TEKA Kom. Mot. i Energ. Roln. – OL PAN, 2010, 10A, 133-138

ANALIZING TRENDS IN THE DEVELOPMENT OF THE WIRELESS DATA TRANSMISSION SYSTEMS

Valeriy Dyadichev, Andrey Kolesnikov

Volodymyr Dal East-Ukrainian National University, Lugansk, Ukraine

Summary. The research of wireless data transmission systems in the management office has been conducted. The methods of organization and interaction of various devices based on wireless technologies has been studied. Recommendations on the choice of wireless equipment for office tasks are given.

Key words: wireless technologies, LAN, access point, broadband access, video recorder, webcam, network traffic, scalability, data warehouse.

INTRODUCTION

Problem of combining several computers in a local network is a common phenomenon because of the fact that the solution of several tasks require collaborated work on a problem. At this point cable technologies are widely used in different structures, due to their greater availability in stock. Everyone solves the problem in different ways but rarely thinks about the introduction of new technologies, because they are not very common and often are lack the expertised specialists for development of a network based on wireless technologies.

BROADBAND INTERNET

Even not long ago, the Internet was needed only for Web browsing and sending e-mail - a pair of tens of kilobits per second, which "betrayed" analog modems, was sufficient to cover the typical needs of an ordinary user. Now the opportunities provided by the network fundamentally increased, users can receive multimedia content, play online games, share large files, communicate via VoIP-services [1].

The most important of the qualities is the lack of exhausting procedure of dialing up ISP. Besides, for a broadband connection breaking the link is a quite a rare situation, occupied Internet phone line during the session connect is also not peculiar to this type of access.

Many devices used to organize the broadband network, provide greater convenience in the joint use of the Internet channel.

An important fact is that in the case of broadband user does not pay for time spent in the Internet (as it is with a dialup connection), but for the amount received / transmitted data (data being transferred, as a rule, are free of charge).

There are many ways to organize a broadband Internet connection. The most effective in terms of price / quality are two methods. They are ADSL and regional networks. ADSL-modem and a splitter is required for connection to an asynchronous digital leased line (the abbreviation ADSL stands for it).

IMPLEMENTATION VIDEO CONNECTION

The most important condition for the implementation of video connection is a channel of access to the Internet with sufficient bandwidth. The fact is that during the videoconference session not only voice data but also video stream are transmitted. Of course, before sending the network transmitted information is compressed using special algorithms that provide multiple compression, but despite this, bandwidth requirements will still remain quite high. It is generally believed that to ensure high-quality voice communication via the Internet "width" of available in the network should be not less than 64 kbit / s, to ensure high-quality video this figure will be at least twice [2].

The most popular way to "capture" images transmitted over the Internet is a web-camera. Besides web cameras, there are other tools organizing video – such as videophones. Videophone is a completely separate device that does not require connection to a computer. This gadget connects to your TV via composite connectors; Internet connection is usually made using the Ethernet-interface. "Call" with the videophone can be done to an owner of a compatible videophone, and a computer with a webcam and installed Windows NetMeeting software.

COMFORTABLE COMMUNICATIONS WITH ANY PLACE OF THE WORLD

VoIP-connection is available for every user who has access to the Internet: a basic set of services provided by the major providers of this service is completely free. This nice feature allows you to reduce to zero the cost of long distance and international calls.

Comfortable in interaction. One of the advantages of VoIP is that within a single communication session the user can interact with several subscribers. This feature is particularly attractive for business people, however, simple users also appreciate it.

In order to understand all the advantages of VoIP you only must have a computer and internet connection (required connection speed is no less than 64 kbit / s). In addition to hardware, special software will be needed. There are two possible options. As we know, there are currently two popular protocol for VoIP: Skype and SIP. For usage of Skype protocol, the same name program created by the developers of this

protocol is used, for the open SIP there is a huge amount of software from third-party manufacturers.

Table 1**. Visual comparison**

PSTN	VoIP
You pay for the time of connection	You pay for the volume of transferred data
Rates are high and depend on the distance	Rates are low and don't depend on the distance
You can be connected to only one person	You can communicate with any number of people
You can only talk	You can not only talk but also share any multimedia data: images, documents, music, video.

REMOTE ACCESS TO PC AT WORK

Modern user often has to deal with "office" work at home. Urgent work knows no day of the week and very often the problem, that requires immediate implementation appear on weekends. Necessary documents are likely stored in a local network. How to get access to it? The solution to remote access to corporate local area network technology is the use of VPN [4].

