# Grid of Security:A New Approach of the Network Security

G.Neeharika[1], K.Lalitha[2]

Sree Vidyanikethan Engineering College, affiliated to JNTUA, neeharika1931@gmail.com
Sree Vidyanikethan Engineering College, affiliated to JNTUA, lalithapc@gmail.com

## ABSTRACT

Network security is in a daily evolving domain. Every day, new attacks, virus or intrusion techniques are released. Hence, network devices, enterprise servers or personal computers are potential targets of these attacks. Current security solutions like firewalls, intrusion detection systems (IDS) and virtual private networks (VPN) are centralized solutions which rely mostly on the analyze of inbound network connections. This approach notably forgets the effects of a rogue station, whose communications cannot be easily controlled unless the administrators establish a global authentication policy using methods like 802.1x to control all network communications among each device. To the best of our knowledge, a distributed and easily manageable solution for the global security of an enterprise network does not exist. In this paper, we present a new approach to deploy a distributed security solution where communication between each device can be control in a collaborative manner. Indeed, each device has its own security rules, who can be shared and improved through exchanges with others devices. With this new approach, called grid of security, a community of devices ensures that a device is trustworthy and that communications between devices progress in respect of the control of the system policies. To support this approach, we present a new communication model that helps structuring the distribution of security services among the devices. Like this, we can secure both ad-hoc, local-area or enterprise networks in a decentralized manner, preventing the risk of a security breach in the case of a failure.

**Key Words:** Network Security,802.1x, Distributed security solution, Firewalls, Intrusion detection systems, Virtual Private Networks.

## 1. INTRODUCTION

Network Security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification or a denial of a computer network and network accessible resources. Network Security involves the authorization of access to data in a network which is controlled by a network administrator. Users choose or assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network devices, enterprise servers and personal computers are some of the targets of these attacks. So security issues plays a major role.

Some of the existing solutions like Firewalls, Intrusion detection systems, virtual Private networks .Firewalls can be effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the internet. Firewall is a crucial component of securing network and is designed to address the issues of data integrity or traffic authentication and confidentiality of internal network .But Firewalls cannot stop internal users from accessing websites with malicious code. Firewalls cannot prevent users or attackers with modems dialing in to or out of the internal network thus bypassing the firewall and its protection completely.

Intrusion Detection is the problem of identifying unauthorised use ,misuse and abuse of computer systems. Outside attacks are the not only problem ,the threat of authorised users misusing and abusing their privileges is equally pressing concern. Intrusion Detection systems (IDS) may become the target of an attack itself. An attacker may utilise the techniques to reduce the ability of IDS to detect an attack inorder to allow the attacker to slip their traffic undetected.

Blind the sensor: By taking advantage of the fact that a NIDS will drop packets on heavily loaded links, an attacker may attempt to flood a link whilst trying to attack a particular asset.

Blind the event storage (snow blind): By simulating a large number of simultaneous attacks, the Administrator will have a hard job when attempting to determine which attack was 'the real one'. Tools such as Nmap have options to run Decoy scans to ensure it is difficult to determine the real source of a scan.

DoS (Denial of Service): Due to the nature of NIDS systems, and the need for them to analyse protocols as they are captured, NIDS systems can be susceptible to same protocol based attacks that network hosts may be vulnerable. Invalid data and TCP/IP stack attacks may cause an NIDS to crash.

Virtual Private Networks (VPN) extends a private network across public network such as the internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network .A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, vitual tunnelling protocols of traffic encryption. One disadvantage of a VPN is the fact that its deployment requires a high-level of knowledge and understanding of such factors as public network security. VPN security requires password and data encryption. Network addresses may also be encrypted for added security. To avoid security and deployment problems, planning is necessary and proper precautions should be taken.

## 1.1.AUTHENTICATION POLICY USING 802.1x

Ensuring the security of wired networks where physical access to outlets is unrestricted is resource-demanding and IEEE 802.1X is the most elegant solution in this respect. IEEE 802.1X is a layer 2 protocol that enforces user or machine authentication. Typically a port is closed to most types of traffic until the connected user or machine has been authenticated. The switch will forward EAPoL traffic between the supplicant (machine) and the RADIUS server.

802.1x Extensible Authentication Protocol (EAP) also known as EAP over LANs (EAPOL) provides the framework for a device to authenticate when it connects to the network. When Port-Based Authentication is enabled, only EAPOL traffic is allowed on that port, everything else is dropped until the client is authenticated.

