Network Access Control on Internal LANs. EAPOL-based security

Associate Professor, Ph.D. Victoria Iordan
West University of Timisoara

REZUMAT. Articolul prezintă câteva studii legare de controlul accesului la rețea, tehnologii şi protocoale implementate şi administrate cu scopul de a reduce la minimum riscul şi efectele unui acces neautorizat la resurse. Lucrarea prezintă câteva protocoale care rezolvă problema controlului accesului la rețea: protocolul **PPP** (Point-to-Point Protocol), care stabileşte termenii de negociere, menținere şi încheiere a comunicației, protocolul **EAP**, care descrie mecanisme de autentificare şi protocolul **RADIUS,** care asigură servicii centralizate de autorizare. Toate acestea permit o administrare şi o monitorizare centralizată a aspectelor legate de controlul accesului la rețea

1 Introduction

Network access control represents the set of mechanisms, technologies and protocols implemented and administrated with the purpose of reducing to minimum the risk and effects of an unauthorized access to resources.

The efficiently and useful authentication, resource access authorization and monitoring need considerable efforts from the interested companies. Large or small companies offer information and services for clients or for their own employees through Internet. Remote access through common telephone lines (dial-up), through the configuration of a communication structure like intranet or extranet, through VPN or wireless technologies enhance the internal activity and the contract with the potential clients or partners.

The resource (information and services) protection from unauthorized access is a must and a priority for all the beneficiaries of the new IT technologies. So the security services centralization is necessary for the

efficient network administration and extended services that are continuously growing. New standards are being define and some old ones are being enhanced, new communication mechanisms are being created or some of the old ones that are not used any more are being reviewed, as there is an ongoing IT community that is full of ideas.

The PPP Protocol (RFC 1661) and the wide implemented authentication mechanisms, for example the EAP Protocol (RFC 2284) together with the centralized authentication services, for example the RADIUS Protocol (RFC 2865), allow an administration, centralized monitoring of aspects referring to network access control.

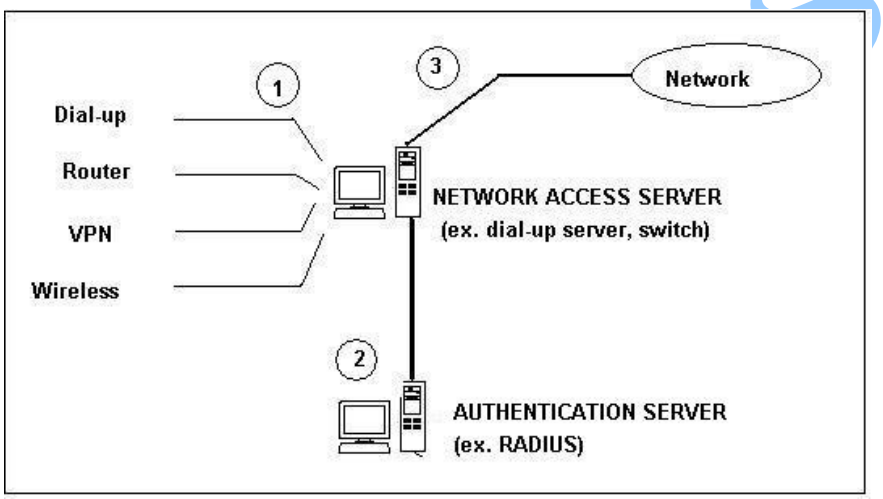

Fig. 1. Network Access Control Model

Fig. 1. represents an easy to implement scheme for network access control. The generic terms NAS (Network Access Server) and AS (Authentication Server) may represent another kind of devices, from switches to dedicated servers.

The Nortel Baystack 450-24T switches offer the possibility of using the EAPOL (EAP over LAN) technique for authentication and authorization, cooperating for that cause with a RADIUS server from Microsoft, IAS (Internet Authentication Service).

