•CENTRAL AUTHENTICATION USING RADIUS AND 802.1X

This is part of my experience I implemented in the Organization while I was doing my summer interns as the Part of my Curriculum. This Entirely is a very much workable solution but need some prerequisites like the understanding of some security protocols like RADIUS, 802.1x and the basic understanding of Linux Operating System.

CHALLENGE

Having information-rich business environment, the network is the base of our daily operation and the foundation for our strategic direction. Companies depend on an efficient network to enable critical business application, communication and collaboration. The network must be highly secure, reliable and available to the external and the internal users.

Making full use of business opportunities and overcoming technical challenges begin with maintaining high performance, high availability and high quality-of service levels in your network. To grow your business and deliver next generation services, you need to evolve your network; migrate to new IP services; and converge data, voice, and video – all while efficiency scaling and deploying diverse and complex technologies.

Coping up with all this above stated challenges need the person to be equipped with all kind of the IT Infrastructure available in the IT market today. But again there is nothing like the Free Lunch ; means every thing bring with it the Security Breach with itself. The Need for the Enterprise Network can be enlisted as below:

1. The Infrastructure should be usable by the different users at the same time should give the Users the Ease for the Usability and the Flexibility to use by providing them the Feel at home with the Desktop Environment.
2. The Authentication mechanism should be properly in place with the authentication done on the Central place to provide the Exact Security needed to the User Information to the Users password and login name database
3. The Password traveling on the Network should be properly encrypted on the network.
4. The User should be given the proper privilege depending upon the user credentials presented to him in the Login and the privilege should be dynamic irrespective of the Machine used by him for login and the Work Purpose
5. There should be central Administrative and Monitoring position available to him for easy maintenance of the User profile and the privileges authorized to him depending upon the login credentials provided by him in the First place.
6. The Network Infrastructure should reflect the Exact Business Domain and the Operational Hierarchy of the Organization with proper policies in place reflecting the same.

• SYMBIOSIS CENTRE OF INFORMATION TECHNOLGY, Pune , *INDIA*
Created By: MOHIT SARASWAT

SOLUTION

The Solution comes in Place with leveraging some very basic technologies available ; the only need lies in exploring the same.

I here propose some workable and easy to implement solution that is very much workable and already tried out and tested by me in the real ti[•]me environment.

802.1x INTRODUCTION

The following are a list of terms and technologies used within 802.1x:

Supplicant (Client) – is the network access device requesting LAN services.

Authenticator – is the network access point that has 802.1x authentication enabled. This includes LAN switch ports and Wireless Access Points (WAP).

Authentication Server – is the server that performs the authentication, allowing or denying access to the network based on username / password. The 802.1x standard specifies that Remote Authentication Dial-In User Service (RADIUS) is the required Authentication Server that supports the following RFC's:

RFC 2284 PPP Extensible Authentication Protocol (EAP)
RFC 2865 Remote Authentication Dial In User Service (RADIUS)
RFC 2869 RADIUS Extensions

EAP – is the protocol that is used between the client and the authenticator. The 802.1x standard specifies encapsulation methods for transmitting EAP messages so they can be carried over different media typed. These include, but are not limited to:

EAP Over LAN (EAPOL)
EAP Over Wireless (EAPOW)

Port Access Entry (PAE) – is the 802.1x "logical" component of the client and authenticator that exchange EAP messages.

[•] SYMBIOSIS CENTRE OF INFORMATION TECHNOLGY, Pune , *INDIA*
Created By: MOHIT SARASWAT

UNDERSTANDING 802.1X

Introduction

The IEEE 802.1x is a standardized method for securing network access from the network devices. Traditionally, network security has predominantly been the domain of network Servers and clients, based on login authentication to specific resources. If a network user wanted access to network server resources (file and print), then a login challenge needed to be successfully completed. In the case of an all Microsoft domain based network, then the login request is presented to the user when they started up their PC. The PC login username / password would be authenticated against a domain controller, and if successful then the user would be granted access to file & print services specified by the network administrator.
This kind of client / server authentication is often used for other network services including email, intranet and other specialized applications

Although client / server authentication is a proven method for securing network resources, it does not provide a total "network" security mechanism that will deter unauthorized access.
To counter this, many network equipment vendors have implemented other network-based administrative solutions, including VLANs, Access Control Lists (ACLs) and Media Access Control (MAC) locks. All of which are an effective mechanism for securing network access, but can be administrator intensive depending on what the security criteria is. Each control provides a unique advantage, but are often unique to each vendor. By complimenting the existing network security methods with 802.1x, administrators can be confident that their network perimeter (edge access) is completely secure, as well as having the confidence with interoperability amongst multiple vendors by deploying an IEEE based standard for security.

