Computer Networking Networks II

10.1 Network resilience

Network resilience is "the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.

Security

Network security

consists of provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and its network-accessible resources.[28] Network security is the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority. Network security is used on a variety of computer networks, both public and private, to secure daily transactions and communications among businesses, government agencies and individuals.

Network surveillance

Network surveillance is the monitoring of data being transferred over computer networks such as the Internet. The monitoring is often done surreptitiously and may be done by or at the behest of governments, by corporations, criminal organizations, or individuals. It may or may not be legal and may or may not require authorization from a court or other independent agency.

Computer and network surveillance programs are widespread today, and almost all Internet traffic is or could potentially be monitored for clues to illegal activity.

Surveillance is very useful to governments and law enforcement to maintain social control, recognize and monitor threats, and prevent/investigate criminal activity. With the advent of programs such as the Total Information Awareness program, technologies such as high speed surveillance computers and biometrics software, and laws such as the Communications Assistance For Law Enforcement Act, governments now possess an unprecedented ability to monitor the activities of citizens.[29]

However, many civil rights and privacy groups—such as Reporters Without Borders, the Electronic Frontier Foundation, and the American Civil Liberties Union—have expressed concern that increasing surveillance of citizens may lead to a mass surveillance society, with limited political and personal freedoms. Fears such as this have led to numerous lawsuits such as Hepting v. AT&T.[29][30] The hacktivist group Anonymous has hacked into government websites in protest of what it considers "draconian surveillance".

End to end encryption

End-to-end encryption (E2EE) is a digital communications paradigm of uninterrupted protection of data traveling between two communicating parties. It involves the originating party encrypting data so only the intended recipient can decrypt it, with no dependency on third parties. End-to-end encryption prevents intermediaries, such as Internet providers or application service providers, from discovering or tampering with communications. End-to-end encryption generally protects both confidentiality and integrity.

Examples of end-to-end encryption include PGP for email, OTR for instant messaging, ZRTP for telephony, and TETRA for radio.

Typical server-based communications systems do not include end-to-end encryption. These systems can only guarantee protection of communications between clients and servers, not between the communicating parties themselves. Examples of non-E2EE systems are Google Talk, Yahoo Messenger, Facebook, and Dropbox. Some such systems, for example LavaBit and SecretInk, have even described themselves as offering "end-to-end" encryption when they do not. Some systems that normally offer end-to-end encryption have turned out to contain a back door that subverts negotiation of the encryption key between the communicating parties, for example Skype.

The end-to-end encryption paradigm does not directly address risks at the communications endpoints themselves, such as the technical exploitation of clients, poor quality random number generators, or key escrow. E2EE also does not address traffic analysis, which relates to things such as the identities of the end points and the times and quantities of messages that are sent.

10.2 Views of networks

Users and network administrators typically have different views of their networks. Users can share printers and some servers from a workgroup, which usually means

they are in the same geographic location and are on the same LAN, whereas a Network Administrator is responsible to keep that network up and running. A community of interest has less of a connection of being in a local area, and should be thought of as a set of arbitrarily located users who share a set of servers, and possibly also communicate via peer-to-peer technologies.

Network administrators can see networks from both physical and logical perspectives. The physical perspective involves geographic locations, physical cabling, and the network elements (e.g., routers, bridges and application layer gateways) that interconnect the physical media. Logical networks, called, in the TCP/IP architecture, subnets, map onto one or more physical media. For example, a common practice in a campus of buildings is to make a set of LAN cables in each building appear to be a common subnet, using virtual LAN (VLAN) technology.

Both users and administrators are aware, to varying extents, of the trust and scope characteristics of a network. Again using TCP/IP architectural terminology, an intranet is a community of interest under private administration usually by an enterprise, and is only accessible by authorized users (e.g. employees).[33] Intranets do not have to be connected to the Internet, but generally have a limited connection. An extranet is an extension of an intranet that allows secure communications to users outside of the intranet (e.g. business partners, customers).[33]

Unofficially, the Internet is the set of users, enterprises, and content providers that are interconnected by Internet Service Providers (ISP). From an engineering viewpoint, the Internet is the set of subnets, and aggregates of subnets, which share the registered IP address space and exchange information about the reachability of those IP addresses using the Border Gateway Protocol. Typically, the human-readable names of servers are translated to IP addresses, transparently to users, via the directory function of the Domain Name System (DNS).

