

RADIUS BASED AUTHENTICATION SYSTEM

Computer Network Mini Project



AUGUST 6, 2020
GIANT METREWAVE RADIO TELESCOPE (GMRT)
Khodad

RADIUS BASED AUTHENTICATION

Student Project

by

Pradnya Mangesh Umbarje

Department of Computer Engineering

Dr. D. Y. Patil Institute of Technology

Pimpri

Under the guidance of

Mr. Ajithkumar B



NCRA • TIFR

**GAINT METREWAVE RADIO TELESCOPE
NATIONAL CENTRE FOR RADIO ASTROPHYSICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
Khodad, Dist.-Pune – 410504**

August 2020

CERTIFICATE

This is to certify that Ms. Pradnya Umbarje of Dr. D. Y. Patil Institute of Technology, Pimpri has completed the project named “RADIUS Based Authentication” under the guidance of Mr. Ajitikumar B at the GMRT observatory NCRA-TIFR as a part of Student Training Program during August, 06 to September, 19 2020.

Ajitikumar B

Group Co-ordinator Backend

GMRT

ACKNOWLEDGEMENTS

I would like to thank the STP (Student Training Programme) Committee for selecting me to do the “**RADIUS Based Authentication**” Project at Giant Metrewave Radio Telescope (GMRT) and for providing the required environment for it. Many thanks to Mr. Ajith Kumar B for being a valuable guide and for helping me every step of the way. Many thanks to Mr. Sumit, a member of computer group, for explaining the GMRT Network and also for assigning me a machine to work on in the network. Last but not the least thanks to all at GMRT for all of their support, patience and suggestions. Most importantly, I would like to thank my entire family for all of their support with this and everything I undertake.

Miss. Pradnya Mangesh Umbarje

PREFACE

GMRT is a research centre for Radio Astrophysics. Since it's a research centre it has a big computer network. Many astronomers visit the site in a year. Astronomers are assigned particular machines. But sometimes there are some visitors, mostly the students, who wish to use the Internet service in their personal laptops apart from the machine assigned to them. So, it is necessary to design and install a system to allow such users to use the network for the only services for which he/she is entitled to. Currently if a user is allowed to connect to the network using DHCP, he gets all the privileges including some unnecessary ones which may cause security threat to the network.

One of the better solutions to this kind of problems is using RADIUS Server in the system. Running RADIUS on a server with MAC authentication will decide who will be allowed in the system and who will be denied or allowed to use pre-decided subset of the network services only. This will be done by maintaining a database of MAC addresses. The following project report is about how to install and configure RADIUS Server with MAC-based authentication. There is a detailed discussion of every component used while configuring the RADIUS Server.

For this project I was assigned a virtual machine running Centos8 on which I installed the RADIUS Server with necessary configurations in the switch. DHCP Servers and VLANs were already set up in the network. Setting DHCP Servers and VLANs is not in the scope of this project.

About GMRT

The Giant Metrewave Radio Telescope (GMRT) Observatory, located near Pune, Junnar, Narayangaon in India, is an array of thirty fully steerable parabolic radio telescopes of 45-meter diameter, observing at meter wavelengths. It is operated by the National Centre for Radio Astrophysics (NCRA), a part of the Tata Institute of Fundamental Research, Mumbai. At the time it was built, it was the world's largest interferometric array offering a baseline of up to 25 kilometers



Figure 2 Radio Telescope (GMRT Antenna)

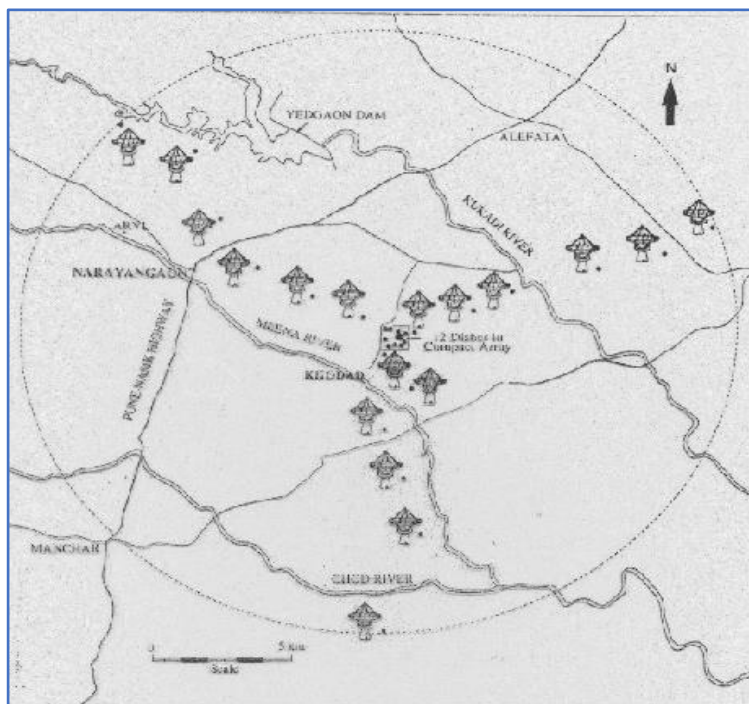


Figure 1 25km array GMRT with 30 Antennas

Contents

Sr. No	Title	Page No.
	Acknowledgements	
	Preface	
	About GMRT	
1	INTRODUCTION TO RADIUS	1
2	BACKGROUND	2
3	AAA PROTOCOL	3
3.1	TACACS, XTACACS and TACACS+	4
3.2	RADIUS and 802.1X	4
3.3	Diameter	5
4	SOFTWARE AND TOOLS USED	6
4.1	Software	6
	4.1.a FreeRADIUS	6
	4.1.b daloRADIUS	6
	4.1.c MySQL	6
4.2	Tools	7
	4.2.a phpMyAdmin	7
	4.2.b Wireshark	8
5	DHCP, VLAN AND SUBNETTING	9
5.1	DHCP	9
5.2	VLAN	10
	5.2.a MAC Address	11
	5.2.b IP Address	11
	5.2.c Network Mask	12
5.3	Subnetting	13
6	WORKING OF RADIUS PROTOCOL	14
7	FREERADIUS	16
	7.1 FreeRADIUS Installation	16
	7.2 Testing the RADIUS Server	17
	7.3 Working of FreeRADIUS Schema	18
8	MYSQL SETTING	19
	8.1 Installing MySQL	19
	8.2 Setting up RADIUS Database	20
9	DALORADIUS SETTING	21
	9.1 Installing Apache web server and PHP	21

	9.2	daloRADIUS Installation	22
10		SWITCH CONFIGURATIONS	24
	10.1	Setting Radius on D-Link dgs-3100-24 st switch	24
		10.1.a Configuring Guest VLAN	24
		10.1.b Configuring RADIUS Server	25
	10.2	Setting RADIUS on Cisco Switch	27
		10.2.a Configuring Guest VLAN	27
		10.2.b Configuring RADIUS Server	28
	10.3	10.3 Testing the complete system	29
		CONCLUSION	30
		REFERENCES	31

List of Figures

Sr. No.	Title	Page No.
1	Radio Telescope (GMRT Antenna)	
2	25km array GMRT with 30 Antennas	
3	FreeRADIUS logo	6
4	daloRADIUS logo	6
5	MySQL logo	7
6	phpMyAdmin logo	7
7	Wireshark logo	8
8	Virtual view of network and its subnetwork	13
9	Working of RADIUS	14
10	RADIUS Authentication & Authorization	16

11	Screenshot of RADIUS Server in debug mode	17
12	Screenshot of MySQL shell	19
13	Screenshot-Setting RADIUS Database	21
14	daloRADIUS Interface	23
15	Screenshot-802.1Q page	24
16	Screenshot-Guest VLAN page	25
17	Screenshot-Authentic RADIUS Server page	25
18	Screenshot-802.1X Setting page	26
19	Screenshot-showing port 16	26
20	Screenshot-Properties page	27
21	Screenshot-RADIUS page	28
22	Screenshot-Adding RADIUS Server	28

1 INTRODUCTION TO RADIUS

RADIUS (Remote Authentication Dial in User Service) is a security protocol used in AAA framework to provide centralised authentication for users who wish to use the network services.

The major Aim of this project is to study the Radius Based Authentication System and its feasibility at GMRT Network.

A RADIUS Server prevents your organization's private information from being leaked to snooping outsiders. It also allows easy depreciation capabilities and enables individual users to be assigned with unique network permissions. It can integrate into your existing system without any significant changes.