You can never know in advance what files from a working computer may be needed at home, all working documents are not able to be carried on a flash drive. In addition, executives often prohibits copying and moving files from desktop PCs - the purpose of protecting corporate secrets. Many users do not like to take home files from work, fearing the "desynchronization" versions of working papers (because it has to follow - a document, "home" or "worker", was amended last). In addition, often the documents are edited collectively - on any instance can run multiple employees. Of course, in this case, the computers should be in the same local network. VPN allows the employee to participate in the work, even with other parts of the globe.

About the "local means of communication" itself a few words should be said. Sometimes these projects are the only means of contact with employees. In many offices, access to the Internet from corporate PCs is blocked for improving the efficiency of workers, resulting in no possibility to send messages, and except on a local chat. Access to such services provided through the VPN will solve the problem of interaction with colleagues.

If you have taken a laptop with you, then the problem is even smaller. To find any working hotspot to connect to the Internet would be enough. You are in the corporate LAN. VPN. The concept of virtual private network is an idea called "tunneling". Tunnel on the Internet at first glance is a stream of ordinary, nothing remarkable package. In fact, they serve only to "wrapper" for encrypted packets. When a packet leaves the insecure Internet zone, passes through the firewall and into the local network of the company - "wrapper" is removed and the inner packet decrypted. Then it goes on a local network to the recipient, as if it was not sent from a remote computer, but from a "local" one. Is this the VPN. It seems pretty simple. However, the effectiveness and safety of the virtual network is influenced by many factors. Used algorithms traffic encryption, authentication methods, means of verifying the integrity

and immutability come packages are just the major ones. These parameters characterize the quality of the concrete implementation of VPN.

INTEGRATION DEVICES

Installing video intercom, integrated with a PC. Based on the computer, accessible and effective security system, fully capable to replace the concierge can be implemented.

Door intercommunication video provides covert surveillance for the visitors, even if they spotted the camera lens, it is impossible to determine the presence of hosts. "Computer" Intercom, among other things has another added convenience - with a video camera can be viewed on screen of PC. Thus, in order to find out who is behind the door, it is not necessary to leave your working place near the computer. Another interesting feature, easily implemented by computer intercom system is based on the recognition of the movement. If the camera "sees" that in its visibility someone moves you get the message to the computer. In other words, the arrival of man can be noticed before he rang the doorbell.

Record of what is happening. Most webcams have a built-in microphone, and sometimes a small speaker.

DVR. Properly configured intercom computer can serve as an additional means of protection office - recording, obtained through a webcam, will be given in evidence against intruders.

Data on the power wiring. Did twisted pair entangle the whole office? "Medicine" from the wires is needed urgently. Unfortunately, Wi-Fi is not always a panacea, sometimes the main requirement for the network infrastructure reads as follows: "stuck in the socket and make things work." That is exactly how the modems that transmit data by conventional electrical wiring work.

Print from anywhere in the office. Until recently, the organization of network printing was available (and relevant) only for the working groups. At the present time, when most houses have several PCs (in the simplest case - a working laptop in the office and media center in the living room) and printers (for example, ink jet and dye-sublimation printer MFP), the problem of optimizing the printing process is very acute. Let's see what we can offer with the possibilities of digital homes in this area.

Independent press. Printers oriented for office users have long been indecently cheap - currently an excellent inkjet printer or MFP can be bought for very little money. Also we can advise the skeptics to use CISS - Continuous ink supply system (unfortunately, the consideration of these devices is beyond the scope of this article). Office print server (not to be afraid of the word "server", which is associated with the most expensive glands oriented corporate application). This server will allow us at a minimal cost to print documents and photos from any office computer, without caring about the inclusion of the required PC.

SECURING THE WIRELESS NETWORK

The most effective and simplest option is the encrypts of network traffic. When using it, any alien device is simply not able to connect to the network, not "knowing" the key for decryption. To add a "friendly" customer network is sufficient to enter the key on it. It is understood that perfectly persistent cipher does not happen, often the encryption algorithms have a "hole", giving "green light" to hackers. However, to protect your home network from hooligans and fans of "free internet" this method is almost perfect [1,2].

