routers can perform load balancing over parallel equal-cost paths to make the best use of available bandwidth.
4. Routers allow the creation of hierarchical network designs that, through delegation of authority, can foster local management of separate regions of the Internet. Routers are necessary to connect a private network to the Internet.

Router Considerations

When analyzing routers in an existing network, consider the following factors:

- What you get in the base configuration
- Hardware upgrade costs
- Software upgrade costs Support for multiple protocols or a single protocol
- Network connectivity support
- Performance characteristics (packets per second)
- Network management capabilities
- LAN architectures supported (Ethernet, Token Ring, etc.)
- Latency

Gateways

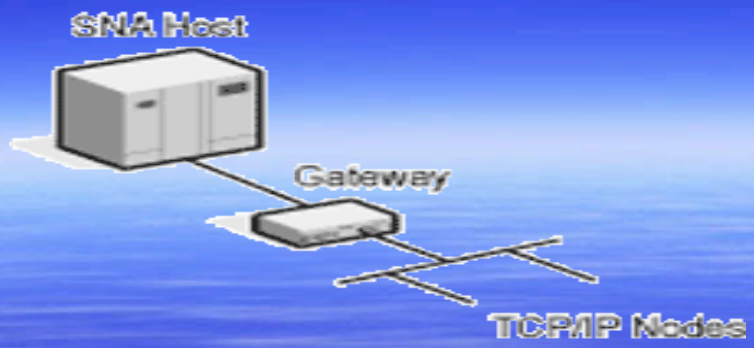
. A gateway, also called a protocol converter, converts data between two distinct types of protocol architectures.

A gateway operates at all protocol levels above the Data Link Layer, and is transparent to both ends of connection.

Gateway Advantages

The advantages of a gateway are described below.

- A gateway is the only internetworking device that can change the form of a network transmission from that of one communications architecture to that of another. For example, a gateway can connect a Transmission Control Protocol/Internet Protocol (TCP/IP) network to an SNA network, as shown on the Gateway Diagram. Another example of a gateway is a node that converts OSI Message-Oriented Text Interchange System (MOTIS) mail to Simple Mail Transfer Protocol (SMTP) for TCP/IP delivery.



Gateway

Gateway Disadvantages

Disadvantages of gateways are presented below.

Protocol conversion is a software-intensive (slow) process, different for each specific pair of protocol stacks. A gateway receives frames from one communications architecture, and must convert them to another architecture by building new headers for every layer of the protocol stack.

When to Use Gateways

Gateways are necessary to connect any two networks that use different communications architectures. For example, we must use a gateway to convert electronic mail (e-mail) as it moves between SNA and TCP/IP environments.

Gateway Considerations

When analyzing gateways in an existing network, consider the following factors:

- What you get in the base configuration
- Hardware upgrade costs
- Software upgrade costs
- System architecures supported
- Network management capabilities
- Performance characteristics

Introduction

- In the Analysis phase, we take precise measurements of network performance and load.
- However, before we can start measuring, we must have some idea of what to look for.
- This discussion introduces and explains the major concepts and terms used to understand network performance.
- The overriding concept of network analysis is the idea of a "bottleneck": a point, or combination of points, that restricts or reduces the flow of data.
- Here we describe factors that can cause a network component to become a bottleneck, and shows you what to look for when hunting for bottlenecks.

- **Key Point**
  Any part of a network may become a bottleneck.

Response Time, Delay, and Latency

• Response time, delay, and latency are interrelated terms. Each attribute has an impact on the performance of a network, and each is based on time. Instead of simply defining each term, it is helpful to also illustrate each concept with some examples.

• Response time is the total time it takes to receive a response after a request for a service has been initiated. It is often used in reference to interactive terminals requesting information from a host computer.

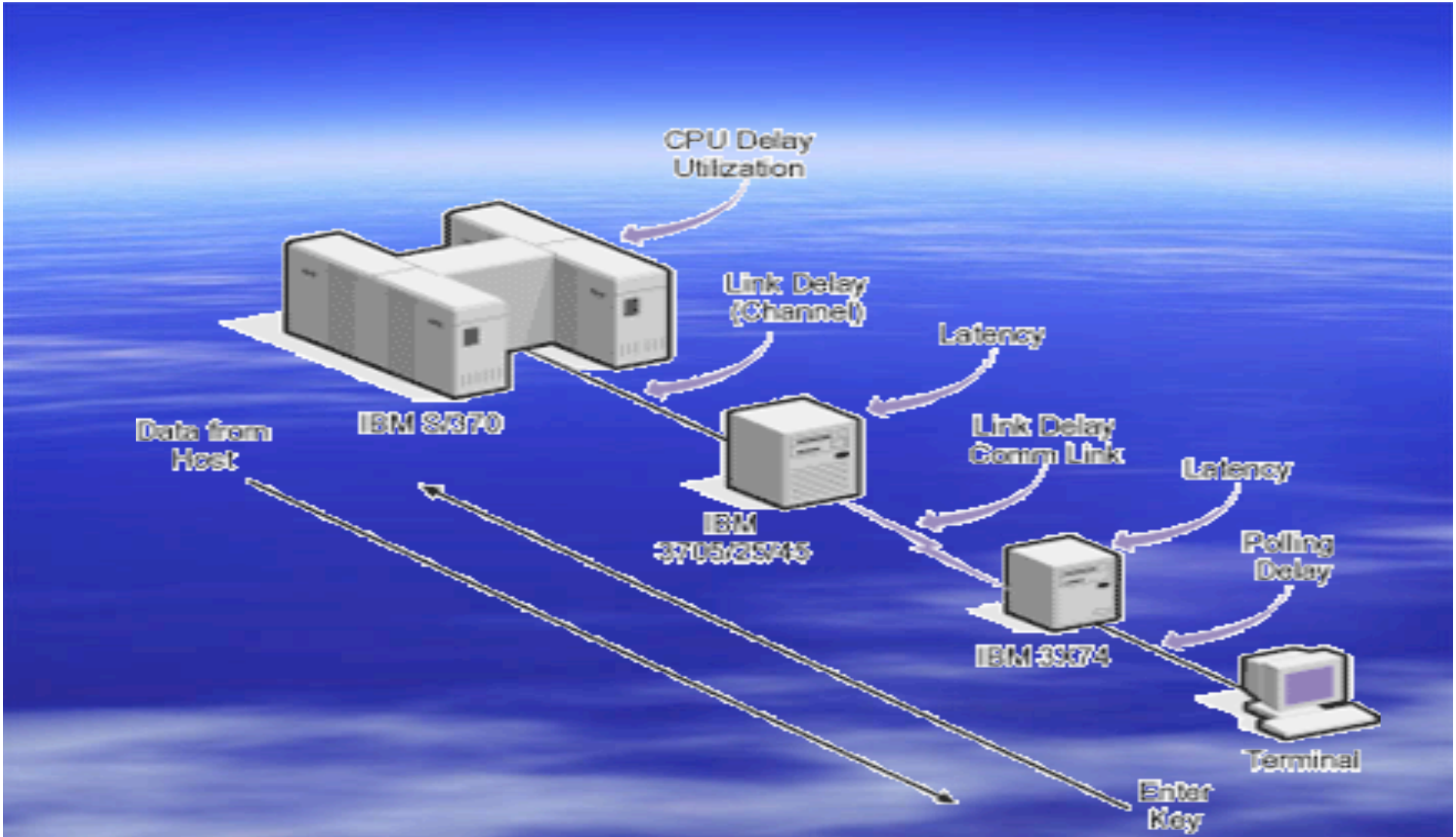
✓**For example, response time is the time that passes between the moment a user presses the ENTER key and the moment a full screen of data is returned to that terminal. It is the time necessary for the user's request to travel through the network to a host, and for the host's response to travel back.**

Response Time in a Master/Slave Configurations

• The Response Time Components (Traditional IBM Network) Diagram illustrates typical response time components in a traditional IBM network.

•As you can see in the diagram, response time is the sum of the time necessary for data to pass through each component of a network.

•Each device, communication link, and process adds its own delay to the overall response time. Some of the most common factors in response time are described below:



Response Time Components (Traditional IBM Network)

- ***Polling Delay***
  - ✓ Polling is a method used to control communication between a master and slave node in an unbalanced data communication configuration.
  - ✓ If a slave device (dumb terminal) has data to send, it must wait until it is polled by the master device (upstream controller or host) before it can send data.
- ***Link Delay***
  - ✓ Link delays describe the speed at which data can be transferred across a communications link.
  - ✓ The higher the link speed, the faster data can travel, and the lower the delay. Common link speeds in this traditional IBM network configuration are 9.6 or 19.2 Kbps.

•***Component Latency***

✓Latency is the amount of time it takes a network device, such as a bridge or router, to analyze and retransmit a received packet.

✓Devices that make simple forwarding decisions, such as switches or bridges, have lower latency than devices that perform complex processing, such as routers or gateways.

- ***CPU Delay***
  - ✓ Central processing unit (CPU) delay describes the time it takes the server CPU to process a request from the network.
  - ✓ In general, the busier the CPU is, the longer it will take to process the request.

- ***NIC Delay***

Different types of NICs introduce various delays. After a client application requests network access, there is a delay while the client NIC processes the request and transmits the data over the physical medium.

- ***Physical Media Delay***

Response time also depends on the transmission speed of the particular LAN architecture. It will take longer for data to traverse a 4-Mbps Token Ring network than a 100-Mbps FDDI network.
It will also take longer to transfer a file using small frame sizes versus larger frame sizes because of the amount of overhead (header and trailer) required for each frame.

- ***Server Delay***

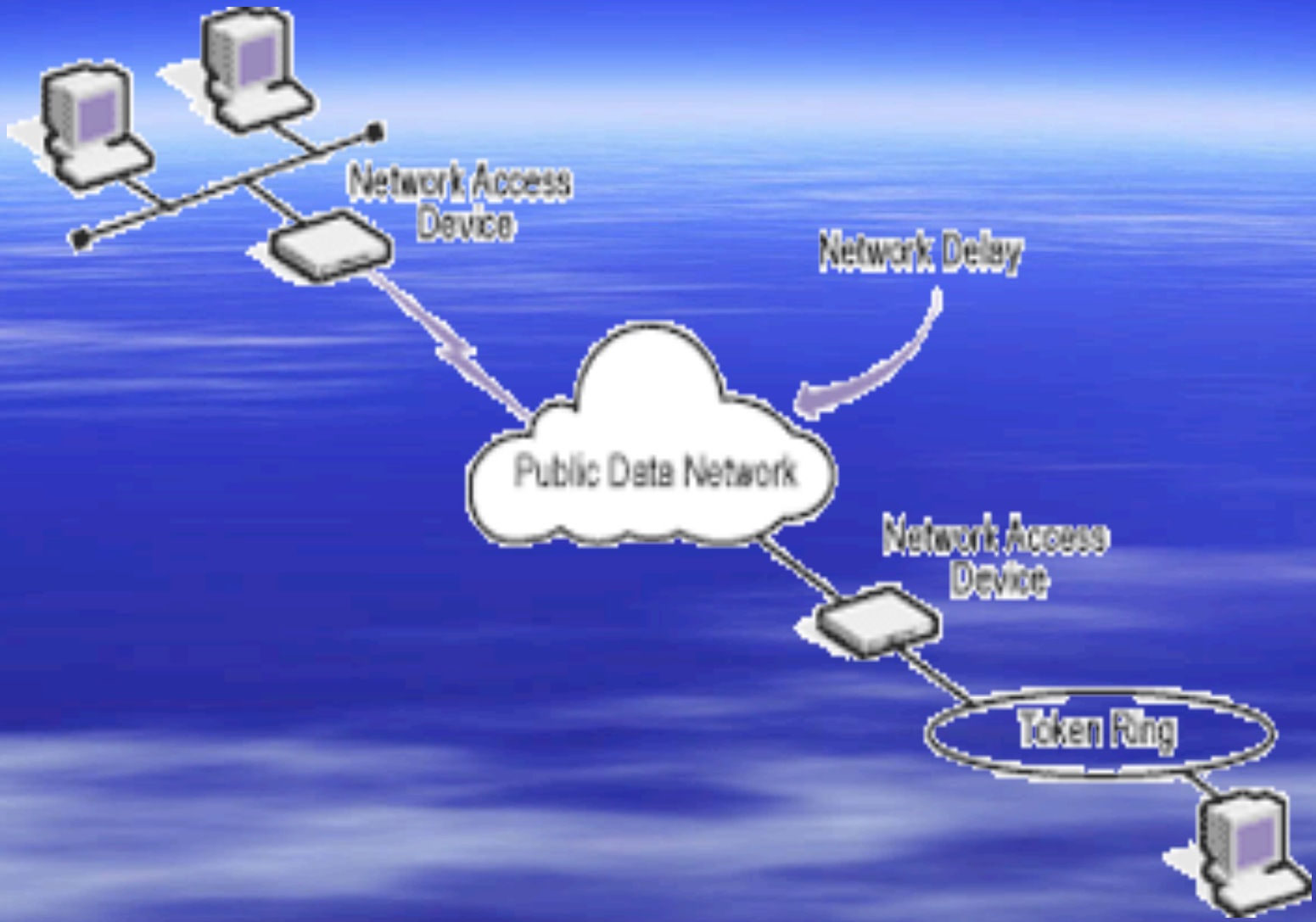
- Depending on the processor speed of the server and the average number of requests the server has to process, server response time may vary widely.
- Other factors in server delay are queue delays and disk access delays.

- ***Public Network Delay***

When request/response traffic travels over a public WAN, response times can vary drastically.

- For example, wide response time variations can occur when using the Internet, even to the point of losing connections because intermediate links "time out" and no longer stay in session.

- Network delays of this type are very hard to predict, and often vary according to the time of day (as overall Internet traffic increases or decreases). The Public Network Delay Diagram Illustrates this concept.



Public Network Delay

3 - Estimating Traffic Volumes and Patterns

Introduction

- In this step of the Analysis phase, we examine the total volumes of network traffic, as well as individual traffic patterns, or flows, that might indicate performance bottlenecks.
- Here we introduce the fundamental concepts used to describe network traffic.
- We then apply those concepts to estimate a network's current traffic and capacity needs, based on user and application requirements.

- Estimates of traffic volume and directional patterns give us insight into the general performance characteristics of a network.
- This broad understanding will guide the more exact traffic measurements to come later in this phase.
- These estimates, plus the later measurements, will provide important input to the Logical Design phase.

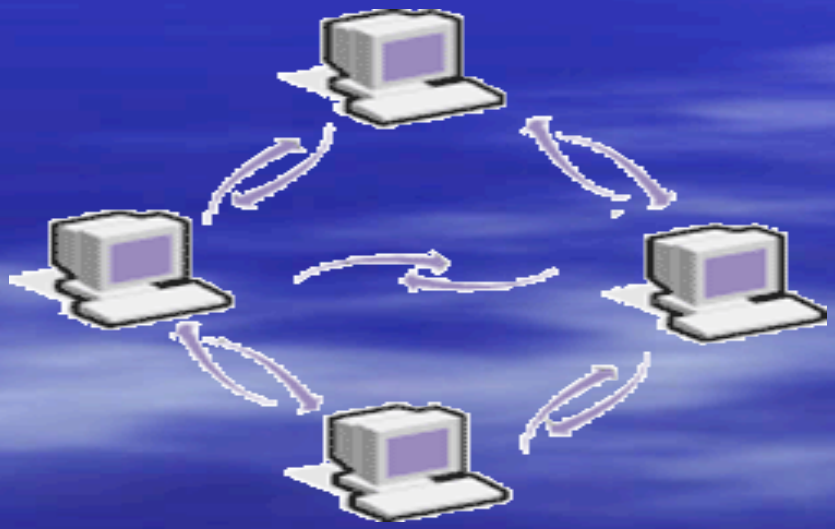
- **Key Point**
  Traffic estimates and traffic measurements are both essential parts of a traffic analysis.

Traffic Direction

- Although it is important to know the traffic volume at key points in a network, it can be just as important to understand the directions in which the traffic flows.
- That's because the direction of traffic can strongly determine the amount of traffic on various network segments.
- Directional traffic patterns are based on three methods of communication between endpoints:
  - ✓ Peer-to-peer
  - ✓ Client-to-server
  - ✓ Server-to-client
- Each network node communicates in one or more of these modes, depending on network resources, node, and application capabilities.

Peer-to-Peer Traffic

- Peer-to-peer traffic is traffic typically seen between similar nodes (clients). The communicating nodes have similar application and communications capabilities, and each node is just as likely as any other to communicate with another node in the network.
  - ✓ A common example of peer-to-peer communications is file sharing between workstations. There is no obvious source or destination traffic pattern, peer-to-peer traffic does not tend to create directional flow patterns. The Peer-to-Peer Traffic Diagram illustrates this concept.



Peer-to-peer Traffic

Client-to-Server and Server-to-Client Traffic

- *Client-to-server traffic, as the name implies, describes communication between any end nodes (clients) and a shared resource (server).*
- *A client may be any type of node that needs access to a common resource, such as a central database.*
- *Servers vary in size and functionality, and can be anything from a PC-based server, to a midrange computer, to a mainframe.*
- *Client-to-server traffic is depicted on the Client-to-Server Traffic Diagram.*

Client-to-Server Traffic

4 - Taking Baseline Measurements of LAN Traffic

Introduction

- In the last discussion, we estimated traffic based on information gathered from the network users. The traffic estimates serve as **a rough guide for the more exact process called "baselining."**

- **Baselining (also called "benchmarking")** documents the performance of a network by measuring its capacity and standard operating efficiency.
- These measurements can identify long-term trends in network operations and their impact on network performance.

- **Baselining** can be used with traffic estimation, as previously described in, or as an alternative to estimates.

- Taking baseline measurements requires special monitoring equipment and applications.

- Because both of these are expensive, many small organizations skip this step and rely on estimates alone. However, whenever possible, it is best to use both estimating and baselining.

Tools for Testing Activity

- If you have an existing LAN, you can probably get detailed reports from the network operating system (NOS) vendor as to the theoretical capacity of the NOS.
- Many NOSs run these reports as Value Added Processes (VAPs) or, as in the case with Novell's NetWare, NetWare Loadable Modules (NLMs).
- Another traffic measuring tool is a LAN analyzer such as Network Associates' Sniffer, Hewlett-Packard's LAN Advisor, or Novell's LANalyzer. Sniffer, Advisor, and LANalyzer can record traffic over a given period of time.
- You can also purchase LAN software emulation packages that monitor networks from a PC. These packages provide tools for:
- Network mapping
- Physical network management
- Network design
- Network planning and simulation

Measuring Shared Resource Utilization

- Shared resources are network elements, such as **servers and printers, that are shared by multiple users.**
- It is often necessary to measure the utilization of such components when analyzing a problem or estimating the usage of an individual component.
- Normally, **a problem arises between multiple clients and a specific server, the network is suspected first**. However, **the server could also be a network bottleneck**.
- If the designer does not understand **the interrelationships between clients, network, and server, this can lead to an incorrect solution.**
- Typically, only the components that contribute the most delay are used in response time calculations. However, any of the following items, on the sending station, receiving station, or both, can cause network performance problems:
  - ✓ **Application**
  - ✓ **CPU/clock speed**
  - ✓ **Input/output (I/O) bus type and data rate**
  - ✓ **Operating system (OS) type**
  - ✓ **Number of tasks running (CPU utilization)**
  - ✓ **Amount of memory**
  - ✓ **NIC delay**
  - ✓ **LAN link delay**
  - ✓ **WAN link delay**
  - ✓ **Protocol stack**
  - ✓ **Internetworking device latency**

Measurement Tools

- Each OS offers different ways to measure the utilization of shared resources.
- Command-line tools such as the System Activity Report (SAR) are often used on a UNIX system to measure CPU utilization.
- On a platform such as Windows NT Server, several graphical user interface (GUI)-based tools can display the performance of the server and the attached network:
  - Peformance Monitor
  - Task Manager
  - Network Monitor

5 - Developing A Traffic Specification Document

Introduction

- The Requirements Specification served as the output of the Requirements Gathering phase, and the input of the Analysis phase. Similarly, the Traffic Specification is the main deliverable of the Analysis phase.
- Together, the Traffic Specification and Requirements Specification provide the two essential inputs into the Logical Design phase.
- The Requirements Specification describes what the new network should do in the future, and the Traffic Specification describes what the current network is doing now.
- The Traffic Specification documents network traffic volumes (estimated or measured), as well as any traffic patterns or performance statistics that might indicate bottlenecks.
- The goal of this document is to accurately summarize what you have learned during your analysis of the existing network, and make design recommendations based on that knowledge and the Requirements Specification.
- The Traffic Specification provides the evidence to support later design choices, such as new equipment or segmentation strategies. It is the second design document that management will formally approve, thus, like the Requirements Specification, it must be both accurate and to the point. Most important, it must describe technical issues in terms that non-technical managers can understand and evaluate.
- **Key Point**
  The Traffic Specification documents network performance, identifies problems, and recommends design goals.

