4. Designing Network Systems

Computers and information networks are critical to the success of businesses, both large and small. They connect people, support applications and services, and provide access to the resources that keep the businesses running. To meet the daily requirements of businesses, networks themselves are becoming quite complex.

4.1. Bandwidth

In computer networks, bandwidth is often used as a synonym for data transfer rate - the amount of data that can be carried from one point to another in a given time period (usually a second). Bandwidth is usually expressed in bits (of data) per second (bps).

Since bandwidth is measured as the amount of bits transmitted over a time interval, it means that over time, bandwidth available on any link approaches infinity. Unfortunately, for any given period of time, the bandwidth provided by any given network connection is not infinite. You can always download (or upload) as much traffic as you like; you need only wait long enough.

Of course, human users are not as patient as computers, and are not willing to wait an infinite amount of time for their information to traverse the network. For this reason, bandwidth must be managed and prioritised much like any other limited resource. You will significantly improve response time and maximise available throughput by eliminating unwanted and redundant traffic from your network.

Importance of Bandwidth

- Bandwidth is limited by physics and technology
- Bandwidth is not free
- Bandwidth requirements are growing at a rapid rate
- Bandwidth is critical to network performance

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	kbps	1 kbps = ~1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = ~1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps = ~1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = ~1,000,000,000,000 bps = 10^{12} bps

Table 4.1.1 Bandwidth Measurements

4.2. Users

Users are the people who engaged with the network system. They will use the all authorized functionalities that the administrator has given.

Users have certain quality expectations towards the network/system.

4.3. Network Requirements

Today, the Internet-based economy often demands around-the-clock customer service. This means that business networks must be available nearly 100 percent of the time. They must be smart enough to automatically protect against unexpected security incidents. These business networks must also be able to adjust to changing traffic loads to maintain consistent application response times. It is no longer practical to construct networks by connecting many standalone components without careful planning and design.

- Most businesses actually have only a few requirements for their network:
- The network should stay up all the time, even in the event of failed links, equipment failure, and overloaded conditions.
- The network should reliably deliver applications and provide reasonable response times from any host to any host.
- The network should be secure. It should protect the data that is transmitted over it and data stored on the devices that connect to it.
- The network should be easy to modify to adapt to network growth and general business changes.
- Because failures occasionally occur, troubleshooting should be easy time consuming.

4.4. Building a Good Network

Good networks do not happen by accident. They are the result of hard work by network designers and technicians, who identify network requirements and select the best solutions to meet the needs of a business. The steps required to design a good network are as follows.

- Step 1. Verify the business goals and technical requirements.
- Step 2. Determine the features 7 functions required to meet the needs identified in Step 1.
- Step 3. Perform a network-readiness assessment.
- Step 4. Create a solution and site acceptance test plan.
- Step 5. Create a project plan.

After the network requirements have been identified, the steps to designing a good network are followed as the project implementation moves forward. Network users generally do not think in terms of the complexity of the underlying network. They think of the network as a way to access the applications they need, when they need them.

Fundamental Design Goals

When examined carefully, these requirements translate into four fundamental network design goals:

- Scalability: Scalable network designs can grow to include new user groups and remote sites and can support new applications without impacting the level of service delivered to existing users.
- Availability: A network designed for availability is one that delivers consistent, reliable performance, 24 hours a day, 7 days a week. In addition, the failure of a single link or piece of equipment should not significantly impact network performance.
- Security: Security is a feature that must be designed into the network, not added on after the network is complete. Planning the location of security devices, filters, and firewall features is critical to safeguarding network resources.
- Manageability: No matter how good the initial network design is, the available network staff must be able to manage and support the network. A network that is too complex or difficult to maintain cannot function effectively and efficiently.

Network Design Methodologies

Large network design projects are normally divided into three distinct steps:

1. Step 1. Identify the network requirements.
2. Step 2. Characterise the existing network.
3. Step 3. Design the network topology and solutions

Step 1. Identify the network requirements.

