TOURO COLLEGE & UNIVERSITY SYSTEM

GRADUATE SCHOOL OF TECHNOLOGY

802.1X and Network Access Control

Md Azizul Rahaman

Touro University Graduate School of Technology

2023

1.0 Introduction

A port-based network access control standard developed by the IEEE (Institute of Electrical and Electronics Engineers) is called IEEE 802.1X. Its major objective is to offer a method of authentication to individuals and devices trying to connect to wired and wireless LANs, ensuring that only approved connections are permitted. The term "Network Access Control" (NAC) has become extensively used to refer to systems that authenticate individuals and devices, much as 802.1X, and validate the security posture of devices trying to join to a network.

2.0 Development History of 802.1X and NAC

Originally created by 3Com, HP, and Microsoft®, 802.1X was acknowledged by the IEEE in January 1999 and adopted as a standard for the first time in June 2001. (IEEE Computer Society, 2001). It was created as a tool to help organizations protect network sockets in open areas of buildings by prohibiting unauthorized access to a LAN at the switch port level. It is crucial to keep in mind that a full 802.1X implementation consists of numerous components, and the technologies have advanced rapidly.

The foundation of the 802.1X standard, EAP, was first created in 1998. RFC 2284, the EAP protocol, underwent major change in 2004 that resulted in the protocol that is now familiar to network managers.EAP was initially associated with Serial technologies rather than Ethernet technologies and was based on the Point-to-Point Protocol (PPP). Link Control Protocol, which outlines how the link should be established, is described in the PPP standard, whereas EAP specifies the authentication step.

The Internet Engineering Task Force (IETF) group developed RADIUS (Remote Authentication Dial-In Users Service) and submitted a draft standard in 1994. The initial RADIUS RFC was published in 1997 and later updated. June 2000 saw the publication of RFC 2865. For the purpose of offering services for contemporary network deployments, RADIUS has undergone a number of extensions. These additions have basically made Diameter, the suggested replacement for RADIUS, unnecessary.

3.0 What is NAC & 802.1x

3.1 NAC

By restricting access to the network using one or more kinds of authentication and restricting access to enterprise resources using one or more types of authorization and policy enforcement, NAC, a tried-and-true networking concept, may identify users and devices.

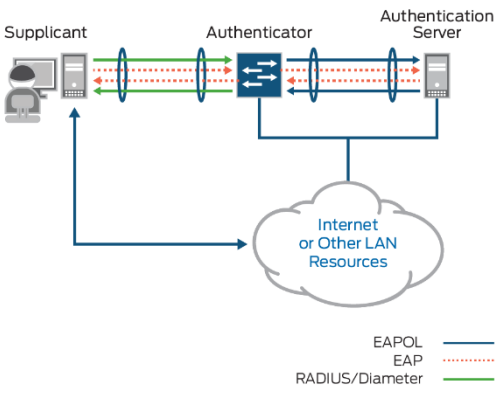
NAC can be deployed in a variety of ways, and during the design and implementation phases, need to make a number of choices based on the particular service level agreements (SLAs) your organization has with your users.

Customers of NAC systems, academic researchers, suppliers, and groups like the IEEE have created a NAC model throughout time, and its components are thought to constitute the fundamental conditions of any efficient NAC system.

3.2 802.1X

For port-based network access control (PNAC) on both wired and wireless access points, the IEEE standard 802.1X protocol is used. The main goal of 802.1X is to provide authentication requirements for any device or person trying to connect to a LAN or WLAN. The 802-family of standards includes 802.1X.

By verifying the person or device trying to access a physical port, generally at a switch or network edge device, 802.1X offers L2 access control. Three parts make up the fundamental 802.1X authentication mechanism: the supplicant, authenticator, and authentication server.

