Design a small business computer network (case study)

Péter Török, Dr. Imre Négyesi

National University of Public Service, Hungary

Abstract

The expansion of the computer network is one of the most significant way of innovation. The need for the expansion of computer networks is required by the display of newer technologies, new networking methods and tools. The need for expansion is further increased by the users' rising demand for local and web networks. The users apply more and more network services on their computers; the use of mobile tools for the continuous reach of remote networks is getting more and more widespread. These needs can only be satisfied by the computer networks by giving ground to continuous development.

Keywords: SOHO, network, computer environment

Introduction

Entertain BT was approached via e-mail by the CEO of Nagy-ker Nagykereskedelmi Kft to request a preliminary survey about designing a computer network for the company's new site.

Before we start the preliminary survey, let's clarify some elements we will use during our work.

The expansion of the computer network is one of the most significant way of innovation. The need for the expansion of computer networks is required by the display of newer technologies, new networking methods and tools. The need for expansion is further increased by the users' rising demand for local and web networks. The users apply more and more network services on their computers; the use of mobile tools for the continuous reach of remote networks is getting more and more widespread. These needs can only be satisfied by the computer networks by giving ground to continuous development.

The development can be materialized by taking the following aspects into account:

- the realization of more physically extensive networks
- bandwidth expansion
- applying new methods and tools
- development of data transmission methods
- formation of a scalable network
- formation of fault-tolerant systems.

For unified interpretation let's review some of the elements.

Bandwidth (transmission speed): The number of bits passing through the data transmission channel (wired or wireless network) per second. (Unit: bit/sec [bps], For the expansion of bandwidth it is often sufficient to develop a new data transmission method on the already existing wired or wireless medium, the latter often does not require change.)

Delay: The delay is the amount of time required for the transmission of packets trough network connection. Factors influencing delay may include:

- endpoints (computer, pda, mobile phone, network printer), which code/decode their network messages in the form of a digital sign for a network medium
- network medium (wired and wireless)
- network intermediary tools (switches, routers).

For the measurement of delay, under Windows for example, the tracert command is used, which shows the passing of network packages trough routers and their delay.

Response time: The period of time a network system requires for responding to the need demanded by the sender. (Typical measurement tool is the PING command, which shows the response time of the package.)

Scalability: One of the cornerstones of the expansion of networks is to design the already existing network in a way, so it's capable of carrying out future extensions. The scalability is feasible trough the extension of a few network tools (e.g. switch), but a WAN-connection (backbone network) tool (router) may be needed to increase the performance..

Fault tolerance: Before discussing the fault tolerance as a new term, let's say a few words of the concept of availability. The availability of network systems usually means a number given in percentage which outlines the constant operability of the network in every moment of the year. The internet provider must provide this number, because it's the customers contractual right to know that what amount of network failure they can allow. In case of business customers even a moment of network failure can cause serious problems and losses. This is why we must create a fault tolerance system, so redundant connections help the fault tolerance and continuous availability of the system.

Beyond the aforesaid details the computers can be tabulated by the size of computer network, operation, transmission method, and many other aspects,

- extent of the network (PAN, LAN, MAN, WAN),
- network topologies (bus, ring, star, extended star, tree, web),
- technology type of data transmission (broadcasting networks, point-point networks),
- network technology implementing data transmission (Ethernet, TokenRing, FDDI).

If we want to illustrate the hierarchy of a large-scale network, we can divide it into three parts

1. The elements of the end systems are devices suitable for running network services (applications), which can be found on the edge of the network. (Such as the computer, server, network printer, PDA, IP-phone, mobile phone etc.).
2. The access networks are appliances (routers) connecting the end system to the network's higher level line, possibly appliances (routers) connected to its ridge line. (These networks may be home, business, or mobile /wireless/ networks as well.).
3. The network core connects the package switches of the end systems with the backbone network of the internet. The core of the network consists of the internet service providers (ISP), regional access providers, and the backbone network. The internet service provider has a point of presence (POP). The POP is the connection point, trough which the business clients can log in to the network. The regional access provider connects POPs belonging to multiple internet service providers, and connects them to a larger scale network.

Lastly the backbone network consists of multiple high speed, high capacity private networks (national providers). These networks overlap, so they can provide bigger capacity, traffic, better load balancing, and reliability. The appliances forming the core of the network can switch the data trough data networks in two ways: circuit switching and packet switching.

There are different methods for switching stations.

Circuit switching: The circuit switched networks occupy the communication channels between the end systems for the whole duration of the session, and the connection lasts until it is interrupted. Phases of circuit switching: building the connection, maintaining and using the connection, and lastly, dismantling the connection. (Analog telephone technology also operates on this principle. It is not economical; today it is occurring in smaller and smaller numbers. Very expensive, slow and isn't capable of reliable data transmission.).