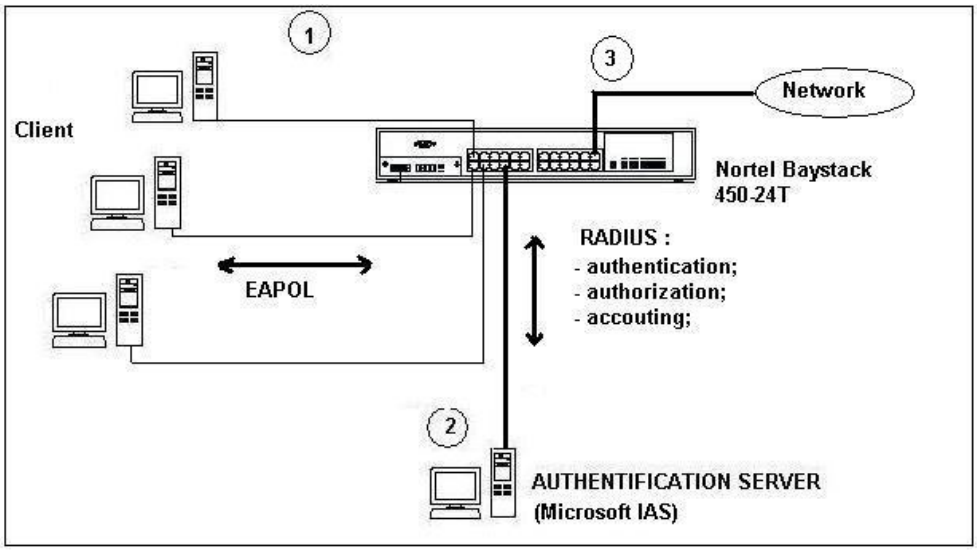

Fig. 2. UVT Network implementation

2 The PPP Protocol

The interconnection mechanism between two devices through a simple direct, full-duplex connection is based on the exchange of messages and the setting of the specific parameters, from the data link point of view as well as from the network protocols supposed to be used.

The PPP protocol defines the elements of a point-to-point link, describing the terms of negotiation, maintenance and closing of the communication. These terms are being defined through the following elements (cf. RFC 1661):

a) multi-protocol packets encapsulation;
b) LCP (Link Control Protocol) for the initiation, configuration and testing of the link;
c) NCPs (Network Control Protocols) for the establishment and configuration of the different network protocols used.

The multi-protocol packets encapsulation offers the possibility of multiplexing much many protocols at a network level simultaneously on the same data link. This way IP, IPX packets can be transmitted at the same time.

LCP (Link Control Protocol) gives PPP portability and control in different communication media. Through LCP, specific data link options are

negotiated, also the testing and closing of the link, and further more authentications of the calling devices.

NCPs (Network Control Protocols) have the role of administration the parameters that is specific to each network protocol that is being used.

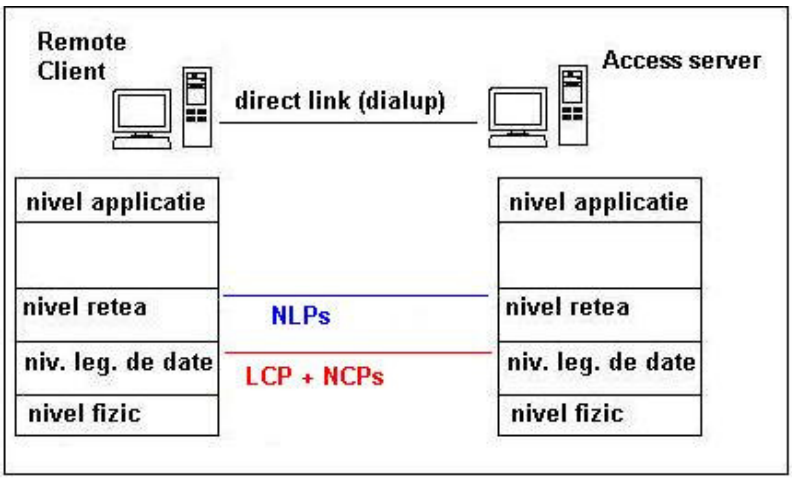

Fig. 3 The action level for LCP, NCPs and NLPs

The authentication, as a security mechanism, guaranties communication between two authorized partners. The communication is negotiated, takes place and closes before the transmission of the high-level protocol packets (NLP). Conform RFC 1661 the authentication phase happens after link establishment phase, but before network-layer phase.
So:

1. **Link establishment phase:**
   a) transmission/receiving of LCP packets for link establishment;
   b) the negotiation of an authentication protocol (PAP, CHAP) and the upper layer protocols that could be used, simultaneously, during communication;
2. **Authentication phase:**
   a) transmission/receiving packets for the authentication protocol that has just been negotiated;
   b) if the authentication succeeded then move to the third phase, else close connection;
3. **Network-layer phase:**
   a) transmission/receiving packets for the network-layer protocols initially negotiated (IP, IPX).

3 EAP PROTOCOL

EAP (Extensible Authentification Protocol) allow the negotiation of many authentication mechanisms (RFC 2284). Unlike PAP or CHAP, two common protocols used by PPP, EAP intermediates the establishment of a third authentication protocol between partners. The advantage is the possibility of using multiple authentication mechanisms, easily extensible, implemented on a diversity of security servers.

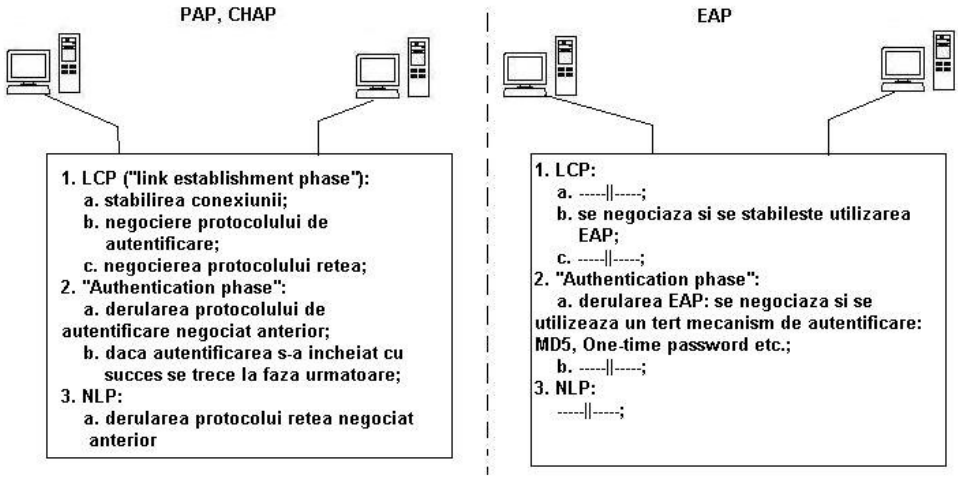

Fig. 4 The difference between EAP and other PPP common authentication protocols

An EAP packet format is:

Code (8 bits)	Identifier (8 bits)	Length (16 bits)	Data

Code : represents the type of the EAP packet.

1 - Request
2 – Response
3 – Success
4 – Failure

Identifier: identifies a request and the corresponding response
Length: represents the length of the EAP packet
Data: contains useful information, depending of the type of the packet specified in Cod

The EAP packets encapsulation through PPP is represented in short like this:

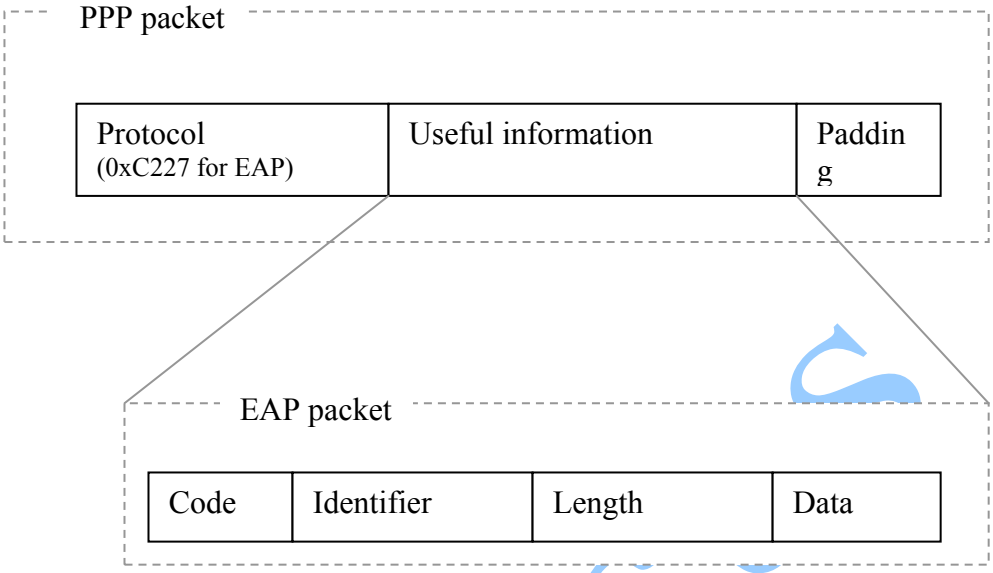

Fig. 5 EAP encapsulation over PPP

4 RADIUS Protocol

RADIUS (Remote Authentification Dial In User Service) is a transport protocol that caries the control, authorization and authentication information from the client, to client device, named access server, to an authentication server.

Remote Access through serial, dial-up or dedicated lines, through modems or other corresponding devices, imposes the creation and administration of an authorized users base, their authentication and authorization being implemented through several security mechanisms.

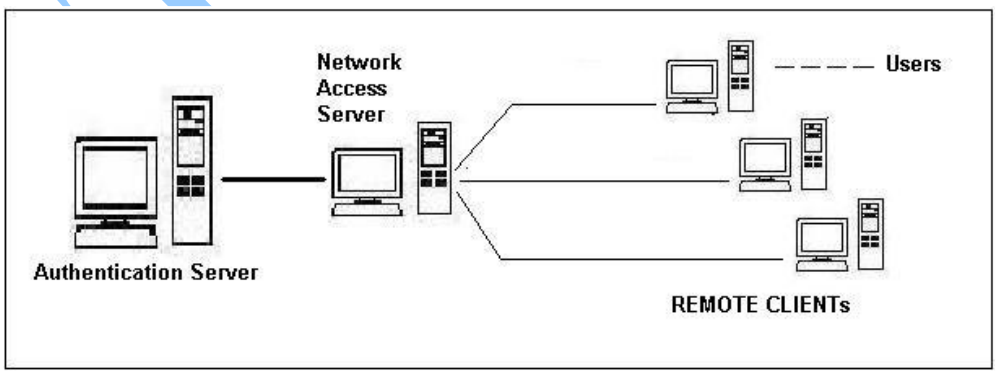

Fig. 6 Control topology of the network access in case of external remote connections

The access server communicates with the client remote, asking the users for their authentication elements (i.e. name and password). Depending on the negotiated protocol during the interrogation, the access server can call UN external server, authentication server, giving it the identification elements that the users provided. In this situation, through its mechanisms, the RADIUS server has the role of access authentication and authorization of a user for the services that are being solicited (UNIX login, rlogin, telnet). For example, in the situation of some remote Windows 2000 clients that are connected through dial-up, this could mean the authentication of those users by consulting an Active Directory service situated on a network domain server.

Access and authentication server's interconnection can be realized in three common schemes (the following figure).