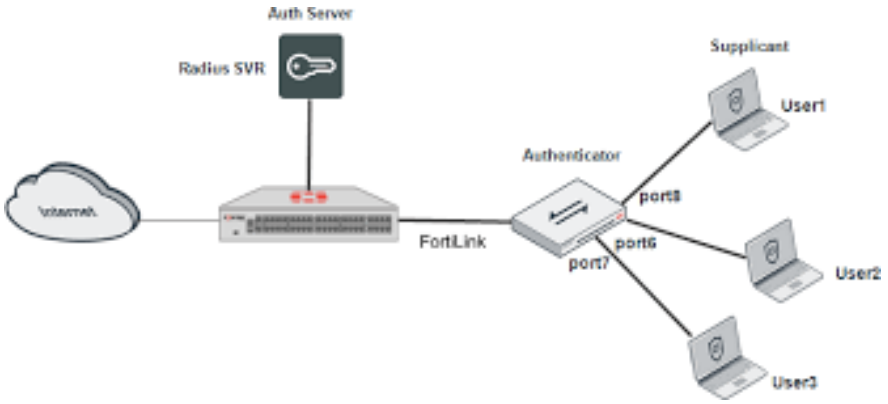


4.0 NAC Methods

For authenticating end systems and/or users, numerous technical techniques might be used. Multiple approaches should be supported by a complete NAC solution

5.0 802.1X (Port based via RADIUS)

The identification of end systems at the network switch port using 802.1X authentication is the most secure authentication technique. Specific capabilities on the switch, client, and local authentication entity are required for this (RADIUS server). Additionally, 802.1X permits user and end system authentication (either separately or as a combined entity).



The 802.1X authentication mechanism may not be suitable in some circumstances. There are some end systems that might not contain or support an 802.1X supplicant (the software agent for authentication). Older printers or IP cameras are two examples of equipment that do not support 802.1X. Some network switches do not support 802.1X, as well. Finally, according to corporate IT standards, it's possible that guests' 802.1X authentication configurations are incorrect.

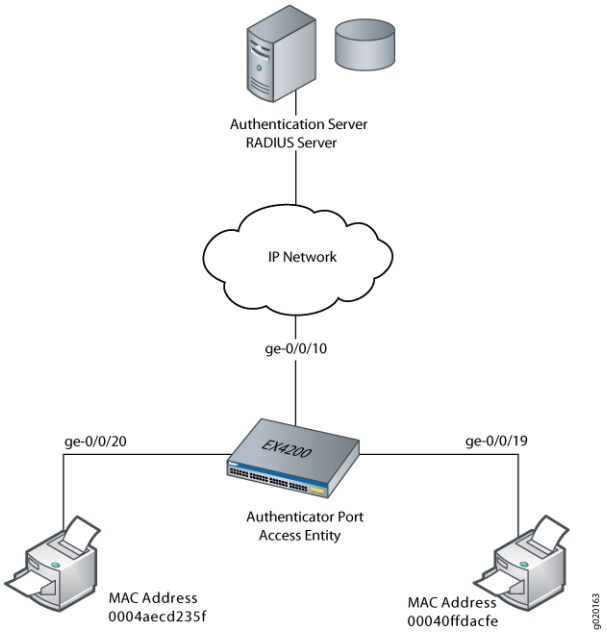
Businesses frequently have heterogeneous networks that only allow some authentication or none at all. Here, we want to use better technologies whenever we can. However, it is typically too expensive to replace the network completely. Any new network switches should enable 802.1X and several separate authentication sessions per port as a minimum requirement.

Additionally, they must enable for per-port flexibility and support various authentications for various end system types (such as VoIP phone plus PC or mini-/office-/cable switches).

If all conditions are met, 802.1X provides a very secure identification at the switch port that is very scalable and dynamic.