Packet switching: In today's modern computer networks the source breaks the message up to smaller packets. Packets received this way pass through a communicational channel and packet switches between the source and the destination. Before reaching their destination the packets travel on variable routes, and only occupy the given communicational channel until they pass the given packet switch. It is also possible, that the packets have to wait at some of the packet switches because of the

accumulated amount of data traffic. (Packet switching is the most common switching method of these days.)

Based on the facts stated above we can say that the network is a very complicated system in terms of structure, which consists of many applications, different kind of end systems and switching methods. To understand the whole system, we must divide it into multiple layers. The layered architecture makes it possible for us to concentrate on a given module of a complicated system. The layered network model is also required for the communication of the appliances made by the network manufacturers between each other, using an appropriate protocol language. The under mentioned models provide an individual service for each layer, which is provided for the layer above it. In other words every layer provides its service by carrying out given tasks inside the layer, and also using the services of the layer below. This is the service model. Inside a given layer the end points apply rules, and they can send messages for each other with this. This is called protocol. The protocol of the different layers are called protocol stack.

After all these, let's take a look at what specific steps do we have to follow while designing a network.

Network design is the first (and fundamental) step of building a network. A network that was not designed properly won't be able to complete its tasks, and the costs of later changes and repairs may even exceed the cost of building it.

The main aspects of designing today's networks (keeping in mind to try to create the most useful network for working using the tools available):

- creating a flexible, reconfigurable network;
- creating a network that satisfies the needs of the future, with possibilities of expansion;
- taking data protection aspects into account;
- providing safety from noises and environmental impacts of foreign origin;
- to meet the requirements of both national and international regulations and standards;
- to be able to serve an appropriate number of end points.

The process of designing can happen in multiple steps:

- designing IT systems (servers, workstations),
- making a network system design,
- making plans of structured local area networks (LAN)
- making plans of structured wide area networks (WAN).

In parallel with the aforesaid the next task is to make a network system design, in which we specify the requirements and parameters of the system to be built, and designing the actual structured network takes place only after this. The cabling and the path design, the installation of appliances and tools according to the standard, and transfer – receipt proceedings must be developed. The plans of structured wide area networks include the description required services, and the selection of the most suitable router. It is also an important rule of design that the segmentation and the development of the VLANs must be done in a way that the workstations belong to the logical network which contains the servers most frequently used by it. This way the load of the ridge direction can be reduced. These are the possible methods of reducing the load:

- Relocation of resources in order to keep the traffic inside the work group.

- Logical relocation of users in a way that the work group can reach the given user more directly.
- Expansion of servers in a way that instead of the ridge they are locally available.

The company

At the request of Entertain Bt, the following summary was delivered by the Chief Executive of Nagy-ker Kft.

"Our company was founded in 1994 under the name Nagy és társa élelmiszeripari Kft. In the beginning, our main field of activity was the production of seasonings and spice mixtures, and we are dealing with the distribution of raw materials and accessories for catering and public catering. Our market has been rapidly developed nationwide, so we are now among the first in Hungary with similar product manufacturers and traders. We have grown our first site, so in 1999 we opened a new site for our increased turnover. In the new place, we built a Cash and Carry store, where we expanded our range of warehouses, catering to confectioners and bakeries.

In 2000, we opened up to a new market segment, we added our palette with "bio" gastronomic articles, expanded our range of products with foodstuffs used in catering and bakery industry, creating a significant turnover, and today our annual turnover is over HUF billions. Our primary trading areas are Budapest, Pest county, in these areas we have developed our hiking trails mainly along the M1 and M7 motorways.

In our C + C store we sell to our crawler customers in a self-service way, but we make a significant part of our turnover with delivery. Our logistics background provides our customers with a daily service that we operate under our HACCP quality assurance system.

Our partners can place their orders by phone, fax or e-mail (vevoszolgalat@nagy-ker.hu) or on our web site (www.nagy-ker.hu) at our customer service.

The company currently employs 44 people in three main organizational units. There are 12 employees in the economic sector and 4 managers. There are 6 people in the store, customer service, billing and cashier, and 8 are salespersons. In the warehouse are 8 people and 6 drivers. "

The project

The size of the network was surveyed during site navigation. Proper installation of network distributors does not require the installation of new signal amplifiers. Workplaces in the three main areas of activity are physically separate. A total of 80 network endpoints will be created for the computer network in 18 rooms.

During a long discussion with the management, the services and the required software environment were clarified.