Preparing the Data

- Like the Requirements Gathering phase, the Analysis phase also creates a large mass of raw data:
  - ✓ user traffic estimates
  - ✓ traffic measurements
  - ✓ resource utilization statistics and more.
- Thus, like the Requirements Specification, the Traffic Specification must summarize all this data in a form that reveals patterns to both the design team and management.
- You can process traffic estimates and measurements using the same spreadsheet applications used to summarize your requirements data. Better yet, good network analysis tools can conveniently summarize data in tables and graphs.
- A good Traffic Specification also includes network diagrams. You can use almost any drawing software to produce these, but a technical drawing application such as Visio can be a real time-saver.
- Later on, your Physical Design documents will require diagrams drawn to scale. You will save time in the long run if you start your early drawings in an application that offers good measurement and scaling features.
- Preserve all of your analysis data, just as you saved the raw requirements. Managers are often more inclined to trust a summary when they read the line, "All source data may be reviewed at your request."

Components of a Traffic Specification

- A Traffic Specification documents the current state of the network: its configuration, internetworking devices, traffic levels, and utilization of shared resources. It may include some or all of the following major elements:
  - ✓Executive Overview
  - ✓Overview of the Analysis Phase
  - ✓Summary of Analysis Data
  - ✓Recommended Design Objectives
  - ✓Approval Section

3: Logical Network Design

1 - Overview of the Logical Design Phase

Introduction

- During the Logical Design phase, a network designer uses information learned in the two previous phases to choose the technologies that will fulfill the network requirements. However, a good logical design is much more than a simple shopping list.
- It is a comprehensive plan that considers every aspect of the network and the business it serves.
- Here we present an overview of the Logical Design phase, then focuses on each of the main factors a network designer must consider.

Key Point

You cannot have it all. A good network design makes trade-offs based on design priorities.

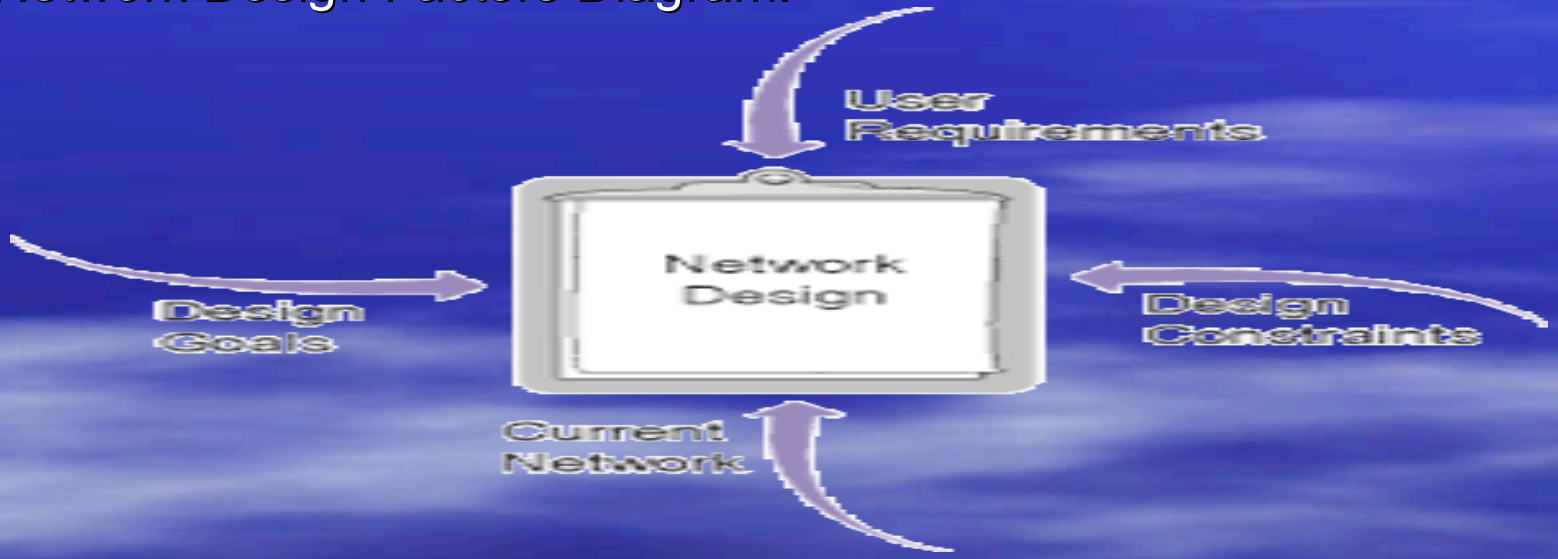
Establishing Design Goals

- Given that every organization and network are unique, network design goals vary from organization to organization.

- However, all design goals strive to satisfy requirements, defined in the Requirements Specification, and deliver certain levels of service. For example, design goals might include:
  - ✓ Minimize operational costs
  - ✓ Increase overall performance
  - ✓ Simplify user-level operation Increase security
  - ✓ Add adaptability and flexibility

Design Factors and Trade-offs

- Networks are designed to fulfill a business need, whether it is the initial implementation of a network or an upgrade in response to user demands for better service.
- Both types of designs must consider several factors, as shown on the Network Design Factors Diagram.



Network Design Factors

- Design factors sometimes contradict each other, thus network design is all about establishing priorities and making trade-offs.
- Typically, there are many ways to solve a problem; therefore, trade-offs occur at many points throughout the design process.
- Much of the work designing a network concerns recognizing conflicting goals and optimizing the design to reconcile them. Consider the trade-offs for the following goals:
  - ✓ **Minimize operational costs**
  - ✓ **Minimize installation costs**
  - ✓ **Maximize performance**
  - ✓ **Maximize adaptability**
  - ✓ **Maximize security**
  - ✓ **Maximize reliability**
  - ✓ **Minimize downtime**

As you can see, regardless of the design goal, a trade-off usually exists.

Evaluating Network Services

- Before you make technology choices, you must consider the services the network should provide. In other words, first decide what to do, then decide how to do it.
- A wide variety of network services may need to be considered during this phase, and these services will vary from design to design. However, two key network services that most designers must consider are:
  - ✓Network management
  - ✓Network security

Network Management

Network management can be divided into several different categories based on the need in a particular network. Considerations include:

Troubleshooting

The need for troubleshooting tools varies with the size of the network. Small networks can usually get along with the troubleshooting tools provided by the network operating systems (NOSs), plus a few individual products. Large, widely dispersed networks usually require more sophisticated products that support remote troubleshooting.

Configuration and Reconfiguration

It can be time consuming and expensive to manually upgrade operating systems (OSs) or applications at each desktop. Network management tools and policies that can configure and reconfigure a network and its workstations can be a worthwhile investment.

Monitoring

The need for monitoring features also varies with network size and complexity. Do you simply want to be notified of catastrophes, or do you want a monitoring service to watch for potential problems or opportunities for improvement?

Network Security

Before designing complex security systems, network designers should take the following steps to determine the optimum level of a network's security services:

Identify Systems That Need Protection

Identify potential network weaknesses that threaten your critical systems, but remember that only some data and applications are mission-critical or confidential. Instead of spreading your security budget thinly over the entire business, discover where you should focus a more intense effort.

Conduct a Risk Analysis

Review network access and auditing procedures, and other established company guidelines, for security loopholes that could provide intruders or employees unauthorized access to information or resources. If possible, close the loopholes immediately; if not, add that information to the Requirements Specification.

Keep it Simple

Some sophisticated security implementations are not worth the extra expense. Physical security, such as locks, is nearly always inexpensive and easy to accomplish.

After considering these points, the network designer should understand the company's optimum security level, and have specific ideas about the actions and policies necessary to achieve that level. Network and system managers must then develop a security plan that identifies the technologies, procedures, and policies that will solve each of the identified security problems.

The security plan must be compatible with the political structure and culture of the organization. In other words, security procedures must not be so strict or complex that they interfere with people's work. A security program is certain to fail if it ignores the corporate climate or working style of its users. People tend to take the path of least resistance; if security procedures become just another obstacle, employees will find ways to circumvent them to get their jobs done.

Evaluate Technology Options

Each type of network technology includes characteristics that should be considered in light of the requirements and existing network situation. These characteristics fall into three main categories:

- ✓ **Broadcast (background) traffic**
- ✓ **Connection type**
- ✓ **Scalability**

Making Technology Choices

- Choosing specific technologies requires a detailed consideration of the relative advantages and disadvantages of each approach.
- Therefore, each of the next seven lessons focuses on a different type of technology, highlighting points to consider in a logical network design.
- Working our way up from the Physical Layer, here we discuss:
  - ✓ Physical Layer considerations
  - ✓ Internetworking devices
  - ✓ WAN performance
  - ✓ Network management
  - ✓ TCP/IP addressing
  - ✓ Security
  - ✓ Firewalls

2 - Physical Layer Considerations

Introduction

- The first choice of the Logical Design phase is the network's Physical Layer technologies: the type of cabling and NICs it will use.
- In a network upgrade project, you must determine whether the existing physical transmission hardware will continue to do the job, or if it must be replaced.

- **Key Point**
  Physical Layer design decisions involve choices of transmission media and NICs.

Using the Requirements and Traffic Specifications as a Guide

- Before you begin to evaluate various Physical Layer options, review the recommendations that summarized your Requirements Specification and Traffic Specification.
- Focus on those requirements that can be met, partially or totally, by a particular choice of Physical Layer technology.

Network Interface Cards (NICs)

A computer's NIC is a big design consideration, because a NIC must be compatible with a network's physical medium, topology, and MAC-layer protocol. The NIC Characteristics Table lists characteristics to consider when choosing a NIC, or deciding whether your existing NICs meet your requirements.

NIC Characteristics

LANs Supported	Ethernet, FDDI, Fast Ethernet, Gigabit Ethernet, Arcnet, ISDN, Token Ring
Computer Bus Supported	MCA, ISA, EISA, PCI, NuBus, VME, USB
RAM Buffer Size	8, 16, and 32 Kbps
Bus Size	8, 16, and 32 bit
Data Rate	4, 10, 16, and 100 Mbps, 1 Gbps
Media Type	10Base2, 10BaseT, UTP, STP, Optical
O/S Supported	VINEs, NetWare, Appletalk, Microsoft Windows NT, etc.
Price/Function	Check current vendor specifications.

NIC Characteristics

3 - Internetworking Device Considerations

Introduction

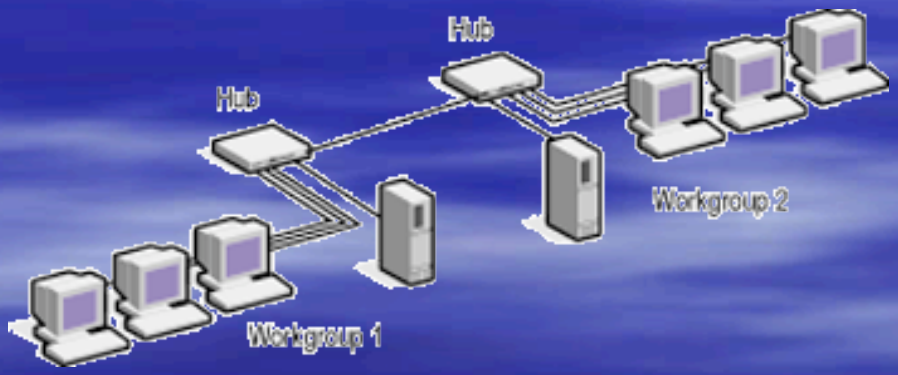
- A logical network design must specify the type of internetworking devices that will connect segments of a LAN, or link multiple LANs over wide area links. These devices nearly always work in combinations, thus here we present a series of examples illustrating how internetworking devices work together in successful design solutions. The examples that follow discuss the benefits and limitations of **using hubs, switches, and routers in workgroup, backbone, and WAN environments.**
- Every network is different, with unique design goals and operational requirements; therefore, the examples presented here are not recommended solutions for specific problems. As a network designer, you must determine your own priorities and use the appropriate technologies to achieve your individual design objectives.
- The efficiency of a network ultimately depends on the elements and components you choose. Therefore, the selection of internetworking devices is not a trivial undertaking. To achieve well-managed growth, you must carefully consider both current user needs and estimated future requirements.

Key Point
Networks can be segmented with switches, routers, or both.

Workgroup Environments

A workgroup is a collection of users that share computing resources. Workgroups may be large or small, located in the same building or dispersed across a campus, and have permanent or project-based membership.

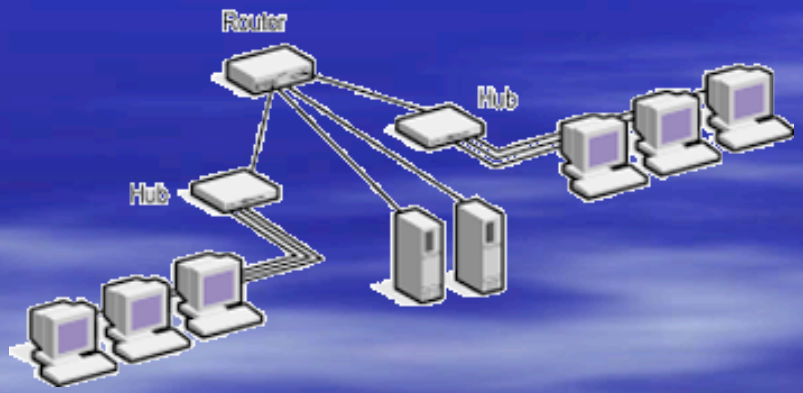
The Typical Hub Workgroup Diagram shows a typical workgroup environment prior to the installation of an internetworking device. Although the diagram shows only two standard hubs, the actual workgroup may contain from 10 to 20 hubs that support more than 200 users.



Typical Hub Workgroup

Routing Solution

The Router Implementation Diagram presents the workgroup topology in the unlikely event that the network manager elects to use a router. Although very few network administrators would actually consider a router for this application, we will discuss this potential solution to illustrate the differences between installing a switch and a router.

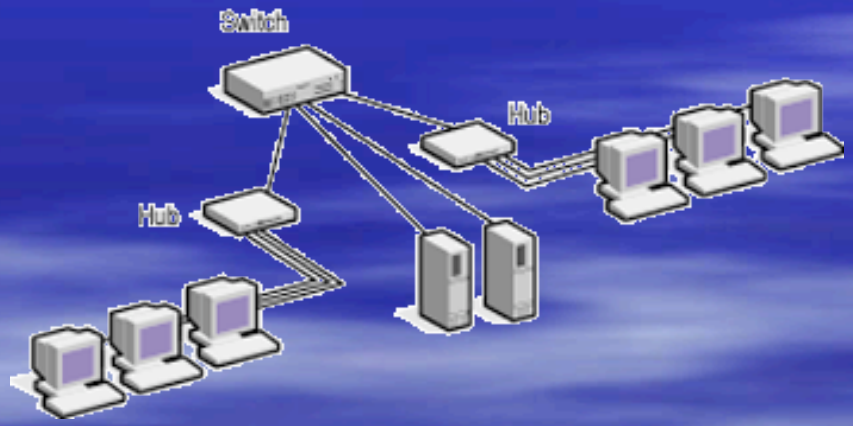


Router Implementation

- The router is configured with a dedicated high-speed interface for the server and a large number of standard Ethernet interfaces assigned to each hub segment and power user.
- By installing a router, the network administrator divides the large broadcast/collision domain into several smaller broadcast/collision domains. Each small domain will notice improved traffic performance between nodes in the same domain.
- However, there are two reasons why a router is not the best economical or technological choice for this application. First, it is more expensive than a switch.
- The router has a higher initial cost per port, and the long-term management expenditures will be greater. Second, the router is more complex than necessary.
- The levels of broadcast traffic likely do not justify the additional complexity of separate broadcast domains created by dividing the workgroup into subnetworks.

Switching Solution

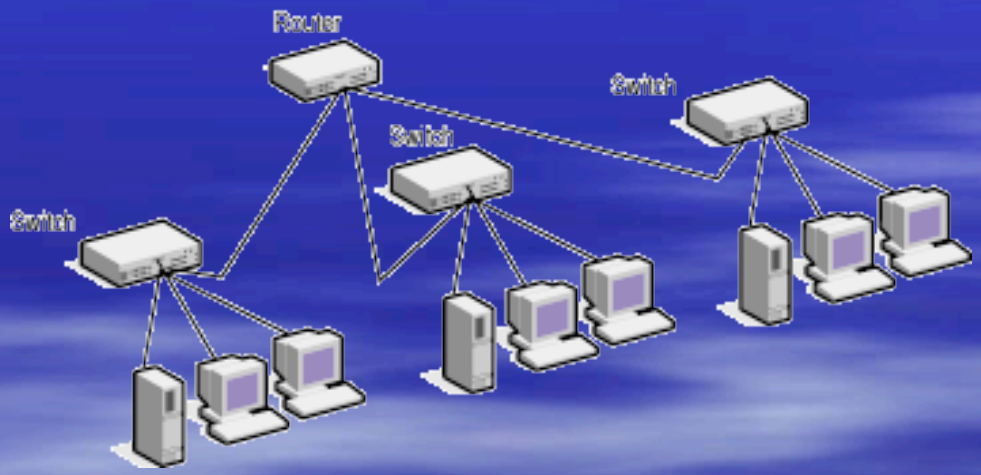
The Switched Workgroup Diagram shows the same workgroup after a LAN switch is installed. In the switched environment, one broadcast domain is divided into four separate 10 Mbps collision domains. Dedicated 10 Mbps access for servers and power users eliminates media access contention for those nodes. Power users can be connected right at the switch.



Switched Workgroup

Physical Segmentation

The Physical Segmentation Diagram illustrates how a router physically segments a network into broadcast domains. In this example, the network administrator installs a router as an insurance policy to guard against effects of a broadcast storm that would bring down the entire network.

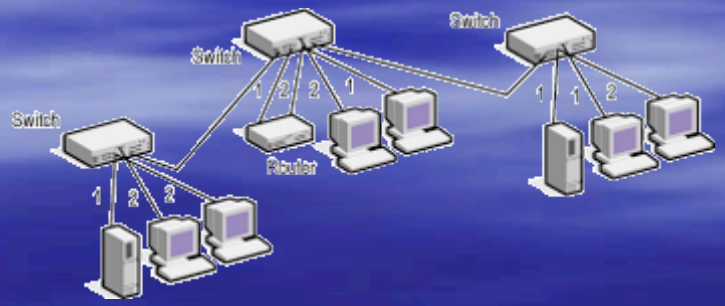


Physical Segmentation

Logical Segmentation

A more flexible way to divide a network into broadcast domains is by using a router to connect separate virtual local area networks (VLANs) created with switches. A VLAN, in its simplest form, allows the creation of virtual broadcast domains within a switched environment, irrespective of the physical infrastructure. With VLANs, the network administrator can define a workgroup based on a logical grouping of individual workstations rather than physical network connections. Traffic within a VLAN is switched at wire speed among members of the VLAN. A router forwards traffic between different VLANs.