6.0 MAC Based Authentication via RADIUS

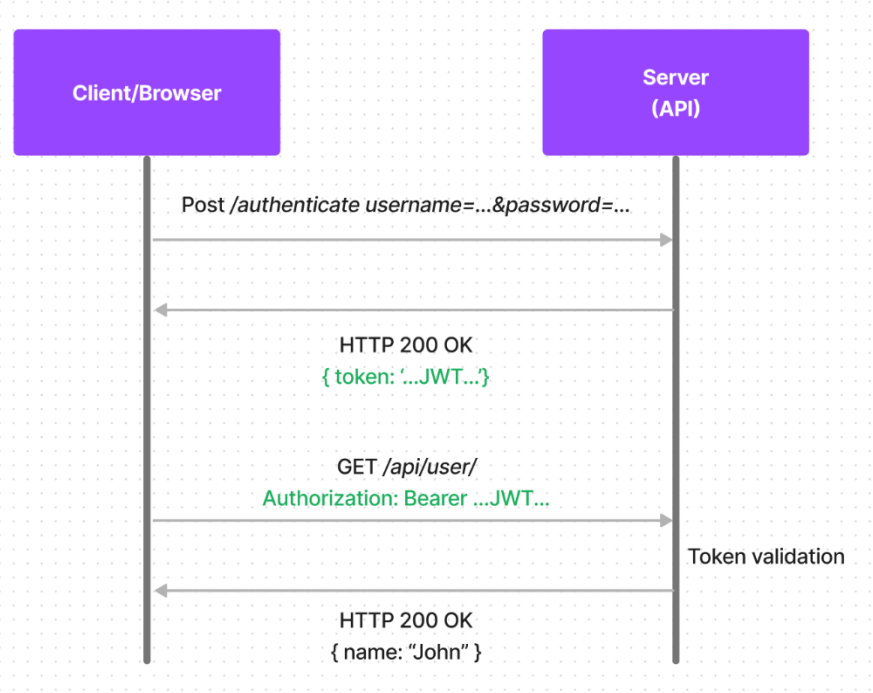
The fundamental components of 802.1X are also used by MAC based authentication. The abandonment of certificates and/or registration data makes a difference. In place of the username, the switch substitutes the MAC address of the end machine and checks this with the RADIUS server. In networks that support 802.1X, this technique can be used to validate all end systems with the RADIUS server without the "supplicant." Starting with MAC-based authentication for the entire network and later switching to 802.1X for end systems with support is a frequent implementation technique. This technique should only be used in conjunction with restrictive authorization because it only provides a minimal level of security. Subsequent authorizations will be linked to the hardware address of the end system because other information, such as the username, is missing. The centralized administration of all users using the RADIUS service is a benefit of this approach.



This approach offers a remedy for unique end systems. As scalability and dynamic port/MAC assignment are the same as for 802.1X, it is preferable to static port/MAC assignment.

7.0 Web Based Authentication

This method of authentication relocates the “supplicant” to a web portal to which a user has to login. With this method, guests and end systems not fulfilling the necessary requirements for network access can also register to the network. Guest access only requires a very basic registration. An elegant example of secure guest access is sponsored registration, where existing users agree to compliance of their guests. With this method, the IT organization can easily audit who has sponsored each guest accessing the network without having to get involved in providing temporary credentials. In this example, a default policy is enforced, only allowing connection to a web portal. Once authentication at the web portal is successful, further services can be allowed. It is interesting to note that many solutions do this via dynamic VLAN configurations. This separates the end system from the production network, but usually does not define any restrictions within the VLAN. VLANs are not sufficient security containers. VLANs are meant to be logical broadcast containers.



A well architected NAC solution may use a different approach. Traffic can be classified by the network switches based on OSI layer 2 through 4 information in the packets, allowing enforcement of firewall-like rules to individual traffic flows in the network. This will be further explained in the Authorization section.

This approach is more of a supplement than an entire authentication strategy. It facilitates access to older devices and reduces the administrative burden for visitors.

8.0 Static Port/MAC Configuration

Manually assigning MAC addresses to switch ports has developed into a security best practice. But static port/MAC configuration is neither automatic detection nor safe access, as the term implies. This arrangement is mentioned here as a very flimsy but affordable technique of access control since many organizations still employ it. The least effective but least expensive NAC solution.

9.0 Dynamic Port/MAC Configuration (SNMP)

Numerous specialized products that aim to mimic the SNMP process of detection and authentication are available on the market. When a directory or RADIUS framework is unavailable, some businesses prefer to use this approach. The out-of-band administration, which works with all SNMP devices, is undoubtedly a plus, but it is also one of the key issues. Many suppliers use SNMP to give inaccurate or incomplete information, making it impossible to guarantee a successful outcome. Additionally, because SNMP requests are made at regular intervals known as polling, authentication via SMNP is non-standard and incapable of operating in real-time.