The company has its own domain name, the related webpage is placed on an external server. The maintenance of the website is carried out by an external company. This does not need to be supported by the network to be established.

The domain mail server, however, is deployed at the company's premises, stores incoming mails on its own, and performs mail forwarding and forwarding independently.

The Internet connection of the site, Internet access for workstations should be regulated locally, and the structure to be developed needs to be supported.

Attacks from the Internet must be protected in a number of (overlapping, complementary) ways.

On a local area network, documents are stored in the directory structure to be created on the server, with access to more access levels at different levels.

Virus protection for servers and workstations, including virus protection for e-mail traffic, must be secured in a prominent way.

In addition to the wired network, wireless (Wifi) access should also be provided. Separate for employees, full network functionality and specially for buyers, guests, visitors only for Internet access.

Client-to-business retailers should be provided with remote access to the local area network. This is only in a reliable, secure way. Among the solutions to be considered, the design of VPN won the leadership's liking.

The company uses customized enterprise management software, which includes inventory inventory records, booking orders, compilation of delivery notes for deliveries and billing. It has a database connection to the accounting software. The program is running on a web interface, so a web server must be installed on the server.

Data and documents stored on the server should be backed up regularly, with the appropriate backup strategy and backup and archiving program required.

It is necessary to ensure the continuous operation of the server, requiring the provision of a suitable, manageable uninterruptible power supply.

The right of access to, and access to, the employees of different fields of activity must be well separated when network is established so that the integrity of the system remains.

Print under centralized control with 10 independent printers.

Designing the hardware environment

With the necessary data you could start planning.

First, summarize the tasks to be performed by the server:

- a file server for storing local users' documents

- printer management to manage 10 network printers

- rescue-archiving solution for documents stored on the server and for correspondence

- a web server to support enterprise software

- mail server, imap and http connectivity

- a packet filtering firewall for the network to protect external attacks

- a central antivirus system with real-time web, mail and file protection

- network address translation to secure Internet access to workstations

- handling VPN connections for remote work

Taking into account the number of users, workstations, and printers, resource requirements for tasks can be met by running a server. This simplifies network administration, no central user management system is required.

After defining the hardware requirements for the server, the number and location of the network devices was determined.

The obvious solution of the separate network structure requested by the customer is breakdown into VLANs. Thus, at the boundaries of the subnets, traffic can be limited by a separate rule system if appropriate Layer3 manageable network devices are used.

The server and network devices are placed in separate VLANs to isolate and protect network devices. The scope of activities is put into separate VLANs, so traffic between them can be restricted or restricted and can be controlled separately by the server.

Separated access for employees and external users was a consideration when designing the wireless network. This can be done by building a dual system or using MultiSSD support tools. In the first case, the network is expensive, the second is the price of access points. Based on the sketches made during the scenes, the number of devices required can be determined. There are 2 in the office, 3 in the store, 1 in the warehouse are needed for proper coverage. Therefore, using the MultiSSD support tools, it is worth solving the dual Wifi network.

Documentation

Based on the needs and the considerations arising from the discussion and planning, the following design documentation was compiled:

This document contains a system design for the IT infrastructure and services of the Nagy-ker Nagykereskedelmi Kft. (Named Nagy-ker) (name conventions, discrete system, network settings, IP domains, IP addresses, passwords, operating system and application versions, management system, firewall policy system, WIFI system)

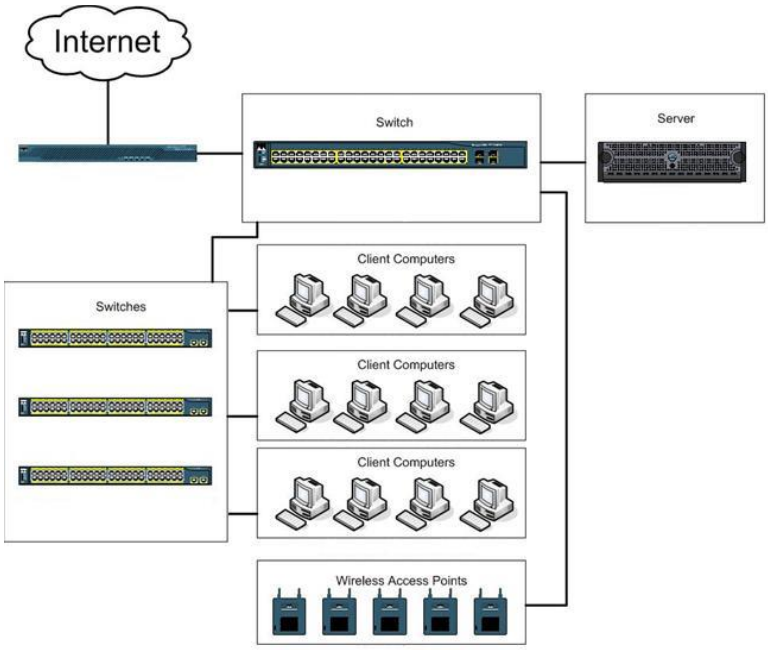

Fig 1. General graph of the network of the Nagy-ker network

User environment on workstations

Hardware

Workstations purchased by Nagy-ker have a unified hardware environment, which greatly facilitates system administration.

