Chapter 1

Network Administration

A branch of engineering that concern the operational management of human-computer systems. Its address both technology of computer systems and the user of technology. Putting together a network of computer (Workstation, PCs and Super Computer).

Note// Network administrators have to take care of network maintenance.

- In the **Unix community**, Network administration mean the management of network infrastructure devices (routers and Switches).

System Administration

System administrators work for users and can use the system to produce their work.

Note// System administrators focus on operating systems, software platforms, and servers.

- **System administrators jobs** concerned about hardware, software, user support, diagnosis repair and prevention. Need to know different skills, i.e: technical, administrative and socio-psychological.
- **System administration term** is used traditionally by **Unix engineers** to describe the **management of computers whether they are coupled by network or not.**
- In the **Community of PCs**, system administration mean the management of PCs in a network.

Applying Technology in an Environment

Task of Network & System Administration is to build hardware configuration and software system configuration.

1. **Hardware requires -** power, a temperature climate, and conformance to basic standards in order to work systematically.
2. **Software requires -** hardware, basic OS infrastructure and conformance to certain standards but not limit by physical concern as long it has hardware to run.

   Modern software need to inter-operate and survive the possible hostilities and incompatible or in hospitable competitors

Ethical Issues

- A Policy for use and management of computer and their users.
- To protect the right of individual.
- To make user lives bearable and to empower users in the production of real work.

Is System Administration a discipline?

- There are academics and software engineers working on system administration.
- System administration requires both theoretical and practical skills.
- SA is a career in engineering.
- Appreciable market exists for consulting services in security and automation of system administrative tasks.

The challenges of system administration

1. Designing a network which is logical and efficient.
2. Deploy large number of machines which can be easily upgraded later.
3. Deciding what services are needed.
4. Planning and implementing adequate security.
5. Providing comfortable environment for user.
6. Developing ways of fixing errors and problem which occur.
7. System administrator also responsible for both hardware of the network and the computers which it connects.
8. Also understanding of how data flow from machine to machine and how machine affect each others.

The Meta Principle of System Administration

1. **Policy is foundation –** System administration begins with a policy – a decision about what we want and what should be, in relation to what we can afford.
2. **Predictability –** The highest priority of system administration is to work towards a predictable system. It is the basis of reliability, trust and security.
3. **Scalability** – Scalable systems are those that grow in accordance with policy. eg: they continue to function predictably, even as they increase in size.

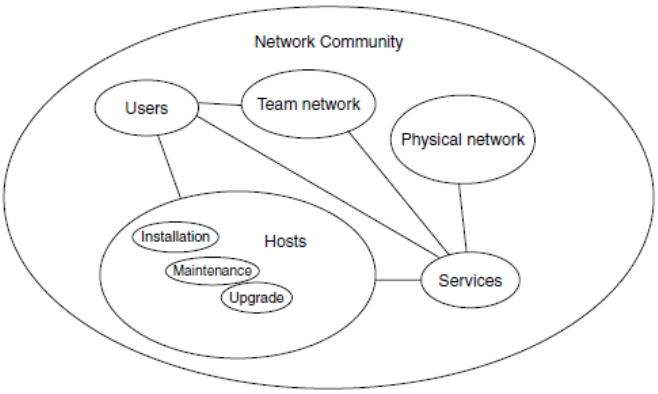
Three main components of Human Computer System

1. **Human**: who use and run the fixed infrastructure
2. **Host computers**: computer device that runs software either in fixed or mobile location.
3. **Network hardware**: cover a variety of specialized device including the key component :
   - Dedicated computing device that directs traffic around the internet. Routers talk at the IP address level or layer 3 .
   - **Switches:** fixed hardware devices that direct traffic around local area network. Switches talk at the level ethernet or layer 2 protocols.
   - **Cables :** There are many type of cable that interconnect device: fiber optic, twisted pair, null modem cables, and etc

Network Infrastructure

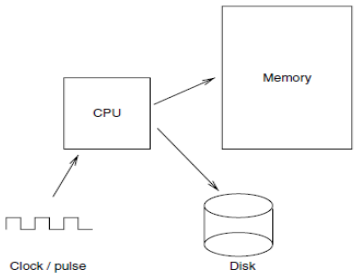
some of key dependencies in system administration

- **Physical network**: The network devices
- **Services**: Applications
- **Hosts**: PCs, Servers
- **Users**: who use the computer
- **Team network**: دبر نفسك