The Pros of RADIUS

- **Added security benefits:** RADIUS allows for unique credentials for each user, which lessens the threat of hackers infiltrating a network since there is no unified password shared among a number of people.
- **Avoids the pain of password management:** Unique credentials ensure that a shared password does not need routine changing, because each person manages their own. This saves time for a network admin, and users do not have to routinely seek out an updated password.
- **Central point for user and system authentication:** Through this, network admins have one point of contact for user management when it comes to authentication, authorization, and password management.
- **Great tool for larger networks managed by multiple admins:** RADIUS makes it easier to control who or what has access, and when. When it comes to hundreds or thousands of users in large corporations, only the correct, authorized people have access to a network of sensitive information. VLAN segmentation via attributes is a critical feature of RADIUS-driven networks.

The Cons

- **Traditionally implemented on-premises:** Maintenance can be difficult and time-consuming for on-premises hardware. Regular upkeep and monitoring means that, over time, the management of on-premises servers can be more intensive and frustrating.

- **Initial setup for a RADIUS server:** This can also be difficult for network admins to implement and integrate in an existing IT landscape, especially if the organization already supports on-premises, legacy services like Active Directory.
- **Vast array of configuration options:** On RADIUS servers, configuration and initial setup can be complicated and daunting with a wide range of protocols and compatibility issues. Even the most experienced network admins have to walk through a complex configuration process.
- **Choosing the right one for you:** When it comes to RADIUS server software and implementation models, it can be hard to know which is right for you. Some options can be costly and require long-term commitments, while others are free, and some require extensive time and effort to implement. The flood of information can be overwhelming and make it hard to choose the right service for you.

Working of RADIUS in Short

When other device wants to access Network Access Server (NAS-client of RADIUS), it will send access-request message to ACS server for the matching the credentials. In response to the access-request of the client, the ACS server will provide an access-accept message to the client if the credentials are valid and access-reject if the credentials do not match. A detailed explanation is given in further Chapters.

2 BACKGROUND

The operating system used on PCs and servers in GMRT network is mostly Linux. All the antenna control, data acquisition, correlator control is done through an inhouse developed software called ONLINE (which is being replaced by new feature rich software called TGC). The network and computers are maintained by the computer group. Linux based workstation and servers are used for data acquisition and analysis. Astronomers can use the computer facility from "Terminal/Image Room" for monitoring telescope operations whereas common computer facility for engineering staff is available at "Computer room". Telescope is mainly controlled from the "Control room" by telescope operators. Also, there are many computers and servers available in various LABs, depending on the LAB requirements which are connected to the GMRT LAN over ethernet.

Visiting astronomers at the GMRT are assigned temporary computer accounts. These accounts can be used to log in on any of the Linux workstations in the Terminal/Image Room.

If visiting astronomers wish to use his/her own laptop, there are many ethernet cables (connected to switch to one side and open at other end) available in the terminal room to which they can connect their laptop and configure it to use "DHCP".

There are no Wi-Fi hotspots provided throughout the GMRT observatory for obvious reason i.e., to avoid RFI which may create disturbance to the on-going, round the clock radio observations.

There are some visitors (like students, or new members) apart from the assigned users, wishing to use their laptops for carrying out various tests and projects. These users need to be given restricted access to the internal network of GMRT. It has been decided to implement this restricted access through RADIUS using open-source software and this is the subject of the project.

3 AAA PROTOCOL

The administrator can access any router or any network device through console. There would be many such devices in a given network physically located throughout the campus. Practically it is very inconvenient to go to the individual device location and access it through console. So, the alternative is to take remote access of the devices.

But as the remote access will be available by using an IP address therefore it is possible that an unauthorized user can take access using that same IP address therefore for security measures, we have to put authentication. Also, the packets exchange between the device should be encrypted so that any other person should not be able to capture that sensitive information. Therefore, a framework called AAA is used to provide that extra level of security.

AAA (Authentication, Authorization, Accounting) –

AAA is a standard based framework used to control who is permitted to use network resources (through authentication), what they are authorized to do (through authorization) and capture the actions performed while accessing the network (through accounting).

1. Authentication–

Process by which it can be identified that the user, which want to access the network resources, valid or not by asking some credentials such as username and password.

2. Authorization–

It provides capabilities to enforce policies on network resources after the user has gained access to the network resources through authentication. After the authentication is

successful, authorisation can be used to determine that what resources is the user allowed to access and the operations that can be performed.

3. Accounting–

It provides means of monitoring and capturing the activities by the user while using the network resources. It even monitors how long the user has an access to the network. The administrator can create an accounting method list to specify what should be accounted and to whom the accounting records should be sent.

Following are some authentication protocols based on AAA architecture –

3.1 TACACS, XTACACS and TACACS+

TACACS is the oldest AAA protocol using IP based authentication without any encryption (usernames and passwords were transported as plain text). Later version **XTACACS** (Extended TACACS) added authorization and accounting. Both of these protocols were later replaced by TACACS+. **TACACS+** separates the AAA components thus they can be segregated and handled on separate servers (It can even use another protocol for e.g., Authorization). It uses TCP (Transmission Control Protocol) for transport and encrypts the whole packet. TACACS+ is Cisco proprietary.

3.2 RADIUS and 802.1X

Remote Authentication Dial-In User Service (RADIUS) is a full AAA protocol commonly used by ISP. Credentials are mostly username-password combination based, it uses NAS and UDP protocol for transport.

RADIUS is a networking protocol, operating on port 1812, that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. RADIUS was developed by Livingston Enterprises, Inc. in 1991 as an access server authentication and accounting protocol and later brought into the Internet Engineering Task Force (IETF) standards. RADIUS is often the back-end of choice for 802.1X authentication as well.

IEEE 802.1X

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The **supplicant** is a client device (such as a laptop) that wishes to attach to the LAN. The

term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The **authenticator** is a network device which provides a data link between the client and the network and can allow or block network traffic between the two, such as an Ethernet switch or wireless access point; and the **authentication server** is typically a trusted server that can receive and respond to requests for network access, and can tell the authenticator if the connection is to be allowed, and various settings that should apply to that client's connection or setting. Authentication servers typically run software supporting the RADIUS and EAP protocols. In some cases, the authentication server software may be running on the authenticator hardware.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. With 802.1X port-based authentication, the supplicant must initially provide the required credentials to the authenticator - these will have been specified in advance by the network administrator, and could include a username/password or a permitted digital certificate. The authenticator forwards these credentials to the authentication server to decide whether access is to be granted. If the authentication server determines the credentials are valid, it informs the authenticator, which in turn allows the supplicant (client device) to access resources located on the protected side of the network.

3.3 Diameter

Diameter is an authentication, authorization, and accounting protocol for computer networks. It evolved from the earlier RADIUS protocol. It belongs to the application layer protocols in the internet protocol suite.

Diameter Applications extend the base protocol by adding new commands and/or attributes, such as those for use with the Extensible Authentication Protocol (EAP).

The name is a play on words, derived from the RADIUS protocol, which is the predecessor (a diameter is twice the radius). Diameter is not directly backwards compatible but provides an upgrade path for RADIUS. The main features provided by Diameter but lacking in RADIUS are:

- Support for SCTP
- Capability negotiation
- Application layer acknowledgements; Diameter defines failover methods and state machines (RFC 3539)

- Extensibility; new commands can be defined
- Aligned on 32-bit boundaries

Since, at present, there is no Authentication System whatsoever in the GMRT LAN and also due to compatibility issues, we started with RADIUS Authentication System which later can be enhanced. In RADIUS Authentication at present, we are using MAC Based authentication which in future can be changed to Single Sign-On (SSO) which will provide a username and password to the user.

4 SOFTWARE AND TOOLS USED

Following is the list of software components and tools with introductory description used to implement the Radius based solution.

4.1 Software

4.1.a FreeRADIUS



Figure 3
FreeRADIUS
logo

FreeRADIUS is a modular, high performance free RADIUS suite developed and distributed under the GNU General Public License, version 2, and is free for

download and use. The FreeRADIUS Suite includes a RADIUS server, a BSD-licensed RADIUS client library, a PAM library, an Apache module, and numerous additional RADIUS related utilities and development libraries. The server is fast, feature-rich, modular, and scalable. Modules included with the server core support LDAP, MySQL, PostgreSQL, Oracle, and many other databases. It supports all popular EAP authentication types, including PEAP and EAP-TTLS.

FreeRADIUS is the most widely deployed open-source server in the world. It serves as the basis for multiple commercial offerings, and it supplies the authentication, authorization and accounting (AAA) needs of many companies.

4.1.b daloRADIUS



Figure 3 daloRADIUS
logo

daloRADIUS is an advanced RADIUS web platform. It features rich user management, graphical reporting and accounting. daloRADIUS is written in PHP and JavaScript and it supports many database systems, among them the

popular MySQL, PostgreSQL, SQLite, MsSQL, and many others.