In the worst situation, SNMP queries may cause an infrastructure device to crash due to the high stress they place on routers and switches. The port/MAC configuration process is dynamically handled in terms of security. With this, it is possible to identify the location of an end system during the previous query. Disabling the port or changing the port's VLAN configuration are frequent countermeasures. The user is not given any insight into the reasons why access to the network has been blocked by either of these choices. Furthermore, if DHCP is in use and the client

does not instantly request a new address, VLAN reconfigurations frequently encounter issues. This approach should only be used in very small environments and only if 802.1X is not available because to the extremely restricted security, numerous additional issues, and the administrative work involved. Simple, affordable solutions for constrained spaces only effective for localizing constrained end systems.

10.0 Kerberos Snooping

Network authentication uses the Kerberos protocol. Typically for Windows Active Directory domains, although not exclusively (Novell NDS uses it as well and it is often used in Linux environments). Kerberos spying can determine whether a system has successfully logged on to a domain by reading encrypted data traffic. The host name and the username are provided by Kerberos as identification attributes.

The benefit of Kerberos spying is that using the Kerberos protocol is the only prerequisite. Since the identification and authentication are independent of the switch, they are frequently implemented with minimal assistance. The drawback is that in order to read the pertinent transmission, you need an in-line device such an intrusion detection system. The appliance offers a lot more features than a switch's typical 802.1X implementation. Such a solution is feasible in circumstances that require a greater level of firewall-like security as well as when there are no other options for identification. Such a device can track WAN changes like VPN access and is frequently employed at the distribution layer of a tier-based network. By using this method, NAC can be quickly implemented without spending money on intelligent access switches.

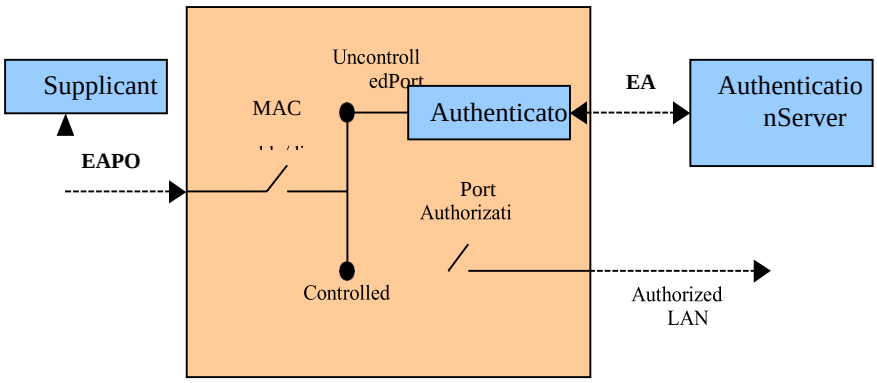
Flexible, simple, and quick to apply solution. Due to costs, it is challenging to roll out for an entire environment and must be in line.

11.0 How 802.1x Works

Access to the LAN services is provided or denied based on the port status of an authenticator. The port initially exists in an unlicensed or uncontrolled condition. Except for 802.1x protocol

packets, no other ingress or egress traffic is permitted through the port while it is in this state. Only 802.1x authentication traffic is permitted to transit across uncontrolled ports.The port switches to an authorized state, also known as a controlled port, after the Supplicant has successfully been validated, enabling all traffic for the Supplicant to go regularly.

Any access to the LAN is additionally governed by the Media Access Control (MAC) connected to the port's administrative and operational status. There is no traffic permitted through a port if it has been administratively disabled.



The protocols and processes described in the following section are used to communicate between the Supplicant and the Authenticator as well as between the Authenticator and the Authentication Server (where the Authentication Server is not allocated with the Authenticator).