Optional Windows 7, Windows 8, Debian Linux Software Environment

Creating a unified software environment in the operating system and the office software environment. For different uses, it is necessary to create multiple operating systems on client machines

Efforts should be made to use as little resources as possible for administration. Improved patches can be distributed centrally in the unified environment. Software failures do not require repair, but the preinstalled software environment can be deployed automated to the workstations to minimize the duration of repairs.

Since client computers can not be dedicated to users, and there are likely to be attempts to modify configuration settings or install software, it is recommended to create the most stringent user access system.

Centrally managed antivirus system

Critical in the antivirus environment is the automation, which can be used to quickly fix the updates, to change the configuration settings centrally, to make the user's intervention impossible. You must also ensure proper logging, which helps you to track virus infections and other events on your clients (such as successful updates). Since workstations can be used for removable media (such as a pendrive), there is a need for enhanced security at the workstations (real-time monitoring of all files that can not be turned off).

Not only need workstation level checks, but also need to filter on a server site (mail server antivirus, Internet traffic monitoring)

Windows network

Workgroup

A working group will be set up for easier administration. The NetBIOS for the Workgroup is NAGY-KER.

Computer name conventions and settings

Basic considerations

In order to simplify system operation, it is important to design a name convention when designing a system that will prevent the computer from being compromised. For servers, you have to choose names that you will not have to change later on. For workstations, frequent change of name may result in administrative overhead work, so it is advisable to create a structure that avoids changing names as much as possible, but the location and user of client computers can be solved using the inventory database.

Kiszolgálók elnevezése	function in brief	OS
name of the server		
srvlin01	DHCP, DNS, file, mail, print, web	Debian Linux 7.3 64 bit

Conventions for User Names and Groups

Basic considerations

Because the Great Circle network can be separated into distinct user roles, it is therefore necessary to define uniform rules and ensure that user names are unique.

Employee's User Accounts

Currently, usernames consist of the first character of the first name and the nickname of the surname. If matching, the first 2 letters from the name, 3 letters for further matches, etc. should be used. For full matches, numbers are allowed. For example: István Szabó: iszabo, isposo, ist'lo, istvanszabo2 etc.

Name Groups

In all network infrastructures that aim at establishing eligibility levels, it is necessary to provide groups to facilitate the administration and registration.

Naming service accounts

Creation of special users for the operation of the system on which the services required for each system are run on behalf and with the rights - if this can not be avoided.

The password must be handled in accordance with the appropriate security requirements.

Special accounts should not be used for interactive login, for each application it must be resolved that it can be administered by operating personnel using the appropriate security groups.

Network settings

When designing a well-functioning network infrastructure, it is essential to develop the right VLANs, primarily based on security and performance considerations.

According to the current concept, Nagy-ker uses the commonly used private IP addresses with the correct translation. The range used is 172.16.0.0

VLAN ID	VLAN name	VLAN Network ID	Subnet Mask	Default Gateway
2	Default	172.16.2.0	255.255.255.0	172.16.2.254
10	Servers	172.16.10.0	255.255.255.0	172.16.10.254
11	Iroda	172.16.11.0	255.255.255.0	172.16.11.254
12	Raktar	172.16.12.0	255.255.255.0	172.16.12.254
13	Uzlet	172.16.13.0	255.255.255.0	172.16.13.254
60	WIFI_Internal	172.16.60.0.	255.255.255.0	172.16.60.254
61	WIFI_External	172.16.61.0	255.255.255.0	172.16.61.254

Table 1. The structure of the IP address of the Nagy-ker network

Network services

DHCP

The main benefits of the service:

The DHCP service allocates network addresses, making it significantly easier to keep records and avoid collisions. You can also set client settings for networking, so any configuration settings can easily be distributed.

The DHCP service was installed on the srvlin01 server.

other parameters

IP address:

Subnet mask 255.255.255.0

Getaway (172.16.x.254)

DNS server (172.16.10.1)

DNS domain name: nagy-ker.local

Set up DNS registration for DHCP-assigned addresses.