4.1.c MySQL



Figure 4 MySQL logo

MySQL is an open-source relational database management system (RDBMS). Its name is a combination of "My", the name of co-founder Michael Widenius's daughter, and "SQL", the abbreviation for Structured Query Language. A relational database organizes data into one or more data tables in which data types may be related to each other; these relations help structure the data. SQL is a language, programmers use to create, modify and extract data from the relational database, as well as control user access to the database. In addition to relational databases and SQL, an RDBMS like MySQL works with an operating system to implement a relational database in a computer's storage system, manages users, allows for network access and facilitates testing database integrity and creation of backups.

MySQL is free and open-source software under the terms of the GNU General Public License, and is also available under a variety of proprietary licenses. MySQL was owned and sponsored by the Swedish company MySQL AB, which was bought by Sun Microsystems (now Oracle Corporation).

MySQL is used with other programs to implement applications that need relational database capability. MySQL is a component of the LAMP web application software stack (and others), which is an acronym for *Linux, Apache, MySQL, Perl/PHP/Python*. MySQL is used by many database-driven web applications, including Drupal, Joomla, phpBB, and WordPress. MySQL is also used by many popular websites, including Facebook, Flickr, MediaWiki, Twitter, and YouTube.

4.2 Tools

4.2.a phpMyAdmin



Figure 5 phpMyAdmin logo

phpMyAdmin is a free and open-source administration tool for MySQL and MariaDB. As a portable web application written primarily in PHP, it has become one of the most popular MySQL administration tools, especially for web hosting services.

Features provided by the program include:

1. Web interface
2. MySQL and MariaDB database management
3. Import data from CSV and SQL
4. Export data to various formats: CSV, SQL, XML, PDF (via the TCPDF library), ISO/IEC 26300 - OpenDocument Text and Spreadsheet, Word, Excel, LaTeX and others
5. Administering multiple servers
6. Creating PDF graphics of the database layout
7. Creating complex queries using query-by-example (QBE)
8. Searching globally in a database or a subset of it
9. Transforming stored data into any format using a set of predefined functions, like displaying BLOB-data as image or download-link.
10. Live charts to monitor MySQL server activity like connections, processes, CPU/memory usage, etc.
11. Working with different operating systems.
12. Make complex SQL queries easier.

Note: This is not an absolute necessary tool. But this tool is very useful to handle the MySQL Database.

4.2.b Wireshark



Figure 6 Wireshark logo

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address. However, when capturing with a packet analyser in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. Port mirroring or various network taps extend capture to any point on the network. Simple passive taps are extremely resistant to tampering.

What does Wireshark do?

Wireshark intercepts traffic and converts that binary traffic into human-readable format. This makes it easy to identify what traffic is crossing your network, how much of it, how frequently, how much latency there is between certain hops, and so forth.

While Wireshark supports more than two thousand network protocols, many of them esoteric, uncommon, or old, the modern security professional will find analyzing IP packets to be of most immediate usefulness. The majority of the packets on your network are likely to be TCP, UDP, and ICMP.

Given the large volume of traffic that crosses a typical business network, Wireshark help you filter that traffic. Capture filters will collect only the types of traffic you're interested in, and display filters will help you zoom in on the traffic you want to inspect. The network protocol analyzer provides search tools, including regular expressions and colored highlighting, to make it easy to find what you're looking for.

Note: Wireshark was used to capture and analyze the requests coming to RADIUS Server in initial setup process.

5 DHCP, VLAN AND SUBNETTING

5.1 DHCP

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks, whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on the network, so they can communicate with other IP networks. A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices. In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address, or to assign itself an APIPA address, the latter of which will not enable it to communicate outside its local subnet.

The DHCP server has a pool of IP address available to it. When a device starts up, it broadcasts a message around the local network to find the DHCP server. Then the server gives it an IP address

from its pool. The server makes sure that it doesn't give the same IP address to more than one device. Also, there's no guarantee that the device will get the same IP address each time.

In GMRT network DHCP server has already been setup, and many ethernet cables have been provided for the its use. Before implementing RADIUS, if user connected his/her laptop to the ethernet cable, he/she used to get an IP address automatically, putting his/her laptop into the internal GMRT network.

In the implementations of RADIUS Based Access Control (MAC address-based access control), we setup a Guest VLAN. The user who connects the free ethernet cable to his/her laptop but has not registered his MAC address to the administrator will be assigned Guest VLAN. This will give user an appropriate IP address which will provide the Internet Connectivity but it will block the user from accessing the internal GMRT Network. Whereas a regular user who should be given access to the internal network needs to get permission from higher authorities and if it is approved, he needs to give the MAC address of his laptop to the administrator. Such user will get an appropriate IP address and the access to the internal network as defined by the administrator along with access to Internet. A database will be maintained of the MAC addresses connected to the RADIUS Server.

5.2 VLAN

A **virtual LAN (VLAN)** is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). *LAN* is the abbreviation for *local area network* and in this context *virtual* refers to a physical object recreated and altered by additional logic. VLANs work by applying tags to network frames and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.

VLANs allow network administrators to group hosts together even if the hosts are not directly connected to the same network switch. Because VLAN membership can be configured through software, this can greatly simplify network design and deployment. Without VLANs, grouping hosts according to their resource needs the labor of relocating nodes or rewiring data links.

To subdivide a network into VLANs, one configures network equipment. Simpler equipment can partition only per physical port (if at all), in which case each VLAN is connected with a dedicated network cable. More sophisticated devices can mark frames through VLAN tagging, so that a single

interconnect (*trunk*) may be used to transport data for multiple VLANs. Since VLANs share bandwidth, a VLAN trunk can use link aggregation, quality-of-service prioritization, or both to route data efficiently.

5.2.a MAC Address

A **media access control address (MAC address)** is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. This use is common in most IEEE 802 networking technologies, including Ethernet, Wi-Fi, and Bluetooth. Within the Open Systems Interconnection (OSI) network model, MAC addresses are used in the medium access control protocol sublayer of the data link layer. As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator. MAC addresses are primarily assigned by device manufacturers, and are therefore often referred to as the **burned-in address**, or as an **Ethernet hardware address**, **hardware address**, and *physical address*.

This is the address which switch finds out by learning process when one connects a laptop to a switch through ethernet cable. In our RADIUS setup, switch acts as a Network Access Server (NAS) which asks the RADIUS server (a server running freeRADIUS) by giving MAC address of the connecting laptop to which VLAN the connected laptop to be put in. The RADIUS server will have the database of privileged MAC id. If the MAC id given by switch is in the database the connecting laptop is assigned the privileged VLAN which will have internal network access capabilities otherwise it will be assigned Guest VLAN which will have minimal network access capabilities as defined by System-administrator. For example, Guest VLAN may have a separate DHCP server which will give complete different set of IP addresses which will be routed such that it will have only Internet access but will not have internal network access.

5.2.b IP Address

GMRT VLANs have IPv4 addresses only. So, following section discusses about IPv4 only.

An IP address is an address used in order to uniquely identify a device on an IP network. The address is made up of 32 bits, which can be divided into a network portion and host portion with the help of a subnet mask. The 32 bits binary addresses are broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot). For this reason, an IP address is said to be expressed in dotted decimal format (for example, 172.16.81.100). The value in each octet ranges from 0 to 255 decimal, or 00000000 - 11111111 binary.

1 1 1 1 1 1 1

128 64 32 16 8 4 2 1 (128+64+32+16+8+4+2+1=255)

And this sample shows an IP address represented in both binary and decimal.

10. 1. 23. 19 (decimal)

00001010.00000001.00010111.00010011 (binary)

These octets are broken down to provide an addressing scheme that can accommodate large and small networks. There are five different classes of networks, A to E.

In a Class A address, the first octet is the network portion. Octets 2, 3, and 4 (the next 24 bits) are for the network manager to divide into subnets and hosts as he/she sees fit. Class A addresses are used for networks that have more than 65,536 hosts (actually, up to 16777214 hosts!).

In a Class B address, the first two octets are the network portion. Octets 3 and 4 (16 bits) are for local subnets and hosts. Class B addresses are used for networks that have between 256 and 65534 hosts.

In a Class C address, the first three octets are the network portion. Octet 4 (8 bits) is for local subnets and hosts - perfect for networks with less than 254 hosts.