The network designer works closely with the customer to document the goals of the project. Goals are usually separated into two categories:

- Business goals: Focus on how the network can make the business more successful
- Technical requirements: Focus on how the technology is implemented within the network.

Step 2.Characterise the existing network.

Information about the current network and services is gathered and analysed. It is necessary to compare the functionality of the existing network with the defined goals of the new project. The designer determines whether any existing equipment, infrastructure, and protocols can be reused, and what new equipment and protocols are needed to complete the design.

Step 3. Design the network topology and solutions

A common strategy for network design is to take a top-down approach. In this approach, the network applications and service requirements are identified, and then the network is designed to support them. When the design is complete, a prototype or proof-of-concept test is performed. This approach ensures that the new design functions as expected before it is implemented.

Impacting the Entire Network

Network requirements that impact the entire network include the following:

- Adding new network applications and making major changes to existing applications, such as database or Domain Name System (DNS) structure changes
- Improving the efficiency of network addressing or routing protocol changes
- Integrating new security measures
- Adding new network services, such as voice traffic, content networking, and storage networking
- Relocating servers to a datacentre server farm

Impacting a Portion of the Network Requirements that may only affect a portion of the network include the following:

- Improving Internet connectivity and adding bandwidth
- Updating access layer LAN cabling
- Providing redundancy for key services
- Supporting wireless access in defined areas
- Upgrading WAN bandwidth

4.5. Network Services and Applications

Network services help the operating system and applications communicate with each other.

DHCP

Dynamic Host Configuration Protocol (DHCP) is used in LAN environments to dynamically assign host IP addresses from a centralised server, which reduces the overhead of administrating IP addresses. DHCP also helps conserve limited IP address space because IP addresses no longer need to be permanently assigned to client devices. Only those client devices that are connected to the network require IP addresses. The DHCP relay agent information feature (option 82) enables the DHCP relay to include information about itself and the attached client when forwarding DHCP requests from a DHCP client to a DHCP server. This basically extends the standard DHCP process by tagging the request with the information regarding the location of the requestor.

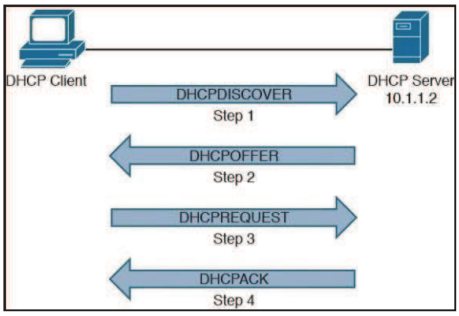


FIGURE 4.5.1.1 DHCP FUNCTIONS

When a DHCP client is first switched on, it sends a broadcast packet on the network with a DHCP request. This is picked up by a DHCP server, which allocates an IP address to the PC, from one of the scopes (the pools of addresses) it has available.

Each DHCP scope is used for a different TCP/IP network segment. On networks with routers that support DHCP, extra information is added to the request by the router to tell the server which

network the request came from. The DHCP server uses this information to pick an address from the correct scope. The server replises to the client, allocating it the TCP/IP address and settings required.

DHCP doesn't allocate the address permanently. It tells the client that it has "leased" the address to it for a specific time period, which you as administrator can control. When the lease expires, the client can ask the server to renew the lease. If the DHCP server doesn't hear from the client beyond the expiry of the lease period, it will put that address back in the pool ready to be re-used.

When the DHCP client obtains a lease on an address, it knows how long the lease period is. So it knows that it can use the address without reference to the DHCP server until the lease expires.

When it does expire, it can request a renewal. The implication of this is that changing DHCP settings on the server won't instantly change all your DHCP client PCs, as they won't find out about the changes until they ask the server to renew their lease. This is one factor you need to consider when you decide your lease period.