Over the Internet, there can be business-to-business (B2B), business-to-consumer (B2C) and consumer-to-consumer (C2C) communications. When money or sensitive information is exchanged, the communications are apt to be protected by some form of communications security mechanism. Intranets and extranets can be securely superimposed onto the Internet, without any access by general Internet users and administrators, using secure Virtual Private Network (VPN) technology.

10.3 Advantages and Disadvantages of Computer Networks

"Computing is not about computers any more. It is about living." -- Nicholas Negroponte, Founder, Massachusetts Institute of Technology's Media Lab

A computer network is a set of electronically connected computers which can share information and resources among themselves. There are communication protocols that define how this sharing should take place.

Like every other technological prospect, computer networks come with its set of advantages and disadvantages.

Advantages of Networks

File Sharing

The major advantage of a computer network is that is allows file sharing and remote file access. A person sitting at one workstation that is connected to a network can easily see files present on another workstation, provided he is authorized to do so. This saves him/her the hassle of carrying a storage device every time data needs to be transported from one system to another. Further, a central database means that anyone on that network can access a file and/or update it. If files are stored on a server and all of its clients share that storage capacity, then it becomes easier to make a file available to multiple users.

Resource Sharing

Resource sharing is another important benefit of a computer network. For example, if there are twelve employees in an organization, each having their own computer, they will require twelve modems and twelve printers if they want to use the resources at the same time. A computer network, on the other hand, provides a cheaper alternative by the provision of resource sharing. All the computers can be interconnected using a network, and just one modem and printer can efficiently provide the services to all twelve users.

Inexpensive Set-Up

Shared resources mean reduction in hardware costs. Shared files mean reduction in memory requirement, which indirectly means reduction in file storage expenses. A particular software can be installed only once on the server and made available

across all connected computers at once. This saves the expense of buying and installing the same software as many times for as many users.

Flexible Handling

A user can log on to a computer anywhere on the network and access his files. This offers flexibility to the user as to where he should be during the course of his routine. A network also allows the network administrator to choose which user on the network has what specific permissions to handle a file. For example, the network administrator can allot different permissions to User A and User B for File XYZ. According to these permissions, User A can read and modify File XYZ, but User B cannot modify the file. The permission set for User B is read-only. This offers immense flexibility against unwarranted access to important data.

Increased Storage Capacity

Since there is more than one computer on a network which can easily share files, the issue of storage capacity gets resolved to a great extent. A standalone computer might fall short of storage memory, but when many computers are on a network, the memory of different computers can be used in such a case. One can also design a storage server on the network in order to have a huge storage capacity.

Disadvantages of Networks

Security Concerns

One of the major drawbacks of computer networks is the security issues that are involved. If a computer is a standalone computer, physical access becomes necessary for any kind of data theft. However, if a computer is on a network, a hacker can get unauthorized access by using different tools. In case of big organizations, various network security software need to be used to prevent theft of any confidential and classified data.

Virus and Malware

If even one computer on a network gets affected by a virus, there is a possible threat for the other systems getting affected too. Viruses can spread on a network easily, because of the inter-connectivity of workstations. Moreover, multiple systems with common resources are the perfect breeding ground for viruses that multiply. Similarly, if malware gets accidentally installed on the central server, all

clients in the network that are connected to that server will get affected automatically.

Lack of Robustness

If the main file server of a computer network breaks down, the entire system becomes useless. If there is a central linking server or a bridging device in the network, and it fails, the entire network will come to a standstill. In case of big networks, the file server should be a powerful computer, which often makes setting up and maintaining the system doubly expensive.

Needs An Efficient Handler

The technical skills and know-how required to operate and administer a computer network is considerably high. Any user with just the basic skills cannot do this job. Also, the responsibility that comes with such a job is high, since allotting username-passwords and permissions to users in the network are also the network administrator's duties. Similarly, network connection and configuration is also a tedious task, and cannot be done by an average user who does not have advanced knowledge of computers and/or networking.

Lack of Independence

Since most networks have a centralized server and dependent clients, the client users lack any freedom whatsoever. Centralized decision making can sometimes hinder how a client user wants to use his own computer.
Computer networks have had a profound effect on the way we communicate with each other today, and have made our life easier. From the World Wide Web to your local office LAN, computers have become indispensable in daily life, and networks have become a norm in most businesses. If networks are designed and configured keeping in mind its pros and cons, they are the best piece of facility you could ever have.