12.0 EAP (Extensible Authentication Mechanism)

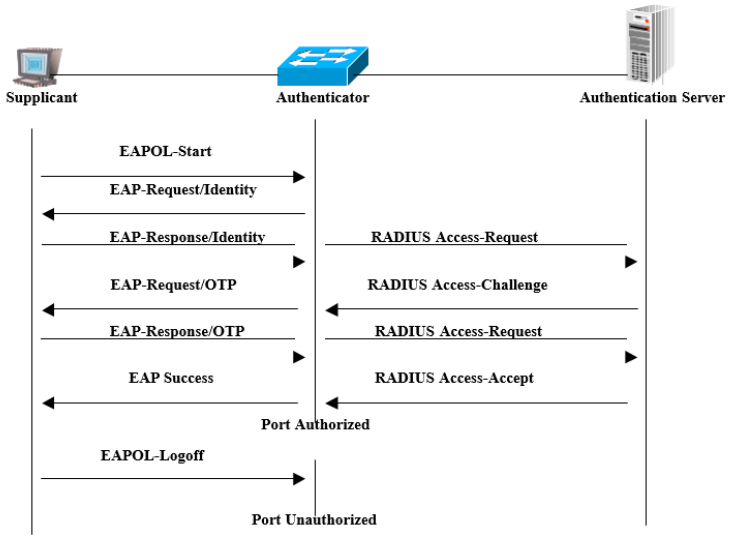
Extensible Authentication Mechanism (EAP), described in IETF RFC 2284, is used by IEEE 802.1x as the protocol for authentication exchange. Within the Point-to-Point Protocol (PPP), EAP is a CHAP/PAP extension that allows for the transmission of authentication data for different authentication mechanisms. Support for a variety of authentication methods, such as smart cards, Kerberos, Public Key, One Time Passwords, and others, may be introduced through the usage of EAP.

Before granting access to a Supplicant, an Authenticator and Supplicant communicate using the EAP protocol. This indicates that EAP messages must be directly encapsulated over a LAN medium. For this reason, EAP over LAN (EAPOL) was developed.

The EAP messages must then be forwarded to the RADIUS Server by the Authenticator in RADIUS packets. Two new properties, EAP-Message and Signature were added as RADIUS extensions in order to support EAP within RADIUS. Without needing to comprehend the protocol, the Authenticator can use the EAP-Message attribute to authenticate the Supplicant using EAP. In an Access- Request packet, the Authenticator inserts the EAP messages it has received from the Supplicant into one or more EAP- Message characteristics before sending them to the RADIUS Server.

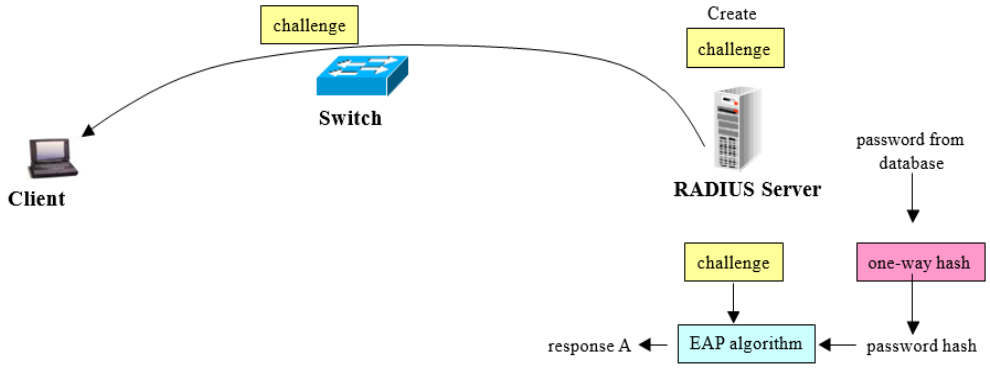
These EAP messages are protected using the Signature feature. The Signature element must be used to authenticate every EAP/RADIUS packet. This Signature is included in the RADIUS packet after being generated by an algorithm. If a RADIUS server that supports EAP-Message determines that the packet's Signature value is incorrect or that it lacks the Signature attribute, it must silently discard the packet.

The RADIUS server can use the Signature property to check the authenticity of packets coming from the Authenticator, and vice versa. This gives the transmission of authentication messages integrity protection.