4.5.1.1. Static vs. Dynamic IP addressing

Static IP Addresses

Static IP addresses are just that: Static. They rarely change. Just like your name, once a static IP address is assigned a network element, it remains there until a decision is made to change the address for some reason. At this time, the basic IP address structure is a 12-number address configured in this pattern: xxx.xxx.xxx.xxx.

For example, a network element might have a static IP address like 209.134.004.168. Referencing that address on the network would always point to that network element, just like your phone number always refers to your phone. The advantage of a static IP address primarily is the speed at which it can be referenced. Since the number never changes, and always refers to the same network element, it can be immediately accessed with no overhead processing.

Dynamic IP Addresses

DHCP, or Dynamic Host Configuration Protocol. As you can guess from its name, DHCP is dynamic. The IP address of different network elements are assigned to it as they come online by a server. This allows for IP addresses to be managed efficiently by providers with a large user base, because not all of the IP addresses are allocated at one time. A DHCP server allows a dynamic assignment of IP addresses in a system to those network elements that require them at a given time.

DNS

A Domain Name System (DNS) server performs the task of resolving a domain name to an IP address. An end user who wants to navigate to the www.ciscopress.com website enters that fully qualified domain name (FQDN) into the web browser. The end user's computer sends a DNS request to the DNS server asking for the IP address that corresponds to www.ciscopress.com. The DNS server responds with 192.168.1.11, and now the end user's computer can send packets to the destination.

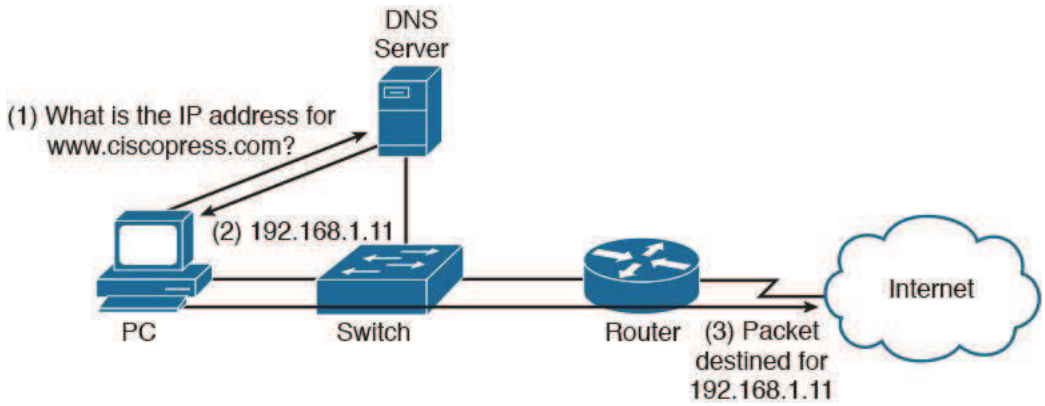


Figure 4.5.2.1 How DNS Works

NAT

Private IPv4 addresses within an organisation's network must be translated to a public IPv4 address before packets can be sent to the public Internet. Network Address Translation (NAT) provides this service.

