Self-defining Virtual LANs (Auto-VLANs) with Access Authorisation

Grzegorz Górski, Józef Wozniak
ggorski@unizeto.pl, jowoz@pg.gda.pl

Information Systems Department, Faculty of Electronics Telecommunications
and Computer Science, Technical University of Gdansk
Gdansk, Poland

Abstract

There are several ways of controlling the access to network resources. Among them directory services seem to be the most popular ones. They assume that there is one central database with all necessary information about users and their particular rights. This solution is strongly promoted by network operating systems manufacturers, due to the fact that directory services are essential parts of their systems. However, these solutions allow, only partially, to administrate modern networks [1].

In the paper authors present an alternative method, which could be implemented in heterogenic environments, i.e., in networks in which software and hardware elements are supplied by different manufacturers. Instead of describing a membership of a given station in a virtual group the proposed algorithm takes into account a user identifier and a set of rules previously defined by a network administrator. A user whose login requirements were verified successfully can gain an access to available resources. New stations can be included into a virtual group based on their attachment to a physical port of a switch, or after satisfying an access rule or authorisation process. All three methods are shortly presented in the paper. Owing to the centrally organised authorisation procedures all users' requests for accessing shared resources can be audited and their results can be written to log files. In the described algorithm three main components have to be implemented in the network environment, i.e., authorisation server, agent and client. Verification process assumes that all three components exchange confidential information and therefore proper secure channels must be created.

The presented algorithm allows for creation and handling of dynamically changing virtual groups. It also significantly improves security of accessing network resources.

Keywords: directory services, static and dynamic virtual LAN, Auto-VLAN, VLAN with authorisation, authorisation server, agent and client, verification process.

1. Introduction

One of the most interesting features of modern switched networks is a possibility to create VLANs (virtual local area networks). A collision domain, defined as a group of workstations communicating with one another, and connected to a common broadcast transmission medium, is one of basic factors of throughput in LANs with a non-deterministic (i.e., CSMA\CD) access method. Contrary to traditional LANs, segmented by bridges, modern LANs with switches can concurrently transmit data between pairs of ports or even send broadcast messages to defined groups of ports (broadcast domain). A VLAN service [2] is then defined as a group of workstations (computers) belonging to different segments (connected to different ports) which can communicate with one another as if they belonged to the same collision domain (local network). There are several methods defining a membership of given computers to specific virtual networks. Although the main concept of VLAN is quite simple, switch providers have developed several different methods [3] to define the membership in a specific VLAN. Very simple but at the same time very popular VLANs offer membership either by port grouping or by MAC addresses. There are also layer 3 based VLANs, IP multicast groups or VLANs based on logical rules. The choice strongly depends on environmental factors, so there is no best method for each real network topology.

2. Dynamic virtual LANs

There are two different kinds of virtual groups. First, mentioned in introduction, is called a static VLAN. The static VLAN algorithms are based on a principle that an administrator statically (off-line mode) associates a given workstation with a VLAN. Based on address information included in incoming packets station creates a list of virtual groups it belongs to. The second type of VLANs are dynamic virtual groups. This kind of network protocols appeared a few years ago when switches started to process control information inserted in packets by the third and higher layer protocols (according to ISO/OSI internetworking model). Unfortunately, dynamic VLAN algorithms have not been commercially implemented yet.

Dynamic VLANs assume that number of computers in a group can vary in time. Because of that dynamic VLAN protocols must additionally handle workstation login and logoff processes. These protocols do not require any administrator intervention so they are called Auto–VLANs. Membership in dynamic groups can depend on types of applications, services launched by a user (for instance mail services available on a chosen TCP port number) or user identifier. VLAN with access authorisation is one of the good examples of dynamic virtual groups. Authorisation process can take into account one of three possible factors, namely: physical port, logical rule or user identifier. User verification, based on a physical port identification, assumes that the administrator defines a switch port as an element of a trusted virtual group. Based on it the whole packet traffic incoming through the port is regarded as authorised. However, this simple solution does not guarantee any high security level. This disadvantage is improved in the model with a logical rule, where a switch port is associated with a list of user network addresses. Only conjunction of a physical switch port and valid user address can guarantee successful user verification. User identifier is the last factor, which can be used in the authorisation process. This method allows for the most secured access to network resources. It implies however, that the required protocol is the most complex one.