Address Rental Time: 5 Days

DNS service

As one of the most important elements of network communication is the DNS service, it is necessary to pay close attention to its design. Important is the automatic update, reverse zone and replication.

The srvlin01 server performs these services with the following settings:

There is a forward zone, zone name: high-level zone

Configure the Forwarder to the Server (ISP later assigned NS)

When creating reverse zones, all subnets (zones 172.16.x.0) have to be added, their settings are the same as the forward zones.

File server, security settings

Home folder

Each user account has a home directory with appropriate security settings, which is automatically connected. You will have to create the WORK, EXPORT, IMPORT directories automatically.

Joint folders

More common drives must be created in the structure specified by the Customer. It's a good idea to create an ACL if someone does not have the right to a directory, then you can not just log in, but do not see it in an administrator.

Recommended quotas:

Warehouse, business workers for home directories: 100 Mbyte

Employers working in home directories: 500 Mbyte

For shared libraries: 1 GByte, which of course depends on the number of libraries.

Remote access:

Because shopkeepers may be justified in accessing the file server remotely, it is necessary to create the ability to access files (for writing and reading) over the Internet. It is recommended that you use VPN to access local network resources over the Internet.

Security settings

Server security configuration:

When installing all of the server services, make sure that the same settings and components are installed for ease of administration (obviously, exceptions are the target functions, such as DNS, DHCP, etc.).

During installation, you must disable any component that the installer offers.

Rename local administrator (from Group Policy, set a complex password.

Logging events that are important for traceability (login, unsuccessful operations, etc.) should be carefully archived.

Client security configuration:

Clients have user rights on workstations. The Windows 7 and Windows 8 operating system level defaults are appropriate for using such a limited account because no configuration options can be changed and access to system files is prohibited.

Password policy:

Password expires in every 90 days

Alert 14 days in advance

Locks the account immediately after the expiration

The password must be different from the previous one in at least 5 characters

Password length minimum 7 characters, complex (lower case, upper case, numbers)

When creating a user, the default password is the birth date (8 characters).

For operator personnel, it is particularly important to enforce these rules because the most critical users are here.

Management and antivir

LanDesk Management + Antivirus Suite 8.8 is installed in the Nagy-ker network.

Features to be introduced:

Hardware Inventory,

Software Inventory,

OS Deplyment,

Software Distribution,

Remote Control,

Antivirus console.

To use this system, you do not need to distribute functions between other servers, you just need to install it on a featured client. The system can be controlled from a console, managed by software deployment, operating system distribution, antivirus control.

Workstations can be remotely deployed by agents, but since it is installed at the same time with Landesk imaging technology, it is more convenient to integrate the operating system image.

WIFI

Since Wifi devices are capable of MultiSSID, it is advisable to configure a multi-level wifi system (to enable or disable internal resources).

VLAN 60

SSID: NAGYKER_private

Authentication: wpa, with a predetermined key

Internal resources are available as internal clients

IP Range: 172.16.60.0/24

VLAN 61

SSID: NAGYKER_public

Authentication: wpa, with a predetermined key

Internal resources for customers are not available, only DNS name resolution, http and https outwards. Further, there is a need to limit bandwidth.

IP Range: 172.16.61.0/24

Firewall

As the system is built into a fundamentally closed organization, it is reasonable to limit the Internet traffic radically. Of course, not all ports should be banned outward because it would make work harder.

Currently, the public IP domain is not yet known because it does not have an ISP contract. As you know the outer domain, you must change the rule system anyway.

Inwards: SMTP, VPN, http and https for srvlin01

Outwards: ICMP and the following TCP and UDP ports:

37, 43, 46, 53, 79, 80, 109, 110, 119, 123, 143, 389, 443, 500, 524, 554, 563, 13, 17, 21, 22, 23, 25 (srvlin01 only) 569, 636, 993, 995

Internet access

To increase security, ASA has to create a privilege user that can edit the ACL.

References

Török Péter, Rikk János: New methods to protect our network systems; AMERICAN JOURNAL OF RESEARCH EDUCATION AND DEVELOPMENT 2017:(1) pp. 4-16. (2017) ISSN 2471-9986

Szabó András: A felhasználók digitális lábnyomának, anonimitásának vizsgálata technikai szempontból I. Rész - személyi számítógépek, Hadmérnök XII. Évfolyam „köfop" szám – 2017. Október

Török Péter, Rikk János: BASH scripting; Henderson: DEVLART, LLC, 2017. 68 p. (ISBN 978-0-9977210-6-5)

Laura Chappell: Network analysis; 2nd edition Chappell University 2013. ISBN 1-893939-9-1