In the Routing and VLANs Diagram, the ports of each switch are configured as members of either VLAN 1 or VLAN 2. If an end station transmits broadcast or multicast traffic, the traffic is forwarded only to ports in the source station's VLAN. Traffic that must flow between the two VLANs is forwarded by the router, which provides security and traffic management. The illustration shows a dedicated router; however, a combination switch/router device may also perform the routing function.



Router/Switch Selection Summary

Either a switch or a router can be deployed to segment a LAN and provide additional bandwidth. If the application needs support for redundant paths, intelligent packet forwarding, or WAN access, a router is required. If the application requires only increased bandwidth to ease a traffic bottleneck, a switch is likely the better choice. Because a switch is a special-purpose device, it provides wire-speed packet throughput for a lower cost per port than a router.

The cost for a given level of performance is the major factor in the decision between a switch or a router in a workgroup environment. Network designers must determine whether there are other requirements, such as redundancy, security, or the need to limit broadcast traffic, that justify the extra expense and complexity of deploying a router within a workgroup environment.

Bandwidth Management

- Bandwidth management features control traffic at the core, allowing network administrators to improve network performance while enforcing traffic flows and other network policies.
- There are two reasons why traditional Layer 2 switches cannot efficiently distribute and control bandwidth across a LAN.
- First, they may be based on ASIC technology, and lack the flexibility and complex functionality required for bandwidth management.
- Second, they may be general-purpose, processor-based devices that deliver high functionality at the cost of slow performance.

4 - Optimizing WAN Performance

Introduction

- WANs provide communications pathways between dispersed geographic sites in a corporate intranet. As corporate intranets become central to an organization's success, the reliability and scalability of its WAN links will determine whether the intranet can effectively support its users' demands.
- WAN environments are very different from LAN environments, as illustrated in the Differences Between LANs and WANs Table. The design criteria for LANs, where bandwidth is readily available and inexpensive and raw performance dominates, are very different from those for WANs, where bandwidth is scarce and expensive.
- Because the fundamental issues are different, an entirely different set of solutions is required for WAN designs.

Differences Between LANs and WANs

LANs	WANs
Switching is dominant	Routing is dominant
Users at the same site	Geographically dispersed users
Private cable plant	Public telephone company facilities
Equipment costs dominate	Line costs dominate
High speed	Low speed
Plentiful bandwidth	Limited bandwidth
Inexpensive bandwidth	Expensive bandwidth
Fast response time	Slower response time

Key Point

A typical WAN circuit is 160 times smaller than a typical LAN.

5 - Network Management with SNMP and RMON

Introduction

- Network management, in its broadest sense, is the management, control, accounting, and troubleshooting of networking devices and information about network devices.
- There are many software and hardware solutions for remote management of networking components; most of these solutions are based on the Simple Network Management Protocol (SNMP).
- The RMON specification enhances the SNMP model with additional functionality and greater efficiency.

- Key Point
  Network management features are essential for proactive management of any network.

Limitations to SNMP Manager/Agent Communication

- In recent years, SNMP has become the dominant mechanism for the management of distributed network equipment.
- SNMP uses agent software embedded within each network device to collect network traffic information and device statistics, as illustrated on the Manager and Agent Communication Diagram.
- Each agent continually gathers statistics, such as the number of packets received, and records them in the local device's management information base (MIB).
- A network management station (NMS) can then collect this information by sending queries to each agent's MIB, a process called polling.

Manager and Agent Communication

6 - TCP/IP Addressing Considerations

Introduction

- Because of the growing demand for Internet connectivity, many NOSs support TCP/IP addressing at the desktop level.
- Therefore, the TCP/IP addressing strategy is an important consideration in any network design.
- Here we discusses three primary strategies a network designer must consider:
  - ✓ **Classic IP routing and subnetting**
  - ✓ **Classless Interdomain Routing (CIDR)**
  - ✓ **Variable-length subnetting**

Review of Internet Addressing

- IP addressing uses a 32-bit address field divided into two parts.
  - ✓ **The first part of the address identifies the network on which the host resides.**
  - ✓ **The second part of the address identifies the host itself.**

Classic IP Subnetting

- Subnet addressing allows an organization to use a single Internet network number for multiple physical networks.
- Subnets may be used with any class of Internet addressing except class D.
- A subnetted Internet address incorporates a network address, subnet address portion, and host address.
- These three pieces of information can be combined within the single binary word in several ways.
- The network address can take 1, 2, or 3 bytes, leaving 3, 2, or 1 bytes for the combined subnet/node address, respectively.
- To further complicate things, the byte(s) used for the subnet/node address can be divided arbitrarily, with certain bits for the subnet address and certain bits for the node address, as explained below.
- Fortunately, as a practical matter in a given network configuration, only one of the many possible schemes of addressing is used.
- In subnetting, the host portion of an IP address is divided into two parts:
  - ✓The left part is used to identify the subnet number.
  - ✓The right part is used to identify a host on the subnet.

7 - Security Considerations

Introduction

- Providing an effective network security strategy is a balancing act. T
- o protect the network from threats, both external and internal, an administrator must erect as many barriers and defenses as possible.
- This multiple-layered approach greatly reduces the chances of being breached because, generally speaking, most intruders are not patient.
- They do not want to spend time battling several different types of obstacles when attempting to access a computing environment.
- However, multiple layers of safeguards are potentially frustrating for a network's users, and can interfere with their ability to perform productive work.
- Therefore, a network designer must balance the need for safety against the users' need for convenience.
- This need for balance means no system can provide 100 percent security and still be usable.
- However, several key security technologies present real barriers to criminals while remaining fairly transparent to users. In this step of the Logical Design phase, you will consider the technologies and architectures that can safeguard both your organization's network and its productivity.

Key Point

If a security system becomes a barrier to productivity, users will likely find a way around it.

Security Threats

Threats to network security come in several forms. A great deal of attention is paid to deliberate threats originating from viruses and criminals; however, accidental damage can be just as devastating. Whether intentional or not, information losses generally fall into three categories:

- Modification
- Destruction
- Disclosure

A person who wants to cause one of these types of damage can attack a computer networking system in a number of ways. These attacks can take several forms:

Crackers--Crackers are criminal hackers, either insiders or outsiders, who are motivated by the thrill of breaching a secure system.

Trojan Horses--Trojan horses are covert programs hidden in system or applications software, or within seemingly innocent utilities. The hidden program may wait to suddenly destroy information using predetermined parameters, or can gather confidential information such as passwords.

Viruses--Viruses are self-replicating, destructive programs that damage executable programs and network data in a variety of ways.

Denial of service--This type of attack leads to disruption of system availability by crashing or overloading a critical device such as a server, router, or firewall.

Theft of information--The attacker, often an insider, acquires proprietary information such as trade secrets or business plans. This can be done by eavesdropping on network transmissions, masquerading as an authorized entity, or a brute-force attack such as the use of a computer program that guesses passwords

Corruption of data--The attacker either destroys or corrupts data stored on disk or corrupts data as it is transmitted across a network.

Physical Security

- Physical security risks most often involve access to machines or people. A number of strategies can be used to enhance physical security:
  - ✓ Provide a secure physical environment for the server (at a minimum, lock the door) that safeguards its console, keyboard, and monitor.
  - ✓ Physical access to a computer is a common opening to an intruder.
  - ✓ Depending on the level of physical security needed, organizations may use receptionists, security guards, physical keys, combination or electronic door locks, or other access controls.

- Destroy sensitive documents, including disks, when no longer used.
- Sophisticated tools can reconstruct files supposedly erased from a disk. Only destroying the disk itself guarantees the destruction of the data it once contained.
- Store digital encryption keys on smart cards, not on disks. Disks can be duplicated; smart cards are more difficult to copy.
- Keep passwords and personal identification numbers (PINs) secure. Remind users to avoid writing passwords down, sending them through e-mail, or placing them in messages that are archived or incorporated in group discussion systems. Explain that writing a PIN on an ID card is as obvious as hiding the front door key under the door mat.
- Lock down portable equipment. As the U.S. State Department now knows all too well, a laptop computer represents one of the greatest physical threats to a security system, because it contains a great deal of information and can so easily be carried off.
- The same is true of other portable devices such as external disk drives, tape backup systems, and the like. These devices must be locked away or bolted to the desk to guard against theft. Basic input/output system (BIOS)-level passwords can help safeguard laptops in the field; however, the best protection is good user training and awareness.

Encryption

- Even if both access control and authentication security systems are completely effective, an enterprise can still be at risk when data communications travel over a third-party network such as the Internet.
- Indeed, the low cost and ease of connecting to the Internet have made it an extremely attractive medium for communication within and between enterprises.
- **Encryption** prevents eavesdropping by making data unreadable to all except those who have the key needed to decrypt the data. It does not matter whether a third party intercepts packets over the Internet; the data still cannot be read.
- This approach can be used throughout the enterprise network, including within the enterprise (intranet), between enterprises (extranet), or over the public Internet to carry private data in a virtual private network (VPN).
- **Encryption** is the process of scrambling data by changing it in a series of logical steps, an encryption algorithm. To increase security, an encryption algorithm uses a numerical pattern, or "key," to guide the scrambling process. This means different algorithms and keys will each produce data scrambled, or encrypted, in different patterns. There are two main methods of encryption:
- **Single-key, or symmetric, encryption** uses the same key to both encrypt and decrypt the message. Therefore, both the sender and recipient must have the same key before they can exchange coded messages. Symmetric encryption systems include Data Encryption Standard (DES), 3DES, (RC5), International Data Encryption Algorithm (IDEA), and other algorithms that are extremely fast. Their strength lies in the length of the key and the difficulty of analyzing the encrypted data.
- **Public-key encryption** uses a pair of encryption keys for each party that needs to receive encrypted information. Each key in the pair acts as a one-way channel. One key (either one) is used to encrypt data; the other is used to decrypt the data. Data encrypted with one key cannot be decrypted with the same key, only with its corresponding "partner" key.
- To use **public-key encryption**, a person or organization freely distributes its public encryption key and safeguards the corresponding private key. Anyone may use the public key to encrypt messages to a recipient, who uses the private key to decrypt them.
- **Public-key encryption** is very CPU intensive. It is typically used for small amounts of data where strong security is required.

8 - Firewall Considerations

Introduction

- As discussed earlier, an Internet firewall is a security solution that includes both hardware and software components.
- Depending on the specific needs of an organization, a firewall may include multiple layers of both hardware and software.
- When designing an Internet firewall, there are a number of issues that must be addressed by the network administrator:
  - ✓ Stance of the firewall
  - ✓ Overall security policy of the organization
  - ✓ Financial cost of the firewall
  - ✓ Components or building blocks of the firewall system

Key Point

A firewall can protect an organization from specific types of external threats. It cannot guard against internal attacks.

Components of a Firewall System

- After making decisions about firewall stance, security policy, and budget issues, an organization can determine the specific components of its firewall system.
- A typical firewall is composed of one or more of the following building blocks:
  - ✓Packet-filtering router
  - ✓Application-level gateway (or proxy server)
  - ✓Circuit-level gateway

  How can these building blocks work together to build an effective Internet firewall system.

9 - Developing a Logical Design Document

Introduction

Logical Design document recommends a specific solution that can move the network from its current state (defined by the Traffic Specification) to its desired state (defined by the Requirements Specification).

In this document, the designer specifically describes the network design features that will meet each design objective listed in the Traffic Specification. Furthermore, each decision is supported by evidence from the Traffic Specification, vendor specifications, and other facts.

The Logical Design is one of the most technically detailed of all the network design documents; however, as much as possible, it must discuss the proposed network in terms of business needs, and in language managers can understand. This approach creates strong communication with management, and keeps the network designer focused on creating a network that serves its users.

- **Key Point**
  A Logical Design document presents your best recommendations, as well as evidence to support them.

1- Overview of a Structured Cable Plant

Introduction:

- In many of today's office environments, the data network cabling has been installed incrementally, responding to changes in technology, networking needs, and organization plans.

- Typically, this leaves a legacy of incompatible systems that may include telephone switching systems, mainframe or minicomputer systems, personal computer (PC)-based LANs, and other office communications equipment.

- Because each system is installed according to its own set of wiring criteria using different types of cable, these systems are difficult to interconnect, and especially difficult to maintain and expand.This situation is typical of the unstructured wiring system, in which there is no single set of standards for interconnection.

- Although initial costs are comparatively low for unstructured wiring, the long-term difficulties and expense of integrating or replacing the incompatible wiring system are considerable.

- In recent years, a clear trend has emerged among network planners, to implement network cabling as a structured wiring system according to uniform standards. This involves a shift in perspective.

- Rather than seeing cabling simply as a way to connect devices, cabling is now seen as an important architectural entity: **the cable plant, cabling system, or premises wiring**.

- The intent is to install a wiring capability that not only provides interoperability for existing networking technologies, but also anticipates future growth by allowing for efficient reconfigurations.

Structured Wiring Systems

- A structured wiring system is more efficient to install when a building is constructed or remodeled, rather than pulling wires through existing walls, ceilings, and floors.
- As a practical issue, architects and building owners often need to install cable before they know what type of network a tenant will want.
- A structured wiring approach can solve this problem by providing guidelines for a universal wiring system that can be adapted to almost any network requirement.

The interest in universal wiring is supported by three technological trends:

- ✓ Convergence on three cable types
- ✓ Use of a hub-based distributed star physical topology
- ✓ Emergence of industry-wide standards

•Cable Convergence

The ability to preinstall a cabling plant is based on the fact that all major LAN technologies can be supported by three types of cable:

- ✓Shielded twisted pair (STP)
- ✓Unshielded twisted pair (UTP)
- ✓ Optical fiber

2- Copper Cables Introduction

•The most common varieties of LAN cabling are made from copper wire. The most prevalent of these are **UTP, STP, and coaxial cable**.

• Each type of copper cable has its own unique features; however, they all use the same physical principles to carry electrical signals.

Key Point

Category 5 UTP cable is the most popular medium for data networks

Transmission Problems and Characteristics

- The signal-carrying performance of copper cable can be dramatically influenced by several typical problems and cable characteristics. These include:

✓ Electrical noise
✓ Crosstalk
✓ Attenuation
✓ Capacitance
✓ DC resistance
✓ Impedance
✓ Continuity and polarity
✓ Cable length

Attenuation

Attenuation is the loss in signal amplitude, or strength, that occurs as a signal passes through a transmission medium. There are two primary sources of attenuation, which is measured in dB:

- Electrical characteristics of the cable, especially resistance
- Insertion losses that occur where the cable is interconnected, terminated, or broken

Attenuation increases with cable length and the number of connections; therefore, it must be measured after it is installed. It can be minimized by making careful connections and using high-quality connectors.

Capacitance

Capacitance is an undesirable tendency of a cable to store electrical energy. Cable is typically tested for capacitance while still on the spool; however, improper installation can kink or stretch the cable, creating small areas of increased capacitance. Competent installation can prevent this kind of cable damage; field testing of installed cable can detect it if it occurs.

DC Resistance

DC resistance is the property of a conductor that opposes the flow of electrical current. It is measured in ohms, and increases with cable length. Cable is tested and certified for acceptable DC resistance by manufacturers.

Impedance

Impedance is the total opposition (including resistance and capacitance) of the flow of electrical current. It is consistent for each type of cable. However, it is frequency dependent, and can be altered or mismatched whenever a physical transition occurs, such as at a punchdown block, patch panel, or device connection. Cable is rated for its characteristic impedance (measured in ohms) and this rating is guaranteed by manufacturers. It is not typically measured on installed cable.

The impedance of cables must match the impedance of electrical components in the interface cards and other circuitry for a given type of LAN. Cables with different impedance values should not be interconnected, because some of the signal will reflect back from the mismatched connection point. This signal reflection can cause an excessive distortion of the data signal which can be misinterpreted as frame collisions.

Continuity and Polarity

The terms continuity and polarity simply refer to correctly connecting each individual wire at each punch-down block and connector. Continuity means that all necessary connections have been made, so that a continuous electrical circuit exists. Polarity means that the connections allow electrical current to flow in the proper direction. For example, each wire pair in a four-pair UTP cable has a plus/minus transmit pair and a plus/minus receive pair.

Misconnecting individual wires so that wires are reversed, or do not match the correct pinout configuration at the connector, will result in failure of the node. Continuity and polarity testing must occur first, before any other tests of installed twisted pair cable.

IBM Cable Types

A simple Web page usually contains a handful of graphic elements, and 10 or 20 hyperlinks.

Type 1

IBM Type 1 cable consists of two STP pairs for data transmission. Each pair is shielded with a foil sheath and an outer shield of plastic or corrugated metal. Type 1 is the historical standard for Token Ring cable. Type 1a is a newer, higher performance cable of the same general type.

Type 2

Type 2 cable includes six pairs of wire: two STP pairs for data, and four UTP pairs for voice. This cable is used where both telephone lines and data lines terminate in the same wall outlet, or to otherwise facilitate the wiring installation of telephone and data lines between wiring closets.

Type 3

Type 3 consists of telephone-grade UTP cables. The original Type 3 cable specification was intended to be compatible with existing telephone-grade wiring, which would be equivalent to EIA/TIA Category 2 UTP. Therefore, Type 3 cable was recommended only for 4-Mbps Token Rings. Currently, IBM recommends the use of data-grade UTP (equivalent to EIA/TIA Levels 3, 4, or 5) for both 4- and 16-Mbps installations. Increasingly, only Levels 4 or 5 are recommended for new installations.

Type 5

Type 5 cable consists of two 100/140 microns (or millionths of a meter) (mm) optical fiber cables. IBM currently also recommends 62.5/125-mm multimode optical fiber for optical fiber installations (where 62.5 refers to the core diameter and 125 refers to the cladding diameter). Fiber optic cable is typically used with a pair of fiber optic repeaters to connect multistation access units (MAUs) in Token Ring LANs. Optical fiber is discussed in detail in the next lesson.

Type 6

Type 6 uses two twisted pairs for data transmission; it is similar to Type 1, but more flexible. Type 6 is used to connect workstations to wall outlets and for patch cords between Token Ring MAUs.

Type 8

Type 8 consists of two shielded pairs with a flat, plastic housing designed for under-carpet use.

Type 9

Type 9 is a thinner, lower cost version of Type 1 cable. Type 9 supports shorter transmission distances than Type 1.

General Installation Guidelines

LAN performance depends on a quality cable installation that takes into account the following considerations:

- ✓ Install enough cable for future needs, especially in a new building. It is almost always more expensive to incrementally add cable within completed walls, ceilings, or floors.
- ✓ Follow local building codes and be aware of state and federal guidelines. NEC specifies many aspects of fire safety for cable installation. Study and understand all aspects of the appropriate structured wiring plan, if you use one.
- ✓ Hire an experienced and reputable cabling contractor familiar with all applicable building codes, your desired network specification, and your chosen structured wiring plan. Some municipalities or organizations may require the use of union labor.
- ✓ Perform certification testing of the cabling plant to ensure it meets your performance criteria
- ✓ Use plenum-grade cable for cable runs through environmental airspaces (plenum area), such as the area above suspended ceilings, and the return-air cavities used for heating, ventilating, and air conditioning (HVAC) systems. Plenum-grade cable has a special jacket that is fire-resistant and does not produce toxic smoke.

