Cambium Networks™

End to End RADIUS Security with Cambium Networks

Table of Contents

3 **Overview**

3 **End to End RADIUS Support with Cambium Portfolio**

3 **High Level RADIUS Architecture**

5 **RADIUS Configuration**

5 Radios RADIUS Configuration

5 RADIUS Server Configuration

6 Sample RADIUS Server Configuration

6 RADIUS Client Configuration

7 RADIUS User Configuration

8 **Summary**

8 **About Cambium Networks**

8 **Glossary**

Overview

Remote Authentication Dial-In User Service (RADIUS) is commonly used to provide centralized authentication, authorization, and accounting for dial-up, virtual private network, and, more recently fixed wireless network access.

Cambium Networks provides an extensive portfolio of fixed wireless broadband solutions ranging from point-to-point to point-to-multipoint to WiFi; and covering both licensed and unlicensed spectrum. Is RADIUS supported by all these products? Can the operator use one single RADIUS server to manage authentication of all the devices and user accounts? The answer is “Yes”.

This article discusses how to implement RADIUS security across the Cambium Networks wireless broadband product portfolio.

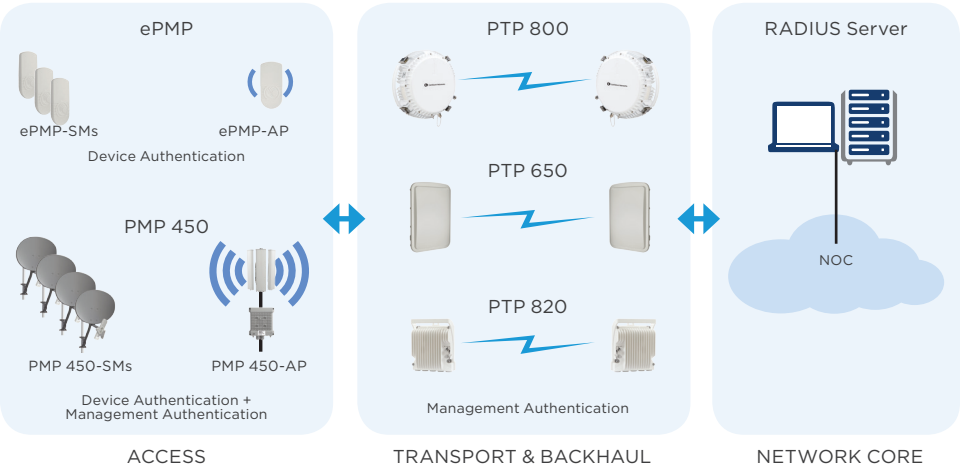

Figure 1: End to End wireless broadband network supported by single RADIUS server

End to End RADIUS Support with Cambium Portfolio

Figure 1 illustrates the relationship between the access, transport and backhaul layers, and the authentication of the administrator accounts by a single RADIUS server. In addition, at the access layer, all Subscriber Module (SM) can be authenticated by the same single RADIUS server residing in the NOC.

Table 1 summarizes which authentication methods/technologies are used by each product.

Product Name	Device Authentication	Admin User Authentication	Device Authentication Method	Admin User Authentication Method
PTP 820	No	Yes	N/A	PAP
PTP 800	No	Yes	N/A	MS-CHAPv2/CHAP
PTP 650 / 700	No	Yes	N/A	MS-CHAPv2/CHAP
PMP 450 AP	No	Yes	N/A	EAP-md5
PMP 450 SM	Yes	Yes	MS-CHAPv2 over EAP-TTLS	EAP-md5
ePMP AP	No	Local Only/Non RADIUS	N/A	N/A
ePMP SM	Yes	Local only/Non RADIUS	MS-CHAPv2 over EAP-TTLS	N/A

Table 1: Authentication methods supported by different products.

High Level RADIUS Architecture

There are three logical components in a RADIUS authentication architecture. They are the RADIUS Server, the RADIUS Client and the RADIUS User.

RADIUS Server is the entity that contains all provisioning information and it authenticates the RADIUS Users. The provisioning/authorization information of the users are stored in the RADIUS server database.