Since 802.1x is only a perimeter security technology, network administrators should continue to deploy existing security policies to control network traffic:
802.1x will deny unauthorized network access, but it will not control network traffic from authorized users. This may be a concern for network administrators that want to secure specific network areas with the use of existing methods including VLANs, ACL's or MAC filtering where it is required.[•]

802.1x Authentication Process

Once 802.1x authentication is enabled (both in the client and authenticator), a successful authentication must be completed before ANY traffic is allowed to transit the network from the client, including critical traffic like DHCP requests regardless of whether link is established between the client and authenticator (switch port).

[•] SYMBIOSIS CENTRE OF INFORMATION TECHNOLGY, Pune , *INDIA*
Created By: MOHIT SARASWAT

Before Authentication

To ensure that no unauthorized traffic is transmitted, before successful authentication, the authenticator's PAE is set to uncontrolled. That means that the only messages that will be accepted from the client is EAP requests which will be forwarded to the Authentication server
– see figure 1
•

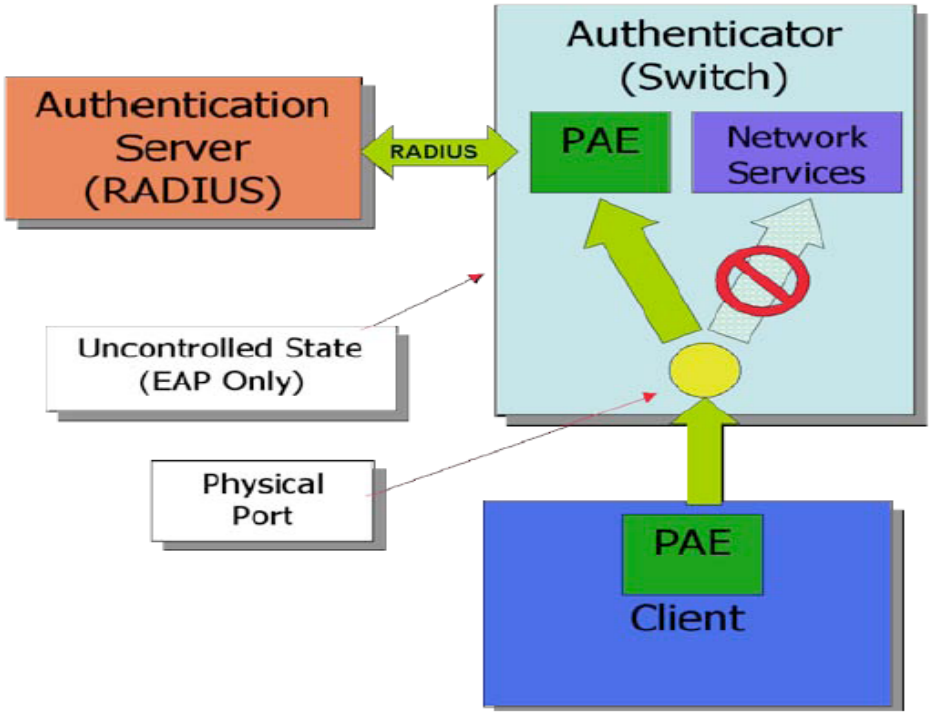


Figure 1 - Before Authentication

Authentication Process

Once activated (powered on and connected to the switch), the 802.1x client will transmit the appropriate EAP message to the authenticator (switch port). The switch port with 802.1x authentication enabled is set to an uncontrolled state, accepting only EAP messages (all other traffic will be discarded). Upon receipt of the clients EAP message, the switch will forward the request to the authentication (RADIUS) server without changing its contents.
Although the EAP contents are not changed, the encapsulation must be translated from the originating EAP message to a RADIUS request, therefore the only supported RADIUS servers are ones that support EAP (see RFC Compliance).

• SYMBIOSIS CENTRE OF INFORMATION TECHNOLGY, Pune , *INDIA*
Created By: MOHIT SARASWAT

Upon receipt of the RADIUS message, the authentication server will grant or deny access to the network. An RADIUS response will then be transmitted back to the switch, which will determine whether the port remains in an uncontrolled state (access denied), or changes to a controlled state (access granted).

If the authentication fails, the authenticator (switch port) will remain in an uncontrolled state, and in some cases the port will be disabled (depends on vendor implementation).

Although the client is the device that requires authentication, either the client or switch can initiate the process. This is determined by timers which are set in both the client and the switch.