- ✓ Label all cables and maintain a wiring plan that identifies all cables, devices, and connectors.
- ✓ Do not unwrap any more of a cable jacket than necessary to make a connection. This can result in excessive crosstalk.
- ✓ Do not untwist the end of twisted pair cable more than absolutely necessary when making connections. This can result in excessive crosstalk.
- ✓ Do not cut corners on material quality. Use the correct grade of cable and connectors for your LAN type. Do not use untwisted (telephone) cables for twisted pair installations.
- ✓ Run data cables perpendicular to power lines whenever possible.
- ✓ Do not run copper cable parallel to electrical power lines at a distance of less than six to eight inches. Keep data cables several feet away from high-capacity power lines.
- ✓ Use cable hangers to support the weight of cables in ceiling areas.
- ✓ Keep patch cables as short as possible so that they do not pick up noise.
- ✓ Make sure every system is properly grounded, has voltage surge and lightning protection, and has an uninterruptible power supply (UPS).

Tutorial Group Activity:
DESIGNING A SMALL NETWORK

Overview

• In our earlier discussions, we presented a series of tasks and considerations that form a phased network development process.

•Here we will apply the network design process as we gather requirements, analyze, and design a small network for an imaginary company.

Afnog, Inc. Nairobi, in this example provides training for software, hardware, and World Wide Web (Web) development. This company has three locations in the Nairobi metropolitan area. Each location provides office space for company employees, and networked classrooms for students. One of these locations is expanding and moving, and the company needs to upgrade that office's network as part of its move. Imagine you are part of a network consulting firm that has been hired to design the new network. From initial interviews with management and key personnel, we determine that our network consulting organization must perform the following services:

1. Gather business and technical requirements
2. Analyze the current network
3. Create the logical network design
4. Create the physical network design
5. Determine implementation options and estimate costs

Designing A Small Network
2 - Logical Design

Introduction

• After the requirements have been gathered and the company managers have agreed upon the recommended project objectives, we are ready to proceed to the Logical Design phase.

• The inputs to this phase are outputs from the previous phases. In larger projects, these may require a separate, detailed Requirements Specification and Traffic Specification.

•In smaller projects, such as this one, the input can be a scaled-down Requirements Specification, combined with a brief traffic analysis. In this lesson we discuss a sample Logical Design document.

Key Point

Technology choices are made in the Logical Design phase.

2 - Logical Design

Logical Design Specification

Presented to: Afnog Inc. Nairobi, Kenya
Date: May 2006-

Executive Overview

This document summarizes the Logical Design of the new network being installed at 1A2B Keneyatta Drive during the week of July 1, 2006. The phases of this project are:

1. Requirements and Analysis
2. Logical Design
3. Physical Design
4. Network Implementation

Phase 1, Requirements and Analysis phase, is complete. The results of this phase are summarized in the Requirements and Traffic Specification document which was approved on May 13, 2006.

Phase 2, Logical Design phase, will be complete after the Logical Design has been approved and signed by company management. After this is signed, we will begin the Physical Design phase of the project.

3 - Designing for Performance: ATM

Introduction

• Each part of an enterprise network has unique priorities. Desktop connections require the lowest possible price per port. Local area backbones must be scalable.

•Wide area specifications need maximum bandwidth efficiency. In response to these priorities, the application of Asynchronous Transfer Mode (ATM) technology has evolved into four solution spaces:

- ✓LAN backbone
- ✓Desktops
- ✓Wide area access
- ✓Wide area transport

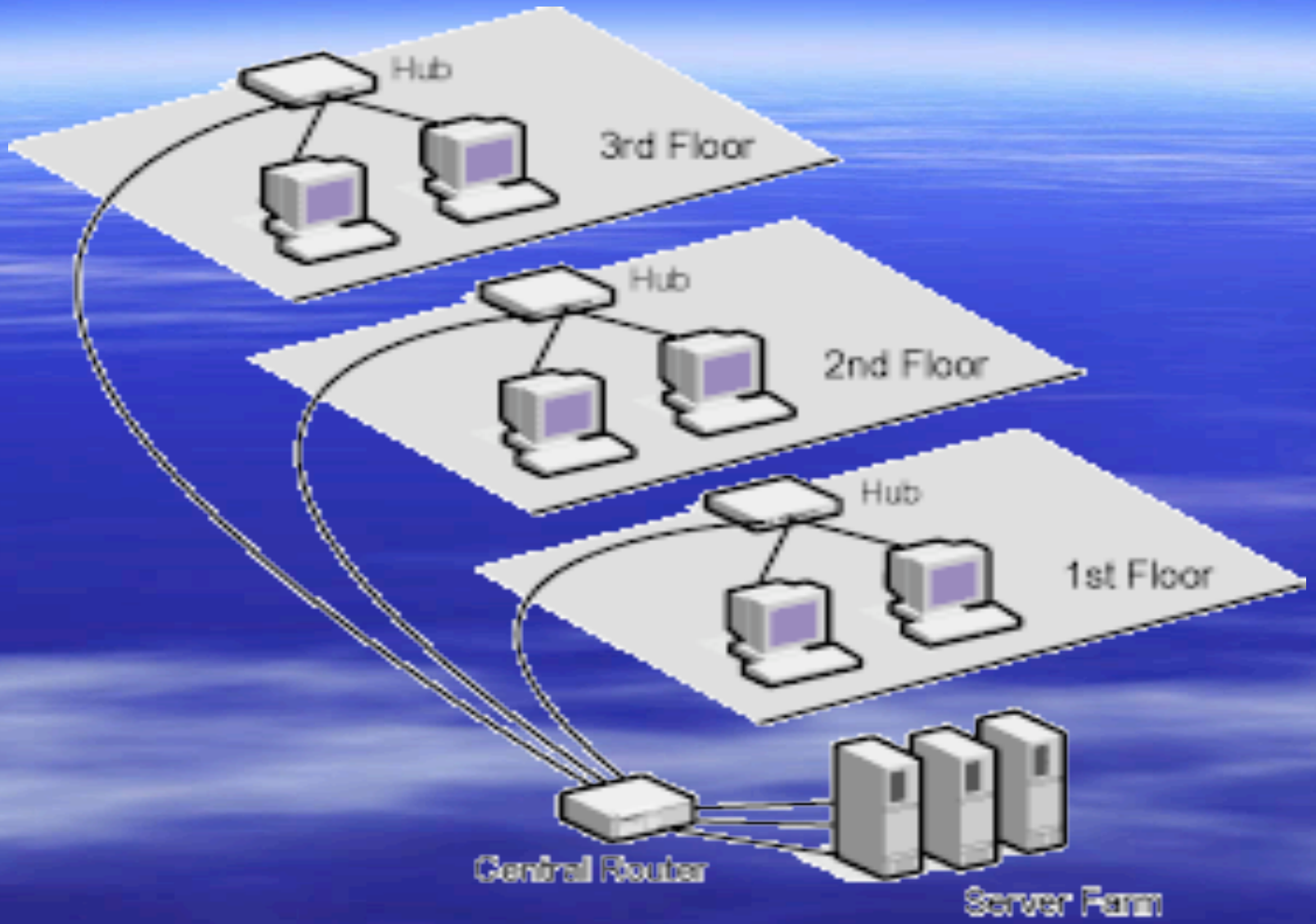
4 – A Three-Stage ATM Migration
Ready for Migration: Collapsed Backbone

• As part of the evolution from a single LAN per building to separate LANs on each floor, many network managers have reconfigured their distributed networks to collapsed back-bones.

•A collapsed backbone configuration eliminates the router on each floor, concentrat-ing all connections in a single backbone device, along with a high-end server farm.

•This architecture, illustrated on the Collapsed Backbone Architecture Diagram, effectively "collapses" the distributed backbone onto the high-speed backplane of the central router.

•The backplane of the central router can move data between LAN segments much faster than on a distributed Ethernet backbone, and also faster than on a Fiber Distributed Data Interface (FDDI) backbone.



Collapsed Backbone Architecture

The migration of a collapsed backbone network to ATM can be performed in three cost-effective stages:

- ✓ Stage 1--Enhance the collapsed backbone with VLANs and workgroups
- ✓ Stage 2--Install high-speed downlinks to increase bandwidth
- ✓ Stage 3--Enhance the collapsed backbone with routed ATM

5 - Converged Networks

Introduction

• As networking technology becomes pervasive, opportunities arise to use it in new and more creative ways. **One example is the use of data networks, rather than traditional circuit-switched networks, to carry voice and video traffic.**

• The generic term for this kind of use is **converged networking.**

• Converged networking offers many benefits. It can **reduce costs** and **enable new, tightly integrated multimedia applications.**
Here we discuss various aspects of converged networking, briefly describes the market forces driving converged networks, and summarizes the approaches to converged network architecture.

The Web as a Converged Network

• The Web has permanently changed the nature of networking. Before its appearance, networking was the province of specialized applications running in private corporations and research institutions. Today, millions of people around the world use networking as casually as television.

• The Internet has also changed the way organizations function, as it becomes the backbone for small business communications. Like most revolutionary technologies, the Web has drawn together previously separate activities and integrated them under a common framework. Web pages no longer provide only text and static graphics; they also provide animated graphics, audio, video, and other multimedia content.

• Consequently, the Web supports the convergence of content delivery over a single type of network. The Web is to content delivery what a backplane bus is to a computer system.

• The Web is one example of a larger trend in networking. Formerly distinct activities are becoming integrated into a common framework.

• Integration is occurring at a number of different levels, most noticeably at the application level.

• Users expect smooth interoperation between different applications, such as Web browsers and calendars, as well as applications that incorporate a diversity of data types, such as documents that embed spreadsheets, graphics, and voice annotation.

• This trend is motivated by the demand for increased ease of use, reduced cost, and increased functionality. By providing a diverse range of functions (voice/data/video integration) over a single network, an organization can spend less on capital

Types of Convergence

The **concept of convergence** describes this **trend toward tighter integration**. **Converged networking encompasses** several aspects, all of which are **related to the aggregation of networking activity.**

• ***Payload***

-**Payload convergence** uses the same communications format to carry different data types. **For example, in the past, audio and video traffic was carried over circuit-switched networks as Layer 1 bit streams, while busty data traffic was carried over packet-switched networks in Layer 3 data grams.**

- Today, **payload convergence** describes the trend to carry both audio/video and busty data traffic in Layer 3 data grams.

- **Payload convergence** does not prohibit a network from handling packets differently, according to their service requirements, it just describes the practice of using the same communications format for all traffic.

• ***Protocol***

- **Protocol convergence** describes the movement from multi-protocol to single protocol (typically IP) networks.

- While legacy networks are designed to handle many protocols (IP, IPX, and AppleTalk) and one type of data (so called "best effort"), **converged networks are designed to support one protocol and provide services necessary for different types of data (voice, one-way video, interactive video, and best effort).**

Physical

Physical convergence occurs when payloads travel over the same physical network equipment regardless of their service requirements. Both multimedia and Web traffic can use the facilities of an edge network, even though the former has more stringent bandwidth, delay, and jitter requirements. Resource reservation, priority queuing, and other QoS mechanisms within the network are used to differentiate the service requirements of one type of traffic from another, and deliver the necessary service to each.

Device

Device convergence describes the trend to support different networking paradigms in a single network device. Thus, a single switch may support Ethernet frame forwarding, IP routing, and ATM switching. Network devices may handle multiple types of data, all carried by a common network protocol (IP for example), that all have separate service requirements (such as bandwidth guarantees, delay, and jitter constraints). In addition, an end system may support both Web-based data applications and IP packet telephony.

Application

Application convergence integrates formerly separate functions into a single, multifunction application. For example, Web browsers allow the incorporation of plug-in applications that allow Web pages to carry multimedia content such as audio, video, high-resolution graphics, virtual reality graphics, and interactive voice.

Technology

Technology convergence satisfies both LAN and WAN requirements by using common networking technologies. For example, ATM can be used to provide both LAN and WAN services.

Organizational

Organizational convergence centralizes all networking, telecommunications, and computing services under a single authority, such as a chief information officer. This consolidation provides the necessary managerial framework for integrating voice, video, and data on a single network.

Converged Network Drivers

Several emerging forces are driving market interest in converged networks:

- ✓ Cost reduction, both in capital outlay and technical support expenditures
- ✓ Emerging technologies that put greater demands on networks
- ✓ Greater network flexibility and functionality
- ✓ Emergence of industry standards

Elements of Network Management

Network management begins with baselining, an essential feature for measuring the state of a network. After baseline performance is measured, an administrator can set thresholds for monitoring performance. The network management software monitors status and identifies key events, helps with troubleshooting and device reconfiguration, and generates reports to help the administrator optimize end-to-end performance and availability.

The major elements of network management systems include:

- **Flexible data collection--** Real-time traffic monitoring intelligence should be placed at key points throughout the network. This intelligence, embodied in RMON and RMON2 probes and related technologies, can be in the form of dedicated devices placed on links of high interest, or software installed in network routers, switches, and other devices.
- **Configuration and control**-- The network management system should make it possible for the administrator to determine and modify device configurations, check device status, track inventory groupings, and generally manage devices--all remotely, from the network management console
- .**Network health monitoring--** This higher level network management functionality should provide the network administrator with enterprise-wide views of overall network health. It should allow for checking status priorities, setting thresholds for action-on-event operations, and reporting fault data in real time.
- **Troubleshooting network problems--** The network administrator should be able to check LAN segments using real-time and historical data displays, perform packet analysis, and monitor traffic to see where bottlenecks--or potential bottlenecks--exist

Tutorial on Wireless LANs

Planning and Deploying a Wireless LAN

Planning for a Wireless Network

- "If you fail to plan, then you plan to fail"
- Some steps involved in planning wireless networks similar to planning wired network
  - Many steps significantly different
- Basic planning steps:
  - Assessing needs
  - Weighing benefits
  - Calculating costs

Assessing Needs: The Need for Mobility

- Two significant changes in business world over last 15 years:
  - Workers have electronic tools to access information and accomplish significantly more
  - Restructuring of organizational hierarchies
    - Organizations are “flatter”
    - Teamwork is essential
  - Together, can result in *decreased* productivity
    - Hinders ability to collaborate and make timely decisions
- “Mobile office” needed

Assessing Needs: The Need for Mobility (continued)

- A solution to need for mobility is WLANs
  - Expand productivity zone of knowledge workers
  - Improve quality and productivity of meetings
  - Work can be performed in more locations at more times
- WLANs have been shown to add one to two hours a day of productive time per worker
  - Enabling worker to respond to customers, partners, and colleagues more quickly
- WLANs too often viewed as *optional* add-on to computer networks

Assessing Needs: Examining the Business Entity

- Determine if business case exists for bringing wireless networking into corporate environment
  - What is the purpose or mission of the organization?
  - Is the current mission expected to change in the future?
  - What is the size of the organization?
  - How much growth is anticipated in the organization?
- Obtaining firm conceptual grip on

Assessing Needs: Reviewing the Current Network

- Question to ask when examining how organization uses current network:
  - How does current network support the organization's mission?
  - What applications run on the network?
  - How many users does network support?
  - Strengths and weaknesses of the current network?
  - Anticipated growth in network technology?
- Examining current network status reveals much of this information

Assessing Needs: Reviewing the Current Network (continued)

- Good time to document network in detail:
  - Number of clients
  - Types of clients
  - Number of servers
  - The topology of the network
  - What media is being used
  - Performance of the network
  - Types of devices connected to the network

Assessing Needs: Reviewing the Current Network (continued)

Number of clients	28
Types of clients	20 – Windows XP Professional 8 – Red Hat Linux
Number of servers	1 – Windows Server 2003
Type of network	Ethernet 100 Mbps switched
Type of media being used	Category 6
Types of devices connected to network	6 laser printers; 1 scanner; switch connects to Gigabit Ethernet campus backbone

Table 6-1: Current network table

Assessing Needs: Reviewing the Current Network (continued)

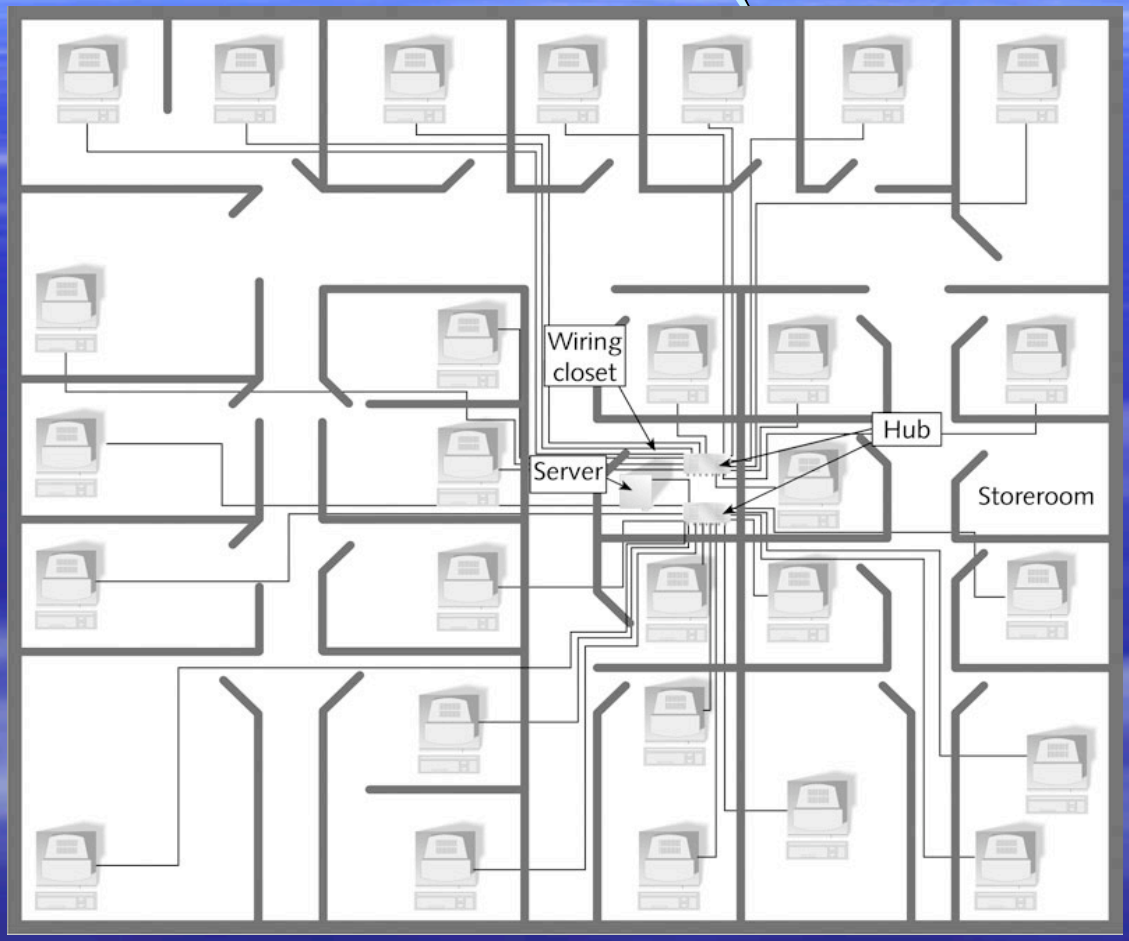


Figure 6-1: Network diagram

Determining Benefits: Hard Benefits

- Benefits that can be easily measured or quantified
  - For WLANs, easily measured in decreased cost of installation
    - e.g., elimination of cabling costs
- Using wireless technology for MAN or WAN can result in even higher savings

Determining Benefits: Soft Benefits

- Benefits that are difficult, if not impossible, to quantify accurately
  - Improved productivity
  - Enhanced collaboration and faster responsiveness
  - Flexible mobility
  - Adherence to standards
  - Improved employee satisfaction

Calculating Return on Investment (ROI)

- **Return on investment (ROI):** Standard measure of profitability of a project
  - Total cost of project
    - Hardware, software, implementation costs, training, operations staff, maintenance staff and services, and connectivity fees
  - Less tangible costs
    - Workload management and customer satisfaction
- Several models for calculating ROI