RADIUS Client is the entity that needs help to decide whether a device is allowed to connect to the network or an administrator is allowed to login to the system. The RADIUS client will communicate with the RADIUS server for authentication of the RADIUS users. Each RADIUS

client needs to be provisioned as a RADIUS client in the RADIUS server with its IP address and have a shared secret with the RADIUS server so it can be trusted by the RADIUS server.

RADIUS User is the entity being authenticated. It can be either network device or network administrator. When the RADIUS user requests access to the network, it will communicate via the RADIUS client to be authenticated by the RADIUS server. If the RADIUS user successfully passes the authentication, the RADIUS server will inform the RADIUS client to allow network access by the RADIUS user.

As a part of the authentication success response message, certain configuration parameters such as Vendor Specific Attributes (VSA) can be passed from the RADIUS server to the RADIUS user for device configuration or user authorization. Each RADIUS user needs to be provisioned in the RADIUS server. The provisioning information will include user name, password and VSA (The VSAs are defined in dictionary files that can be downloaded from Cambium Website). Device user authentications are done via EAP-TLS secure tunnel while administrator user authentications are done with less secure technologies such as EAP-MD5 and CHAP etc. because the administrators are typically logging in from the NOC.

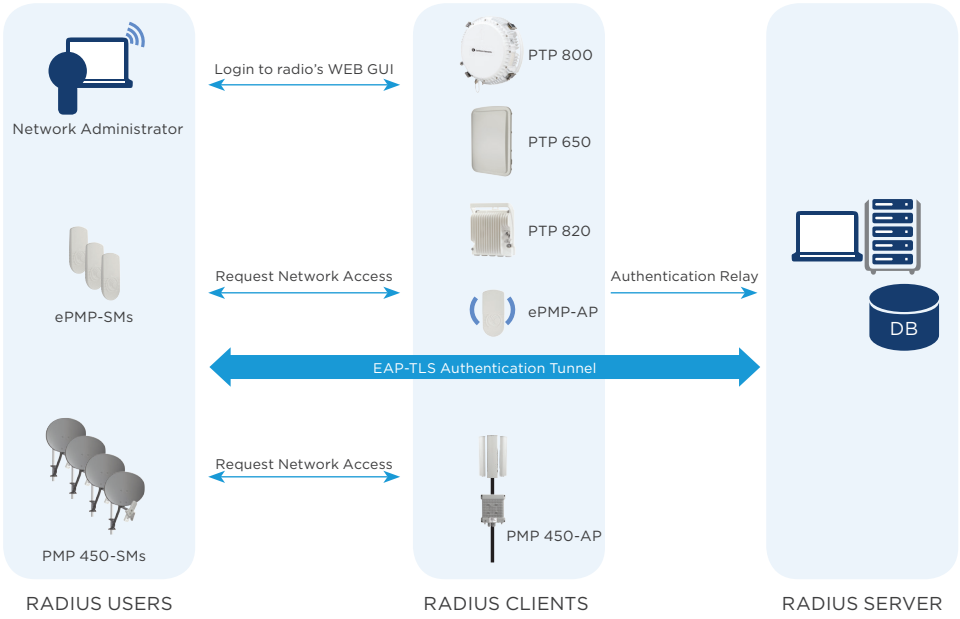

Figure 2: End to End wireless broadband network supported by single RADIUS server

Figure 2 shows the logical entities in a Cambium product portfolio based authentication system. One can see that device authentication is performed through an EAP-TLS tunnel between the RADIUS server and the device (RADIUS user). As a result, the RADIUS server needs to have an X509 certificate of its own and knows about its private key while the device needs to be pre-installed with the RADIUS certificate/public key. Administrator user authentication however does not require installation of X.509 certificate.

Note that both the PMP 450 AP and SM support RADIUS authentication for the administrator to login to the web GUI. While the PMP 450 AP supports this authentication by acting directly as a RADIUS client, for the PMP 450 SM, this authentication is in fact relayed to the PMP 450 AP that the SM is registered with. So the SM does not need to act as a RADIUS client for this purpose while letting the AP performs the job of RADIUS client on its behalf.