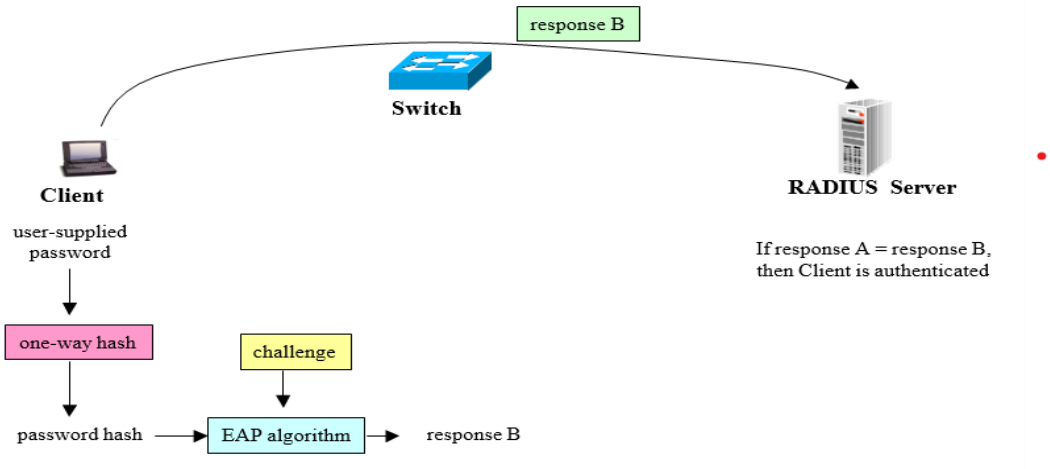
12.1 Authentication Process Of EAP

- A Supplicant or Client can start the authentication process at boot-up by sending an EAPOL-start packet, which instructs the attached Authenticator—in this case, an Ethernet switch—to ask for the client's identity.
- Authentication can also be started by the switch or the authenticator. If the switch has enabled authentication on a particular port, the switch must start the authentication process whenever it notices that the link status is active or changes from down to up. It then asks the Supplicant for its identity by sending an EAP-request/identity frame.



- The Client replies to the Authenticator with its identification in a "EAP-Response/Identity" packet.
- The Authenticator will pass a RADIUS Access-Request packet to a RADIUS server acting as the Authentication Server, copying the content of the EAP-Response/Identity into the User-Name attribute of RADIUS. This packet is often used by the RADIUS server to decide which EAP type should be used for the user. A RADIUS Access-Challenge packet will be returned by the RADIUS server if it supports EAP. The RADIUS server will respond with an Access-Reject if EAP is not supported.

- The RADIUS server will make a user database check using the client's identification. After that, a challenge will be generated and delivered to Authenticator. In order to generate a response that will be later compared with the client's response, the EAP algorithm uses this challenge and the client's password.



- The RADIUS Server sends the client's challenge.
- In order to provide a response for the RADIUS server, the Client does the same calculation as RADIUS using the challenge and the user-supplied password.
- If the client's response matches the one previously calculated by the RADIUS server, the client's credentials are valid, and the RADIUS Server reacts by sending a success message that is then forwarded to the client. Now that the port used by the Authenticator is authorized, the Client is permitted access to the LAN.

12.2 Authentication Types Of EAP

In the LAN context, IEEE 802.1x specifies an encapsulating mechanism that permits the transfer of EAP packets between the Supplicant and Authenticator. A standardized system for supporting additional authentication techniques within PPP is provided by the EAP. Support for a variety of authentication methods, such as smart cards, Public Key, One Time Passwords, and others, may be introduced through the usage of EAP.

12.3 EAP-MD5

EAP-Message Digest 5 (EAP-MD5) is an EAP type that generates challenges and responses from the client to the RADIUS server using an MD5 hash of a login and password. The Wired Equivalency Protocol (WEP) key used in a Wireless LAN context with EAP-MD5 authentication is a static key. This static WEP key compromises wireless LAN security because it makes it simple for someone who sniffs your wireless traffic to decode all of the data he has collected.

Additionally, EAP-MD5 does not support mutual authentication. It just enables the client to be verified by the server. Because of this, EAP-MD5 is regarded as the least secure EAP authentication method.