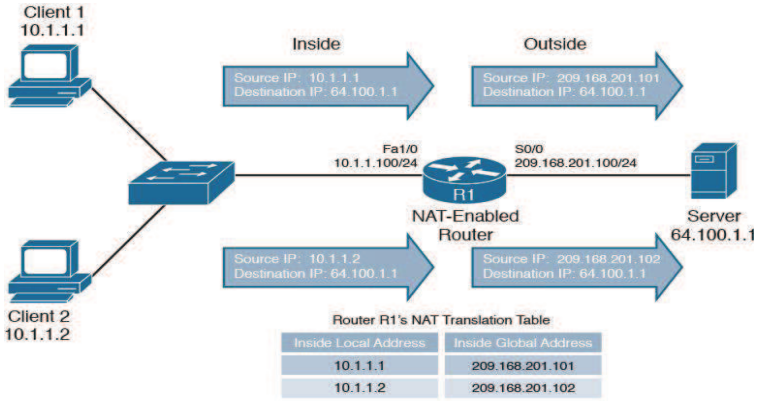


Figure 4.5.2.2 How NAT Works

Implement and Diagnose Networked Systems

4.6. Introduction

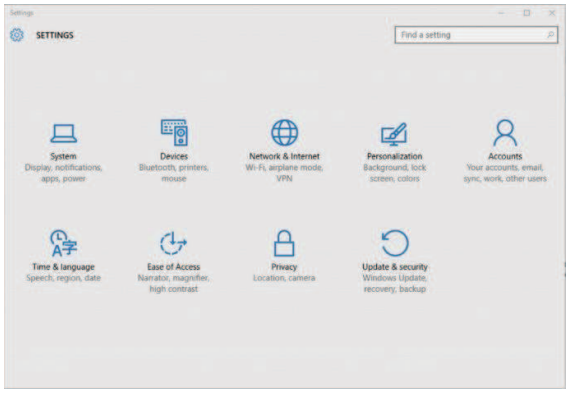
Windows usually detects the presence of a network adapter automatically; typically, you don't have to install device drivers manually for the adapter. When Windows detects a network adapter,

Windows automatically creates a network connection and configures it to support basic networking protocols. You may need to change the configuration of a network connection manually, however.

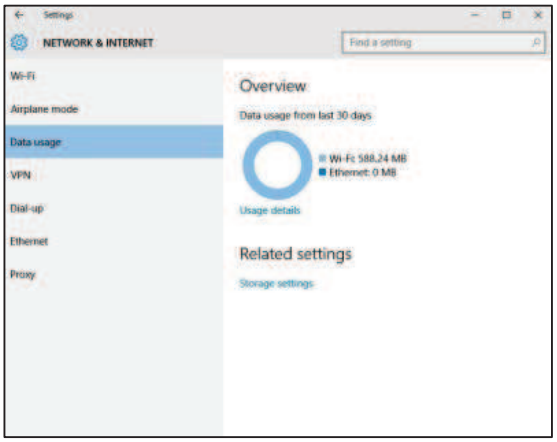
4.7. Installation of Communication Devices

The following steps show how to configure your network adapter on a Windows 10 system.

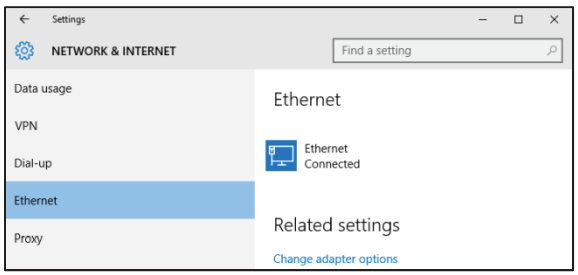
- Click the Start icon (or press the Start button on the keyboard), and then tap or click Settings. The setting page will appear.



- Click Network & Internet. The Network & Internet page appears.



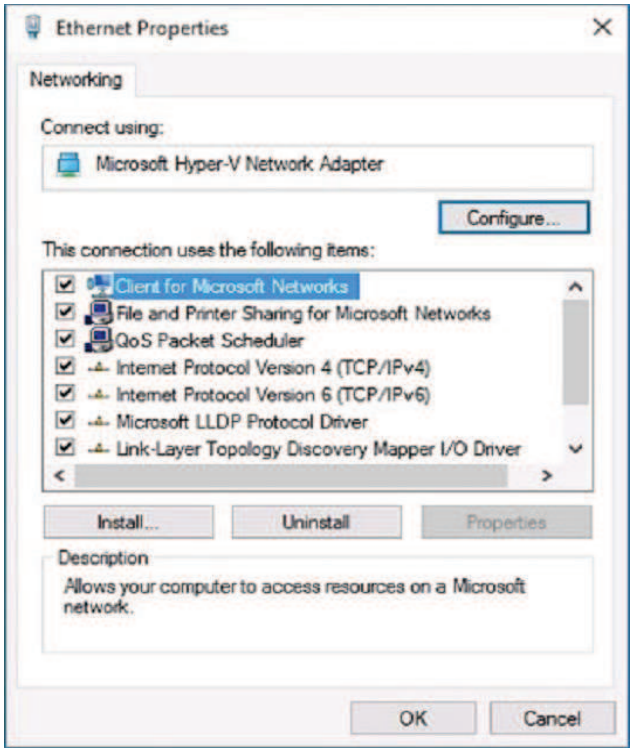
- Click Ethernet. The Ethernet settings page appears.