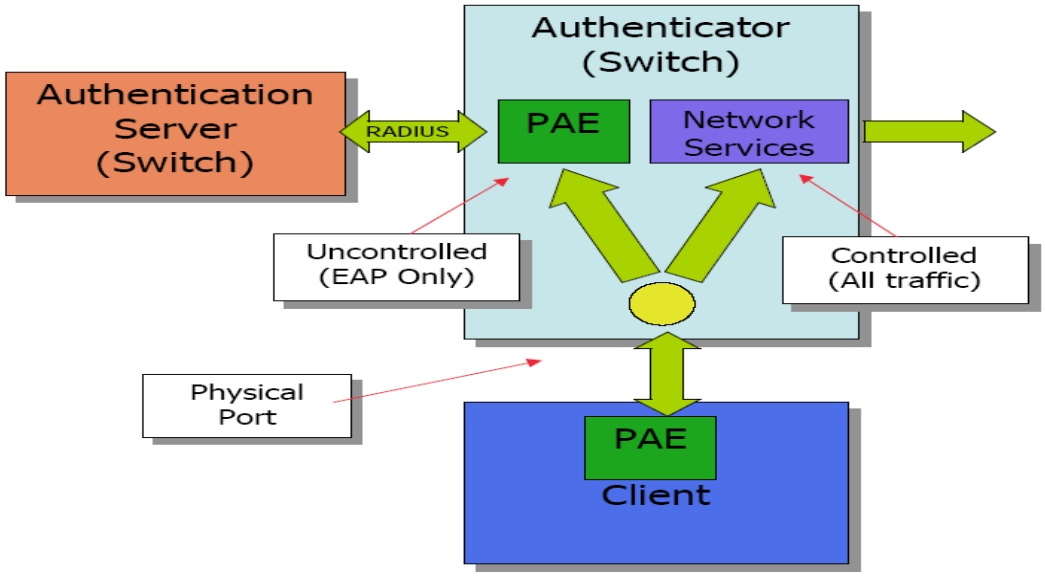
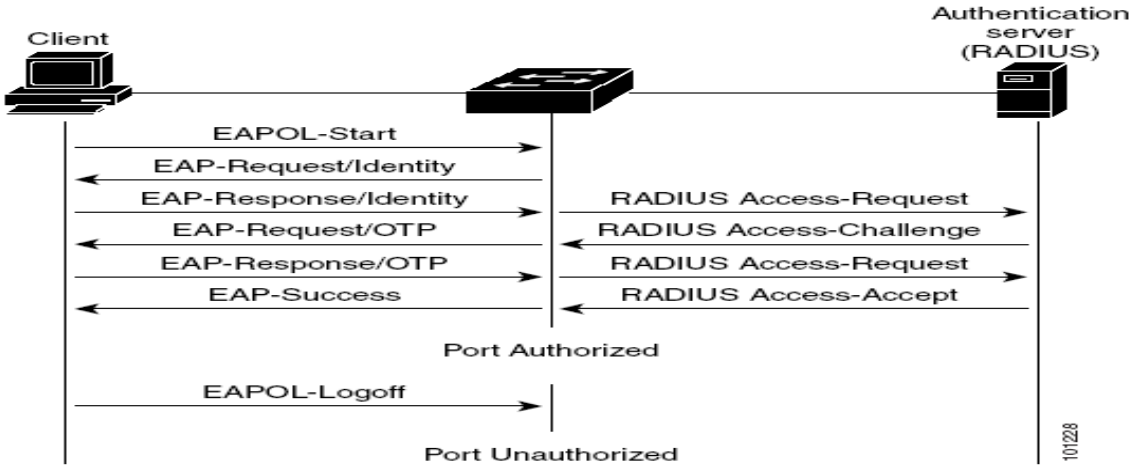