3. Virtual LANs with access authorisation

A presented protocol allows for flow control of packets. It assumes utilisation of a user identifier and a set of rules (rights) defining network privileges associated with a given user account. According to this method user can only access resources designated for him not necessary all available in a virtual group. A user can join its virtual LAN only if its login request is verified successfully. Administrator creates users' profiles, which consist of list of network resources and periods of time they are available. Owing to the fact that the authorisation process is centrally managed all user requests can be audited and their results can be written to log files.

A virtual LAN with access verification consists of three independent components. An authorisation server stores users' profiles (this information includes: user identifier, password, verification method, list of available resources, periods of time when a user can login). The sever must also contain addresses of all switches directly connected to it, and proper authorisation keys for establishing secure channels for exchanging data with other protocol components. Another VLAN component is a authorisation agent. Authorisation agents are installed as dedicated software in switch operating systems. Implementation of this component strongly depends on a switch model and its firmware. Due to this fact, however, the agent software can be used in heterogenic network environments. The agent operates in one of two modes, namely, standby mode - if there is no active VLAN group, and active mode in the opposite situation. Any time an authorisation agent is launched, a secure channel to the main authorisation server is created. For security reasons each agent keeps a list of authorisation servers used when the main server fails. Such configuration requires independent definition of the IP address and an authorisation key (for cryptographic algorithm) for each available server. An authorisation agent is a central protocol component, which takes part in verification process and for security reasons separates the authorisation server and clients. All of user resource access requests must be processed by the agent. Due to this, the monitoring program has to be additionally implemented in the switch. It counts down number of unsuccessful users' logins and sends a trap message to the system administrator. The last element of the proposed VLAN structure is an authorisation client. A client dedicated software is installed on PC computers for communication with authorisation agents. The client has to discover network addresses of available agents - that is why login process usually starts with a broadcast packet from a client workstation. Such solution does not require unique client software configuration for each computer in a network.

The described algorithm has been divided into three main steps. Transmission of a user login request initiates the first step. An authorisation client discovers IP addresses of switches with installed agent services and sends authorisation descriptor to an agent using a TCP port appropriate for this service - previously defined by the administrator. This step is presented in Fig. 1.

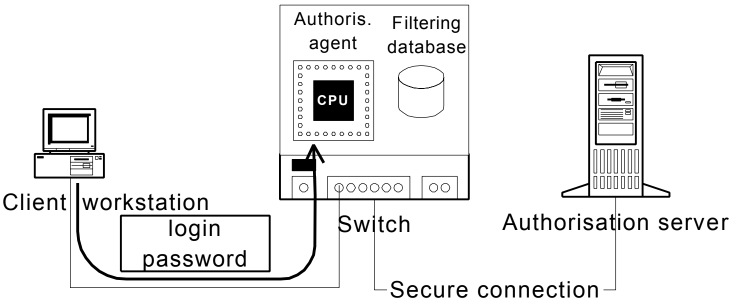

Figure 1. First step of the authorisation process – user login request.

In the next step, the authorisation agent processes an incoming request. First it adds to user's descriptor new information like login time, user address and switch port, and then sends it to the authorisation server using previously established secure channel. Based on information included in the descriptor like user identifier, password, network address, system time, the authorisation server decides to grant user access to network resource or not. This is the third and the most important step in the whole verification process. In the case of successful authorisation the server completes the descriptor with a list of network resources available for a given user and sends it back to the agent.