- Click Change Adapter Options.

The Network Connections page appears. This page lists each of your network adapters. In this case, only a single wired Ethernet adapter is shown. If the device has more than one adapter, additional adapters will appear on this page.

- Right-click the connection that you want to configure and then choose Properties from the contextual menu that appears. This action opens the Ethernet Properties dialog box

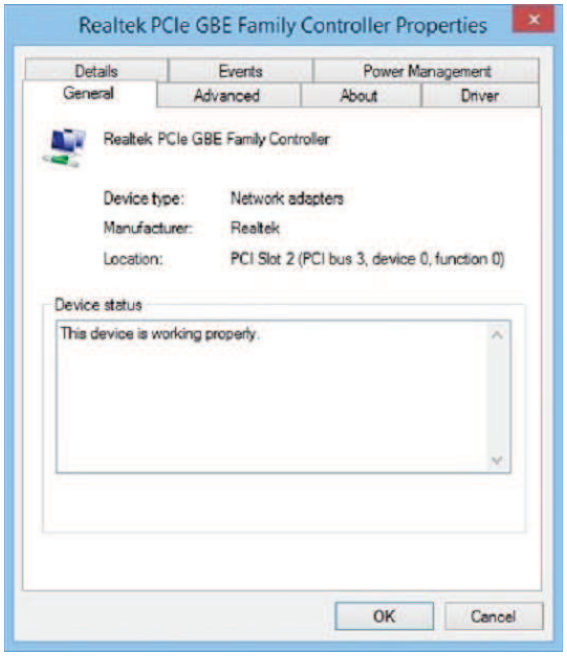


- To configure the network adapter card settings, click Configure. The Properties dialog box for your network adapter appears. This dialog box has seven tabs that let you configure the adapter.

1. General: Shows basic information about the adapter, such as the device type and status.

2. Advanced: Lets you set a variety of device-specific parameters that affect the operation of the adapter.
3. About: Displays information about the device's patent protection.
4. Driver: Displays information about the device driver that's bound to the NIC and lets you update the driver to a newer version, roll back the driver to a previously working version, or uninstall the driver.
5. Details: With this tab, you can inspect various properties of the adapter such as the date and version of the device driver. To view the setting of a particular property, select the property name from the drop-down list.
6. Events: Lists recent events that have been logged for the device.
7. Power Management: Lets you configure power management options for the device.

When you click OK to dismiss the dialog box, the network connection's Properties dialog box closes and you're returned to the Network Connections page. Right-click the network adapter and choose Properties again to continue the procedure.



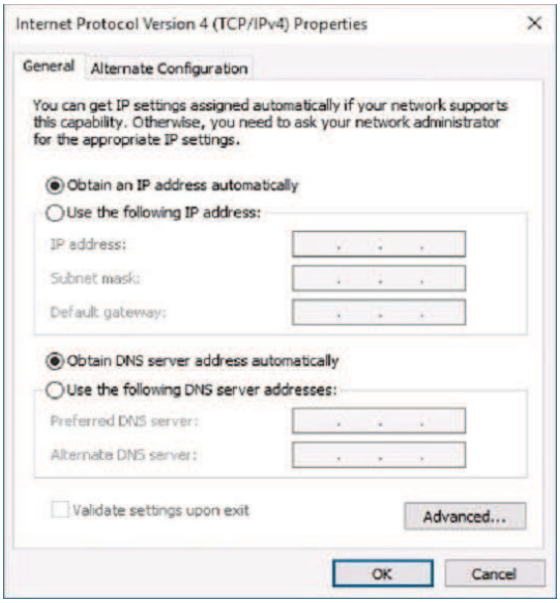
Review the list of connection items listed in the Properties dialog box.

