Network Security using Integrated IP Address Management Framework

Bora Tejashri[1], Prof. Rokade M.D[2]

[1,2]*Dept. of Computer Engineering, SPCOE, SPPU, Maharashtra, India*

---***---

Abstract – *Networking has become an important factor in day to day life. It is having an great impact on development of country and it's economy. The distribution of digital service which are offered by telecom operators, relies on secure and consistent networks. The networks should be protected via the execution of a strict access control scheme for use of IP address & various resources. There is a need for an effective IP address management (IPAM) scheme which can be widely valid across the telecommunication management network. It is commended that all IP addresses for use in a telecommunication management network be statically allocated and must be registered before use. In a telecom operator, the operations and management of networks are usually carried out through a set of OSSs with different functions or managing scopes. In this paper, we will propose an IPAM framework which can be integrated with these OSSs. The proposed IPAM structure is constructed by the processes of IP address discovery and network access control systems.*

***Key Words*: Networking; IPAM; IP Address Discovery; Network Access Control; OSS Integration**

1. INTRODUCTION

Networking is a practise of connecting multiple computing devices in order to share resources, exchange files, & allow electronic communication. Now-a-days many different types of services are provided via networks. Many telecom operators adopted digital transformation to introduce digital technologies into all aspects of their business. In the world of digital transformation, telecom operators make use of a variety of digital technologies to create new revenue and to reduce operating expense (OPEX). The success of digital services relies on secure and reliable underlying networks. Here the cyber security plays an important role.

The increase of cyber security threats is a big challenge in the management of networks [1]. Some cyber security attacks occur in the intranet. As per the report [2] , over a quarter (28%) of attacks come from insiders. It is calculated that 20% of cyber security incidents and nearly 15% of the data ruptures derived from employee within the organization. [3] Furthermore, critical infrastructure is a high-value target for threat actors. [4] Therefore, telecom operators have become a big target for cyber attacks. Telecom operators provide network access widely in telco offices. A effective way to protect networks in telco offices is the implementation of a strict access control scheme for use of IP resources.

2. RELETED WORK

2.1 Problem Statement

There has been lot of problems regarding cyber security. The increase of cyber security threats is a big challenge in the management of telecom networks. Hence we propose an IPAM framework to flawlessly integrate IP address discovery and network access control with the current OSSs. IPAM framework will also help in detecting illegal or unregistered IP addresses.

3. ACCESS CONTROL & DISCOVERY OF IP ADDRESS

The work program NGOSS (New Generation Operations Software and Systems) [5] developed by TM Forum is to deliver a framework that will help in producing New Generation OSS(Operations Support Systems) solutions. Adapt quickly to a highly complicated and constantly changing operational environment, those OSSs also continuously evolve in the direction of the Open Digital Architecture (ODA) [6]. This paper addresses the need of efficient IP Address Discovery and Access Control (IPDAC) in OSSs.

The objective of IPDAC scheme is that the single OSS structure will have all subnets of the management network into a central control.The use of invalid IP addresses can be detected quickly. Immediately following the detection of invalid IP addresses is a network access control scheme, which limits the overflowing of illegal IP traffic. Thus, the IPDAC scheme can excellently confine the misuse of IP addresses within a small network area.

3.1 Concept of system design

In a telecommunication management network, most management functions are performed by OSSs. OSSs apply configurations to the network substructure to activate network services. OSSs are also in charge of network monitoring for confirming network QoS. With this a network administrator could remotely rescue the current states of network devices, make configuration changes, as well as perform other maintenance tasks. IPAM also treated as the source of truth for IP resources on the management network. But the IPAM functions, such as assignments and reconciliation of IP addresses, are often affected by OSSs.

Telecom operators typically have their own operations process with multiple management functions involved, like network inventory management, fault management, as well as service provisioning organization. Those supervision functions may change the configurations of IP resources. Hence, IPAM should not be an insulated island among OSSs. This paper suggests an IPDAC framework integrated with OSSs. The IPDAC structure cooperates with the inventory management and a centralized network controlling system to perform IP address detection and access control functions on the management network. There are four functional requirements in IPAC, stated as follow-

1) Registration of IP Address: Network list management is essential to enable network automation. For actual IPAM, the information connected to IP resources, containing network subnets as well as network devices, is essential to put into the inventory. The system should agree the registration of the IP addresses by manual operations otherwise automatic imports from the inventory. Audit logs should be delivered to allow administrators to track all the changes of IP resources.

2) Access Control of Network : This article enforces policy on network devices with access control, indicated in ACL. ACL is nothing but the Access Control List. The ACL can be designed based on layer-3 IP addresses otherwise layer-2 MAC addresses used for filtering IP and MAC layer traffic. The configuration of ACL can be consummate by Command-Line Interface (CLI) with commands varying from different network devices.