5.2.c Network Mask

A network mask helps you know which portion of the address identifies the network and which portion of the address identifies the node. Class A, B, and C networks have default masks, also known as natural masks, as shown here:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

5.3 Subnetting

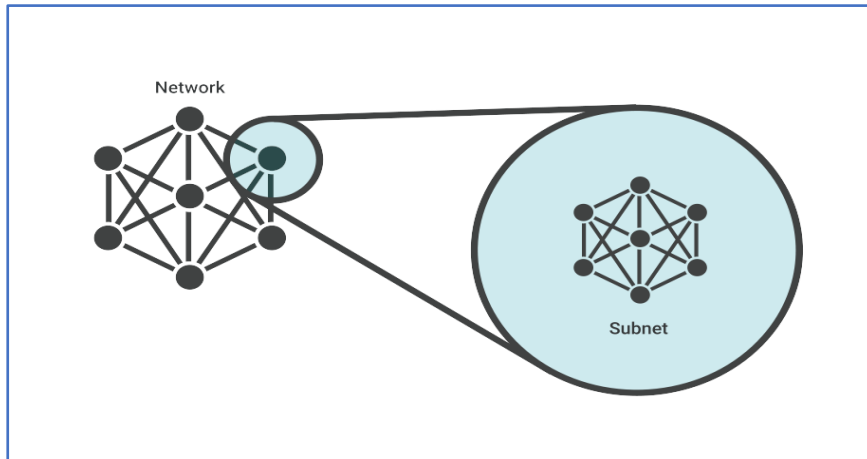


Figure 7 Virtual view of network and its subnetwork

A **subnetwork** or **subnet** is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called **subnetting**.

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic.

Each data link on a network must have a unique network ID, with every node on that link being a member of the same network. If you break a major network (Class A, B, or C) into smaller subnetworks, it allows you to create a network of interconnecting subnetworks. Each data link on this network would then have a unique network/subnetwork ID. Any device, or gateway, that connects n networks/subnetworks has n distinct IP addresses, one for each network / subnetwork that it interconnects.

In order to subnet a network, extend the natural mask with some of the bits from the host ID portion of the address in order to create a subnetwork ID. For example, given a Class C network of 204.17.5.0 which has a natural mask of 255.255.255.0, you can create subnets in this manner:

```
204.17.5.0 - 11001100.00010001.00000101.00000000
255.255.255.224 - 11111111.11111111.11111111.11100000
                -----|sub|----
```

By extending the mask to be 255.255.255.224, you have taken three bits (indicated by "sub") from the original host portion of the address and used them to make subnets. With these three bits, it is

possible to create eight subnets. With the remaining five host ID bits, each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device *since host ids of all zeros or all ones are not allowed*. So, with this in mind, these subnets have been created.

- 204.17.5.0 255.255.255.224 host address range 1 to 30
- 204.17.5.32 255.255.255.224 host address range 33 to 62
- 204.17.5.64 255.255.255.224 host address range 65 to 94
- 204.17.5.96 255.255.255.224 host address range 97 to 126
- 204.17.5.128 255.255.255.224 host address range 129 to 158
- 204.17.5.160 255.255.255.224 host address range 161 to 190
- 204.17.5.192 255.255.255.224 host address range 193 to 222
- 204.17.5.224 255.255.255.224 host address range 225 to 254

Note: The explanation in this part (DHCP, VLAN and Subnetting) was solely for understanding and study purpose. Two DHCP server (one in Guest VLAN and other in existing VLAN), VLAN and many subnets were already set up in the network.

6 WORKING OF RADIUS PROTOCOL

Communication between a network access server (NAS) and a RADIUS server is based on the User Datagram Protocol (UDP). RADIUS is a client/server protocol that runs in the application layer. The RADIUS client is typically a NAS and the RADIUS server is usually a daemon process running on a LINUX, UNIX or Windows NT machine. The client passes user information to designated RADIUS servers and acts on the response that is returned. RADIUS servers receive user connection requests, authenticate the user, and then returns the configuration information necessary for the client to deliver service to the user. This figure shows the interaction between a dial-in user and the RADIUS client and server.

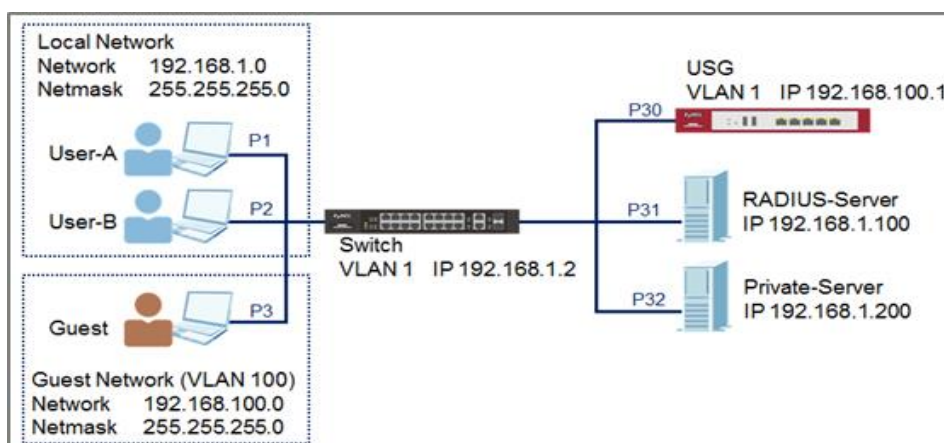


Figure 8 Working of RADIUS

1. User initiates PPP authentication to the NAS.
2. NAS prompts for username and password (if Password Authentication Protocol [PAP]) or challenge (if Challenge Handshake Authentication Protocol [CHAP]).
3. User replies.
4. RADIUS client sends username and encrypted password to the RADIUS server.
5. RADIUS server responds with Accept, Reject, or Challenge.
6. The RADIUS client acts upon services and services parameters bundled with Accept or Reject.

Authentication and Authorization

The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms.

Typically, a user login consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server. The Access-Request packet contains the username, encrypted password, NAS IP address, and port. The early deployment of RADIUS was done using UDP port number 1645, which conflicts with the "data metrics" service. Because of this conflict, RFC 2865 officially assigned port number 1812 for RADIUS.

When the RADIUS server receives the Access-Request from the NAS, it searches a database for the username listed. If the username does not exist in the database, either a default profile is loaded or the RADIUS server immediately sends an Access-Reject message. This Access-Reject message can be accompanied by a text message indicating the reason for the refusal.

In RADIUS, authentication and authorization are coupled together. If the username is found and the password is correct, the RADIUS server returns an Access-Accept response, including a list of attribute-value pairs that describe the parameters to be used for this session. Typical parameters include service type (shell or framed), protocol type, IP address to assign the user (static or dynamic), access list to apply, or a static route to install in the NAS routing table. The configuration information in the RADIUS server defines what will be installed on the NAS. The figure below illustrates the RADIUS authentication and authorization sequence.

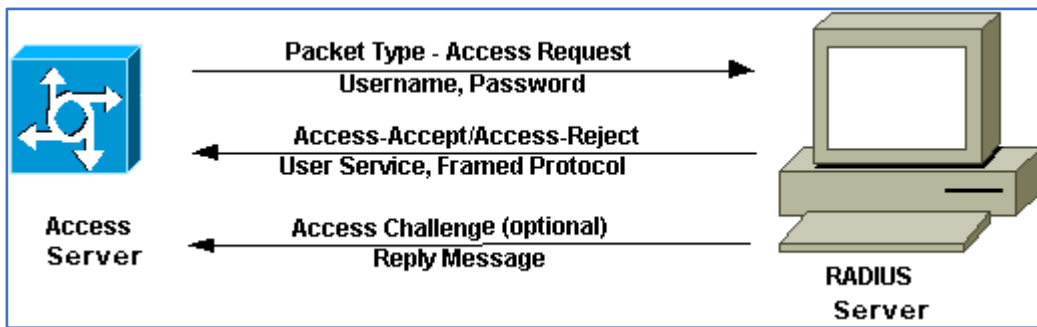


Figure 9 RADIUS Authentication & Authorization

Accounting

The accounting features of the RADIUS protocol can be used independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of sessions, indicating the number of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use RADIUS access control and accounting software to meet special security and billing needs. The accounting port for RADIUS is 1813.

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, user passwords are sent encrypted between the client and RADIUS server to eliminate the possibility that someone snooping on an insecure network could determine a user's password.

7 FREERADIUS

Following steps were carried out on gmrtad3, a CentOS 8 based virtual machine, which acted as RADIUS server.