1. Client for Microsoft Networks: This item is required if you want to access a Microsoft Windows network. It should always be present.
2. File and Printer Sharing for Microsoft Networks: This item allows your computer to share its files or printers with other computers on the network. This option is usually used with peer-to-peer networks, but you can use it even if your network has dedicated servers. If you don't plan to share files or printers on the client computer, however, you should disable this item.

3. Internet Protocol Version 4 (TCP/IPv4): This item enables the client computer to communicate by using the version 4 standard TCP/IP protocol.
4. Internet Protocol Version 6 (TCP/IPv6): This item enables version 6 of the standard TCP/IP protocol. Typically, both IP4 and IP6 are enabled, even though most networks rely primarily on IP4.
    - If a protocol that you need isn't listed, click the Install button to add the needed protocol. A dialog box appears, asking whether you want to add a network client, protocol, or service. Click Protocol and then click Add. A list of available protocols appears. Select the one you want to add; then click OK.
    - To remove a network item that you don't need (such as File and Printer Sharing for Microsoft Networks), select the item, and click the Uninstall button.
    - For security reasons, you should make it a point to remove any clients, protocols, or services that you don't need.
    - To configure TCP/IP settings, click Internet Protocol (TCP/IP); click Properties to display the TCP/IP Properties dialog box; adjust the settings; and then click OK.

The TCP/IP Properties dialog box lets you choose among these options:

1. Obtain an IP Address Automatically: Choose this option if your network has a DHCP server that assigns IP addresses automatically. Choosing this option dramatically simplifies administering TCP/IP on your network.
2. Use the Following IP Address: If your computer must have a specific IP address, choose this option and then type the computer's IP address, subnet mask, and default gateway address.
3. Obtain DNS Server Address Automatically: The DHCP server can also provide the address of the Domain Name System (DNS) server that the computer should use. Choose this option if your network has a DHCP server.
4. Use the Following DNS Server Addresses: Choose this option if a DNS server isn't available. Then type the IP addresses of the primary and secondary DNS servers.



4.8. Verification of Configuration and Connectivity

Ping

One of the most popular utilities that is used by network engineers for quick reachability verification is the ping command. At its most simple, the ping command is used to send a group of five Internet Control Message Protocol (ICMP) packets to a destination which in turn will return five packets (should reachability exist). Since a normal routing or switching device typically has many outgoing interfaces, the command can be extended and customised with several different options, including source interface, count, datagram size, timeout, pattern, and Type of Service (TOS), among others.

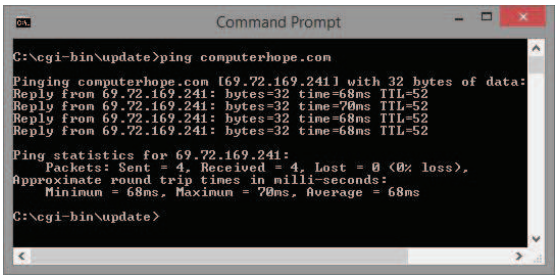


Figure 5.3.1.1 Ping Command

Traceroute

The traceroute command is one of the commonly used tools to verify correct network operation. The traceroute command will send a number of packets out to determine the path from source to destination, which is done by taking advantage of the Time to Live (TTL) functionality built into the IP header. The TTL field allows a source to set the number of “hops” that a packet is allowed to travel before being dropped. The typical reaction of a device that is processing a packet where the TTL has expired is to return a ICMP port unreachable message; the traceroute utility receives this packet and notes the source address. The traceroute utility will continue sending packets until the source address matches the intended destination device starting with a TTL set to 1, then 2, then 3 and so on.