10.4 Most Common Computer Network Problems

Whether you are a system administrator in an organization or someone who has a networked setup in your home, troubleshooting networking glitches is an inseparable part of your life. For a person, who ensures the smooth functioning of networked computers, frantic calls of help are the norm rather than the exception. While disasters do happen, most of the calls demanding assistance are a result of

some very basic troubles; troubles that do not require a lot of skill, but just a little patience. Learn how to fix the most common networking and Internet problems right here.

Common Network Problems

IP Address and Network Card Issues

Sometimes, two computers are assigned the same IP address erroneously; and because the IP address is the identifying feature of a computer, it leads to obvious connectivity issues. On the other hand, network cards enable computers to link, and faults in the network cards obviously disrupt connectivity.

Fix it: Simply enough, changing the IP address on one computer will fix this problem in no time. To resolve the network card issue, pinging another computer is how you test the network card's functioning, which should tell you if it needs to be fixed.

Network Related Problems

Problems related to connectivity plague us perpetually, and more often than not, the solution lies in checking your physical connections and connection devices. Even with Wi-Fi network, there could be some unreachable areas where radio signals simply refuse to venture; and with a multiple client WLAN, you must choose a central location to install the router or WAP.

The Solution: A quick inspection of your router or hub will tell you if some machine is disconnected, or if the culprit is a faulty cable.

Absence of Connectivity

Certain computers remain undetectable even after the naming rules for computers and domains have been followed. If you aren't using TCP/IP already (especially with home setups), it is recommended you do so as the functionality it offers is unmatched.

Fix it: Ensure all the computers are within the same subnet with individual IP addresses. This is elementary; but, just check if the file and printer sharing option is installed and functioning, and also define network shares on each computer. Tweaking Firewall settings may also help.

Slow-moving Connectivity

Slow connectivity is the mark of a haphazardly planned network, leading to extra collisions, which the network is incapable of handling. Heavy file transfers bring down the speed tremendously. At times, the network card, which is actually in charge, may also be overtaxed.

The Solution: Users must be told to zip bulky files while transferring, which lowers the pressure on the network. Also, check if the network card is not suspended in the transmit mode, which indicates that the card is working overtime. All you need to do in such cases is, to replace the faulty components; having done that, never forget to test the functionality.

Drop in Internet Connections

Troubleshooting Internet connection drops should begin with an examination of the router and a check for any configuration problems. Before you do that, just confirm if your signal strength is fine, and if it is, the problem is obviously internal.

Fix it: In case you have a wired setup, examine the network cables, as you're likely to notice that the source of the problem is a faulty cable. With wireless setups, it gets a little difficult to identify the source of the problem. However, in most cases, as mentioned before, the rogue computer could just be placed in a network-unfriendly zone.

Problems Caused by Firewall Status

Along with providing the necessary security, Firewall settings can interfere with file sharing on connected computers. It is true that disabling security features can make your system vulnerable to attacks, but lowering security levels should not cause too much trouble.

The Solution: Rigid Firewall settings need to be adjusted to allow networked computers to share data. You may consider disabling the security settings temporarily, after having thoroughly considered all security related threats.

Problems related to networking rarely venture far from the mundane. Having gone through the common networking problems and the mistakes to avoid, ensure that

you keep them at bay and stay away from trouble with a finely operating networked system.

10.5 Different Types of Servers

The word 'server' refers to a specialized computer or hardware on which the server software works and provides services to other computers or clients. This article throws light on different types of servers available in the market, these days.

A server has many functions, and they come in different types to facilitate different uses. Let's have a brief idea on what is a server before getting to know about the different types of servers.

What is a Server

A server is a device with a particular set of programs or protocols that provide various services, which other machines or clients request, to perform certain tasks. Together, a server and its clients form a client/server network, which provides routing systems and centralized access to information, resources, stored data, etc. At the most ground level, one can consider it as a technology solution that serves files, data, print, fax resources and multiple computers. The advanced server versions, like Windows Small Business Server 2003 R2 enable the user to handle the accounts and passwords, allow or limit the access to shared resources, automatically support the data and access the business information remotely. For example, a file server is a machine that maintains files and allows clients or users to upload and download files from it. Similarly, a web server hosts websites and allows users to access these websites. Clients mainly include computers, printers, faxes or other devices that can be connected to the server. By using a server, one can securely share files and resources like fax machines and printers. Hence, with a server network, employees can access the Internet or company e-mail simultaneously.