A client that connects to the network sends an EAPOL Start frame to initiate authentication, and the switch responds with an EAP Request/ID frame to request credentials. The client then sends an EAP Response/ID frame which contains credentials to the switch. The switch passes those credentials to the authentication server which then sends an EAP Request frame to the client to request a specific EAP Method for authentication. The client responds with an EAP Response frame. EAP Request frames and EAP Response frames are passed back and forth until the authentication server sends a EAP-Success message to the switch. At this point, the client is authenticated and normal traffic is allowed. When the client logs off, an EAPOL Logoff frame is sent to the switch and the port becomes unauthenticated.

You can view the statistics of 802.1x EAP on a given port on the 200/300 Series Managed Switches to check the current authentication activity. This article explains in detail the statistical information given about the 802.1x EAP activity for a given port on the 200/300 Series Managed Switches.

### 1.1.1.View EAPOL Traffic Statistics

Step 1. Log in to the web configuration utility and choose **Status and Statistics > 802.1x EAP**. The *802.1x EAP* page opens:

Step 2. Choose the port that you would like to view the 802.1x EAP statistics on from the Port drop-down list in the Interface field.

Step 3. Click one of the available radio buttons to refresh the 802.1x EAP statistic information in the Refresh Rate field. The available options are:

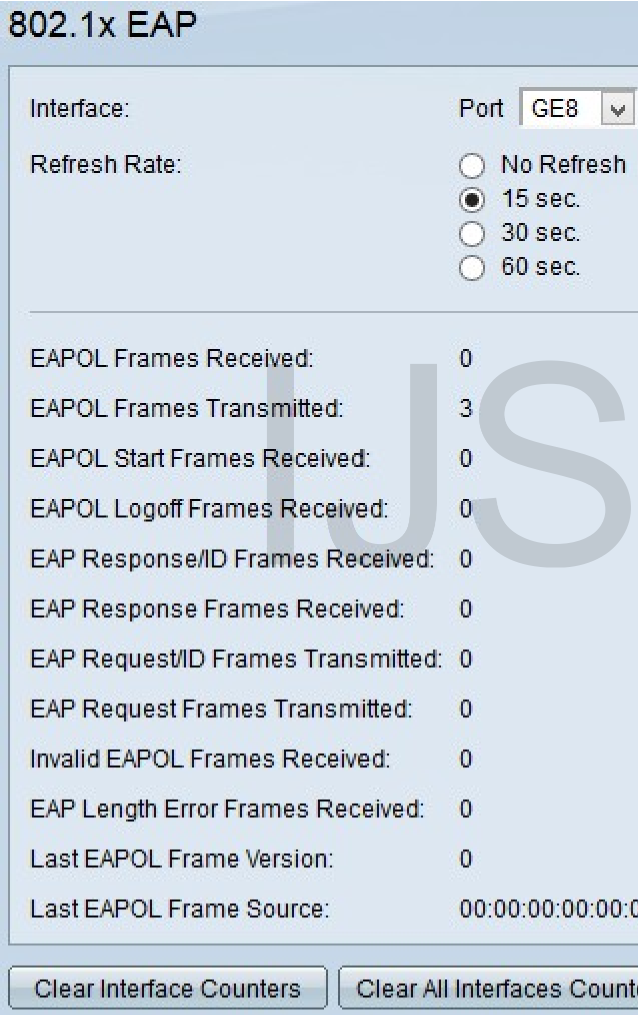
- No Refresh — Choose this option to not refresh the *802.1x EAP* page.

- 15 sec — Choose this option to refresh the *802.1x EAP* page every 15 seconds.

- 30 sec — Choose this option to refresh the *802.1x EAP* page every 30 seconds.

- 60 sec — Choose this option to refresh the *802.1x EAP* page every 60 seconds.

The *802.1x EAP* page displays the following 802.1X EAP traffic information on the chosen port:



802.1x EAP

Interface: Port GE8

Refresh Rate: ○ No Refresh ● 15 sec. ○ 30 sec. ○ 60 sec.

EAPOL Frames Received: 0
EAPOL Frames Transmitted: 3
EAPOL Start Frames Received: 0
EAPOL Logoff Frames Received: 0
EAP Response/ID Frames Received: 0
EAP Response Frames Received: 0
EAP Request/ID Frames Transmitted: 0
EAP Request Frames Transmitted: 0
Invalid EAPOL Frames Received: 0
EAP Length Error Frames Received: 0
Last EAPOL Frame Version: 0
Last EAPOL Frame Source: 00:00:00:00:00:0

- EAPOL Frames Received — Number of EAPOL frames received.