Telnet

Telnet is a system protocol utilized on the Internet or neighborhood to give a bidirectional intelligent content arranged correspondence office utilising a virtual terminal association. Client information is sprinkled in-band with Telnet control data in an 8-bit byte turned

SSH

Secure Shell (SSH) is a cryptographic system protocol for secure information correspondence, remote summons line login, remote order execution, and other secure system benefits between two organized machines. The encryption utilized by SSH is planned to give secrecy and uprightness of information over an unsecured system, for example, the Internet.

4.9. System Monitoring

Network monitoring is a frequently used IT term. Network monitoring refers to the practice of overseeing the operation of a computer network using specialised management software tools.

Network monitoring systems are used to ensure availability and overall performance of computers (hosts) and network services. They let admins monitor access, routers, slow or failing components, firewalls, core switches, client systems and server performance among other network data.

Key Features in Network Monitoring

A network monitoring system can detect and report failures of devices or connections. It normally measures the CPU utilization of hosts, the network bandwidth utilization of links, and other aspects of the operation. It often sends messages—sometimes called watchdog messages—over the network to each host to verify it is responsive to requests.

When failures, unacceptably slow response or other unexpected behavior is detected, these systems send additional messages called alerts to designated locations such as a management server, an email address or a phone number to notify system administrators.

Network monitoring systems are typically employed on large scale corporate and university IT networks.

Monitoring your system resources is a necessary part of troubleshooting. Resources include memory, mass storage, network access, processor power, and so on.

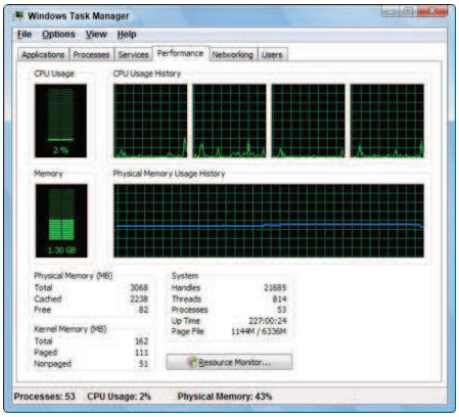


Figure 5.4.1.1 Task Manager

When your program needs a hardware resource, it makes a request to the operating system. Windows then tries to fulfil the request and provide the software that the resources requested. If it doesn't, you'll find your computer difficult to operate.

Begin by monitoring resource consumption. The easiest way to do so is from the Task Manager window, on the Performance tab. Summon the Task Manager by pressing Ctrl+Shift+Esc. Click the Performance tab to view some simple resource information.

Network Monitoring Software Tools

The ping program is one example of a basic network monitoring program. Ping is a software tool available on most computers that send Internet Protocol (IP) test messages between two hosts.

Anyone on the network can run basic ping tests to verify the connection between two computers is working and to measure the current connection performance.

While ping is useful in some situations, some networks require more sophisticated monitoring systems in the form of software programs that are designed for use by professional administrators of large computer networks.

Examples of these software packages are HP BTO and LANDesk.

One specific type of network monitoring system is designed to monitor the availability of web servers. For large enterprises that use a pool of web servers that are distributed worldwide, these systems help to quickly detect problems at any location. Website monitoring services available on the Internet include Munities.

Simple Network Management Protocol

Simple Network Management Protocol is a popular management protocol that includes network monitoring software. SNMP is the most widely used network monitoring and management protocol. It includes:

- The devices in the network that is being monitored
- Agent software on the monitored devices
- A network management system (NMS), which is a toolset on a server that monitors each device on a network and communicates information about those devices

Administrators can use SNMP monitor and manage aspects of their networks by:

- Gathering information on how much bandwidth is being used on the network
- Active polling the network devices to ask for a status at specified intervals
- Notifying the admin by text message of a device failure
- Collecting error reports, which can be used for troubleshooting
- Emailing an alert when the server reaches a specified low disk space level

SNMP v3 is the current version. It should be used because it contains security features that were missing in versions 1 and 2.