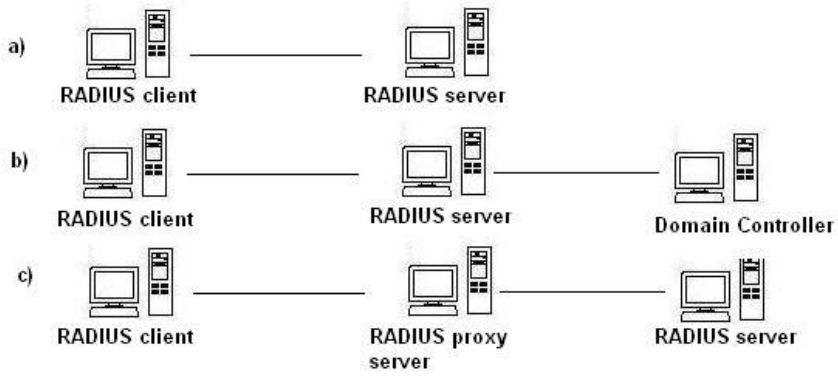

Fig. 7 Three common topologies for the interconnection of the access and authentication elements

The client side (access server) may be: dial-up server, VPN server, Wireless Access Point, Ethernet switch, DSL etc.

The server side (authentication server) may contain the RADIUS module, as well as the directory client authentication and authorization service.

There are 6 types of messages:

- Access-Request;
- Access-Accept;
- Access-Denied;
- Access-Challenge;
- Accounting-Request;
- Accounting-Response.

RADIUS packets have 2 components:

Header	Attributes

Attributes are defined in many documents, standard and proprietary. Where is the case of Nortel Baystack switches VLANs, PVID and priorities can be specified:

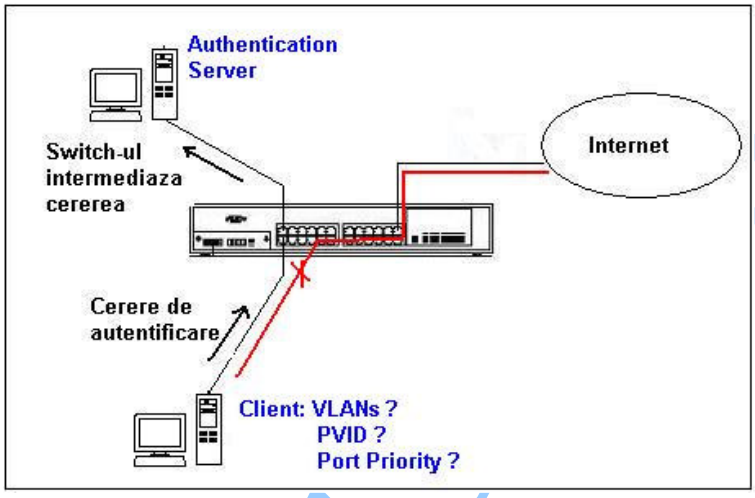

Fig. 8 Authentification request

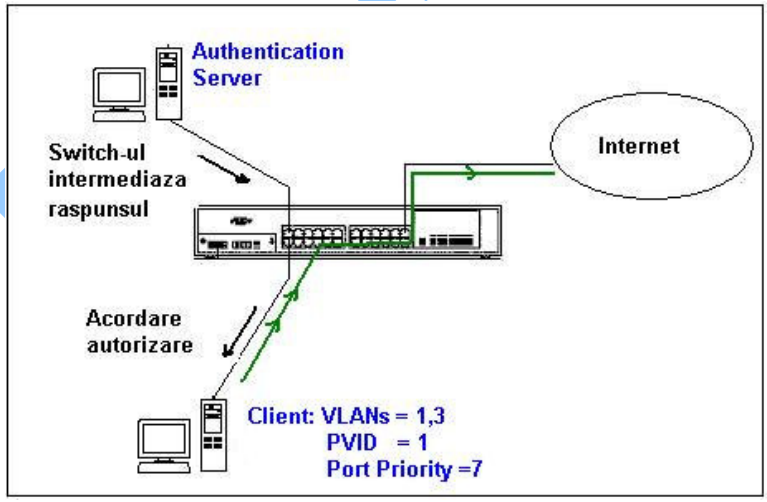

Fig. 8. Network access authorization and authentication, VLAN + Priority –dynamic configured;