RADIUS Configuration

Based on the discussion above, we can now list out what parameters are to be configured at each network entity to get the RADIUS authentication to work. Table 2 shows the role of each radio device in the RADIUS architecture and the parameters required to fulfill the role.

Product Name	Role	Parameters for RADIUS
PTP 820	RADIUS CLIENT	RADIUS server shared secrect, RADIUS server IP
PTP 800	RADIUS CLIENT	RADIUS server shared secrect, RADIUS server IP
PTP 650	RADIUS CLIENT	RADIUS server shared secrect, RADIUS server IP
PMP 450 AP	RADIUS CLIENT	RADIUS server shared secrect, RADIUS server IP
PMP 450 SM	RADIUS USER	RADIUS server root certificate, user name (by default, MAC address of the radio), password
ePMP SM	RADIUS USER	RADIUS server root certificate, user name (by default, MAC address of the radio), password

Table 2: Radios RADIUS Configuration.

RADIUS SERVER CONFIGURATION

In addition to installing an X.509 certificate on the RADIUS server for EAP-TTLS secure tunnel setup, as well as installation of the VSA dictionary files for the products, we need to provision the RADIUS Clients and Users on the RADIUS server.

The product VSA dictionary files can be downloaded from Cambium Network product support website. For FreeRadius, these files are typically stored under the /usr/share/freeradius directory.

- **Provisioning of RADIUS Clients**

All the network devices that will be acting as RADIUS client will need to be provisioned in the RADIUS Client Table. That means all the PTP radios and all the PMP 450APs IP address, along with the shared secret between the RADIUS server and the client need to be provisioned in the Client Table. The clients can use a common shared secret.

- **Provisioning of RADIUS Users**

As discussed earlier, there are two type of RADIUS Users. A RADIUS User can be a Network Administrator or a Network Device.

Each RADIUS user needs to be provisioned in the RADIUS user table.

For network management and administration, operators would typically create one or a few (if they need different level of access authorizations) administrator accounts. These accounts can be used to log onto the Web GUIs across all the radios in the network.

For device authentication, one provisioning entry is required for each ePMP SM or PMP 450 SM.

Each user provisioning record contains a username, a password, and a set of VSAs. These VSAs can be used to define the user account authorizations (e.g. level of access to the information or a subscriber module's SLA – Service Level Agreement parameters, and etc.).

SAMPLE RADIUS SERVER CONFIGURATION

The end to end RADIUS security solution was tested on a Linux Based Free Radius server. The following highlights the key sample configurations.

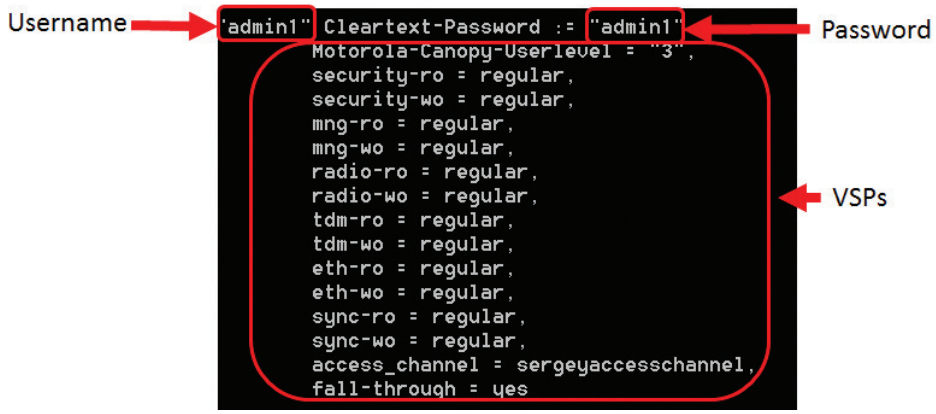

Figure 3: RADIUS server provisioning of Administrator Account

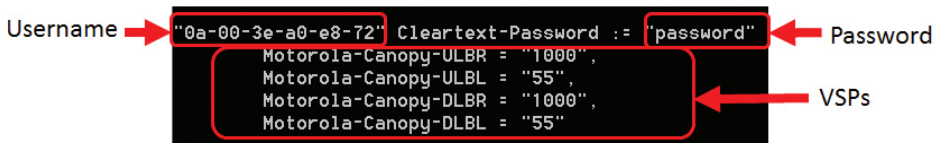

Figure 4: RADIUS server provisioning of Device User Account

1. Administrator User Provisioning

Figure 3 shows provisioning of an administrator account.