7.1 FreeRADIUS Installation

1. Use the **dnf module list** command to list the modules available to our system related to **FreeRADIUS**.

```
$ sudo dnf module list freeradius
```

2. Install the FreeRADIUS module, FreeRADIUS client utilities, and the MySQL module for FreeRADIUS.

```
$ sudo dnf install -y @freeradius freeradius-utils freeradius-mysql
```

3. Start the RADIUS service:

```
$ sudo systemctl enable --now radiusd.service
```

4. Check the status of the service to make sure it's active and there are no issues so far

```
$ systemctl status radiusd.service
```

7.2 Testing the RADIUS Server

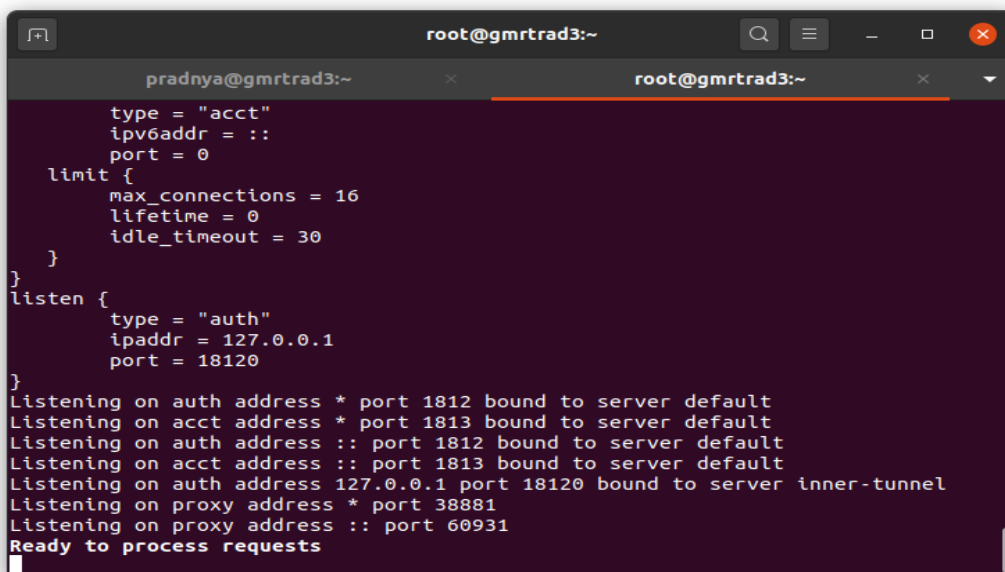
To test that FreeRADIUS works we'll run it in **debug mode** which is a very useful feature of FreeRADIUS in testing mode. To do this we'll first have to stop the current running process. If we run it in debug mode while the other process is still running, then we'll get an error.

To stop the current process, stop the service by running:

```
$ sudo systemctl stop radiusd.service
```

Run the RADIUS server in debug mode:

```
$ sudo radiusd -X
```



```
root@gmrtrad3:~  
pradnya@gmrtrad3:~  
type = "acct"  
ipv6addr = ::  
port = 0  
limit {  
    max_connections = 16  
    lifetime = 0  
    idle_timeout = 30  
}  
listen {  
    type = "auth"  
    ipaddr = 127.0.0.1  
    port = 18120  
}  
Listening on acct address * port 1812 bound to server default  
Listening on acct address * port 1813 bound to server default  
Listening on auth address :: port 1812 bound to server default  
Listening on acct address :: port 1813 bound to server default  
Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel  
Listening on proxy address * port 38881  
Listening on proxy address :: port 60931  
Ready to process requests
```

Figure 10 Screenshot of RADIUS Server in debug mode

If the output looks good then stop debug mode by pressing Ctrl+C, and start the service again by running:

```
$ sudo systemctl start radiusd.service
```

7.3 Working of FreeRADIUS schema

The SQL module employs two sets of check and reply item tables for processing in the authorization stage. One set of tables (radcheck and radreply) are specific to a single user. The other set of tables (radgroupcheck and radgroupreply) is used to apply check and reply items to users that are members of a certain SQL group. The usergroup table provides the list of groups each user is a member of along with a priority field to control the order in which groups are processed.

When a request comes into the server and is processed by the SQL module, the flow goes something like this:

- Search the radcheck table for any check attributes specific to the user
- If check attributes are found, and there's a match, pull the reply items from the radreply table for this user and add them to the reply
- Group processing then begins if any of the following conditions are met:
 - The user IS NOT found in radcheck
 - The user IS found in radcheck, but the check items don't match
 - The user IS found in radcheck, the check items DO match AND Fall-Through is set in the radreply table
 - The user IS found in radcheck, the check items DO match AND the read_groups directive is set to 'yes'
- If groups are to be processed for this user, the first thing that is done is the list of groups this user is a member of is pulled from the usergroup table ordered by the priority field. The priority field of the usergroup table allows us to control the order in which groups are processed, so that we can emulate the ordering in the users file. This can be important in many cases. For each group this user is a member of, the corresponding check items are pulled from radgroupcheck table and compared with the request. If there is a match, the reply items for this group are pulled from the radgroupreply table and applied.
- Processing continues to the next group IF:
 - There was not a match for the last group's check items OR
 - Fall-Through was set in the last group's reply items (The above is exactly the same as in the users file)

- Finally, if the user has a control: User-Profile attribute set or the Default Profile option is set in the `sql.conf`, then steps 4-6 are repeated for the groups that the profile is a member of.

8 MYSQL SETTING

8.1 Installing MySQL

1. Install the MySQL 8.0 server by using the CentOS package manager as root or user with sudo privileges

```
$ sudo dnf module -y install mysql:8.0
```

2. Run the `mysql_secure_installation` script that performs several security-related operations and sets the MySQL root password:

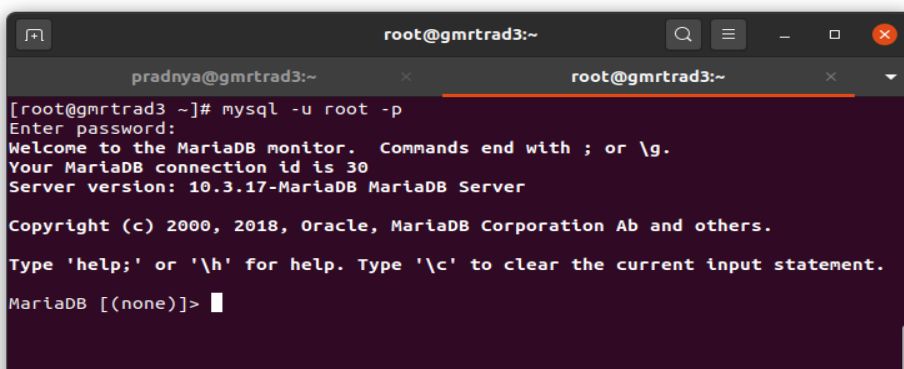
```
$ sudo mysql_secure_installation
```

Once you set the root password, the script will also ask you to remove the anonymous user, restrict root user access to the local machine, and remove the test database. You should answer “Y” (yes) to all questions.

3. To interact with the MySQL server from the command line, use the MySQL client utility, which is installed as a dependency. Test the root access by typing:

```
$ mysql -u root -p
```

Enter the root password when prompted, and you will be presented with the MySQL shell



```
root@gmrtrad3:~  
pradnya@gmrtrad3:~  
root@gmrtrad3:~  
[root@gmrtrad3 ~]# mysql -u root -p  
Enter password:  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 30  
Server version: 10.3.17-MariaDB MariaDB Server  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
MariaDB [(none)]> |
```

Figure 11 Screenshot of MySQL shell

8.2 Setting up RADIUS database

1. First, we need to create a new empty 'radius' database in SQL and a database user with permissions to that database.

```
mysql -u root -p
    CREATE DATABASE radius;
    GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY
    "radpass";
    exit
```

Note: use a more secure password than "radpass" in the above example

2. Next import the RADIUS MySQL schema into the newly created database:

```
$ sudo su -l
$ mysql -u root -p radius < /etc/raddb/mods-
config/sql/main/mysql/schema.sql
```

3. Create a soft link for SQL under /etc/raddb/mods-enabled/

```
$ sudo ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-
enabled/
```

4. Now we'll configure FreeRADIUS to use MySQL. We do this by editing the file **/etc/raddb/mods-available/sql**. You can use your favorite text editor.

```
$ sudo vim /etc/raddb/mods-available/sql
```

The file is long, due explanations and lines that are commented out, but we'll just edit a few lines:

1. Change driver = "rlm_sql_null" to driver = "rlm_sql_mysql"
2. Change dialect = "sqlite" to dialect = "mysql"
3. Uncomment **server**, **port**, **login**, and **password**, and also change some of their values.

Change them by uncommenting them and changing their values to correspond to the database and user you created earlier:

```
server = "localhost"
port = 3306
login = "radius"
password = "radius"
```

Figure 12 Screenshot-Setting RADIUS Database

4. Uncomment the line containing `read_clients = yes`, by removing the `#` symbol at the beginning of the line.
5. Save the file.

5. Now change the group rights of the file we just edited to **radiusd**:

```
$ sudo chgrp -h radiusd /etc/raddb/mods-enabled/sql
```

And restart the **radiusd** service:

Since we've made significant changes, we'll test again in debug mode to make sure FreeRADIUS is working. Stop the **radiusd** service. And run it in debug mode.

FreeRADIUS is installed and working with MySQL on your CentOS 8 server.