5 EAPOL Based Security

Port level network access control is based on the implementation of the authorization and authentication services laying on the physical access characteristics in the LAN networks. EAPOL is the security mechanism based on the EAP protocol, which allows network access control through the use of some standard authentication and authorization protocols.

IEEE 802.1X is a standard adopted for the reglementation of authentication mechanisms adopted by the devices compatible in LAN IEEE 802 networks (IEEE 802.3 Ethernet, IEEE 802.11 Wireless), detailing the aspects referring to port level network access control.

The components of a LAN network access control are (cf IEEE 802.1X):

- Authenticator: the entity from one end of a point-to-point network segment, which has the task of authentication the entity that is connected at the other end of the segment;
- Supplicant: the entity from one end of a point-to-point network segment, which will be authenticated by the entity connected at the other end of the network segment;
- PAE (Port Access Entity): logical module that implements the needed algorithms and protocols for the authentication realization;
- Authentication Server: the entity that offers the authentication service of an authenticator;

Shortly, the above elements can be represented like this:

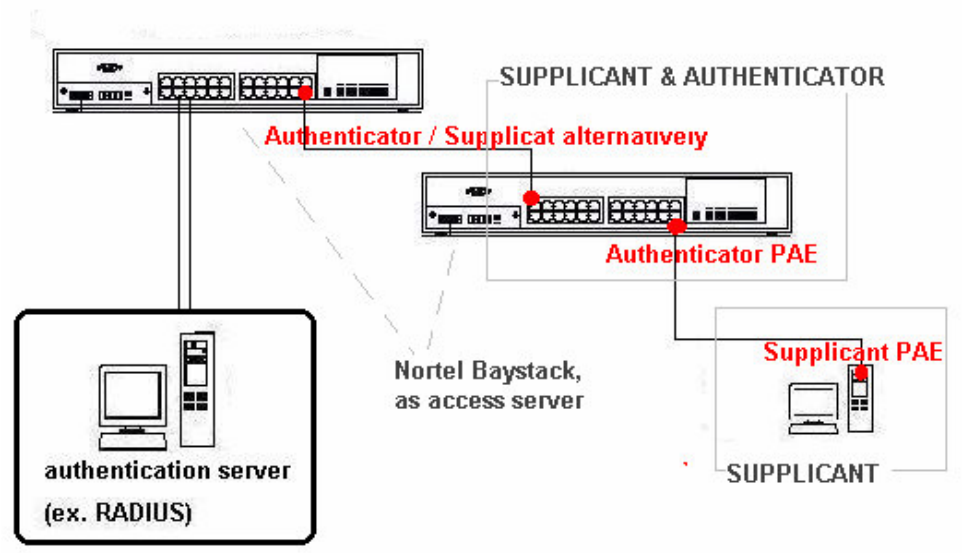

Fig. 10

EAPOL defines an encapsulation mechanism of the priory described EAP protocol on different access physical media, for example 802.3 Ethernet and Token Ring. The encapsulated packets are transmitted to the access server for the authentication and authorization process, taking advantage from a specialized server services, for example Microsoft IAS.