رسمة وتعاريف غبية ماتدري ماهو تبغا

Computers



The basic elements of the von Neumann architecture

Operating System

- **Multi user**
  - Allow multiple user to share resources of single host.
- **The legacy of insecure operating systems**
  - Mostly home computer operating system did not address security issue.
- **Securable operating systems**
  - To restrict access to the system , it required a notion of ownership and permission.
  - To distinguish them from insecure OS, we shall refer to OS like **Unix** and **NT** as securable OS.
  - Main reason why DOS and Windows 9X and Macintosh are so susceptible to virus attack – user can change the OS files.
- **Shell or command interpreters**
  - Shells can be used to write simple programs called scripts or batch files which often simply repetitive administrative task.
- **Log & audits**

  Note// is the process of documenting activity within the software systems used across your organization.
  - OS kernels share resources and offer services,
  - Can keep list of transactions which have taken place so that one can later go back and see we exactly happened at given time.
  - Auditing became issue again in connection with security. Organization become afraid of break – ins from system cracker and want to able to trace activities of the system in order be able to look back and find out the identity of cracker. Some organization , auditing are important. – one use for auditing is so called non repudiation or non –denial (a security feature which encourage users to be responsible for their actions).
- **File systems**
  - File and file systems are at the very heart of what system administration about.
  - Every task in host administration or network configuration involves making changes to files.
  - Need to acquire a basic understand of the principles of systems.
  - For instance, fact that old file systems were only 32 bit addressable and therefore supported a maximum partition size of 2GB or 4GB
  - Newer file systems are 64bit addressable and therefore have essentially no storage limits.
  - Unix use an index node system of block addressing, Dos use tabular lookup system.
- **Unix**
  - Has a hierarchical file system – make use directories and subdirectories to form a tree.
  - All file systems based on index nodes or inodes
  - Every file has index entry stored in a special part of the file systems.
  - Inode contain extensible system of pointers to the actual disk block- associated with the file
  - Inode also contains essential information needed to located a file on the disk.
  - Start of the Unix file tree is call root filesystems or '/'.

Chapter 2

Operating System

The operating system is the software layer between the applications and the hardware.

Network Configuration

1. **Dynamic Configuration**
   In a **dynamic configuration**, the machine asks the network what its configuration parameters should be.
   Note// it talks to a service on the network, which responds with those parameters.
   DHCP
2. **Hardcoded Configuration**
   In a **hardcoded or static configuration**, the configuration parameters are stored on the machine itself.
   Static
3. **Hybrid Configuration**
   Servers can also have a **hybrid configuration**, where the network parameters are defined in local files, but the server periodically checks the network parameters via DHCP.
   DHCP & Static

The diagram depicts five states: new, clean, configured, unknown, and off:

- **New:** A completely new, unconfigured, machine
- **Clean:** A machine on which the OS has been installed but no localizations performed
- **Configured:** A correctly configured and operational environment
- **Unknown:** A computer that has been misconfigured or has become outdated
- **Off:** A machine that has been retired and powered off

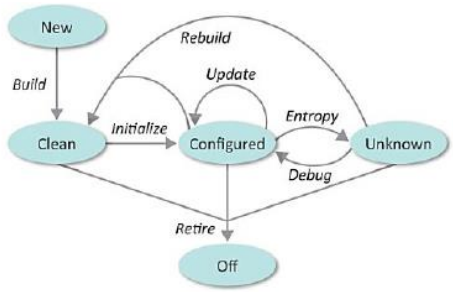


Figure 7.1: Evard's life cycle of a machine and its OS

Configuration Management Systems

CM systems are specialized programming languages that permit you to describe the details of what a properly configured system should look like, called the **desired state** of the machine.
Note// you can use these systems to configure a newly installed machine, or run them periodically.

DHCP Configuration

The new configuration (IP, gateway IP, DNS IP) will be distributed to all clients in the network.
Note// This is often more useful for workstations than servers.

Automation

All modern OS vendors provide a mechanism to automate OS installation.

- Microsoft Windows has Microsoft Deployment Toolkit (MDT) and other options.
- RedHat Linux has KickStart, Debian has Debconf, and so on.
- Solaris has JumpStart.
- There are also third-party products like KACE and Fully Automatic Installation (FAI).

Cloning

One machine is installed and configured as desired, and a snapshot of that machine's disk is saved somewhere. Subsequently, any new machine is installed by copying that image to its hard disk.
Note// The original machine is known as the golden host and the snapshot is called the golden image.

golden image.

