MECHANIKA
CZASOPISMO TECHNICZNE
TECHNICAL TRANSACTIONS
MECHANICS
WYDAWNICTWO POLITECHNIKI KRAKOWSKIEJ
2-M/2010
ZESZYT 8
ROK 107
ISSUE 8
YEAR 107

PAWEŁ BRANDYS*

A CONCEPT OF SECURE LOCAL AREA NETWORKS ARCHITECTURE IN UNIVERSITY STRUCTURES

KONCEPCJA BEZPIECZNEJ ARCHITEKTURY SIECI LOKALNYCH W STRUKTURACH UNIWERSYTETU

Abstract

This paper presents a concept of solution of local area network based on dynamic VLAN, QoS and 802.1x authentication for University. In the paper was presented a new concept of the network of the Institute of Computing Science, new access restriction to the network and hardware and software solution of physical and logical topology. Proposed solution ensure adequate level of security and mobility as well as higher efficiency.

Keywords: University LAN, dynamic VLAN, security access

Streszczenie

W artykule przedstawiono koncepcję sieci lokalnej szkoły wyższej opartą na wykorzystaniu dynamicznych sieci wirtualnych VLAN, QoS i autoryzacji dostępu zgodnie z normą 802.1x. Omówiono propozycje nowej topologii sieci w Instytucie Informatyki Stosowanej, metodę autoryzacji dostępu do sieci i sprzętowo-programowe rozwiązanie topologii fizycznej i logicznej sieci. Rozwiązanie to zapewnia odpowiedni stopień bezpieczeństwa i mobilność użytkowników sieci oraz zwiększa jej wydajność.

Słowa kluczowe: sieć uczelniana, dynamiczne VLAN, bezpieczeństwo dostępu do sieci

* PhD. Paweł Brandys, Institute of Applied Infomatics, Faculty of Mechanical Engineering, Cracow University of Technology.

BIBLIOTEKA CYFROWA POLITECHNIKI KRAKOWSKIEJ

1. Introduction

Educational institutions have a unique set of challenges to computer network design. Usual requirements of network users is a high bandwidth and scalability. Additional demand are security and high flexibility. During the past few years, students and university staff can communicate on university network with the use of mobile devices over wireless technology. It is a strong risk for network security. Existing network at the Mechanical Department of Cracow University of Technology do not satisfy requirements in domain of mobility and security. This problem is especially important regarding the skills of an advanced network users which are computer science students. Such students pose a constant threat to network security. They have the ability, time and often the inclination to probe for every weakness in the network security set-up.

This paper presents existing network topology of the Institute of Applied Infomatics of CUT, which was created five years ago, and new proposal for the modern network based on dynamic VLAN, QoS and 802.1x authentication. This proposal will be easy to extend on Mechanical Department or even University network. Obviously, it requires a hardware and software modernization.

2. Existing network topology

Existing network of the Institute of Applied Informatics based on Fast Ethernet topology with unmanaged switches. In this network exists about 120 computers and 7 servers. Network equipment and servers was located in a IDF (Intermediate Distribution Frame). A large majority of computers are located in 8 computer laboratories. One of the laboratory has own DF. Rest of computers are in staff offices which are located in two buildings. Institute network consist of a few network printers as well as WLAN Access

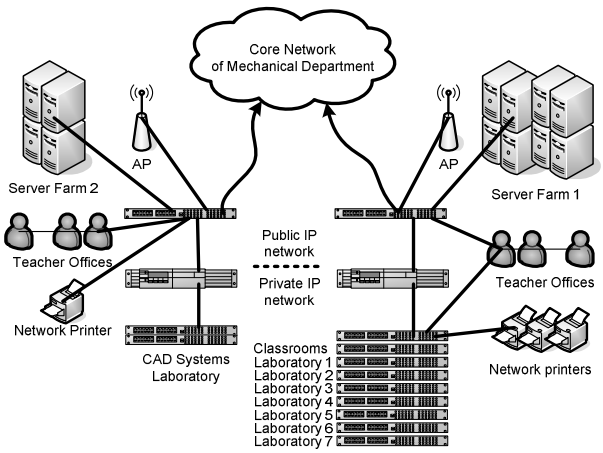

Fig. 1. Diagram of existing network topology of the Institute

Rys. 1. Schemat aktualnej topologii sieci w instytucie

BIBLIOTEKA CYFROWA POLITECHNIKI KRAKOWSKIEJ

Points. Servers are located in a public area on department network. Each subnet is connected to department core network trough a router with NAT and firewall. Normal communications between subnets is impossible. At each subnet there is non-security communication between any computers. Description of above network is shown schematically in Fig. 1.