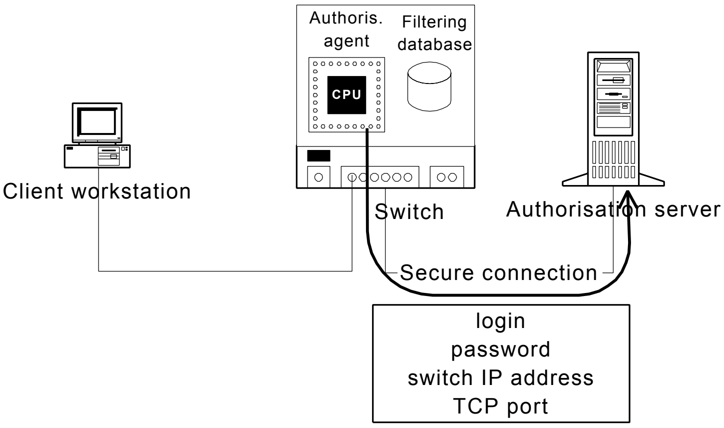

Figure 2. Second step of the authorisation process – agent processing.

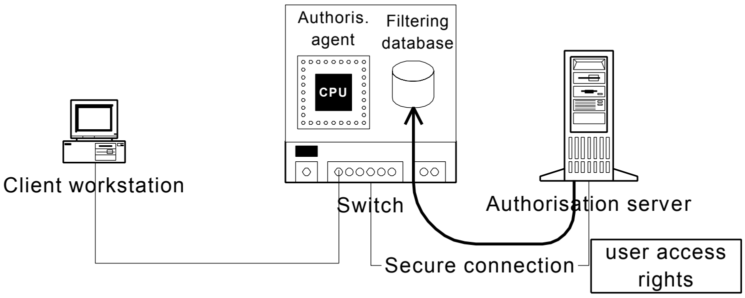

Figure 3. Third step of the authorisation process – server processing.

Upon receiving a full user descriptor by the authorisation agent it first writes the information concerning a processing request to a log file. This action is the beginning of the last step of the authorisation process, which is called a filtering database modification. Based on the list of available resources coming from the server the agent associates resources with their network localisation. Such a user table is only a part of the entire available network resources database, which authorisation is handled by the agent. The user table is then used by a switch CPU for controlling the traffic incoming from and sent to a given user.

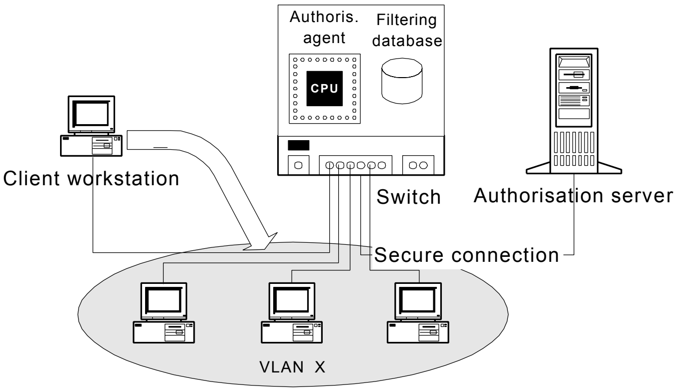

Figure 4. Fourth step of the authorisation process – filtering database modification.

Auto-VLAN protocols must also handle a logoff activity. Typically disconnection of a station from a network resource can be done after the agent receives a logoff request from a client. However, there maybe several abnormal session terminations. For instance, if a switch discovers a lack of a signal on a user physical port it disconnects the workstation from the authorised VLAN. Other reasons for connection termination include: long station idle time intervals, or a too long period of time when a given resource is accessed. The last information is sent from the authorisation server during the third step of the verification process.

The following diagrams present three typical sequences for the designed protocol taking place during user login and logoff processes.