A small industry is devoted to helping companies with this process and providing specialized cloning hardware and software. An early product was called Ghost. Clonezilla and FOG (Free and Open Ghost) are now popular open source alternatives.

Disadvantages of Cloning

if the hardware of the new machine is significantly different from that of the old machine, you have to make a separate master image. Another problem occurs when a new release of the operating system arrives. It is likely to be difficult to reproduce the same changes in the new operating system.

Chapter 3

Workstations Versus Servers

- Servers have higher **uptime requirements** than workstations.
- Servers have higher **data integrity requirements** than workstations.
- Servers have higher **CPU and memory requirements** than workstations.
- Server **hardware** is different from workstation hardware.
- Server **operating systems** are different from workstation operating systems.

Server Hardware Design Differences

Server hardware is designed with different priorities than workstation hardware. Workstations are designed for an individual user to sit in front of, and interact with directly.

- More CPU performance
- High-performance I/O
- Expandability
- Upgrade options
- Rack mountable
- Front and rear access
- High-availability options
- Remote management

Server OS and Management Differences

Servers use a different OS and their configurations are managed differently. Server hardware runs a server OS. Microsoft Windows Server Edition includes additional software for providing services such as ActiveDirectory.

// Server OSs are often **patched** on a different schedule. While workstations are **updated** frequently.
// It also is tuned for server operation instead of interactive performance

Server Reliability

Because servers need to be more reliable, and have higher uptime than workstations, one of the ways we prepare for equipment failure is to buy server hardware with additional features for reliability and data integrity.

1. **Levels of Redundancy**
   Servers often have internal redundancy such that one part can fail and the system keeps running. For example, there may be two power supplies in the system. Either can fail and the system keeps running.
2. **Data Integrity**
   Hard disks and SSDs eventually wear out and die. In turn, we must have a plan to deal with this eventuality. Not having a plan is as irrational as assuming our storage systems will last forever.
3. **Hot-Swap Components**
   Hot-swap refers to the ability to add, remove, and replace a component while the system is running.
   // Server has many redundant components, and these components should be hot-swappable.
4. **Servers Should Be in Computer Rooms**
   Servers should be installed in an environment with proper power, fire protection, networking, temperature and humidity control, and physical security. That means a computer room or DataCenter.
   // Cooling is required to remove the heat they generate.

Separate Administrative Networks

This separation of the network should be engineered to use separate equipment so that it will not be affected by outages in the main network.

// It is common for servers to have a separate NIC that is connected to a dedicated administrative network. the administrative network is often more stable and static, while the service network is more dynamic. For example, the service NIC of a server might reconfigure itself frequently as part of a load-balancing and failover mechanism. The administrative network often has more restrictive firewall policies than the service network, since it has more critical systems.

Server Hardware Details

1. **CPUs**
   the choice of a few high-speed cores versus many slow cores. Depending on the architecture of the software that will run on the machine, this decision can determine whether your service is fast and efficient or underutilizes the capacity of the machine.
   // Instead of a CPU that is twice as fast, you can get a single CPU with two CPU cores, each able to run a program or execution thread in parallel.

2. **Memory**
   Random access memory (RAM) is where running programs and their data are stored. A server needs to have enough RAM to support the applications that are running.
3. **Caches**
   A cache stores frequently used or soon-to-be used data close to the CPU for faster access.
4. **Network Interfaces**
   Servers often have multiple network interface cards (NICs) because they are connected to different networks.
5. **Disks: Hardware Versus Software RAID**
   RAID can be achieved through hardware or software.
   - **Software RAID**
     Software RAID is part of the operating system. This setup provides RAID via device drivers.

   // Disks, particularly those with moving parts (HDD), are the most failure-prone components in most systems.

6. **Power Supplies**
   The second-most failure-prone component in a server is the power supply. It is very common to have N + 1 redundant power supplies so that if one fails, the system can keep running.
   // Generally, a second power supply is enough to provide N + 1 redundancy
   // Each power supply should draw power from a different source: a separate circuit or uninterruptible power supply (UPS).
   // Generally each power distribution unit (PDU) in a datacenter is its own circuit, so plugging each power cord into a different PDU assures two power sources.

Chapter 4

// A site's network is the foundation of its infrastructure.
// A poorly built network affects all other components of the system. A network cannot be considered in isolation.

Physical Versus Logical

A network can be depicted in two different ways: as the physical network and as the logical network.

- The **physical network** consists of the **physical wires** and **devices** that make up the network.
- The **logical network** describes the **software-based partitions**, **segments**, and **connections** that we overlay on the physical network.