Calculating Return on Investment (continued)

- Intel Corporation's wireless LAN model:
  - Implement a pilot
  - Develop a report
  - Assemble data
  - Calculate ROI

Number of Users	Network Costs	Wireless Costs	Total Costs	Cost per User	Benefits	ROI
32	$8,500	$11,300	$19,800	$620	$300,000	$280,200
150	$15,000	$57,000	$72,000	$480	$1,000,000	$928,000
800	$57,000	$351,000	$409,000	$510	$5,000,000	$4,591,000

Table 6-2: Three-year WLAN costs and benefits

Calculating Return on Investment (continued)

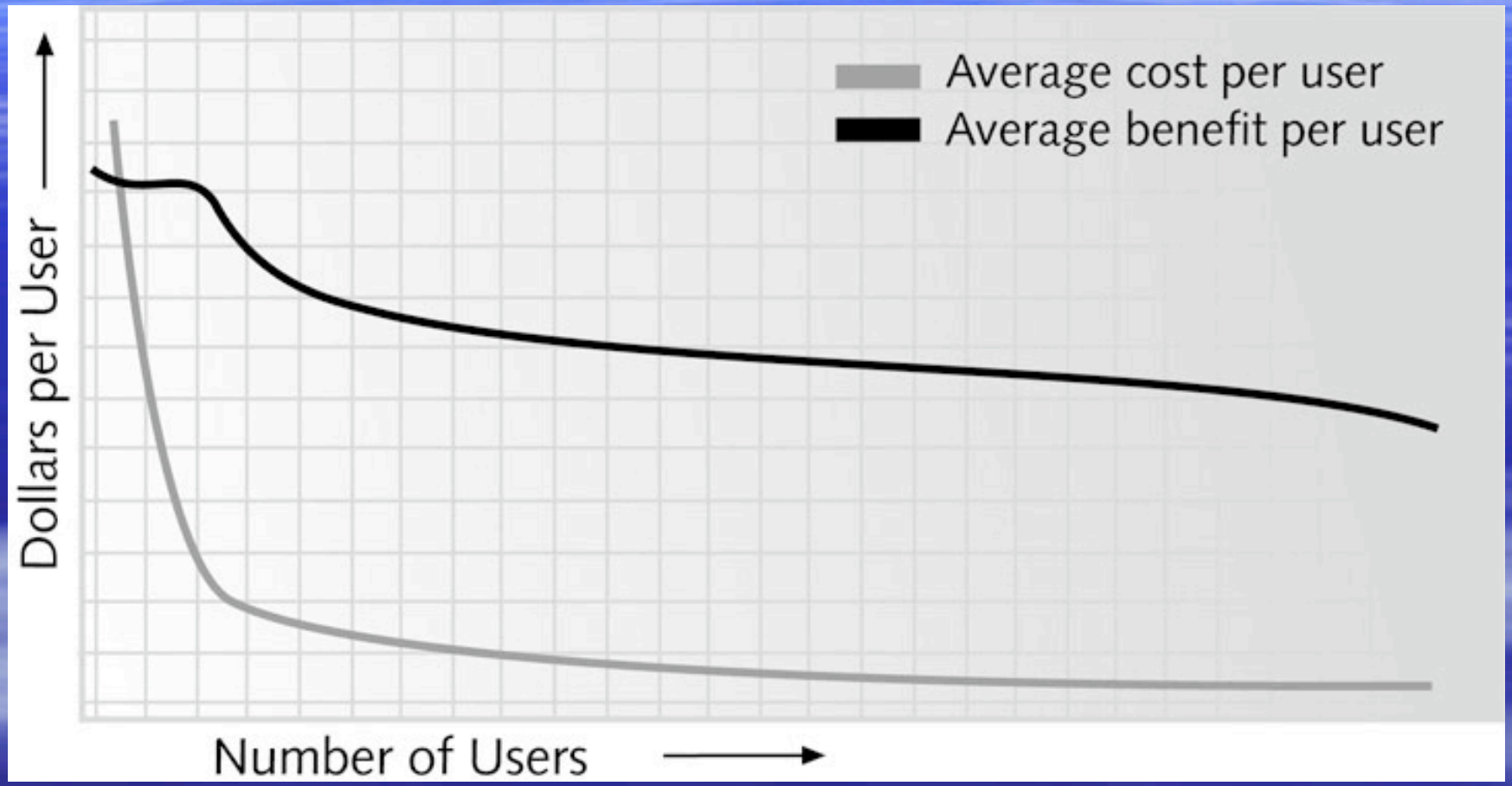


Figure 6-2: Intel's ROI model for WLANs

Designing the Wireless LAN

- Involves determining:
  - Which deployment scenario is best
  - Which IEEE wireless network standard should be used
  - Type of AP management to implemented
  - Where wireless devices should be located

Determining the Deployment Scenario

- First step in designing a WLAN is to decide on correct deployment scenario:
  - *Ad hoc*: Not connected to wired infrastructure
    - Useful where wireless infrastructure does not exist or services to remote networks not required
  - *Infrastructure*: WLAN devices connect to wired corporate network via AP
    - Most corporate wireless LANs
  - *Hotspot*: Provides wireless LAN service, for free or for a fee, from variety of public areas
  - *Point-to-point remote wireless bridge*: Typically interconnects two LAN segments

Determining the Deployment Scenario (continued)

- Deployment scenarios (continued):
  - *Point-to-multipoint remote wireless bridge*: Connects multiple LAN segments
  - *Ethernet to wireless bridge*: Connects single device that has an Ethernet port but not an 802.11 NIC
  - *Wireless gateway*: Provide single mechanism for managing and monitoring the wireless network

Selecting the IEEE Wireless Network Type

- IEEE 802.11b, 802.11a, or 802.11g
- Decision may depend on many factors
  - Do other devices in area use same frequency range as one of the network types?
  - What kind of coverage is needed?
  - What types of applications will be used?
- If broader area of coverage needed, 802.11g standard should be considered first
  - Good balance of coverage area with speed

Selecting the IEEE Wireless Network Type (continued)

- If interference is an issue, then 802.11a standard should be considered
- Only consider 802.11b in areas where low bandwidth is acceptable or ad hoc wireless network will be used
  - Slow speed and susceptibility to interference

Deciding upon Access Point Management

- If using infrastructure wireless network, must decide type of AP management
- **Fat access point:** AP serves as management point
  - Configuration must be done through via AP
- **Thin access point:** Lacks management functions
  - Management functions moved to Ethernet network switch
  - Management simplified, centralized
  - Handoff time reduced

Deciding upon Access Point Management (continued)

- Thin AP approach does not provide overall solution for managing entire network (wired and wireless)
- Several vendors working on comprehensive network management solutions
  - Integrate wireless networks into same deployment, operations, and management as wired network
  - e.g., Cisco's Structured Wireless-Aware Network (SWAN)

Determining the Location of the Wireless Devices

Object	Example	Type of Interference
Open space	Courtyard or open cafeteria	None
Wood	Door or floor	Low
Plaster	Inner wall	Low
Synthetic materials	Office partition	Low
Cinder block	Exterior wall	Low
Asbestos	Ceiling insulation	Low
Glass	Clear window	Low
Wire mesh in glass	Security window	Medium
Human body	Large group of people	Medium
Water	Aquarium	Medium
Brick	Outer wall	Medium
Marble	Floor	Medium
Ceramic	Floor	High
Paper	Roll or stack of paper stock	High
Concrete	Floor pillar	High
Bulletproof glass	Security booth	High
Silvering	Mirror	Very high
Metal	Elevator shaft or filing cabinet	Very high

Table 6-3: Interference by objects

Ad Hoc Mode

- Wireless devices communicate directly without an AP
- Three main considerations:
  - Stations must be arranged so that they are all within proper distance limits
  - All stations must send and receive signals on same frequency
  - Hidden node problem must be avoided

Ad Hoc Mode (continued)

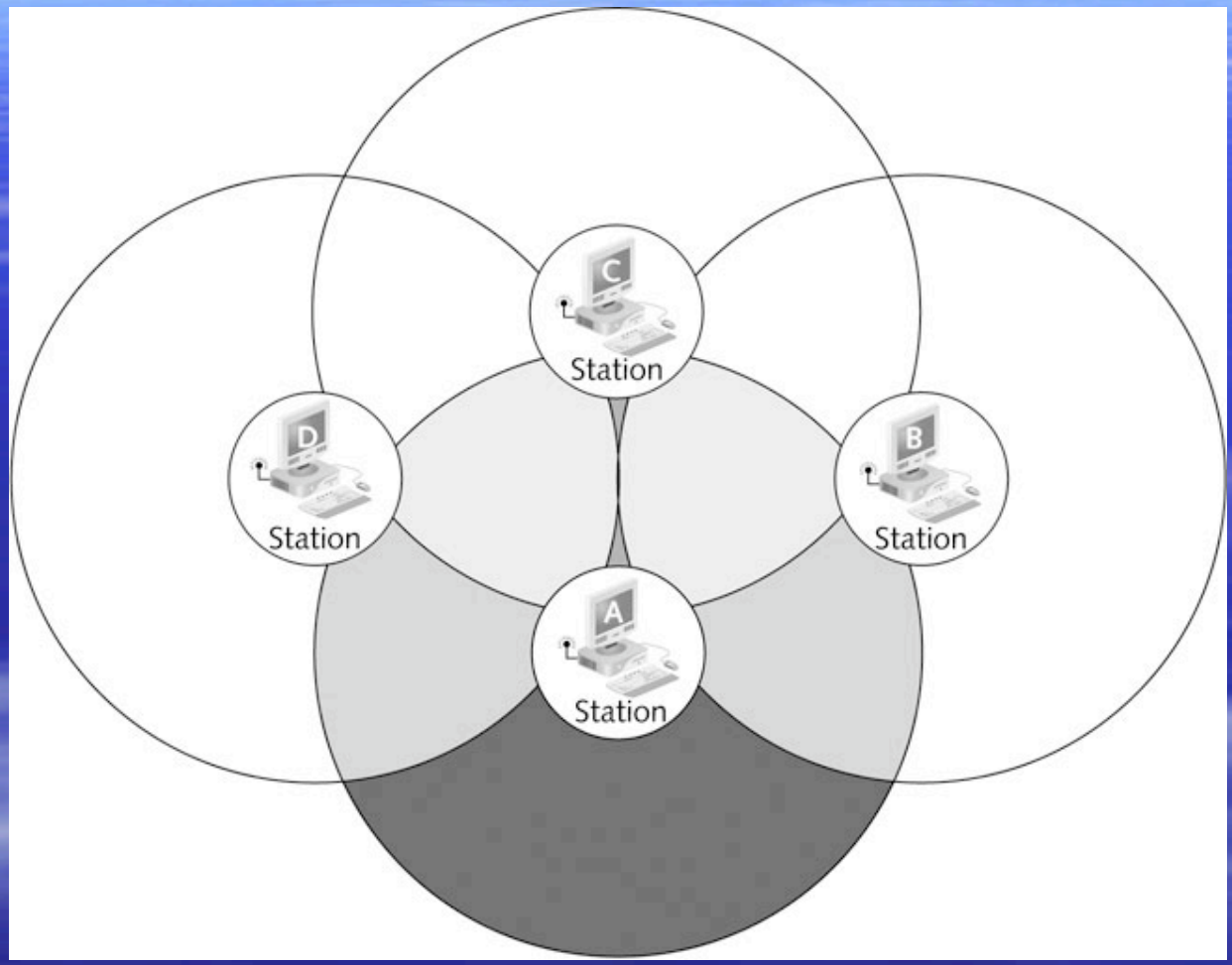


Figure 6-3: Ad hoc hidden node problem

Infrastructure Mode

- Positioning APs correctly for an infrastructure WLAN is critical for ensuring that coverage area is sufficient
  - Interference by objects must be taken into consideration
  - Signal should not extend beyond building's exterior walls for security reasons
- In an ESS infrastructure network with multiple APs, important that each AP's channel set correctly
  - Adjacent APs using same channel can cause

Infrastructure Mode (continued)

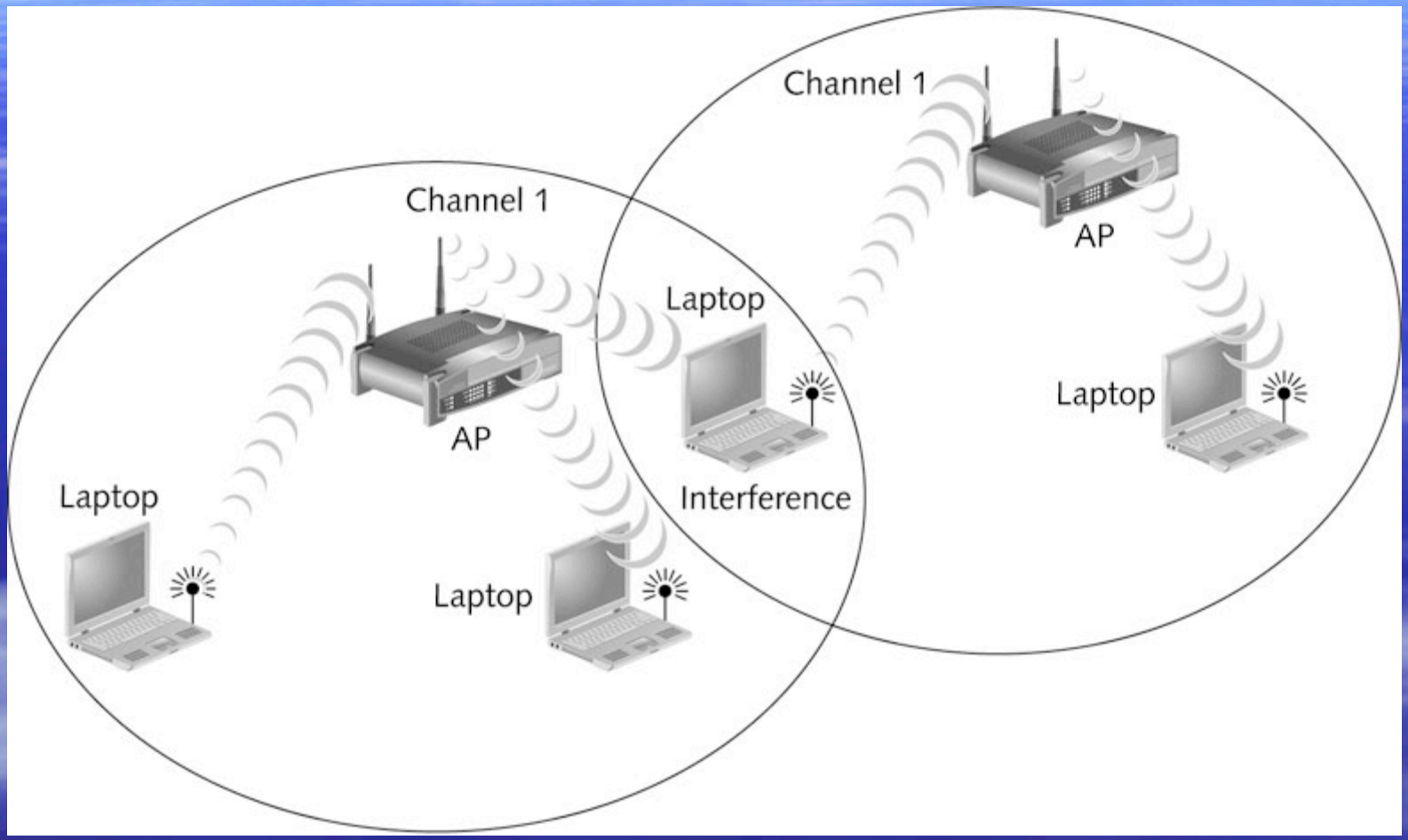


Figure 6-4: Interference from using same channel

Infrastructure Mode (continued)

- IEEE 802.11b and 802.11g networks divide frequency spectrum into 14 overlapping and staggered channels
  - Only channels 1, 6,and 11 do not overlap
- **Channel reuse:** Adjacent APs use nonoverlapping channels (1, 6, and 11)
- IEEE 802.11a networks have eight nonoverlapping channels
- Must ensure APs properly overlap
  - No gaps, but not too close together

Infrastructure Mode (continued)

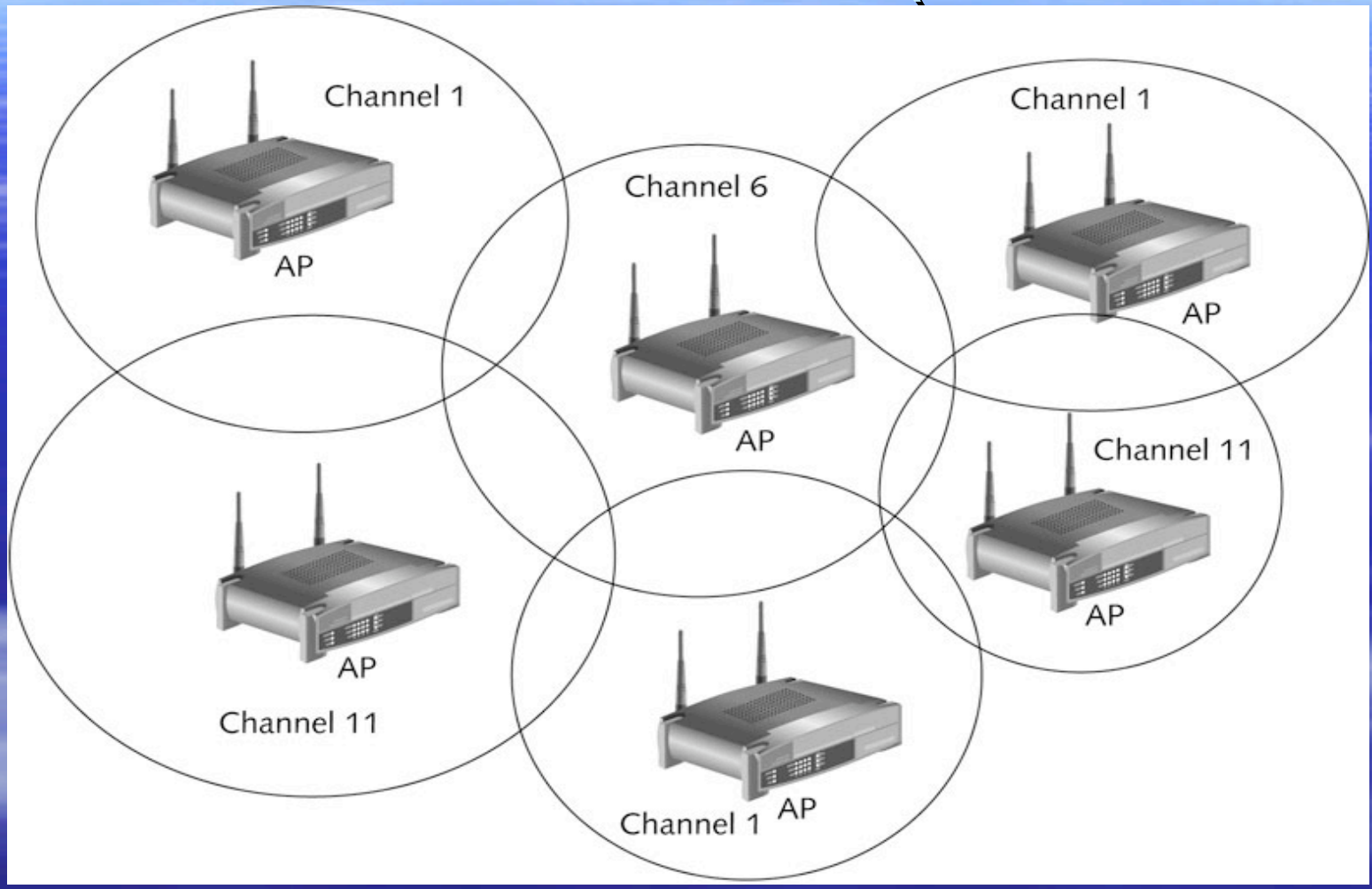


Figure 6-5: Channel reuse

Infrastructure Mode (continued)