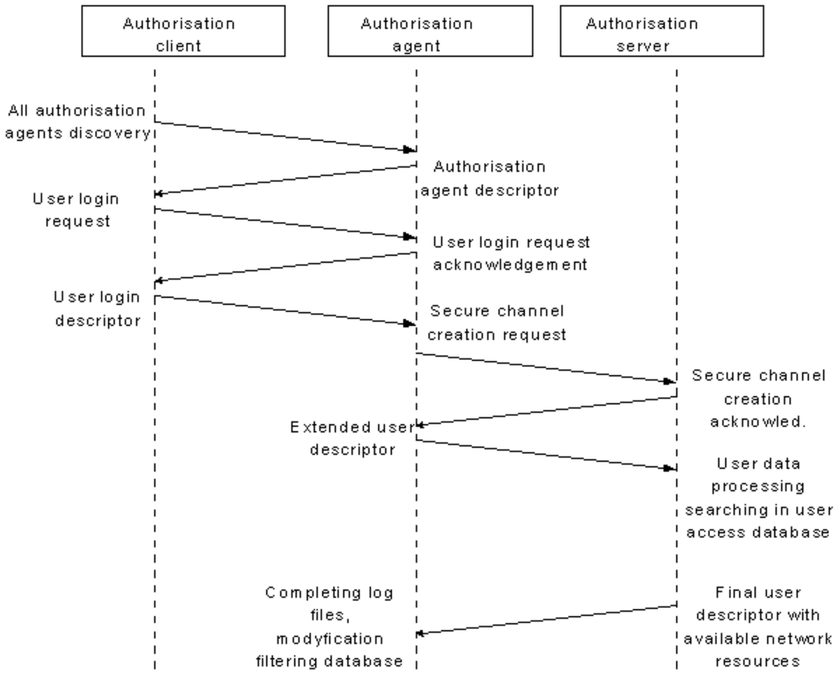
Authorisation client
Authorisation agent
Authorisation server
All authorisation agents discovery
Authorisation agent descriptor
User login request
User login request acknowledgement
User login descriptor
Secure channel creation request
Secure channel creation acknowled.
Extended user descriptor
User data processing searching in user access database
Completing log files, modyfication filtering database
Final user descriptor with available network resources

Figure 5. The user verification process diagram.

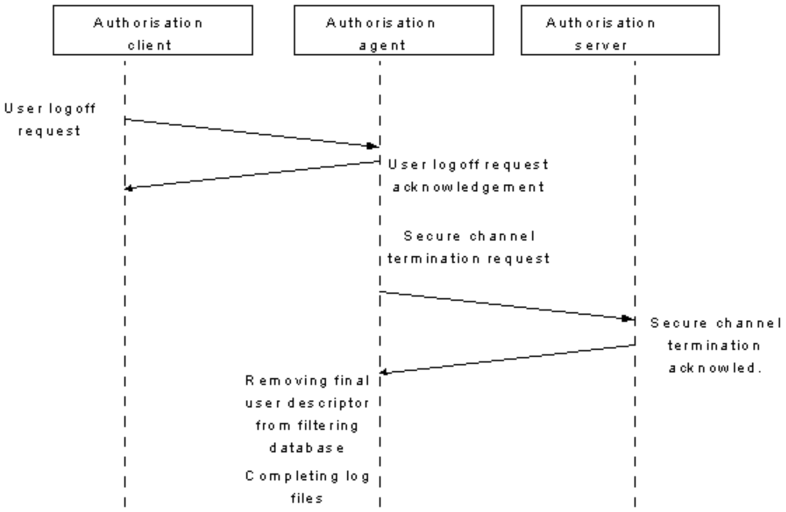
Authorisation client
Authorisation agent
Authorisation server
User logoff request
User logoff request acknowledgement
Secure channel termination request
Secure channel termination acknowled.
Removing final user descriptor from filtering database
Completing log files

Figure 6. Diagram of the user logoff process arranged by authorisation client.

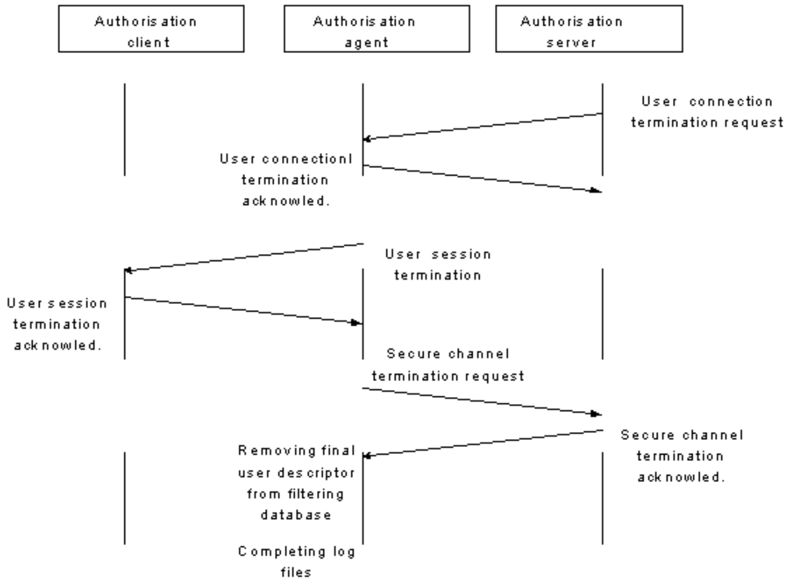
Authorisation client
Authorisation agent
Authorisation server
User connection termination request
User connectionl termination acknowled.
User session termination
User session termination acknowled.
Secure channel termination request
Secure channel termination acknowled.
Removing final user descriptor from filtering database
Completing log files