- EAPOL Frames Transmitted — Number of EAPOL frames sent.

- EAPOL Start Frames Received — Number of EAPOL Start frames received. EAPOL Start frames are sent by the client who attempts to initiate authentication.

- EAPOL Logoff Frames Received — Number of EAPOL Logoff frames received. EAPOL Logoff frames are sent by the client when it logs off, in order to revert the port state of the switch back to unauthenticated.

- EAP Response/ID Frames Received — Number of EAP Response/ID frames received. EAP Response/ID frames are sent by the client and these frames contain credentials in response to an EAP Request/ID frame sent by the switch.

- EAP Response Frames Received — Number of EAP Response frames received. EAP Response frames are sent by the client in response to EAP Request frames sent by the authentication server until the port becomes authenticated.

- EAP Request/ID Frames Transmitted — Number of EAP Request/ID frames sent. EAP Request/ID frames are periodically sent by the switch, or in response to an EAPOL Start frame, to an unauthenticated client to request credentials.

- EAP Request Frames Transmitted — Number of EAP Request frames sent. EAP Request frames are sent by the authentication server to the client in order to request information for authentication.

- Invalid EAPOL Frames Received — Number of unrecognized EAPOL frames received.

- EAP Length Error Frames Received — Number of EAPOL frames with an incorrect packet body length in the header received.

- Last EAPOL Frame Version — The protocol version of the most recent EAPOL frame received.

- Last EAPOL Frame Source — The source MAC address of the most recent EAPOL frame received.

Step 4. (Optional) To clear the EAPOL traffic statistics for the chose port, click **Clear Interface Counters.**

Step 5. (Optional) To clear the EAPOL traffic statistics for every port on the switch, click **Clear All Interfaces Counters.**

### 1.1.2.THE ELEMENTS OF IEEE 802.1X

In IEEE 802.1X, three parties are involved in the authentication process; the supplicant (on the client machine), the authenticator (the switch) and the authentication server (RADIUS). In addition there is usually a user database in a directory server (LDAP/AD/SQL) to which RADIUS refers. If eduroam (802.1X in a wireless network) is already in use, the RADIUS and directory servers can be re-used.

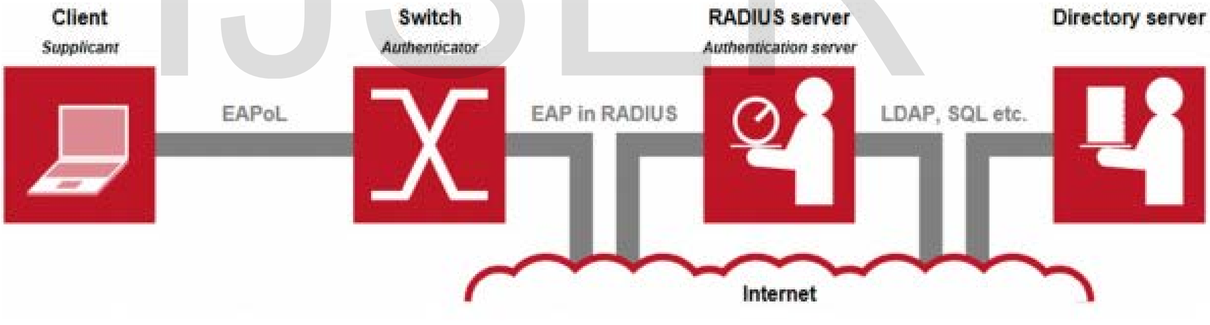


*Figure 1: The elements of IEEE 802.1X*

When connecting to an IEEE 802.1X activated switch, this will (if the client is configured for 802.1X) forward EAPoL traffic to the RADIUS server. If a client without 802.1X configuration or functionality is connected to the network, the switch configuration will determine what access the client will be granted. This may be no network connectivity at all; i.e. the switch port shuts down, or as we recommend, the switch port is assigned to a VLAN with restricted access. Such restriction can be achieved by means of access lists or a firewall, and may vary depending on what the current security policy is. For example, only Internet access may be granted or only access to certain parts of an internal network. IEEE 802.1X is based on mutual authentication between client and RADIUS server. The client may authenticate using a username and password or a certificate. The RADIUS server must authenticate using a certificate. It is possible to use 802.1X without the client checking the validity of the server certificate or the name of the certificate; however this is not a recommended solution. Hence we implement the grid mechanism to ensure security among community of devices.