The OSI Model

Table 23.1: The OSI Network Model

Layer	Name	Description
1	Physical	The physical connection between devices: copper, fiber, radio, laser
2	Data link	Interface (or MAC) addressing, flow control, low-level error notification
3	Network	Logical addressing (e.g., IP addresses) and routing (e.g., RIP, OSPF, IGRP)
4	Transport	Data transport, error checking and recovery, virtual circuits (e.g., TCP sessions)
5	Session	Communication-session management (e.g., AppleTalk name binding, or PPTP)
6	Presentation	Data formats, character encoding, compression, encryption (e.g., ASCII, Unicode, HTML, MP3, MPEG)
7	Application	Application protocols (e.g., SMTP for email, HTTP for web, and FTP for file transfer)

// Open Systems Interconnection (OSI) model for networks has gained widespread acceptance

Logical Design

The office network is divided into individual network segments. One of the factors to consider when deciding on the size of the office subnets is the amount of broadcast traffic there will be on the network. This is a combination of the number of devices and the amount of broadcast traffic generated by the device OS and applications it runs.
// A stronger limit on the number of hosts per VLAN is **uplink capacity**. VLAN and the other VLANs. If 100 hosts are on a VLAN and all generate 10 Mbps of traffic destined to other VLANs, then the uplink must be at least 1000 Mbps.
// On top of the physical infrastructure is the logical design.

- One big subnet
- Floor plan–centric
- Security level
- Change control level
- Device function

Network Access Control (NAC)

determines whether a device that connects to your network is permitted to join, and which VLAN it should be in.
// NAC is relatively **rare** today but should be a requirement for corporate networks.
// Without NAC, anyone can find a free jack and plug right into the corporate network.

- **MAC based**
  involves checking the MAC address of the machine against a database of authorized MACs.
  // It is the **weakest** form of NAC
- **Authentication based**
  involves the end user supplying credentials to connect to the network.
  // These may be a simple username and password or two-factor authentication
- **Certificate based**
  involves a one-time verification that the person is who he claims to be
  // and then installs a certificate on the person's machine.

Location for Emergency Services

Another consideration for your logical network design is how you will pass location information to emergency services. If someone dials emergency services from the soft phone on his or her workstation to report a life-threatening situation.

Wireless Office Networks

Wireless networks (WiFi) have gone from being an expensive niche technology to the primary way for most people to access a network.

1. **Physical Infrastructure**
   important aspects of wireless network are that it has good coverage and sufficient bandwidth.
2. **Logical Design**
   As with wired networks, you should have some network access control. NAC will put devices into different VLANs, based on the type of device and device authentication.

Datacenter Networks

The datacenter has a higher density of machines and higher bandwidth demands. Rather than jacks connected to IDFs, we have racks of equipment.
A datacenter network design can be separated into physical and logical aspects. **physical design** covers the network devices and the cable plant. **logical design** describes the subnet strategy for datacenter.
// The LAN in your datacenter has different requirements than the LAN in your office.

- **Physical Infrastructure**
  There are a number of different strategies for wiring a datacenter. The three most popular are having a central switch, individual switches in each rack, and datacenter fabric systems.
- **Logical Design**
  Servers and services within a datacenter should never rely on any machines outside the datacenter.

WAN Strategies

Offices and datacenters are connected via long-distance network technologies. This interconnection between locations is called a wide area network (WAN). There are two primary aspects to this strategy: **topology** and **technology**. The **topology** is the network diagram. The **technology** is the equipment and protocols used to make those connections.

Routing

Routing is a fundamental component of a network. One of the primary ways to do so is to develop an IP addressing scheme that is easy to understand and supports you in simplifying routing and enabling route summarization.

- **Static Routing**
  Static routing takes advantage of the fact that a router always knows how to talk directly to a subnet that is directly connected to it.
- **Interior Routing Protocol**
  routing protocol, such as OSPF and EIGRP, that enables each router to communicate with its neighboring routers to advertise which subnets are connected to it.
- **Exterior Gateway Protocol**
  This routing protocol communicates between autonomous systems.

Software-Defined Networks (SDN)

An SDN makes routing as programmable as any other application. It enables applications to specify their needs to a network controller. The network controller has an overview of the network. It can dynamically configure the network devices to create a specific path through the network for that application's traffic.