The content of an EAPOL packet in an Ethernet environment is:

PAE Ethernet Type
Protocol Version
Packet Type
Packet Body Length
Packet Body

***PAE Ethernet Type*:** dimension 2 bytes, integer value which represents the Ethernet type assigned to a PAE entity;

***Protocol Version*:** dimension 1 byte, integer value that represents the EAPOL version implemented by the entity, which transmitted the packet;

***Packet Type*:** dimension 1 byte, integer value which represents the type of the transmitted packet, i.e. EAP – packet, EAPOL-Start, EAPOL-Logoff;

***Packet Body Length*:** dimension 2 bytes, integer value which represents the dimension (bytes) of Packet Body;

***Packet Body*:** variable dimension contains packet type specified by Packet Type field, for example an EAP packet.

The order of transmitted and received messages through a usual configuration of network access control with EAPOL can be represented like this (fig.11):

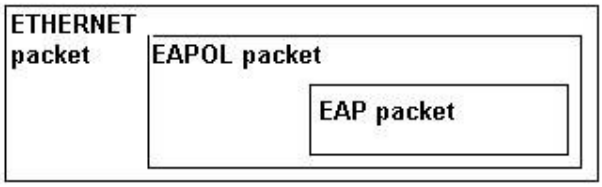

Fig. 11 EAP packet encapsulation in an Ethernet Network

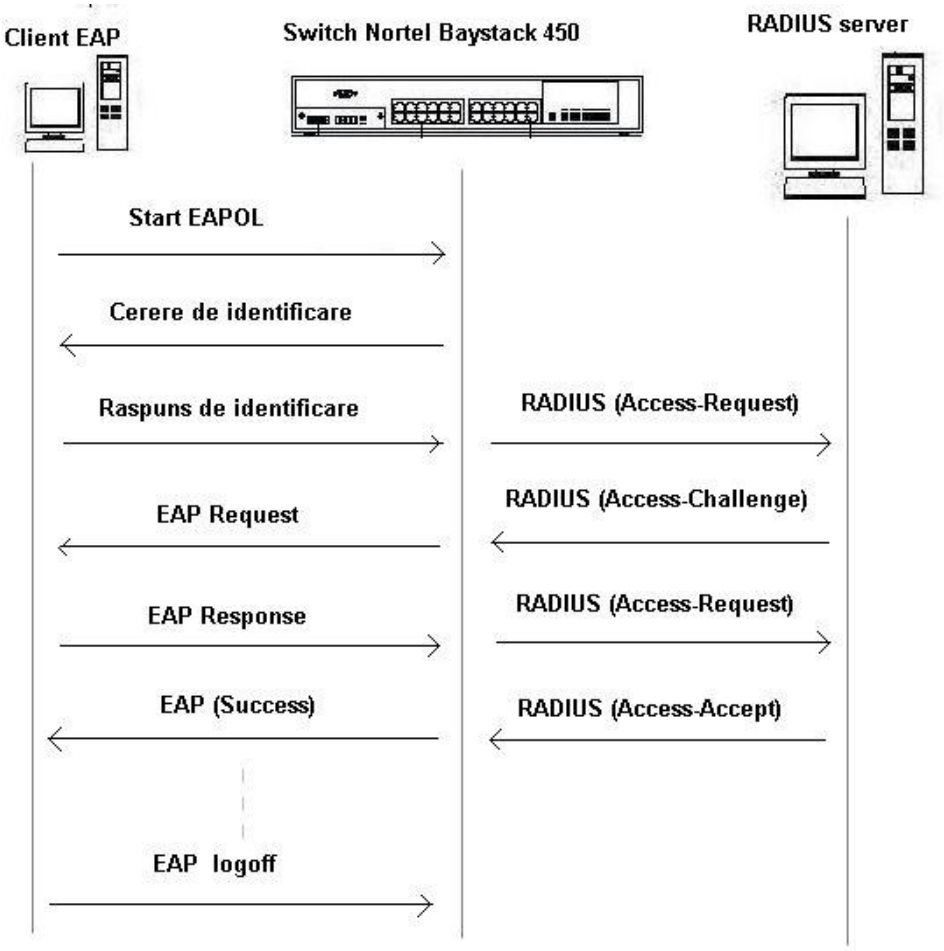

Fig. 12 Delivery of Messages through un usual configuration with EAPOL

6 Conclusion

The open manner in which local network are typically implemented enhances the risk of unauthorized access. The cables and commutation equipments (switches) infrastructure represents the elements that are physically exposed to public access, through systems that are already in use and through adding others, unauthorized.