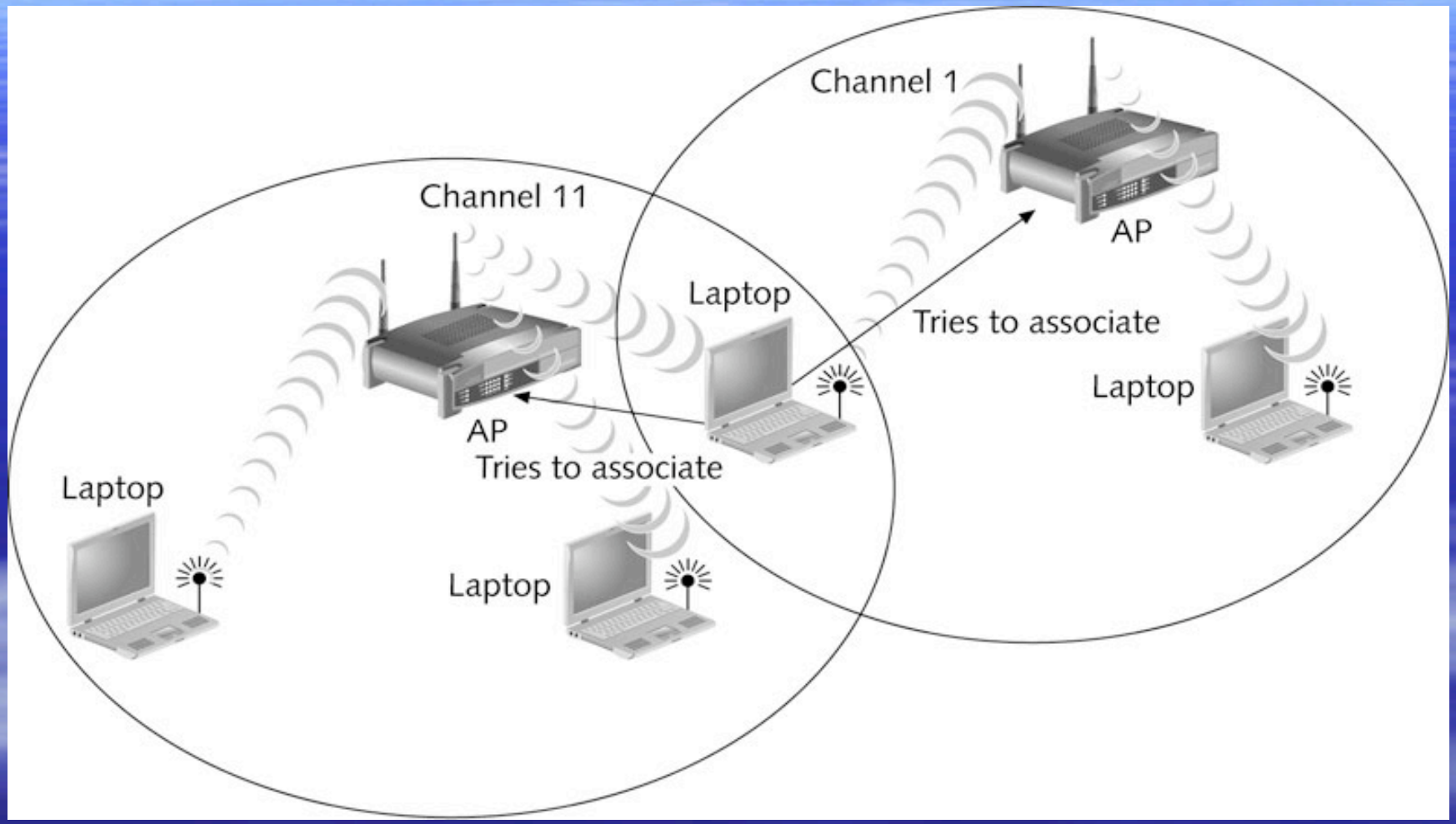


Figure 6-6: Flip flop between access points

Infrastructure Mode (continued)

- Must consider number of users who will be associated with APs
  - Consider not only how many users will be associated with each AP but also what they will be doing

Deploying a Wireless Network

- If planning/designing done correctly, deploying can be easiest step
- Must consider actual placement of APs
  - Place APs exactly where they were designed to go
  - To avoid interference, better to place APs higher
    - Be careful if placing APs in **plenums**
    - If needed, can use PoE
- Good idea to configure WLAN on own network segment

Providing User Support: Training

- Planning, designing, and deploying WLAN pointless if users don't receive required support
- Training is vital to use of a WLAN
  - Users must know how to use new hardware and software
  - Support staff must know how to manage network and diagnose problems
  - Increases effectiveness of new wireless network
    - Minimizes drop in productivity normally associated with installation of a new system

Providing User Support: Training (continued)

- Group training session often most effective training setting
  - Preferably done at same time users receive wireless-enabled laptops
- Important to set appropriate user expectations for support and how they should request it

Providing User Support: Support

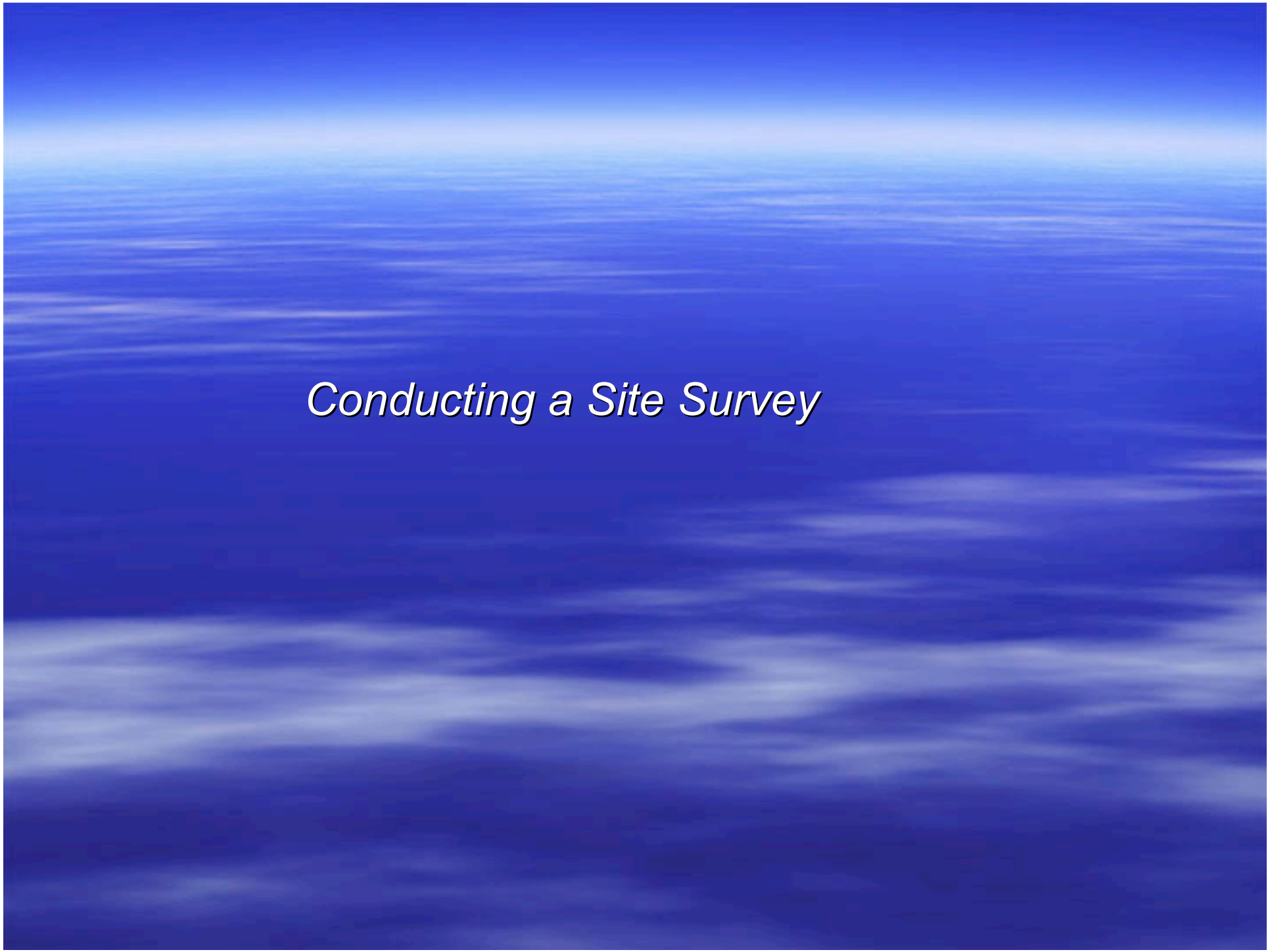
- Involves continuing follow-up in answering questions and assisting users
- User support functions can be organized in variety of ways:
  - Establishing informal peer-to-peer support groups
  - Creating formal user support groups
  - Maintaining a help desk
  - Assigning support to the information technology department

Providing User Support: Support (continued)

- Establishing and staffing internal help desk is one of most effective means of support
  - Central point of contact for users who need assistance using network
  - Suggestions regarding a help desk:
    - One telephone number for help desk
    - Plan for increased call volume after network installed
    - Problem tracking
    - Use surveys to determine user satisfaction
    - Periodically rotate network personnel into help desk
    - Use info from help desk to organize follow-up training

Providing User Support: Support (continued)

- User feedback essential when installing new WLAN
  - Possibly more essential than technical feedback
  - May have IT personnel contact users for feedback
  - May schedule meetings with users to gather feedback


Conducting a Site Survey

What is a Site Survey?

- When installing a WLAN for a University, areas of dead space might not be tolerated
  - Ensure blanket coverage, meet per-user bandwidth requirements, minimize “bleeding” of signal
- Factors affecting wireless coverage goals:
  - Devices emitting RF signals
  - Building structure (walls, construction materials)
  - Open or closed office doors
  - Stationary versus mobile machinery/equipment

What is a Site Survey? (continued)

- Factors affecting wireless coverage goals (continued):
  - Expansion of physical plant or growth of organization
  - Existing WLANs
    - Both inside organization, and within nearby organizations
- **Site survey:** Process of planning a WLAN to meet design goals
  - Effectiveness of a WLAN often linked to thoroughness of the site survey

What is a Site Survey? (continued)

- Design goals for a site survey:
  - Achieve best possible performance from WLAN
  - Certify that installation will operate as promised
  - Determine best location for APs
  - Develop networks optimized for variety of applications
  - Ensure coverage will fulfill Universitie's requirements
  - Locate unauthorized APs

What is a Site Survey? (continued)

- Design goals for a site survey (continued):
  - Map nearby wireless networks to determine existing radio interference
  - Reduce radio interference as much as possible
  - Make wireless network secure
- Survey provides realistic understanding of infrastructure required for proposed wireless link
  - Assists in predicting network capability and throughput
  - Helps determine exact location of APs and power levels required

What is a Site Survey? (continued)

- When to perform a site survey:
  - Before installing a new wireless network
  - Before changing an existing wireless network
  - When there are significant changes in personnel
  - When there are changes in network needs
  - After making physical changes to a building

Site Survey Tools: Wireless Tools

- Most basic tool is AP itself:
  - Position AP in various locations, monitor signal as you move
  - APs should have ability to adjust output power
  - APs should have external antenna connectors
    - Test effectiveness of different antenna types in different situations
  - May need DC-to-AC converter for testing
- Notebook computer with wireless NIC also essential for testing
  - Previously configured and tested

Site Survey Tools: Wireless Tools (continued)

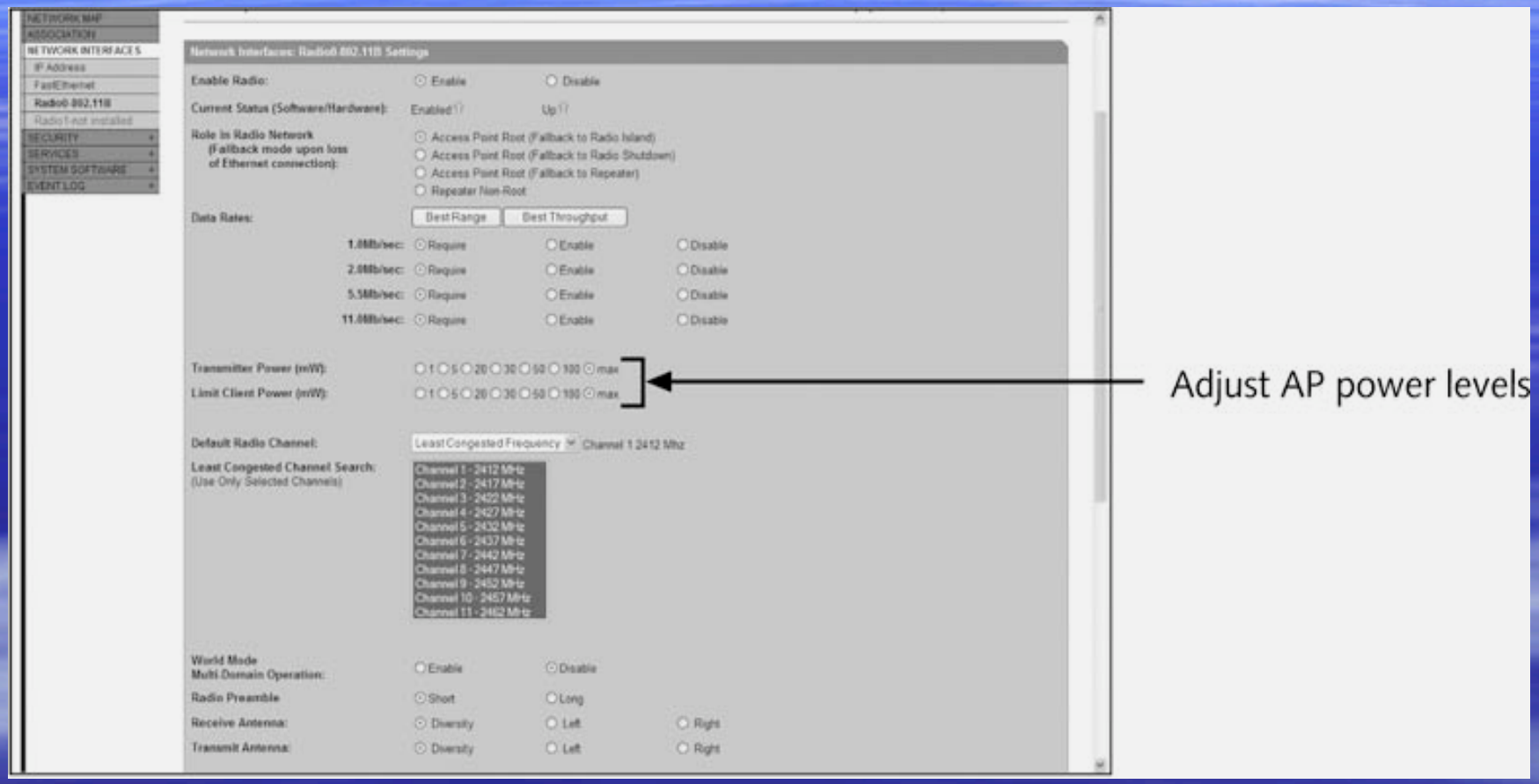


Figure 7-1: Adjusting AP power levels

Site Survey Tools: Wireless Tools (continued)

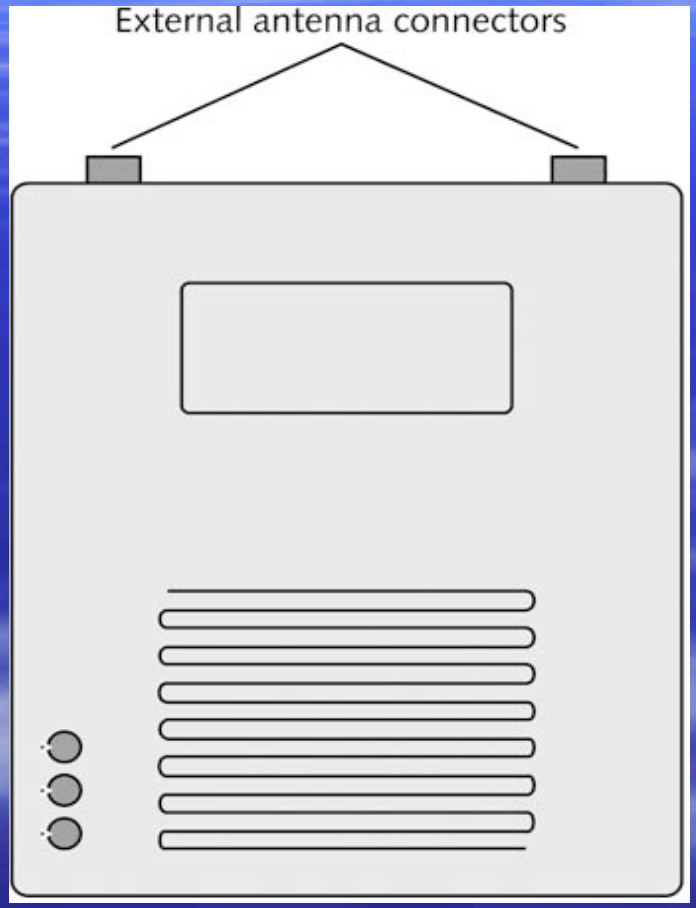


Figure 7-2: External antenna connectors

Site Survey Tools: Measurement Tools

- **Site Survey Analyzers:** Specifically designed for conducting WLAN site surveys
  - Software often built into AP
  - **Receive Signal Strength Indicator (RSSI)** value
  - Full-featured site survey analyzer software settings:
    - Destination MAC Address
    - Continuous Link Test
    - Number of Packets
    - Packet Size

Site Survey Tools: Measurement Tools (continued)

- **Site Survey Analyzers (continued):**
  - Full-featured site survey analyzer software settings (continued):
    - Data Rate
    - Delay Between Packets
    - Packet Tx Type
      - Unicast or multicast
    - Percent Success Threshold
  - Basic survey analyzer software contains far fewer features

Site Survey Tools: Measurement Tools (continued)