// SDN takes a different approach than traditional routing to control the flow of traffic between devices on the network.
// SDN enables network administrators to make the best use of their network
// SDN enables network administrators to specify how particular types of network traffic flows should

Monitoring

Network operations starts with monitoring. Monitoring provides visibility that facilitates all other operational tasks.

items that should be monitored for a network:

- Network devices (routers and switches, not endpoints such as PCs):
  - Health (up/down status)
  - Internal components (blades, slaves, extensions)
  - Resource utilization (memory, CPU, and so on)
- For each WAN link, LAN trunk plus the individual links that make up a bonded set:
  - Health (up/down status)
  - Utilization (how much capacity is in use)
  - Error counts

Management

Management means controlling device configuration and firmware versions. Network management tools have lagged behind the corresponding tools that are readily available for managing workstations and servers.

Documentation

Network documentation has two main purposes. The first is to assist people in troubleshooting problems. The second is to explain what the network looks like

There are four main types of documentation. The first is **network design and implementation**, **DNS**, the **CMDB**, and **labels**.

1. **Network Design and Implementation**
   This form of documentation is used to bring new team members up to speed.
   // Network design and implementation consists of logical and physical network diagrams

2. **DNS**
   Make sure that every interface of every device has matching forward and reverse DNS entries
3. **CMDB**
   Another essential piece of documentation for troubleshooting and resolving incidents is an accurate inventory system, or CMDB, which tells you the make, model, serial number, and optional components of the device that is causing problems
4. **Labeling**
   Physical devices should be labeled on their front and back with their name and asset ID.

Support

A helpdesk that responds to alerts and end-user queries and problems, performs triage, and spends a limited amount of time on each issue is level 1 (L1) support. Specialists who take on longer-running or more challenging problems in their area of expertise are level 2 (L2) support. And subject matter experts (SMEs) who usually work on projects, but are also the final point of escalation within the company, are level 3 (L3) support

Chapter 5

Three Stages of a Maintenance Window

Table 20.1 Three Stages of a Maintenance Window

Stage	Activity
Preparation	• Schedule the window. • Pick a flight director. • Prepare change proposals. • Build a master plan.
Execution	• Disable access. • Determine shut-down sequence. • Execute plan. • Perform testing.
Resolution	• Announce completion. • Enable access. • Have a visible presence. • Be prepared for problems.

Maintenance Window

Is a short period in which a lot of systems work must be performed, is disruptive to the rest of the company, and so the scheduling must be done in cooperation with the customers.

1. **Scheduling**
   In scheduling periodic maintenance windows, you must work with the rest of the company to coordinate dates.
2. **Planning**
   As with all planned maintenance on important systems, the tasks need to be planned by the individuals performing them
3. **Directing**
   deciding on any cuts for that maintenance window, monitoring the progress of the tasks during the maintenance window
4. **Managing Change Proposals**
   A good way of managing this process is to have all the change proposals online in a revision-controlled area.
   // What changes are going to be made? • What machines will you be working on? • What will be affected by the change? • Who is performing the work? • etc.
5. **Developing the Master Plan**
   A master plan chart shows all the tasks that are being performed over the entire time, who is performing them, the team lead, and what the dependencies are.
6. **Disabling Access**
   The very first task in the maintenance window is to disable or discourage system access and provide reminders that it is a maintenance window.
   - Placing on all doors into the campus buildings notices with the maintenance window times clearly visible
   - Disabling all remote access to site, whether by VPN, dial-in, dedicated lines, or wireless
   - Making an announcement over the public address system in the campus buildings to remind everyone that systems are about to go down
   - Changing the helpdesk voicemail message to announce that this is a maintenance window and stating when normal service should be restored
7. **Ensuring Mechanics and Coordination**
   Some key pieces of technology enable the maintenance window process described here to proceed smoothly.
   1. **Shutdown/Boot Sequence**
      In most sites, some systems or sets of systems must be available for other systems to shut down or to boot cleanly.

Table 34.2: Template for a Boot Sequence

Stage	Function	Reason
1	Console server	So that SAs can monitor other servers during boot.
2	Master authentication server	Secondary authentication servers contact the master on boot.
	Master name server	Secondary name servers contact the master on boot.
3	Secondary authentication server	So that SAs can log in to other servers as they boot. Unix hosts contact NIS servers when they boot. Rely on nothing but the master authentication server.
	Secondary and caching name servers	Almost all services rely on name service. Rely on nothing but the master name server.
4	Data servers	Applications and home directories are here. Most other machines rely on data servers. Rely on name service.
	Network config servers	Rely on name service.
	Log servers	Rely on name service.
	Directory servers	Rely on name service.
5	Print servers	Rely on name service and log servers.
	License servers	Rely on name service, data servers, and log servers.
	Firewalls	Rely on log servers.
	Remote access	Relies on authentication, name service, and logging.
	Email service	Relies on name, log, and directory services and data servers.
6	All other servers	Rely on servers previously booted and not each other.
7	Desktops	Rely on servers.