Network encryption - WEP. WEP (Wired Equivalent Privacy) is the oldest of all the standard encryption of traffic in wireless networks. First of all, many devices do not support the new standards. Such a situation arises, for example, with many wireless media player. In addition, setting parameters WEP is much easier - so it is better for the beginners to start with it. To connect to the network client needs to know the "key". For the user it is five or thirteen characters (depending on the version of WEP). They need to put in a query window, and if no entry errors made, the computer is already in the network. In terms of computing device, the key is a sequence of 128 or 64 bits. A special algorithm of five (or thirteen) symbols "user key" turned into forty (or one hundred and four) bits. The remaining twenty-four bits are dynamically generated during operation. Thus, the key is constantly changing, which complicates the work of burglars [1].

Network encryption - WPA and WPA2. WPA (Wi-Fi Protected Access) - a more modern standard encryption, which offers a lot of innovations. Standard WEP allows hackers to replace the information packets sent over the network. In fact, it was possible to pick up keys constant requests to computers. WPA also checks the correctness of the key pre-destination packages. If the package did not come from the expected sender, it is ignored. WPA2, the most modern standards currently requires traffic encryption algorithm, AES, whereas in previous standards used less reliable RC4.

Implementation of the selected data store. Office LAN allows you to exchange files between computers, but its implementation of data synchronization problem stays open. Where is the important document that has taken so much time to do it? On the desktop, laptop, flash drive or even lost in the smartphone? The obvious solution is to organize shared storage accessible from any home device via Wi-Fi. Single file storage relieve the owner from the problems of finding files on the local network machines.

Files security. Customers wishing to ensure the greatest possible level of security and privacy may be calm. Network Storage for all the openness to any client home network can be transformed into overprotected bastion. If necessary, on a folder with important information you can set a password, or even make encrypted files using special software. In the security policy it is always possible to establish a list of MAC-addresses, which is available from the hard drive. Aliens computers simply can not "see" it [1].

Office security. Modern security systems do not replace traditional means of protecting the home, such as sturdy and reliable door lock, they are their complements. Even the most expensive door with a clever locking mechanism could only briefly delay the entry of skilled attacker. Besides, burglars often get into office not through the door, but through the windows. And, as experts note, for professionals the presence of bars on

them doesn't matter. Grilles are protruded from the walls with a crowbar, cut off with the grinder, powerful lever shears, a portable gas burner, a jigsaw for metal and other means. The same forces compete with electronic protection systems can not even present "as" a criminal case: motion sensors, volume and open, as well as the control unit itself, of course, can be destroyed, but to stop sending a signal to control security is virtually impossible [5,6].

CONCLUSION

1. Analysis of existing wireless technologies has shown that the existing standards are very well made and there are plenty of actual implementations.
2. The basis of the proposed type of equipment in the wireless Internet access through which the user part of the corporate network may be organized, which satisfies the demand in the variety of traffic, bandwidth, scaling, and the lowest cost in the case of restrictions on the organization of cable access.

REFERENCES

1. Miroshnikov V. Information protection in computer systems. - M.: Finance and statistics, 1997. – 267 p.
2. Shahnovich S. Modern wireless technologies. - Spb.: PITER,2004. – 453 p.
3. Vishnevskiy V., Lyahov A., Portnoy S., Shahnovich I. Broadband wireless transmissions - Spb.: PITER,2004. – 356 p.
4. Jim Geyer. Wireless networking - M.: VILYAME, 2005. – 246 p.
5. http://www.wi-fi.org
6. http://www.wi-fizone.org
7. Jim Geyer. Wireless networking - M.: VILYAME, 2005. – 376 c.
8. http://www.wifi-connect.ru
9. http://www.d-link.ru
10. http://www.ixbt.com

АНАЛИЗ ТЕНДЕНЦИЙ РАЗВИТИЯ СИСТЕМ БЕСПРОВОДНОЙ ПЕРЕДАЧИ ДАННЫХ

Дядичев В., Колесников А.

Аннотация. Проведено исследование систем беспроводной передачи данных в управлении офисом. Рассмотрены способы организации и взаимодействия различных устройств на основе беспроводных технологий. Даны рекомендации по выбору беспроводного оборудования для решения задач офисом.

Ключевые слова. беспроводные технологии, локальная сеть, точка доступа, широкополосный доступ, видеорегистратор, веб-камера, сетевой трафик, масштабируемость, хранилище данных.