Figure 4 shows a sample provisioning record for a PMP 450 SM.

2. RADIUS Client Provisioning

Figure 5 shows provisioning record of a PMP 450AP acting as RADIUS Client.

RADIUS CLIENT CONFIGURATION

It is very simple to configure the PTP and PMP 450 AP as RADIUS client to authenticate the RADIUS users such as administrator or PMP SMs. All are needed is to set the RADIUS server's IP address and the Shared Secret.

Figure 6 through Figure 9 show examples on how this is configured on different product's Web GUI.

```
client 169.254.1.3 {
        secret = CanopySharedSecret
        shortname = Canopy
}
```

Figure 5: RADIUS server provisioning of a PMP 450 AP as a RADIUS Client

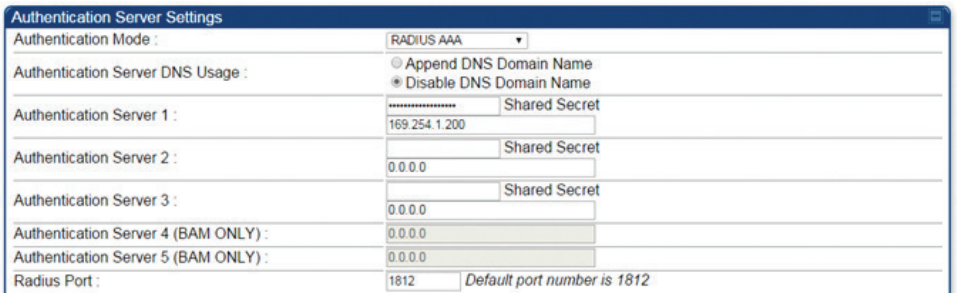

Figure 6: PMP 450 AP RADIUS Client Configuration

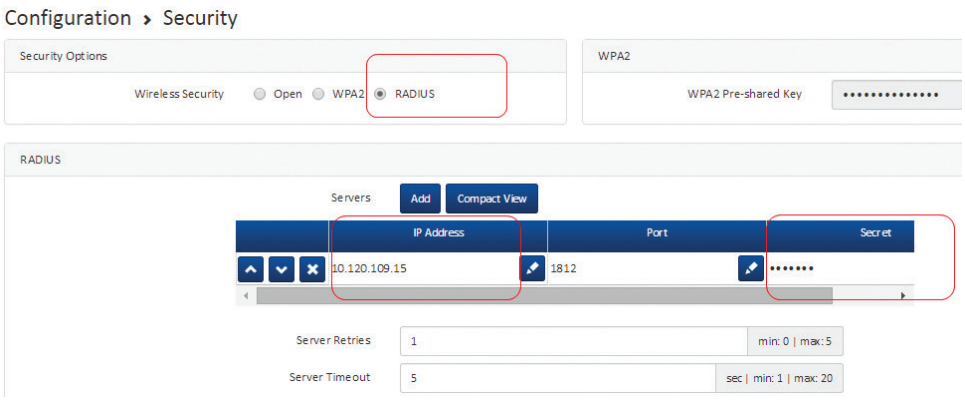

Figure 7: ePMP AP RADIUS Client Configuration