3) Reports: Statistics reports facilitate the accepting of each network subnet. In overall, statistics reports are useful for network security risk evaluation, IP resource measurement, as well as further provisioning of network resources.

4) Open APIs: A RESTful web service is essential to provide IPAM functions openly for the integration with OSSs. IPAM should support real-time security event notifications in a normal fashion for integration with the Security Information Event Management (SIEM) system used in OSSs. Critical security alerts will be sent out to inform security staff though abnormal activities are found.

3.2 Architecture of the proposed System

From the following Fig. 1, three OSSs Telecom are convoluted to offer IPDAC functionalities. The Provisioning and Management System (PAMS) is an OSS for network resource allocation as well as management. All register information of networks is operated in PAMS. The Security Information Event Management (SIEM) system delivers security log collection, security alert correlation analysis, and security event notification. The third OSS is *Argus*, a centralized network supervisory system for Network Operation Center (NOC).

Beyond the above three OSSs is the Rinpoche Integrated Network Operations System (RINOS), which is an SNMP-based OSS, which is an included NMS for Fault, Configuration, Accounting, Performance, and Security (FCAPS) management of underlying networks as well as devices. REST APIs are provided for communications between RINOS and the other OSSs. In the production environment, there are a single PAMS and an Argus system for all regions, however multiple RINOS systems are organized on telco offices for effective network monitoring on a large scale.

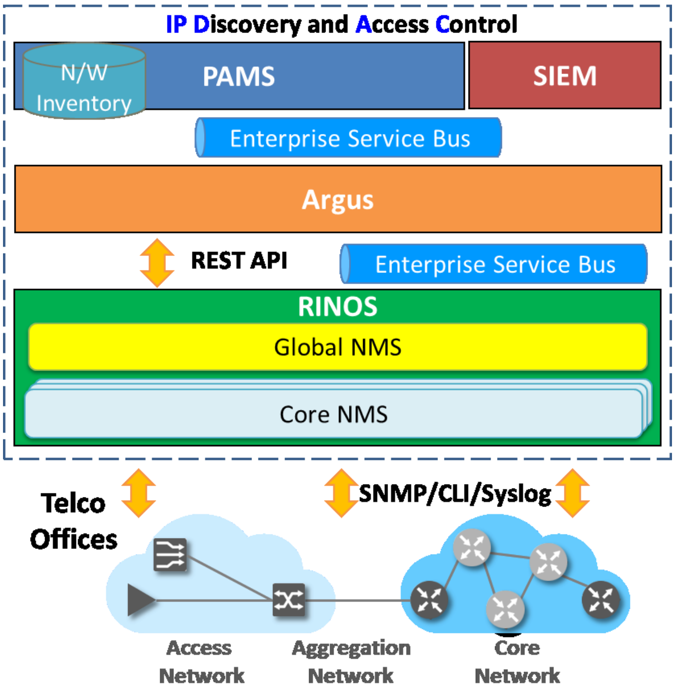

Fig. 1. System Framework of IPDAC

PAMS offers Argus with device inventory information including network subnets, IP addresses, MAC addresses, device types, corresponding administrators, and physical locations of network devices. The information is transported via the Enterprise Service Bus (ESB). When any unregistered IP address is noticed, SIEM will receive an alert from Argus via ESB, and then emit a security event to the corresponding administrator of the IP subnet where the unregistered IP address is located. Argus presents an integrated view of IP resources for the entire network. Argus is responsible for assigning administrators of IP subnets, approving IP address registration, and preparing analytical and statistical reports. The discovery of unregistered IP address is also performed by Argus. Argus periodically gathers a list of active IP/MAC addresses and makes a comparison with the registered IP/MAC addresses list to find any inconsistence.

There are two cases - One is the detection of a new IP address which is not registered before and the second is the inconsistent mapping of IP address and MAC address. Both will trigger security alerts sent to the SIEM. Argus gathers the list of the active IP/MAC addresses through RINOS. Actually, the two kernel functions of IPDAC, i.e., IP address discovery also access control, are performed by RINOS.

RINOS adopts a two-layered hierarchical model and consists of two entities, Global NMS and a set of Core NMSs.

Global NMS has a global view of all managed devices also can raise management tasks simultaneously across all Core NMSs. To provision the management of multi-vendor devices, RINOS unifies the view of manage devices via a variety of resource adaptors, which provide an intermediary abstraction of devices. The Global NMS in RINOS provides REST APIs to permit Argus to configure the access list of gateways. In addition, RINOS sends active IP/MAC address lists to Argus periodically via ESB. RINOS collects ARP tables from the gateways located in telco offices in every fifteen minutes.