KVM and Console Service

Two data center elements that make management easier are KVM switches and serial console servers. Both can be instrumental in making maintenance windows easier to run by making it possible to remotely access the console of a machine.

keyboard, video, and mouse (KVM) switches, **serial console servers**, **lights-out management (LOM)** are tools that make management of datacenter devices easier.

// They can be instrumental in making maintenance windows easier to run by providing remote access to the console or other functions of a machine when it is not fully up and available on the network.

- **KVM switch**
  permits multiple computers to all share the same keyboard, video display, and mouse.
  // A KVM switch saves space in a datacenter
  // sophisticated console access systems can be accessed from anywhere in the network.
- **Serial Console Server**
  connects devices with serial consoles—systems without video output, such as network routers, switches, and many Unix servers
- **LOM**
  provides a management interface that allows an SA to remotely power-cycle the machine, in addition to providing KVM over IP and serial console access.

Deadlines for Change Completion

A critical role of the flight director is tracking how the various tasks are progressing and deciding when a particular change should be aborted and the back-out plan for that change executed.

Comprehensive System Testing

The final stage of a maintenance window is comprehensive system testing. If the window has been short, you may need to test only the few components that you worked on.

// tests could include logging in, checking for particular service, or trying to run particular application

Post-maintenance Communication

Once the maintenance work and system testing have been completed, the flight director sends out a message to the company, informing everyone that service should now be fully restored.

Re-enable Remote Access

The final act before leaving the building should be to reenable remote access and restore the voicemail on the helpdesk phone to normal.

Be Visible the Next Morning

It is very important for the entire SA group to be in early and to be visible to the company the morning after a maintenance window.

Postmortem

By about lunchtime of the day after the maintenance window, most of the remaining problems should have been found. SAs should sit down and talk about what went wrong, why, and what can be done differently. That should all be noted and discussed with the whole group later in the week.

// Over time, with postmortem process, the maintenance windows will become smoother and easier.

Communication

For maintenance windows that extend beyond a single campus, the best way to communicate is typically to have one or more conference bridges that remain open during the entire maintenance window.

Table 34.3: Comparison of Radio Technologies

Type	Requirements	Advantages	Disadvantages
Line-of-sight	Frequency license Transmits through walls	Simple	Limited range Blocked by obstacles
Repeater	Frequency license Radio operator license	Better range Overcomes obstacles	More complex Skill qualifications
Cellular	Service availability	Simple Wide range Unaffected by terrain Less to carry	Higher cost Available only in cellphone providers' coverage area Company contracts may limit options Multiple channels may not be available

Chapter 6

Monitoring

Monitoring is the primary way we gain visibility into the systems we run. It is the process of observing information about the state of things for use in decision making.

Types of Monitoring

1. **Historical monitoring**
   is used for recording long-term uptime, usage, and performance statistics. It has **two components**: collecting the data and viewing the data.
   - **Gathering the Data**
     How you intend to use the data that you gather from the historical monitoring will help to determine which level of detail you need to keep and for how long.
   - **Storing the Data**
     Historical data can consume a lot of disk space. This potential problem can be mitigated by data summarization or expiration.
     - **Summarization** means reducing the granularity of data.
     - **Expiring data** simply means deleting older data.
   - **Viewing the Data**
     The output that you generally want from this type of monitoring system is **graphs** that have clear units along each axis.
2. **Real-time monitoring**
   alerts the SA team of a failure as soon as it happens. It has **two components**: monitoring component that notices failures, alerting component that alerts someone to the failure.
   // A real-time monitoring system tells you when a host is down, a service is not responding, or some other problem has arisen.
   // A real-time monitoring system should be able to monitor everything you can think of that can indicate a problem.

Building a Monitoring System

- Typically, historical and real-time monitoring are performed by **different systems**.
- Monitoring uses network bandwidth, so make sure that it doesn't use too much.
- Monitoring also uses CPU and memory resources, and you don't want your monitoring to make your service perform poorly.
- Security is important for monitoring systems because they have more access to other systems.
- Greater access can be leveraged by an attacker to compromise other systems or to initiate a denial-of-service attack.
- Strong authentication between the server and the client is best.
- Older monitoring protocols, such as SNMPv1,have weak authentication.