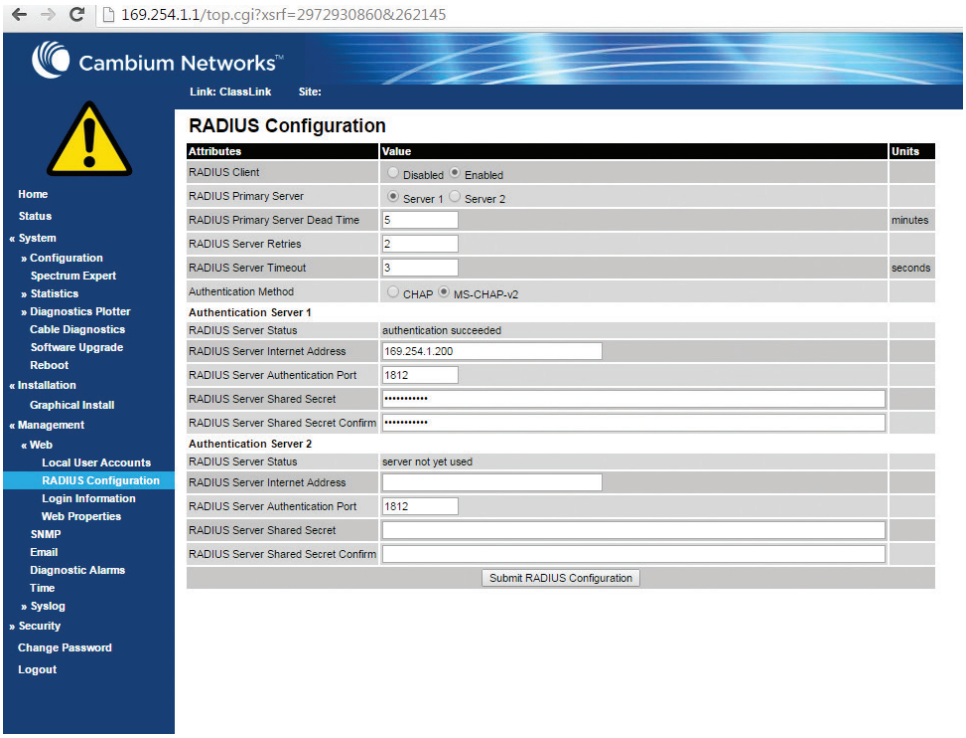

Figure 8: PMP 650 and PTP 800 RADIUS Client Configuration

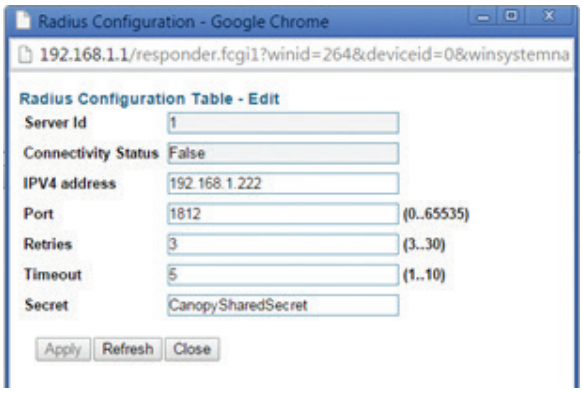

Figure 9: PTP 820 RADIUS Client Configuration

RADIUS USER CONFIGURATION

Configuration of the PMP 450 SM and ePMP SM as RADIUS user involved loading a root certificate that can validate the RADIUS server's certificate, User Name and Password as provisioned in the RADIUS server.

Figure 10 through Figure 11 shows screenshots of PMP 450 SM and ePMP SM RADIUS user configurations.

Note that although all the PMP 450 and ePMP SMs come pre-installed with a default root certificate, it is not recommended to use this in commercial deployment because this could open a loophole for security violation. For example, a rouge AP with a rouge RADIUS server can use the default certificate downloaded from Cambium website and intercept SM connections.