EAP-MD5 CHAP is frequently used to verify a client's credentials utilizing username and password security mechanisms.

12.4 EAP-TLS

EAP-Transport Layer Security (EAP-TLS) is an EAP type that is used in contexts with certificate-based security and is defined in RFC 2716. Mutual authentication is provided via the EAP-TLS message exchange since the client and server use certificates to validate one another.

EAP-TLS offers dynamic WEP key generation in wireless networks, enhancing wireless LAN security. Due to the extensive PKI infrastructure support needed for EAP-TLS deployment, the strength of EAP-TLS security comes at a considerable cost. EAP-TLS requires extra work to administer because it needs user-side and server-side certificates. User certificates need to be managed and could add to administrative complexity.

12.5 EAP-TTLS

A development of EAP-TLS called EAP-TTLS does away with the requirement for client-side certificate configuration and solely uses server-side certificates. EAP-management TTLS's is simpler than EAP- TLS's. Due to the fact that users are authorized to the network using standard password-based credentials, EAP-TTLS still maintains mutual authentication like EAP-TLS.

12.6 Lightweight-EAP (LEAP)

This Cisco-developed EAP authentication type is mostly utilized in Cisco Wireless LAN equipment. It is a Cisco-exclusive kind of authentication. Using dynamically generated WEP keys, the Wireless LAN encrypts data transmission and supports mutual authentication.

LEAP was created to replace EAP-MD5 in Wireless LAN environments when WEP keys are static and mutual authentication is not offered. Because the client will authenticate the RADIUS server after it has been authenticated, LEAP offers mutual authentication.

12.7 Protected EAP (PEAP)

One-Time Password (OTP), Windows NT or 2000 domain, and LDAP user databases are all supported by PEAP authentication over a wireless LAN. It is based on EAP-TLS authentication but instead of using a client certificate for authentication, it employs a password or PIN. Data encryption in Wireless LAN is performed by PEAP using a dynamic session based WEP key that is derived from the client adapter and RADIUS server.

13.0 Security Issue and Defenses

Over time, the security problems that Enterprise networks face have changed, shifting from mitigating external attacks to minimizing internal intrusions and the penetration of malicious software. This internal protection places a heavy burden on network administrators since it necessitates extensive interaction with each device on a network. By using cutting-edge switching technology as a component of Network Access Control, Allied Telesis reduces this expense and offers an efficient solution to internal network security (NAC).

14.0 Conclusion

As security professionals attempt to address the issue of dynamic endpoints—laptops and other devices that enter and exit networks at will—Network Access Control (NAC) and 802.1x have grown in popularity as conversation topics. They are challenging to control and frequently introduce malware into a network that is otherwise "clean."

A NAC environment enables context-driven quarantine and remediation, network port-based authentication, security posture checks, and occasionally persistent monitoring. On the basis of

identification, 802.1x participates in the authentication feature to enable or deny a device access to a network.

In order to begin the installation process, some businesses think that 802.1x is sufficient and sufficiently similar to a complete NAC solution. Organizations frequently discover that while the 802.1x story appears to be quite straightforward and uncomplicated, the deployment is far more challenging. Architectures frequently break easily and don't offer much resilience. More significantly, 802.1x does not address the whole user population of those utilizing unmanaged devices.

This white paper provides a thorough description of a NAC environment before contrasting it with an 802.1x deployment. It offers a case study that serves as a practical illustration of the necessity for a solution that is more lenient in its deployment and more comprehensive than 802.1x, in this case ForeScout's CounterACT. In the end, the substantial advantages of NAC surpass the minimal requirements and support for 802.1x offered by network and client manufacturers.

15.0 References

https://www.giac.org/paper/gsec/2534/ieee-8021x-port-based-network-access-control-implementation/104381

https://cipherwire.net/wp-content/uploads/2013/06/802.1X_and_NAC___Best_Practices_for_Effective_Network_Access_Control.pdf

https://www.techdata.ca/techsolutions/networking/files/feb2009/Enterasys%20NAC%20Planning%20Guide.pdf

https://www.black-box.de/_AppData/cms/file/Files/Whitepaper/DE/1006_WP_NAC_EU_.pdf