3. Problems of the Institute network

Analyzing the network of the Institute the following problems might be noticed:

- Difficult communications between subnets disturb non-failure operations with license servers, network printers and others;
- Network users are very mobile – students and staff typically move between many locations in the courses of a day, from classrooms to labs, to libraries to offices;
- Restricting physical access to network connection points is very difficult in a mobile environment, because students, staff and even ordinary people frequently
- come and go between buildings, and it is almost impossible to monitor all of them all the time. In spite of this, parts of the network must be kept secured. Staff must have access to certain network resources, particularly server drives, to which students must not have;
- Fast Ethernet topology in the core network is inefficient. Particularly this concern a server farm.

4. The proposal of the network

Proposal of the network will base on VLAN functionality directly connected with 802.1x authentication protocol on the edge switch ports. An additional requirements is higher efficiency in the core network what can be realized by application of a Gigabit Ethernet topology. The solution has to also guarantee the access to the network only for trusted users and computers. Dynamic VLAN puts a verified users into an appropriate VLAN, based on their authentication credentials. Therefore users share the same network environment no matter which place they connect from. The 802.1x authentication protocol and dynamic VLAN assignment prevent unauthorized access to the network while still giving users appropriate access to network resources, regardless of where they physically connect to the network. The 802.1x authentication protocol ensures that users cannot even send packets into the network until they have provided valid authentication credentials.

Another issue of the solution is hardware filtering on the switch in the core. Hardware filters guarantee no leakage of traffic between certain IP subnets. A different restriction is necessary on the edge switches. There must be no communication at all between different hosts in the student VLAN, to stop students from looking at each other accounts.

Physically, the solution consists of managed switches on the edge with gigabit uplinks back to a Layer 3 switch in the core. But the real value in the network lies in the features that are implemented on these switches. In particular, the key requirements of simultaneous flexibility and security are provided by the 802.1x authentication process.

BIBLIOTEKA CYFROWA POLITECHNIKI KRAKOWSKIEJ

4.1. The VLAN

In basic proposal the network consists of 5 VLANs. Some of the VLANs reach right out to the edge of the network, and some are confined just to the core. The VLANs are:

– Staff VLAN (VID = 10). This VLAN reach to the edge of the network, and staff members are placed into this VLAN, based on their user IDs.
– Servers VLAN (VID = 20). The VLAN that contains the Institute servers. This VLAN has to extend to the uplink port of each edge switch, because it includes the RADIUS servers used by 802.1x.
– Printers VLAN (VID = 30). The VLAN that contain the printers for the Institute. This VLAN is constrained to the core of the network and to the edge switch in other building.
– Students VLAN (VID = 50). The VLAN into which 802.1x places students when they connect. This VLAN gives them only the access to the servers the students need. It reaches to the edge of the network.
–Firewall (VID = 5). The VLAN that contains the firewall, to provide access from the network out to the Department Core Network.
– Untrusted (VID = 500). The guest VLAN that ports reside in by default (except for the ports that are permanently reserved for servers, printers, edge switches, the firewall, and the uplink from an edge switch to the core). When a port receives valid authentication credentials, it is taken from this VLAN and put into the VLAN relevant to the person who has just been authenticated on the port.

4.2. Details of the network

Figure 2 shows a diagram of the network. All ports of edge switches are permanently in the untrusted VLAN if they are not assigned to other VLAN by authorization process.