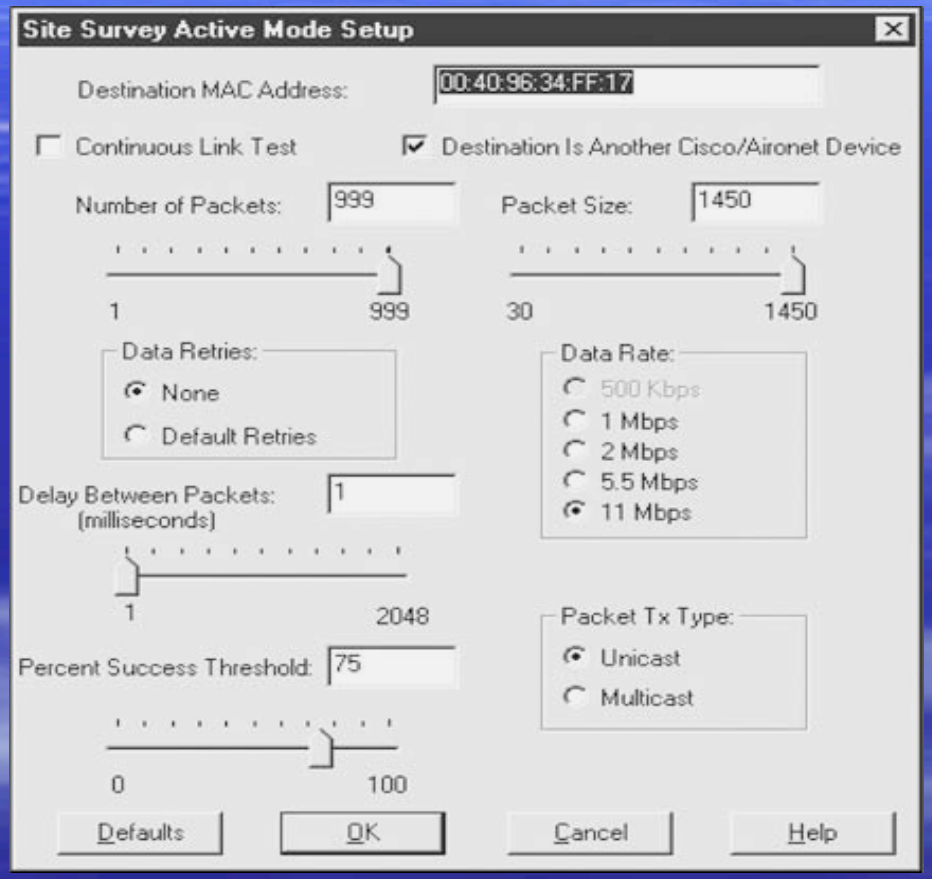


Figure 7-3: Full-featured site survey analyzer software setup

Site Survey Tools: Measurement Tools (continued)

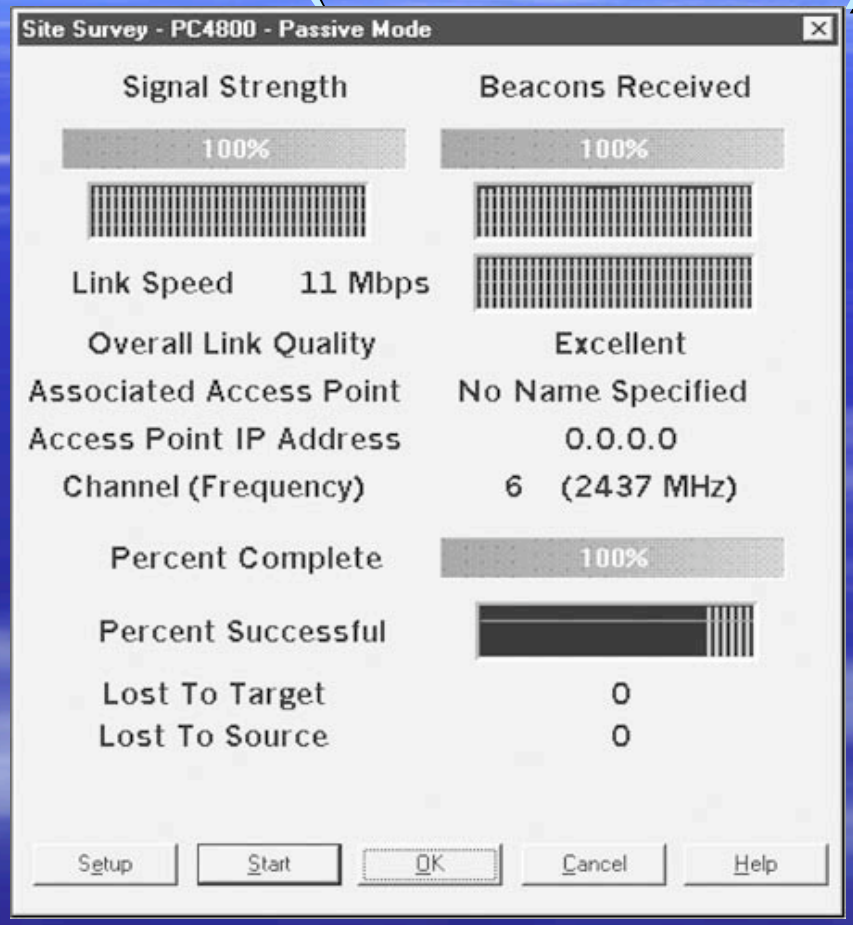


Figure 7-4: Full-featured site survey analyzer software results

Site Survey Tools: Measurement Tools (continued)

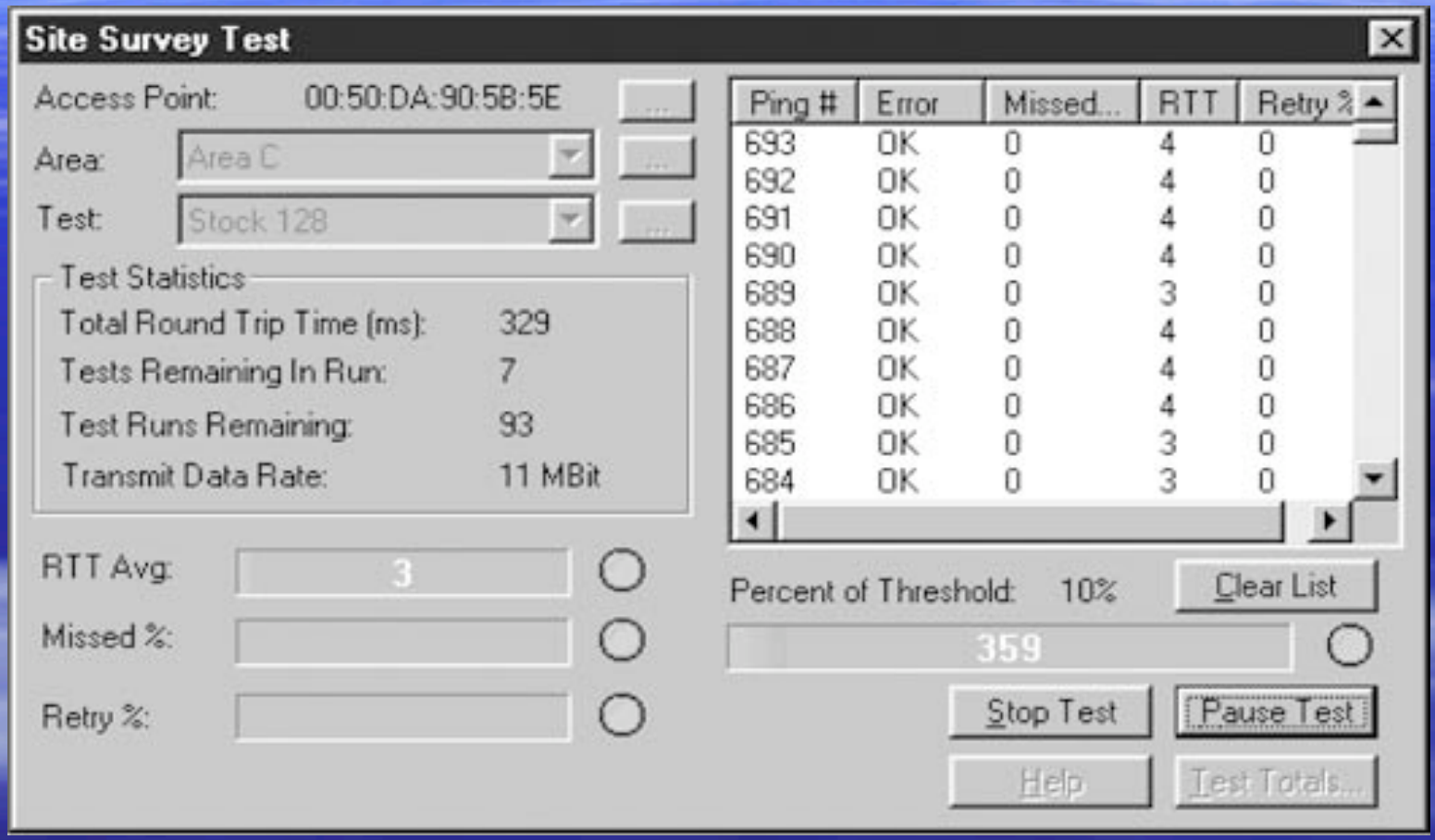


Figure 7-6: Basic site survey analyzer software results

Site Survey Tools: Measurement Tools (continued)

- **Spectrum Analyzers:** Scan radio frequency spectrum and provides graphical display of results
  - Typically measure signal-to-noise ratio
  - Single-frequency analyzers measure signal-to-noise ratio at specified frequency
  - Helpful in identifying interference problems
    - Thus, helps properly position/orient AP

Site Survey Tools: Measurement Tools (continued)

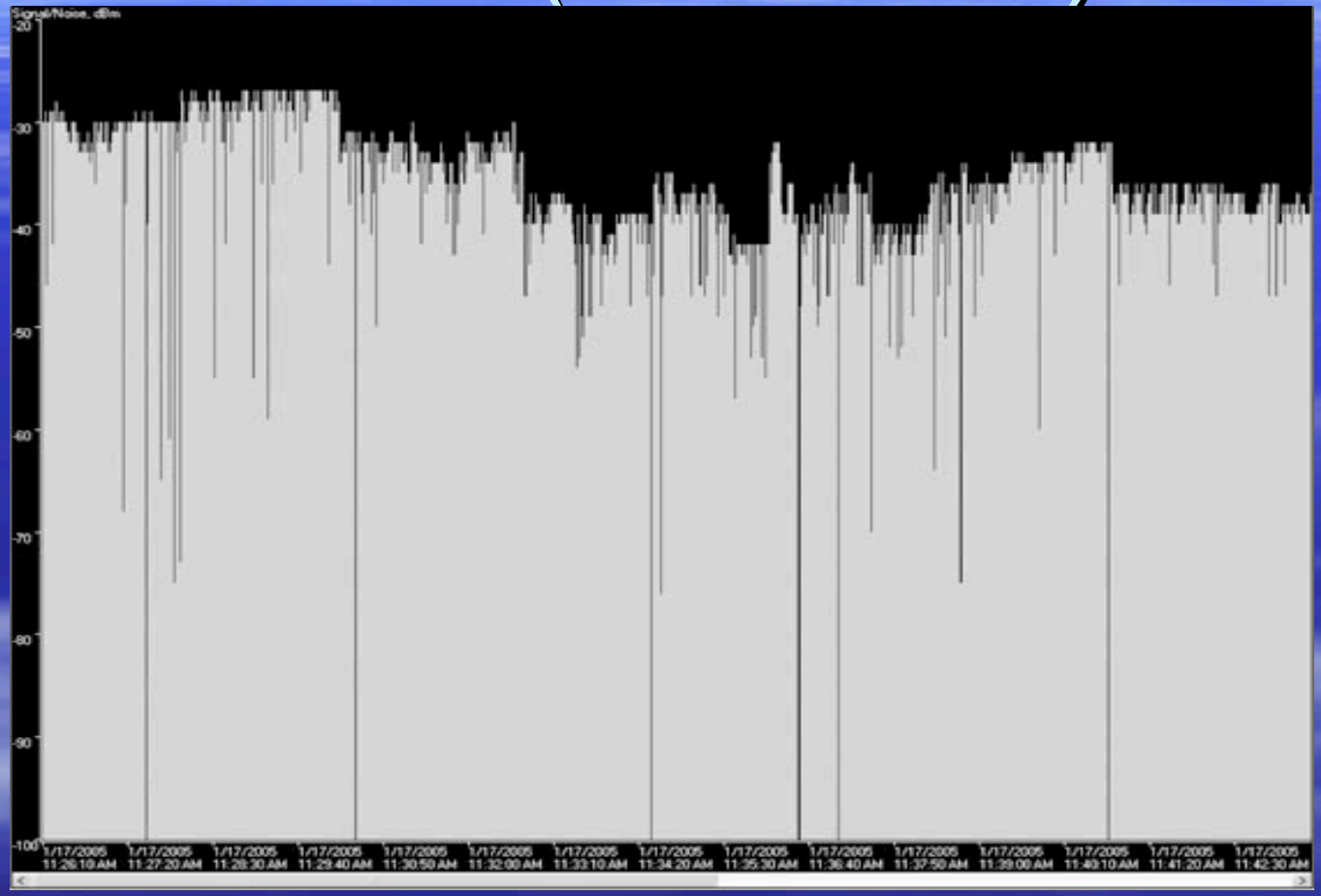


Figure 7-7: Single-frequency analyzer

Site Survey Tools: Measurement Tools (continued)

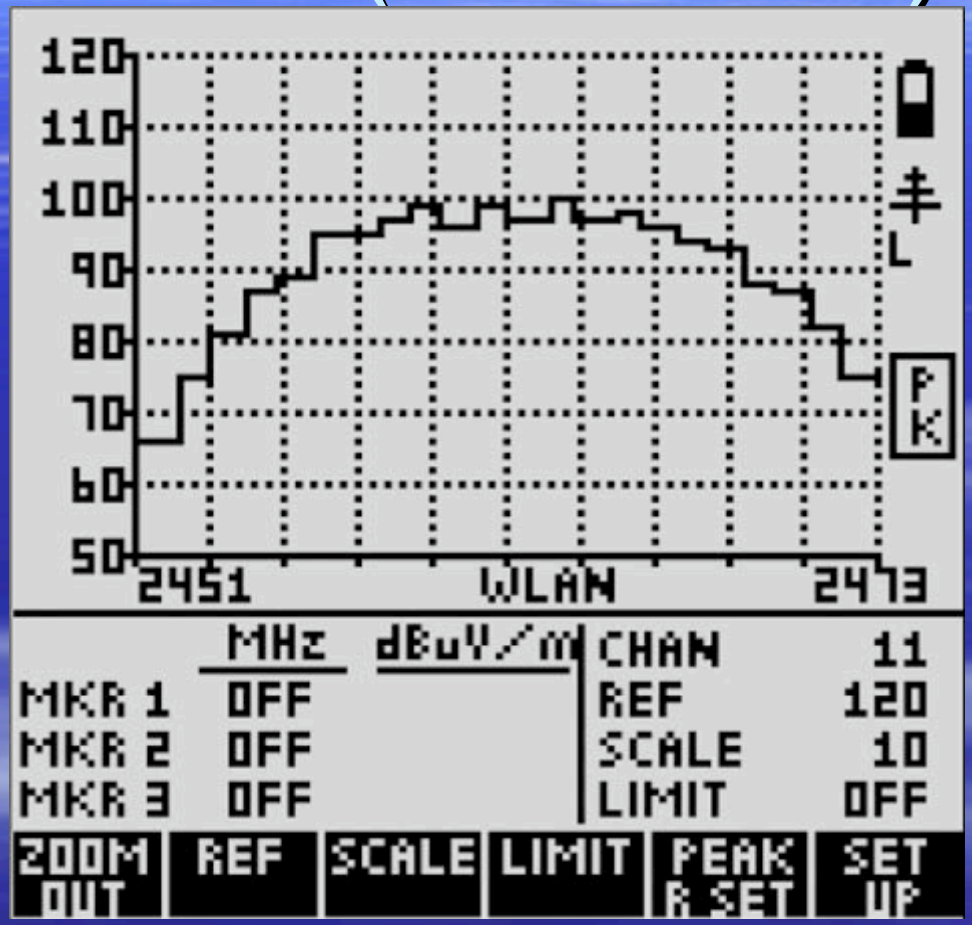


Figure 7-8: Spectrum analyzer

Site Survey Tools: Measurement Tools (continued)

- **Network Analyzers:** Can be used to pick up packets being transmitted by other WLANs in area
  - Provide additional information on transmissions
  - Packet sniffers or protocol analyzers
  - Not used in placement of AP

Site Survey Tools: Documentation Tools

- Create a “hard copy” of site survey results
  - Make available for future reference
  - No industry-standard form for site survey documentation
- Site survey report should include:
  - Purpose of report
  - Survey methods
  - RF coverage details (frequency and channel plan)
  - Throughput findings

Site Survey Tools: Documentation Tools (continued)

- Site survey report should include (continued):
  - Problem zones
  - Marked-up facility drawings with access point placement
  - Access point configuration
- Use plain paper and building layout blueprints as tools
- Advisable to create database to store site survey information and generate reports

Site Survey Tools: Documentation Tools (continued)

Device Identifier	XXX1SO1AP01
Description	Lab 214 AP 1
Location Details	
AP Location Identifier	AP-214A74
AP Location Notes	The Access Point is located on the interior wall close to the inner core of the building as indicated in Figure 1.
AP Mounting Notes	The Access Point should be mounted to the wall using the supplied mounting brackets.
AP Coverage Notes	The coverage for this access point is indicated by Figure 2 below.
AP Power Supply	Alternating current
Antenna Location	See figure 9
Antenna Location Notes	The antenna is located at the same position as the access point.
Antenna Mounting Notes	The antenna is mounted to the inner wall. The antenna must be mounted vertically with the antenna facing towards the exterior of the building.
Hardware Specifications	
AP Manufacturer	Cisco Systems
AP Model	AIR-AP1220B-A-K9
Antenna Manufacturer	Cisco Systems
Antenna Model	AIR-ANT2012 (Wall Mount, Diversity directional 6.5 dBi gain)
Antenna Diversity	Yes
Configuration Details	
Channel	11
Data Rate Configuration	11 Mbps – YES; 5.5Mbps – BASIC; 2 Mbps – NO; 1 Mbps - NO
RF Power Output	0 dBm (1 mW)
ERIP Output	6 dBm

Figure 7-9: Sample site survey form

Performing a Site Survey: Gathering Data

- **Obtaining Business Requirements:** Determine business reasons why WLAN being proposed or extended
  - If this step skipped, almost impossible to properly design and implement the network
  - Primary data gathering method is interviewing
  - Must determine type of mobility required within organization
  - Must determine per-user bandwidth requirements
    - May be different "types" of users with different

Performing a Site Survey: Gathering Data (continued)

- **Defining Security Requirements:** Consider type of data encryption and type of authentication that will take place across WLAN
  - Consider existing security policies and procedures
- **Gathering Site-Specific Documentation:**
  - Blueprints, facility drawings, and other documents
    - Show specific building infrastructure components

Inspecting the site

Performing a Site Survey: Gathering Data (continued)

- **Gathering Site-Specific Documentation (continued):**
  - Behind-the-scenes site inspection
    - May require ladder, flashlight, and an escort
- **Documenting Existing Network Characteristics:** New or expanded WLAN will "dovetail" into network already in place
  - Determine degree to which WLAN will interact with other wired networks
  - Legacy systems may require additional equipment to support WLAN

Performing a Site Survey: Performing the Survey

- **Collecting RF Information:**
  - Note objects in and layout of room
    - Use digital camera
  - Position AP
    - Initial location will depend on antenna type
    - Document starting position of AP
  - Using notebook computer with site survey analyzer software running, walk slowly away from AP
    - Observe data displayed by analyzer program
      - Data rate, signal strength, noise floor, and signal-to-noise ratio

Performing a Site Survey: Performing the Survey (continued)