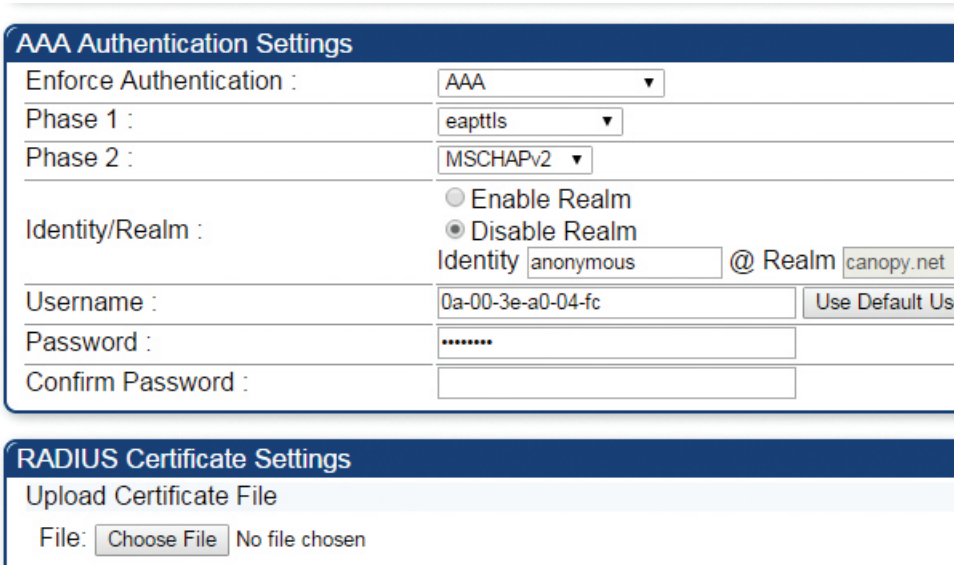

Figure 10: PMP 450 SM RADIUS User Configuration

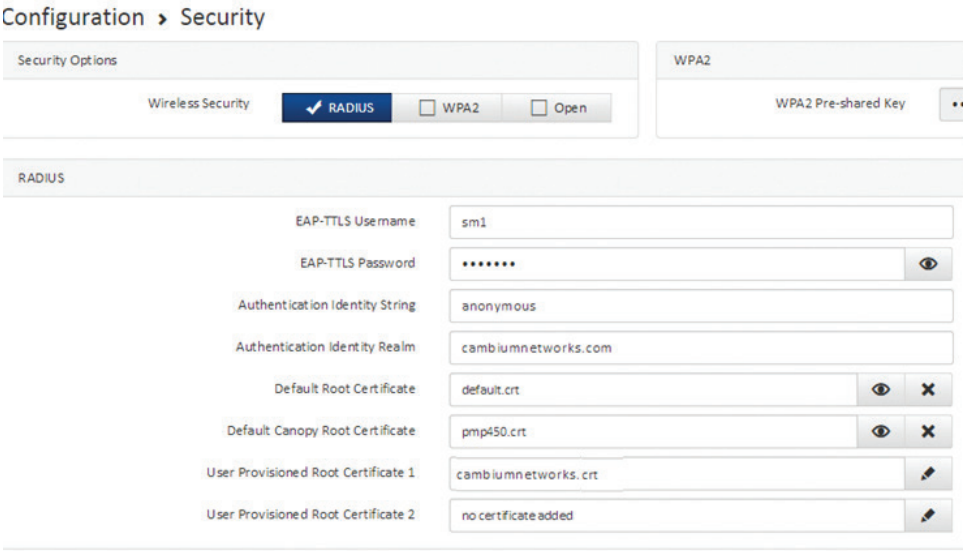

Figure 11: ePMP SM RADIUS User Configuration

Summary

In summary, the Cambium Network Wireless Broadband product portfolio supports end to end RADIUS security with single RADIUS server. This makes it cost effective for the network operator to provide RADIUS security across the network using Cambium Networks products.

About Cambium Networks

Cambium Networks provides world-class wireless broadband access and microwave solutions for Service Providers, enterprise customers, military, government, and municipal networks around the world.

It currently has more than 4 million modules deployed in thousands of networks in over 150 countries.

Our innovative technologies provide reliable, secure, cost-effective connectivity that's easy to deploy and proven to deliver outstanding metrics. Cambium's ecosystem of partners, development engineers, and support teams work together to design and deliver innovative, forward-looking solutions that provide data, voice and video connectivity when and where it's needed.

GLOSSARY

EAP	Extensible Authentication Protocol
PAP	Password Authentication Protocol
TTLS	Tunneled Transport Layer Security
MD5	Message Digest 5 Hashing
CHAP	Challenge-Handshake Authentication Protocol
WiSP	Wireless Internet Service Provider
RADIUS	Remote Authentication Dial-In User Service
NOC	Network Operating Center
MS-CHAPv2	Microsoft Challenge-Handshake Authentication Protocol version 2
VSA	Vendor Specific Attributes

Cambium Networks™

11/2015