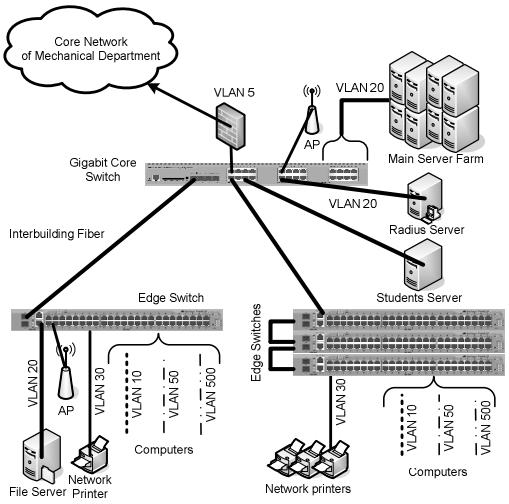

Fig. 2. Diagram of proposal network topology of the Institute

Rys. 2. Schemat proponowanej topologii sieci w instytucie

BIBLIOTEKA CYFROWA POLITECHNIKI KRAKOWSKIEJ

4.3. Communication between the VLANs

This proposal strictly controls whether hosts in different VLANs can communicate with each other. The untrusted VLAN cannot send data, so in effect it cannot communicate with any other VLAN.

Basic solution assumes full communication in the network for staff VLAN, limited access for students VLAN and no access for untrusted users (blocked already on the switch port). In case of necessity the number of users group can be extended as well as access policy for users. The table below shows which VLAN user can (Y) and cannot (–) communicate with others.

Table 1

Communication between the VLANs

VLAN	Staff	Servers	Printers	Students	Firewall	Untrusted
Staff		Y	Y	–	Y	–
Servers	Y		–	Y	Y	–
Printers	Y	–		–	–	–
Students	–	Y	–		Y	–
Firewall	Y	Y	–	Y		–
Untrusted	–	–	–	–	–	

To create the above restrictions, this configuration can be obtained in the following way: on the core switch, a set of hardware filters blocking communication between the IP subnets used on different VLANs. On the edge switches, inter-VLAN communication does not need to be blocked by filters. This is because 802.1x puts the edge ports of those switches into one of only three possible VLAN's – staff, student, untrusted – and these VLANs do not have Layer 3 interfaces on the edge switches. There is no possibility of Layer 3 switching between them. However, there must be no communication at all between different hosts in the student VLAN, to stop students from looking at each other accounts. Instead, this configuration uses a clever set of L3 filters to block any traffic in the student VLAN between pairs of edge ports, and to force broadcast/multicast packets in the student VLAN up to the network core.

5. Hardware solution

To implement the idea of the network it has to be used switches with 802.1Q VLAN, 802.1x features. Devices of Allied Telesis are recommended for the proposal due to the fact that core network of the CUT is based on the devices of Allied Telesis. It is also convenient to have all hardware compatible.

At the core of the network is a AT-9924T switch. It is 24-ports managed gigabit ethernet switch Layer 3 with 4 SFP Combo ports to Fiber Optic modules. At the edge switches can be any of Fast Ethernet managed switches Layer 2+ with Gigabit uplink ports like AT-8600 series switches or new AT-8000S series switches.

BIBLIOTEKA CYFROWA POLITECHNIKI KRAKOWSKIEJ

6. Conclusions

Existing network at the Mechanical Department of CUT does not satisfy requirements for high bandwidth and security. Modern network equipment ensure scalability and high flexibility. It is possible to achieve this by using dynamic VLAN and based on authentication credentials according to 802.1x standard.

Solution that fulfill such requirements was proposed on example of the network of the Institute of Computing Science. It might be extended on the network for the Mechanical Department of CUT.

References

[1] T a n e n b a u m A.S., *Sieci komputerowe*, Wydawnictwo Helion, Warszawa 2004.
[2] O p p e n h e i m e r P., *Projektowanie sieci metodą Top-Down*, PWN, Warszawa 2007.
[3] Hardware Manual, White Papers and How To Notes, Allied Telesis Resource Center.

BIBLIOTEKA CYFROWA POLITECHNIKI KRAKOWSKIEJ