There are two ways to recover ARP tables- One is the retrieval of the ipNetToMediaTable objects in MIB II by the SNMP protocol. This method put on to most gateways which support SNMP. The other is the custom of CLI commands for those gateways which will not show ARP tables on the Virtual Routing and Forwarding (VRF) interfaces. Next the collection of IP/MAC addresses, the active IP/MAC address list is presented in an XML document. The data in the XML document holds ARP tables of multiple network subnets, which are owned by those managed gateways in the NMS. In normal, each device contains of multiple ports and each port contains multiple elements (ARP entries) accessible in a hierarchical structure.

After an unregistered IP address is noticed and confirmed, appropriate access control will follow. RINOS is also in charge of the configuration of ACLs in gateways to permit network access of registered IP addresses and to prohibit the flooding of traffic from and to unregistered IP addresses in telco offices. The NAC operation is activated by Argus and is then implemented by RINOS.

4. NETWORK ACCESS CONTROL WITH ACL

This feature applies policy on network devices with access control, denoted in ACL (Access Control List). The ACL can be designed based on layer-3 IP addresses otherwise layer- 2 MAC addresses for filtering IP along with MAC layer traffic flow. The configuration of ACL can be proficient by Command-Line Interface (CLI) with commands varying from different network devices. Access Control List or ACL is an supplementary layer of security for your Amazon Virtual Private Cloud. Access Control List acts as a firewall for controlling opening and outlet traffic of one or more subnets.

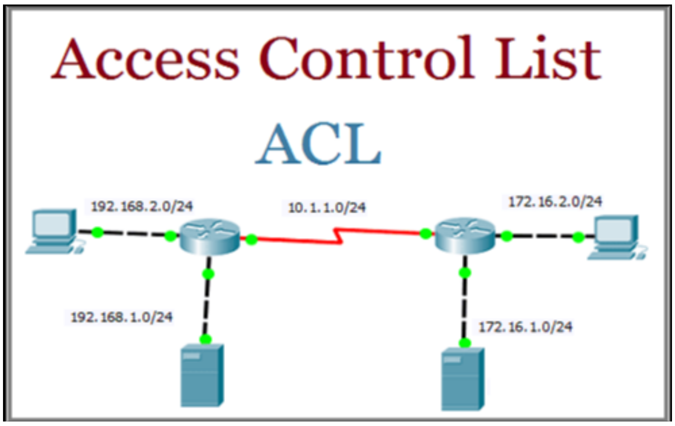

Figure 3.1: Network Access Control with ACL

5. APPLICATION

1. Security protection of a telecom management network.
2. Unregistered IP address discovery and network access control.
3. This framework can be used in various places where there is utilization of network or networks like- In company, in schools and colleges, in industries etc.
4. Protect networks against unauthorized access.
5. Useful in device Maintenance by providing protection from outer and inner attacks.

6. CONCLUSION

In the era of digital transformation, telecom operators make use of a variety of digital technologies to create new proceeds and to reduce operating expense (OPEX). The framework is meant to address the challenges facing in the security protection of a telecom management network and then projected a combined methodology for unregistered IP address discovery with network access control. As a result, the management cost for protecting networks can be reduced accordingly. The proposed IPDAC structure can protect networks against unapproved access, which is a dynamic task for telecom operators. Instead of developing an remote system, we recognize IPDAC functionalities through the existing OSSs.

ACKNOWLEDGEMENT

Authors want to acknowledge Principal, Head of Computer department and the guide for all the support and help rendered. To express profound feeling of gratitude to the regarded guardians for giving the motivation required to the finishing of paper.

REFERENCES

[1] Tse-han Wang, Yen-Cheng Chen, Yu-Tang Huang "IPDAC: An Integrated IP Address Management Framework for Telecommunication Management Networks" IEICE – The 20th APNOMS 2019

[2] Verizon, "2018 Data Breach Investigations Report," https://enterprise.verizon.com/resources/reports/2018/DBIR_2018_Report_execsummary.pdf, 2018.

[3]Verizon, "Insider Threat Report," https://enterprise.verizon.com/resources/reports/2019/insider-threat-report.pdf, 2019.

[4] Accenture, "Cyber Threatscape Report 2018: Midyear cybersecurity risk review," https://www.accenture.com/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf, September 2018.

[5] Timothy Rooney, "Introduction to IP Address Management," Wiley-IEEE Press, 2010.

[6] J. Strassner, J. Fleck, J. Huang, C. Faurer, T. Richardson, "TMF White Paper on NGOSS and MDA," November 2003.

[7] TM Forum, "Open Digital Architecture," https://www.tmforum.org/resources/whitepapers/open-digital-architecture, August 2018.