9 DALORADIUS SETTING

9.1 Installing Apache web server and PHP

We'll use Apache httpd server to host daloRADIUS on CentOS 8 system. Install both httpd and PHP packages with the following command.

```
$ sudo dnf -y install @httpd @php
```

```
$ sudo dnf -y install php- {cli, curl, mysqlnd, devel, gd, pear,
mbstring, xml, pear}
```

```
$ sudo pear install MDB2
```

If you have firewall enabled, we need to enable HTTP connections to Apache

9.2 DaloRADIUS Installation

1. Install **wget**

```
$ sudo dnf -y install wget
```

2. Download the daloRADIUS from GitHub:

```
$ cd /tmp && wget  
https://github.com/lirantal/daloradius/archive/master.zip
```

Unzip the daloRADIUS archive, and move it into the DocumentRoot.

Document root file is the folder where website files for a specific domain are stored. It's important to have a unique folder for each domain as cPanel allows for multiple domains (subdomains and add-on domains).

3. After installation of Apache, the document root file is located at the `/var/www/html/` by default but we can change the location of the directory later.

```
$ sudo dnf -y install unzip  
$ unzip master.zip  
$ sudo mv daloradius-master/ /var/www/html/daloradius
```

4. Navigate via **cd** in the daloradius folder **/var/www/html/daloradius** so we can easily import daloRADIUS MySQL tables:

```
$ cd /var/www/html/daloradius  
$ mysql -u root -p radius < contrib/db/fr2-mysql-daloradius-and-  
freeradius.sql  
$ mysql -u root -p radius < contrib/db/mysql-daloradius.sql
```

5. Now change the ownership of the daloradius folder to the Apache webserver, and we'll also make the daloradius.conf.php configuration file writable by the webserver.

```
$ sudo chown -R apache:apache /var/www/html/daloradius/  
$ sudo chmod 664  
/var/www/html/daloradius/library/daloradius.conf.php
```

6. Open the `daloradius.conf.php` configuration file so we can edit MySQL information:

```
$ sudo vim /var/www/html/daloradius/library/daloradius.conf.php
```

Change the values to your database user/password/database name:

```
$ configValues['CONFIG_DB_HOST'] = 'localhost';  
$ configValues['CONFIG_DB_PORT'] = '3306';  
$ configValues['CONFIG_DB_USER'] = 'radius';  
$ configValues['CONFIG_DB_PASS'] = 'Somestrongpassword_321';  
$ configValues['CONFIG_DB_NAME'] = 'radius';
```

7. Save and exit the file

8. Restart the **radiusd** service and check its status to make sure it's working.

Now the daloRADIUS will be installed and working. To use it visit the daloRADIUS site:

<http://localhost/daloradius/login.php>

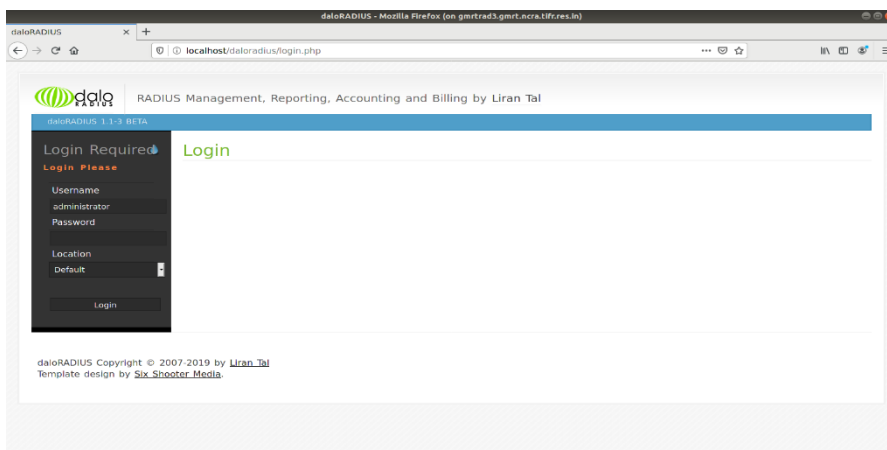


Figure 13 daloRADIUS Interface

Change the password of daloRADIUS, default password is radius.

10 SWITCH CONFIGURATIONS

As per the requirement, the incoming user, if authenticated and authorized, should be allowed by RADIUS in the GMRT network. And if the user is not authorized it is to be put into the guest VLAN where he will get the Guest privileges only as set up by the Administrator. This authentication and authorization will be MAC based as stated earlier. So, in the switches to be configured there are two important settings to be done

- 1) Guest VLAN set up and
- 2) RADIUS Set up.

There are mainly two types of the edge switches in GMRT in the visitor areas.

- a) D-Link DGS-3100-24 ST
- b) Cisco SG300-28 28-Port Gigabit Managed Switch

Both switches are managed switches and they were configured for RADIUS as follows.

10.1 Setting RADIUS on D-Link DGS-3100-24 ST Switch

10.1.a Configuring Guest VLAN

1. In order to configure a guest VLAN, the user is required to create a VLAN first. In the following example we create VLAN 22 via **L2 Features > 802.1Q VLAN**. This opens 802.1Q VLAN page:

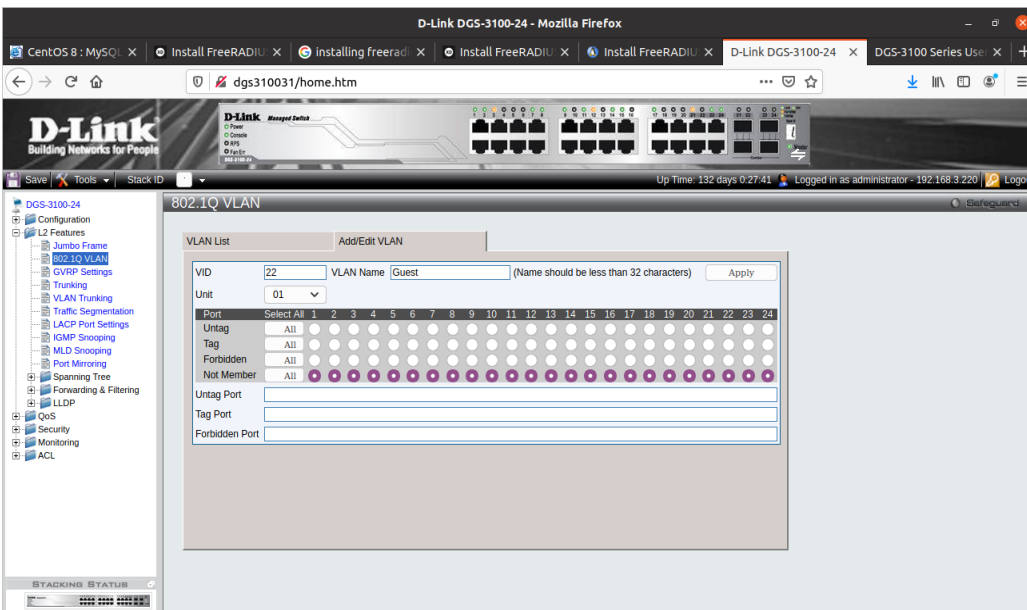


Figure 14 Screenshot-802.1Q page

2.To assign ports to the Guest VLAN click **Security > Guest Vlan**. The Guest VLAN Page opens:

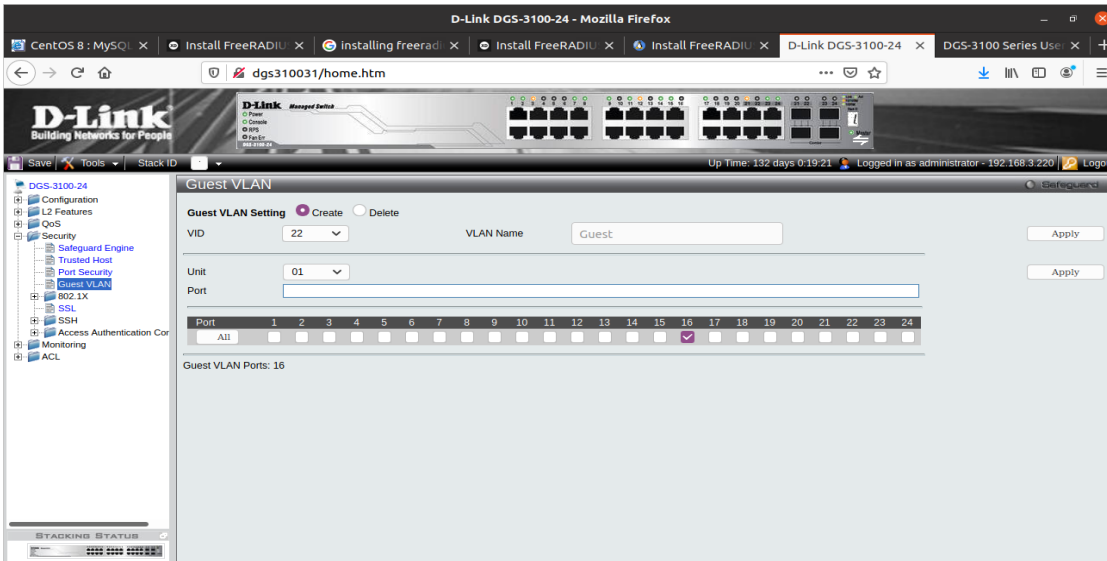


Figure 15 Screenshot-Guest VLAN page

3.Click Create in Guest VLAN Setting. Select the VLAN to be made as guest VLAN from VID drop down list which is 22 in this example.