Figure 7. Diagram of the user logoff process triggered by an autorisation server.

To improve security level all packets coming form clients (network addresses) different from those registered in the user verified list are discarded at switch ports.

4. Security of the dynamic VLANs protocol

Security of operation of dynamic VLANs with access authorisation strongly depends on the way how protocol components exchange confidential information. The presented protocol assumes that communication between an authorisation agent and an authorisation server uses a secure connection and all data is encrypted. There is a limited number of authorisation agents which requests can be processed by the server. Administrator can easily create in off-line mode a profile containing cryptographic keys for establishing secure connection for each agent in authorisation server database. Because of that the most important security issue of the proposed protocol is user's autorisation process. User verification process given in Fig.5 presented overall information exchange among authorisation client, agent and server. In this chapter the authors describe authorisation process with details.

Authorisation is a procedure the network follows to verify or validate a request from a user. The procedure usually occurs in the background and is not seen by the user. Authorisation called sometimes authentication guarantees the following:

- Only the purported sender build the message.
- The message came from the workstation where authentication data was created.
- The message contains no information counterfeited form another session.
- The message has not been tampered with or corrupted.

Authentication starts with the initialization process. When the user logs in, the authorisation agent sends the client (workstation) an encrypted private key, a key specific to this user. The user's password is the key for the encryption. The workstation decodes the private key with the password and removes password from workstation memory. The workstation then creates a data structure called an authenticator. It contains information identifying the user, the workstation and the session. Next the client creates an encryption, called signature, using the authentication information and the private key. The private key is then removed from memory, while the authenticator and signature remain in memory throughout the entire session. The signature identifies that the user is valid. With these components, the client can authenticate itself. A request for authentication is sent to the authorisation agent and includes the message, the authenticator and a proof. A proof is an encryption based on signature and the message (signature never leaves the client). The authorisation agent validates the proof as an authentic construct of the authenticator, the private key and the message.

5. Conclusions

VLAN technology seems to be a very efficient vehicle for management of operation of users deployed to LANs segmented with switches, bridges or routers [3]. For the growing VLAN market it is important to commercially implement efficient algorithms for dynamic virtual groups. They will operate without administrator intervention and tune the size of virtual groups, according to user demands. Auto-VLAN can be created taking into account applications, services or user identifiers. VLANs with access authorisation can be an alternative solution to directory services in heterogenic environments. Proper implementation of such an algorithm allows for control of the packet traffic inside and outside virtual groups, and improves security in the access to network resources.

6. References

[1] Górski, G., Wozniak, J.: Metody zarzadzania zasobami w nowoczesnych sieciach heterogenicznych, in Proceedings of Krajowe Sympozjum Telekomunikacji'99, Bydgoszcz, vol. C pp.304-310, 1999.

[2] IEEE Standards for LAN and MAN: Virtual Bridged LAN. Draft Standard P802.1Q/D9, 30th July 1998.

[3] Górski, G.; Malicki, K., Wozniak, J.: Simulation models for different VLAN Solutions, in Proceedings of the 13th International Conference on Systems and Science, Wroclaw, vol. III pp.29-36, 1998

[4] Górski, G., Wozniak J.: Dynamic virtual LANs with access authorisation, in Proceedings of IX Regional Conference On Military Communication And Information Systems 2000, Zegrze, vol.III 89-93, 2000.