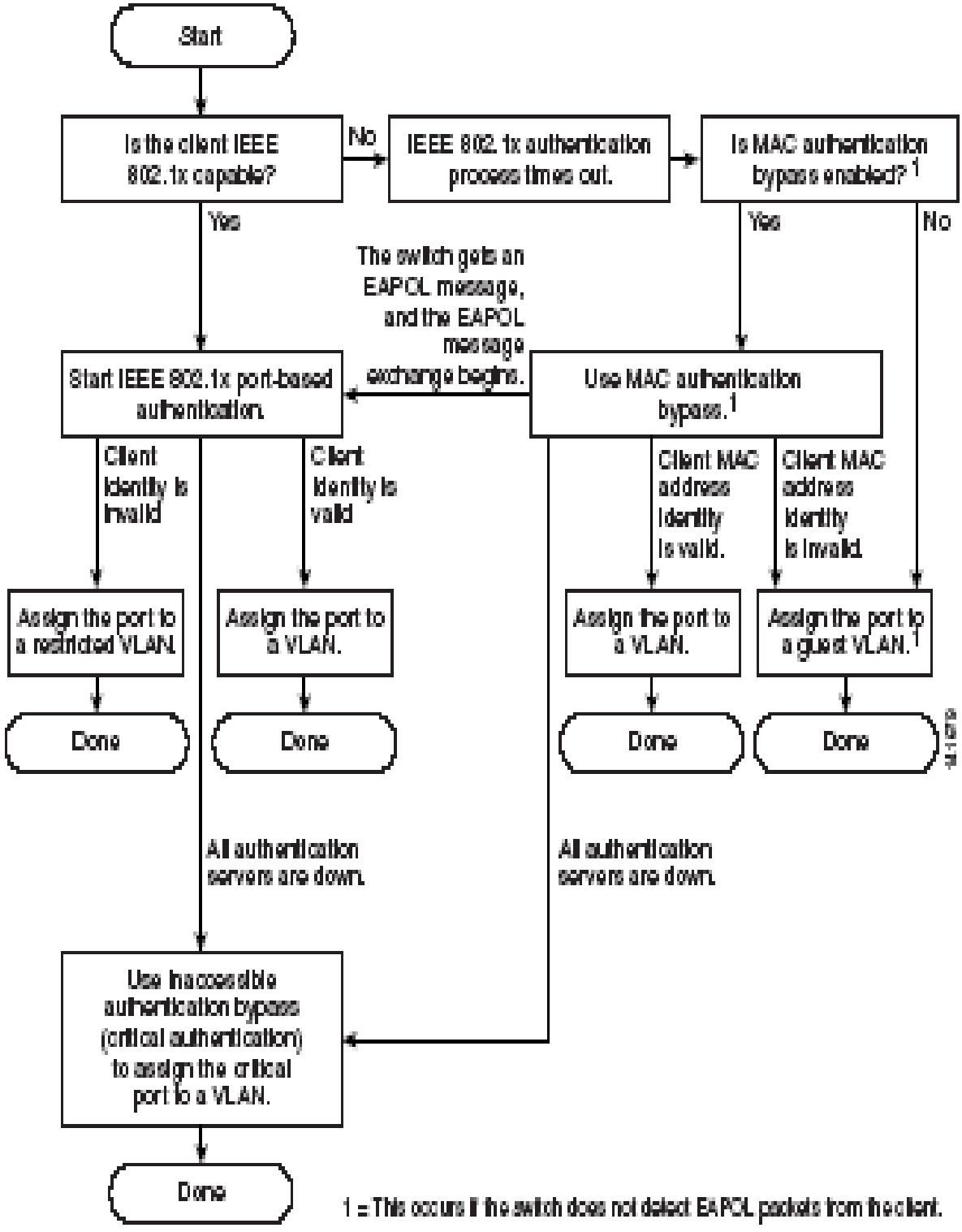
Figure 2 - After successful authentication

•



• SYMBIOSIS CENTRE OF INFORMATION TECHNOLGY, Pune , *INDIA*
Created By: MOHIT SARASWAT

•**AUTHENTICATION FLOWCHART**



• SYMBIOSIS CENTRE OF INFORMATION TECHNOLGY, Pune , *INDIA*
Created By: MOHIT SARASWAT

SUMMARY:

By implementing IEEE 802.1x, administrators can protect the network from unauthorized user access, minimizing potential security breaches including Denial of Service (DoS) attacks within their network infrastructure. Although implementing 802.1x provides enhanced network edge security, it •is important for network administrators to plan and deploy this technology based on their requirements, taking into consideration devices like VoIP phones and Wireless Access Points.

It is important to note that 802.1x technology is complimentary with existing security technologies, and is not a replacement. Since 802.1x can be considered to be a perimeter security measure, there will still be the need for network security techniques like VLANs and ACLs.

• SYMBIOSIS CENTRE OF INFORMATION TECHNOLGY, Pune , *INDIA*
Created By: MOHIT SARASWAT

REFRENCES:

- IEEE RFC 3580
- •CISCO CATALYST SWITCH SOFWARE CONFIGURATION GUIDE, *Cisco IOS Release 12.2(37) SE May 2007*
- www.freeradius.org
- www.ietf.org

• SYMBIOSIS CENTRE OF INFORMATION TECHNOLGY, Pune , *INDIA*
Created By: MOHIT SARASWAT