10.1.b Configuring RADIUS server

After the ports are assigned to the Guest VLAN, the user needs to configure a Radius Server that will hold the MAC Authentication database.

1. Click **Security > 802.1X > Authentic RADIUS Server** page according to the example below. Give the correct IP of the RADIUS Server and apply it.

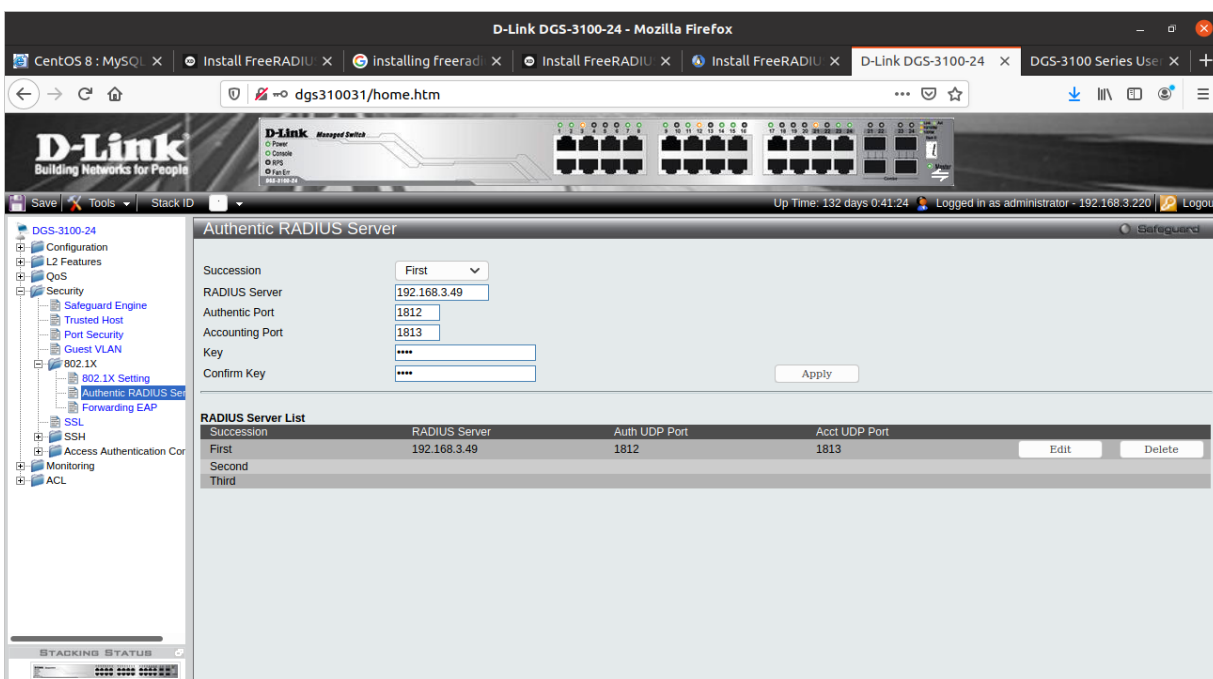


Figure 16 Screenshot-Authentic RADIUS Server page

2. Click **Security > 802.1X > 802.1X Setting page**: first, 802.1x should be enabled globally and in the port level menu, 802.1x Control should be configured as ‘ForceAuthorized’.

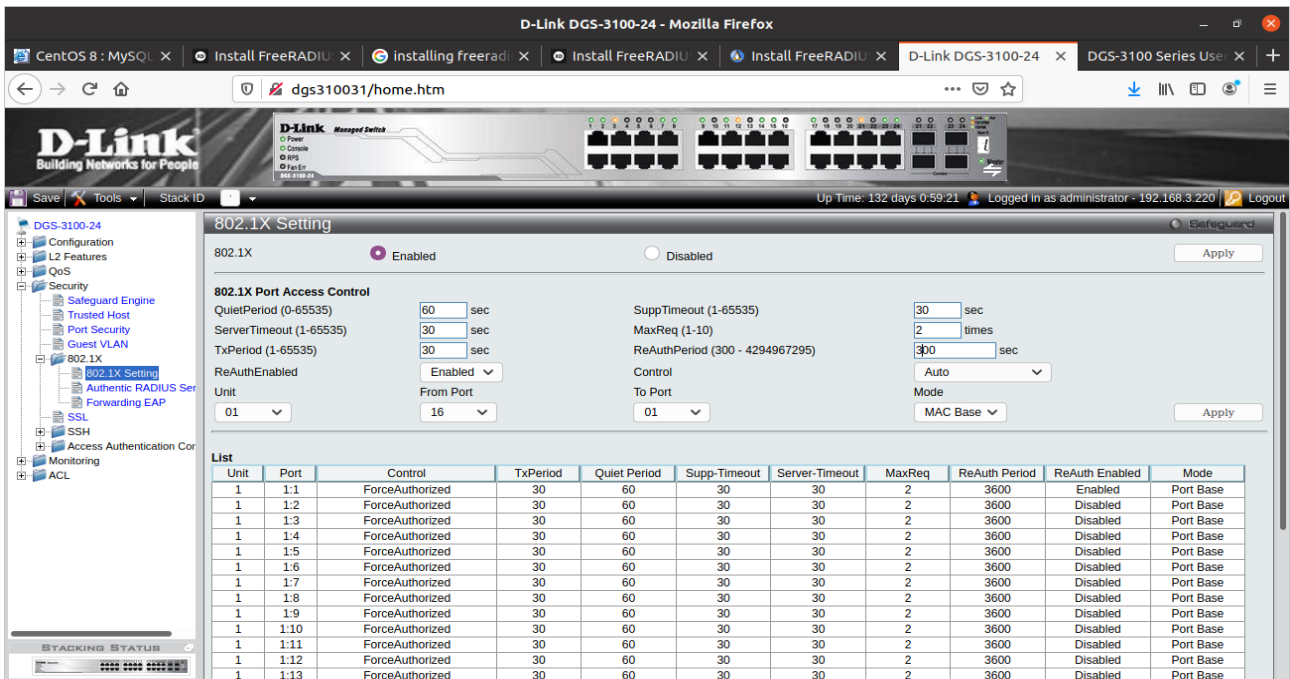


Figure 17 Screenshot-802.1X Setting page

3. Configure the required ports as ‘MAC Based’ authentication (opposite to ‘Port Based’ authentication)

4. Set the port control to ‘Auto’, this will complete the setting of MAC Authentication for the required ports.

The screenshot shows a detailed view of the port configuration table. Port 1:16 is highlighted, showing its configuration as 'Auto' control, 'MAC Base' mode, and 'Enabled' ReAuth status. The rest of the table is identical to the one in Figure 17.

Unit	Port	Control	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled	Mode
1	1:1	ForceAuthorized	30	60	30	30	2	3600	Enabled	Port Base
1	1:2	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:3	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:4	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:5	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:6	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:7	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:8	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:9	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:10	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:11	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:12	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:13	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:14	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:15	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:16	Auto	30	60	30	30	2	300	Enabled	MAC Base
1	1:17	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:18	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:19	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:20	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:21	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:22	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:23	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base
1	1:24	ForceAuthorized	30	60	30	30	2	3600	Disabled	Port Base

Figure 18 Screenshot-showing port 16

Now, when a user connects to the 16th port of the switch, it’s MAC Address will be checked in the radius schema. If MAC address is present the user will be in GMRT network or else it will be put

into Guest VLAN 22 by the FreeRADIUS.