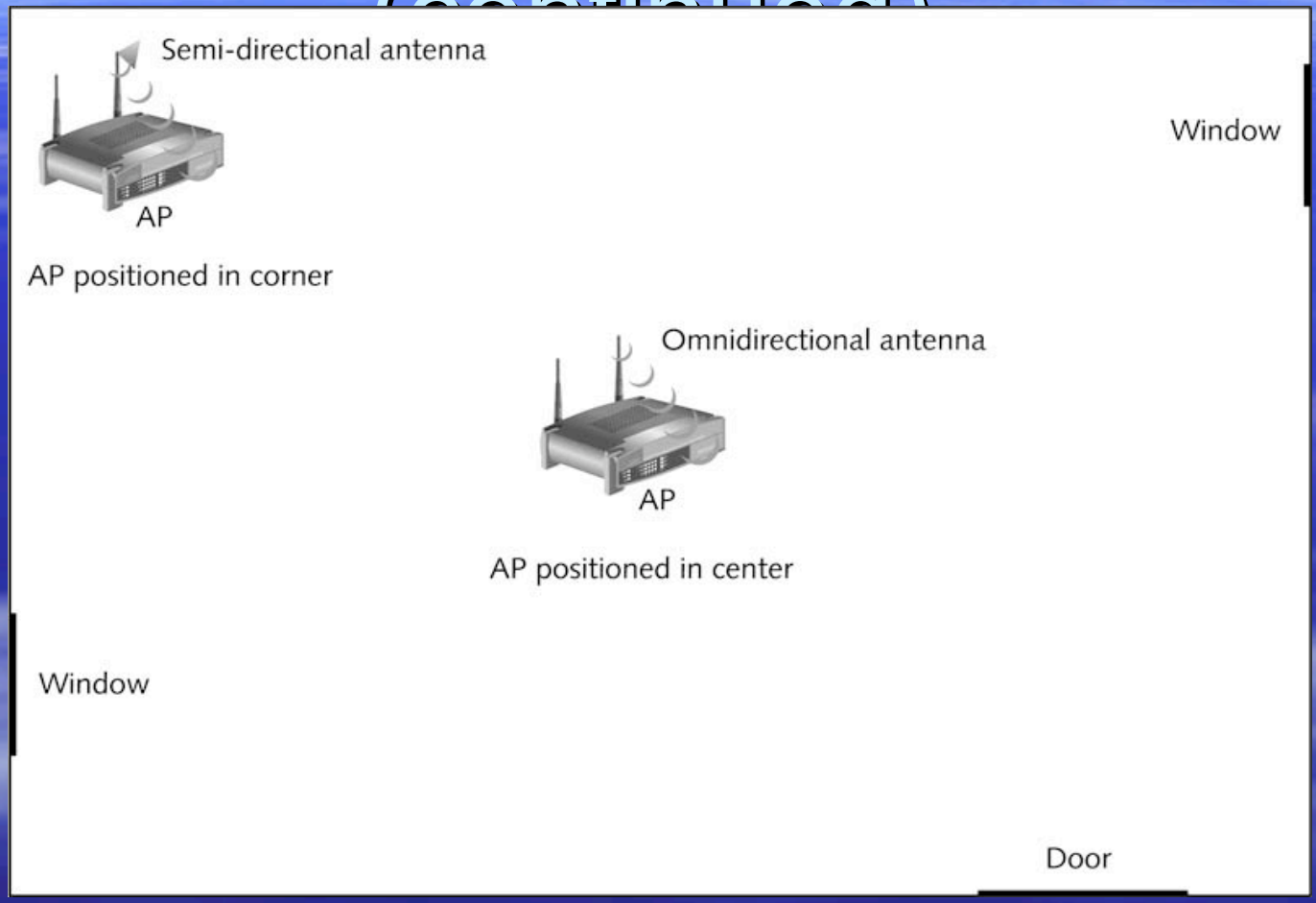


Figure 7-10: Position of APs

Performing a Site Survey: Performing the Survey (continued)

- **Collecting RF Information (continued):**
  - Continue moving until data collected for all areas
  - Data collected used to produce:
    - **Coverage pattern:** Area where signal can be received from the AP
    - **Data rate boundaries:** Range of coverage for a specific transmission speed
    - **Throughput:** Number of packets sent and received and data rates for each
    - **Total transmission range:** Farthest distance at which signal can be received by wireless device

Performing a Site Survey: Performing the Survey (continued)

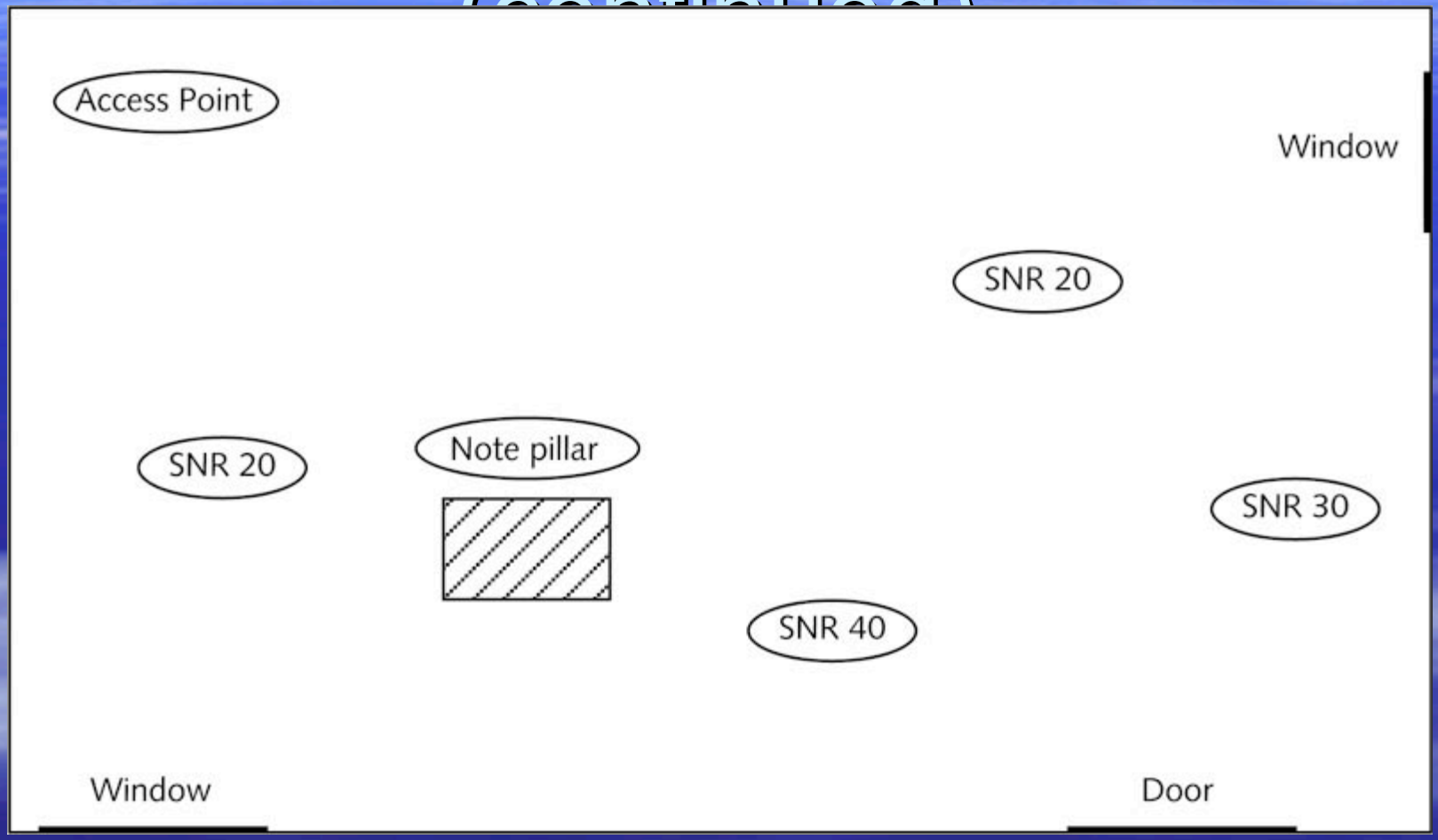


Figure 7-11: Coverage pattern

Performing a Site Survey: Performing the Survey (continued)

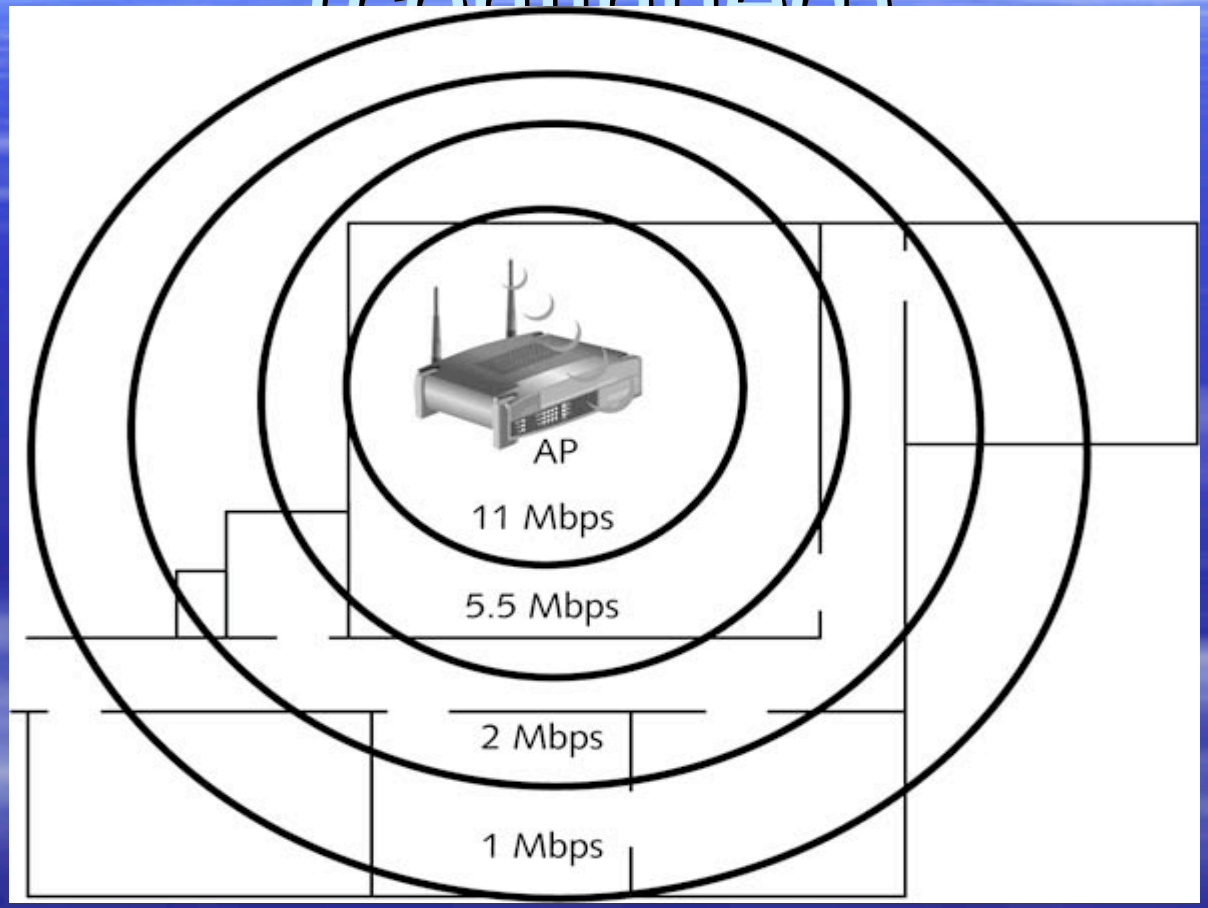


Figure 7-12: Data rate boundaries

Performing a Site Survey: Performing the Survey (continued)

- **Collecting Non-RF Information:**
  - Sources of interference can include:
    - Wire mesh security windows, Aquariums, Outer walls, Ceramic or marble floors, Concrete floors or pillars, Security booth bullet-proof glass, Mirrors, and Elevator shafts or filing cabinets
  - Electrical and network connections
- **Outdoor Surveys:** Similar to indoor surveys, but must consider climatic conditions, trees, different possibilities for antenna positions

Performing a Site Survey: Performing the Survey (continued)

- **Outdoor Surveys (continued):**
  - Different tools may be required
    - GPS
    - Range finder
    - Tape measure
    - Lighting beacons, flares, and spotlights
- **Finalizing the Survey Documents:** Final result is map of optimal areas of coverage for placement of access point
  - If results unacceptable, must relocate AP and start over

Performing a Site Survey: Creating the Site Survey Report

- **Narrative section:**
  - State customer requirements
  - Outline methodology
    - Outline all steps taken during survey
  - Clearly state results of measurements
    - May have tables of measurements
  - Recommendations
    - Should always address security

Performing a Site Survey: Creating the Site Survey Report (continued)

↓ Y	X →	−181 – −144ft	−144 – −107ft	−107 – −70ft	−70 – −33ft	−33 – 4ft	4 – 41ft	41 – 78ft	78 – 115ft	115 – 152ft	152 – 189ft
210 – 173ft	Data Points	0	25	92	127	145	42	64	50	68	29
	Signal to Noise Ratio	0.0 σ=0.00	17.7 σ=1.95	28.6 σ=10.05	38.4 σ=1.84	23.0 σ=8.28	21.9 σ=4.78	20.6 σ=3.71	25.6 σ=3.29	20.6 σ=5.30	15.4 σ=1.30
173 – 136ft	Data Points	0	24	85	74	81	45	37	47	42	21
	Signal to Noise Ratio	0.0 σ=0.00	37.0 σ=12.25	43.7 σ=5.15	42.2 σ=2.12	29.0 σ=7.51	25.3 σ=4.41	24.8 σ=1.66	33.6 σ=3.41	25.6 σ=4.27	20.3 σ=1.39
136 – 99ft	Data Points	0	56	101	58	93	58	48	48	26	48
	Signal to Noise Ratio	0.0 σ=0.00	43.4 σ=1.97	41.8 σ=10.70	41.5 σ=5.30	31.2 σ=6.87	30.6 σ=4.17	28.4 σ=3.49	32.7 σ=6.23	24.9 σ=4.54	20.2 σ=2.43

Figure 7-13: Table of measurements

Performing a Site Survey: Creating the Site Survey Report (continued)

- **Graphic section:**
  - Generally includes maps and diagrams of coverage area
    - Data rate coverage map
    - Signal-to-noise ratio plot

Performing a Site Survey: Creating the Site Survey Report (continued)

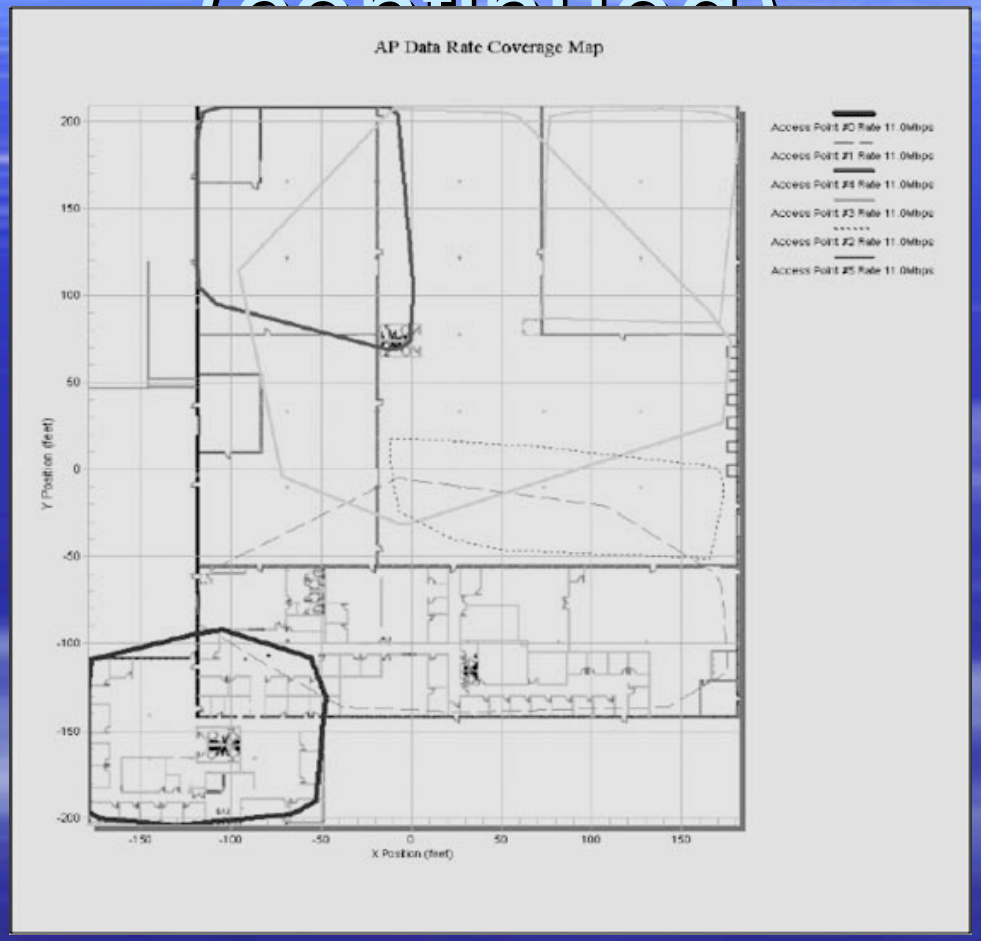


Figure 7-14: Data rate coverage map

Performing a Site Survey: Creating the Site Survey Report (continued)

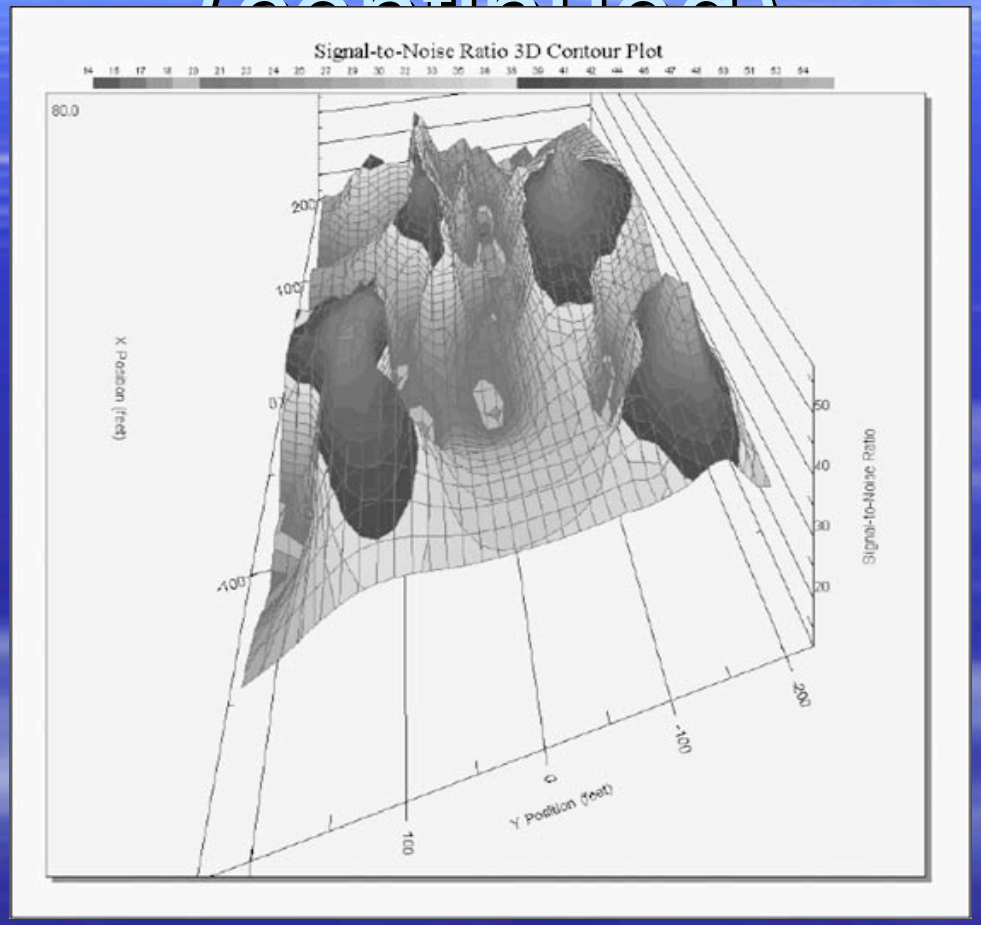


Figure 7-15: 3-D signal-to-noise ratio plot