4.10. System Maintenance

Regular maintenance of the networked systems helps them to run more smoothly as well as reduce the risk of break downs. By having a well-designed maintenance schedule assists you in organizing your maintenance tasks.

Maintenance Schedule

Although 24/7 access to servers is often necessary, routine maintenance and upgrades are equally necessary. To prevent inconveniences, you must establish weekly maintenance times for major systems as follows.

Table 5.5.1.1 Maintenance Schedule

System	Maintenance Times	Notice
Administrative Systems	8 am – 8 pm, Sundays, only as needed	Will provide 24-48 hours' notice when taking down our administrative servers.
Network Services	8 am – 8 pm, Sundays, only as needed	Will provide 24-48 hours' notice when taking down our Novell servers.
Moodle	5:00 am to 7:30 am, Thursdays	When a longer down time is required, will provide 24-48 hours' notice.
Servers	5:00 am to 7:30 am, Thursdays Typically, windows servers will be patched either the third or fourth Thursday of each month.	When a longer down time is required, will provide 24-48 hours' notice.
Networking and Internet Infrastructure (including wireless system)	5:00 am to 7:30 am, Thursdays	No additional notice.
Telephone	No weekly schedule required	Will provide 24-48 hours' notice when taking down the phone/ voicemail service.
VMWARE Infrastructure	No weekly schedule required	When maintenance is required, affected users will be contacted

Activity

Design a maintenance schedule to support a networked system

4.11. Policies and Procedures

Policies and procedures are designed to influence and determine all major decisions and actions of an organization, and all activities take place within the boundaries set by them. Procedures are the specific methods employed to express policies in action in day-to-day operations of the organization.

AUP (Acceptable Use Policy)

Purpose: To inform all users on the acceptable use of technology.

The AUP sets the stage for all employees to assure that they know the rules of the road. In this policy we cover defining corporate resources: The company's computer network, host computers, file servers, application servers, communication servers, and mail servers, fax servers, etc.

The following are important areas to cover in an AUP.

Access	Monitoring of Computer Resources	Remote Access
Use of Computer Resources	No expectation of privacy	Illegal copying
Computer security	Altering attribution information	Inappropriate or unlawful material
Responsibility for passwords	Standard footers for e-mail	Duty not to waste computer resources

Table 5.6.1.1 Areas of AUP

Security awareness

Purpose: To consistently inform all users regarding the impact their actions have on security and privacy.

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing relevant security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some actions that can be taken to reduce the risk and drive down the cost of security incidents.

Information security

Purpose: To lay the foundation for the enterprise data risk management program; People, process and technology.

Policies related are;

- System Access Control
- Information Access
- User-IDs and Passwords

- User-ID Issuance for Access to corporate Information
- Anonymous User-IDs
- Password Policy

DR/BCP (Disaster Recovery, Business Continuity plan)

Purpose: To assure that the business has DR/BCP plans that are accurate and tested.

A DR/BCP plan helps manage real-time risk. It includes everything from responding to denial-of-service attacks, floods, fires, hurricanes or any other potential disruption of service. Business continuity seeks to keep the business running no matter what and thus includes redundant systems and personnel plans to assure the business stays up and running.

Change management

Purpose: to assure that changes are managed, approved and tracked.

Often things are moving very fast in any corporate IT department. Systems and software are being updated, modified or replaced for a number of reasons. Without change management a firewall may be updated and suddenly stop business traffic from flowing or perhaps cause unexpected data loss or data leaks by not being restrictive enough. Unexpected things often happen when we go to make a change or update.