10.2 Setting RADIUS on Cisco Switch

10.2.a Configuring Guest VLAN

1. Click **Security > 802.1X/MAC/Web Authentication > Properties.**

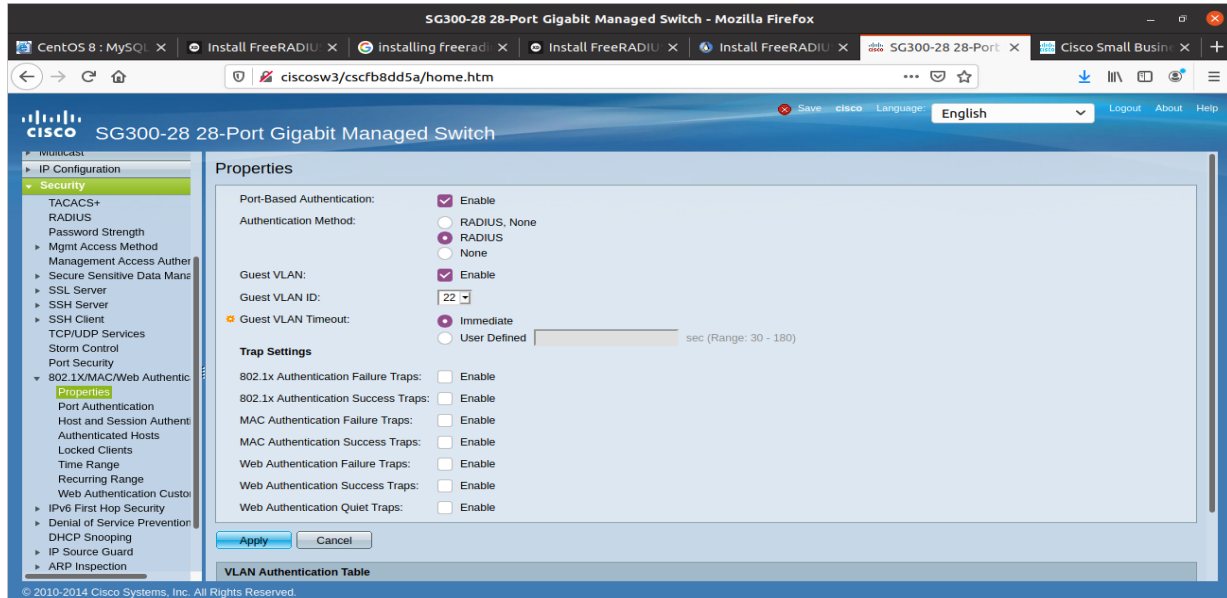


Figure 19 Screenshot-Properties page

2. Select Enable in the Guest VLAN field.
3. Select the guest VLAN in the Guest VLAN ID field.
4. Configure the Guest VLAN Timeout to be either Immediate or enter a value in the User defined field.
5. Click **Apply**, and the Running Configuration file is updated.

10.2.b Configuring RADIUS server

1. Click Security > RADIUS.

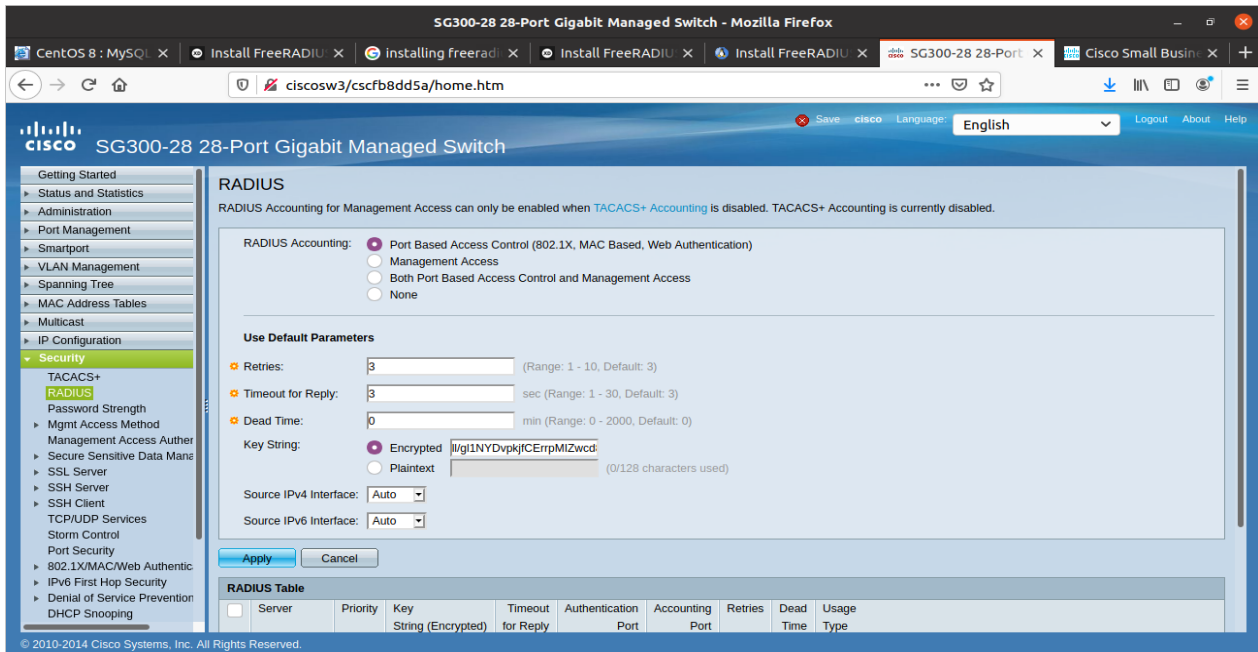


Figure 20 Screenshot-RADIUS page

2. Enter the RADIUS Accounting option.

3. Enter the default RADIUS parameters if required. Values entered in the Default Parameters are applied to all servers. If a value is not entered for a specific server (in the Add RADIUS Server page) the device uses the values in these fields.

4. Click **Apply**. The RADIUS default settings for the device are updated in the Running Configuration file.

To add a RADIUS server, click **Add**.

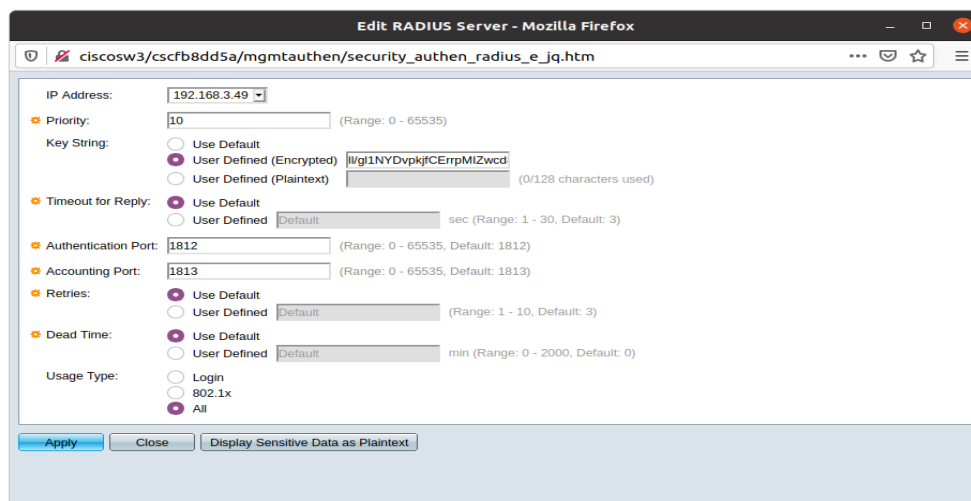


Figure 21 Screenshot-Adding RADIUS Server

5. Enter the values in the fields for each RADIUS server. To use the default values entered in the RADIUS page, select Use Default.
6. To display sensitive data in plaintext form in the configuration file, click Display Sensitive Data as Plaintext.
7. Click Apply. The RADIUS server definition is added to the Running Configuration file of the device.

10.3 Testing the complete system

On both of these switches on specific ports where RADIUS authentication is configured, we connected the laptop once with entry into the RADIUS database and once removing the entry from the database using the daloRADIUS interface.

When we connected with entry, the laptop got the correct internal VLAN IP through DHCP server and seamlessly integrated into the GMRT internal LAN. Also, when we removed the entry from the RADIUS database laptop got different IP address through which the laptop was getting Internet Connectivity but was not reaching to the internal network.

CONCLUSION

The uses and benefits of RADIUS Servers are wide-reaching.

RADIUS is open standard; therefore, it can be used on most of the devices. It has greater extensive accounting support than TACACS+.

It can be integrated into the existing system without any significant changes.

In future, it can be modified to use Username and Password from centralized user authentication database like LDAP instead of MAC Based Authentication.

REFERENCES

- ✓ Official site of GMRT: <http://www.gmrt.ncra.tifr.res.in/>
 - <http://www.ncra.tifr.res.in/>
- ✓ Official site of FreeRADIUS: <https://freeradius.org/>
- ✓ daloRADIUS Interface: <http://daloradius.com/>
- ✓ BOOK: Computer Networks, 5e (5th edition) By Andrew S. Tanenbaum
- ✓ Site for some commands: <https://bytexd.com/freeradius-centos/>
- ✓ D-Link DGS-3100 User Manual
- ✓ Cisco SW3 User Manual
- ✓ Wikipedia