### 1.2.Possible Solutions of Grid Of Security:

We assume to provide a global security among enterprise networks and a distributed security solution is deployed using grid approach by structuring the services among devices correctly without violating system policies. Generally grid may be defined as a bounded environment i.e., a collection of networked applications or services and resources which is treated as a whole. Enforcing correct reachability is critical for an enterprise network to achieve global security policy, access control, privacy protection and so on.

Like an Electrical grid, we need to implement a security grid. Grid of security is an interconnected network for providing security to solve some malicious issues. Since the solution doesn't exist aptly so far, we provide some solutions to provide the grid of security and its possibilities.

**Identity management and access control:** Secure utility facilities, assets, and data with user authentication and access control custom-built for grid operations. Cisco products supported include Cisco Secure Access Control Server, Cisco Identity-Based Network Services, and Cisco Network Access Control.

**Threat defense**: Build a layered defense that integrates firewall, VPN, intrusion prevention, and content security services to detect, prevent, and mitigate threats. Cisco products supported include Cisco ASA, Cisco IOS® Security, Cisco Intrusion Prevention System (IPS), and Cisco Security Agent.

**Data center security**: Turn network, computing, and storage solutions into a secure, shared pool of resources that protects application and data integrity, secures communications between business processes and applications within the utility, and secures connectivity to external resources such as providers of renewable energy. Cisco products supported include Cisco ASA, Cisco IPS, server and data center firewalls, and Cisco ACE Web Application Firewall.

**Utility compliance**: Improve risk management and satisfy compliance and regulatory requirements such as NERC-CIP with assessment, design, and deployment services.

**Security monitoring and management:** Identify, manage, and counter information security threats and maintain compliance through ongoing monitoring of cyberevents. Cisco products supported include Cisco Security Monitoring, Analysis, and Response System (MARS); Cisco Security Manager; and Cisco LAN Management System.

**Physical safety and security:** Provide physical security to utility environments with access control and video surveillance for real-time monitoring. Cisco products supported include Cisco Physical Access Gateways, Cisco Physical Access Manager, Video Surveillance (media servers, IP cameras, video storage, and video operations), and Cisco IP Interoperability and Collaboration System (IPICS).

**Professional services**: Engage Cisco experts in building end-to-end secure architectures to help plan, build, and run grid security solutions that help meet regulatory compliance requirements and provide protection from cybersecurity and physical security

Cisco Services for Grid Security deliver network and physical security to the grid by assisting utilities in defining security requirements, developing future-state grid security architectures, coordinating the deployment and integration of security solutions, and then delivering ongoing optimization and managed services. These services, available from Cisco and smart grid ecosystem partners, are based on industry best practices and proven methodologies for planning, building, and running end-to-end security infrastructures.

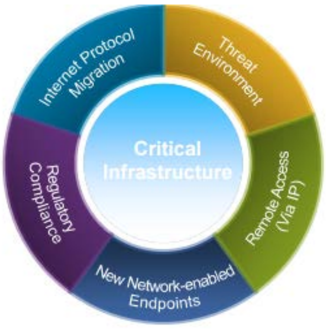


Figure 2: Critical Infrastructure

The above described are the some of the possibilities to provide grid security.Routers and Switches provide a number of mechanisms that, when properly implemented, increase the overall security and performance of the local network.

Hence the assumption of combination of routers and switches embedded in the form of grid may provide global security from base level to higher level.

## Future Work:

Implementation of Grid of Security with the inclusion of several resources effectively to acquire complete security over vast networks such as enterprise networks is under study.

## Conclusion:

In this paper, a knowledge of grid of security and its implementation possibilities are briefly explained with thorough study. The importance of grid of security lies in where the secured transmission and detection of data is needed within complex or huge network system.

## References:

[1] https://enwikipedia.org/wiki/Network_security

[2] http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf

[3] https://www.giac.org/paper/gsec/235/limitations-network-intrusion-detection/100739

[4] Network Security, Roberta Bragg, Mark Phodes-Ousley, Keith Strassberg, Tata McGraw-Hill Edition 2004

[5] Grid Computing, Joshy Joseph, Craig Fellenstein, Pearson Education 2004