The physical level security mechanism, like MAC filtration, are hard to administrated under complex, dynamic network conditions and external remote access.

The need to realize the authentication at the first point of physical contact with the network which led to the standardization of some security mechanisms based on access authorization to resources.

Port level security through authentication at the user level represents a flexible and scalable solution in actual network environments. The scalability derives from the possibility to protect many switches using a single RADIUS server. The integration in an actual authentication system is also possible with users that initiate dial-up, wireless, leased lines, DSL connections...

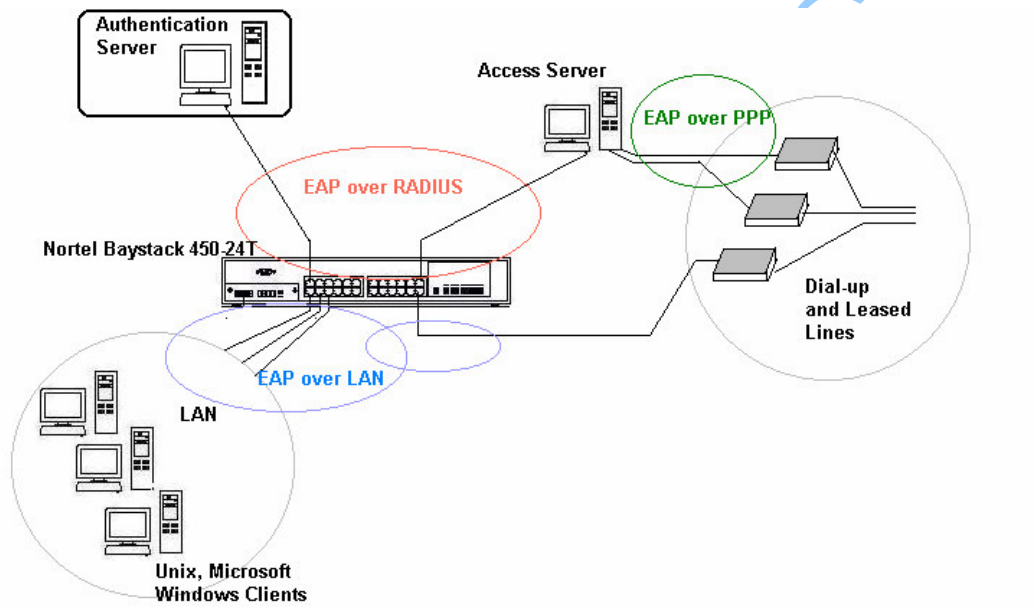

Fig. 13 EAPOL control mechanism integration in a bigger security system

References

[1] **RFC 1661**, "*The Point-to-Point Protocol (PPP)*", 1994;

[2] **RFC 2284 ,** "*PPP Extensible Authentication Protocol (EAP)*", 1998;

[3] **RFC 2865**, "*Remote Authentication Dial In User Service (RADIUS)*", 2000;

[4] **RFC 2866**, "*RADIUS Accounting*", 2000;

[5] ~ **"***Internet Authentication Service for Windows 2000***",** white paper, Microsoft Corporation 2000;

[6] **Josep Davies**, **"***RADIUS Protocol Security and Best Practices***",** white paper, Microsoft Corporation 2002;

[7] ~ **"***Using the BayStack 450 10/100/1000 Series Switch***",** users book, Nortel Networks Inc., 2001

[8] **Arunesh Mishra, William Arbaugh, "***An Initial Security Analysis of the IEEE 802.1X Standard***"**, University of Maryland, 2002

[9] **LAN/MAN Standards Committee of IEEE**, **"***Port Based Network Access Control***"**, IEEE Computer Society, 2001