APPLICATION NOTE

Port Access Control – How to Configure IEEE802.1X with RADIUS Authentication for the RAPTOR®

INTRODUCTION

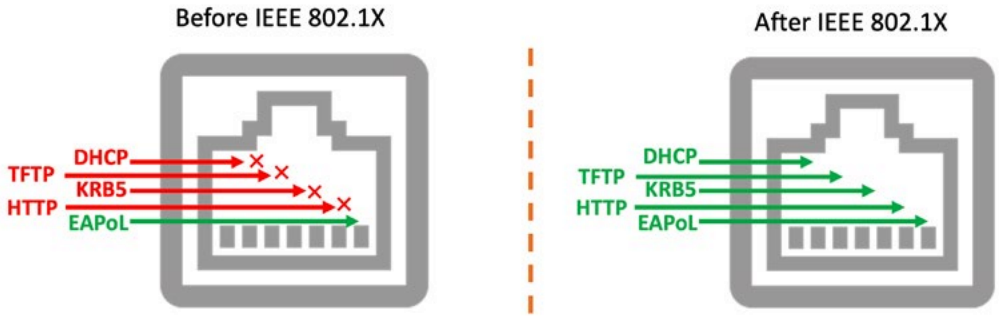
Growing security concerns in communication networks increase the need for identity-based networking. Allowing access to the network and its services based on the user's identity is becoming more challenging as the number and type of devices requiring access to network resources increases.

IEEE802.1X is an IEEE security standard, and it is considered one of the most secure standards for network access control. It is supported by various operating systems and devices, and it provides user authentication for both wired and wireless connections, making it the go-to protocol for identity-based access control.

APPLICATION DESCRIPTION

IEEE 802.1X defines a client-server-based access control and authentication protocol that enforces authentication for clients connecting to a LAN through publicly accessible ports. An authentication server verifies every client connected to each port before making available any device or network services. Prior to client authentication, IEEE 802.1X access control only permits Extensible Authentication Protocol over LAN (EAPOL) and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After successful authentication, regular traffic can pass through the port.

*Figure 1 - **Default Network Access Before and After 802.1X***



ARCHITECTURE

IEEE 802.1X defines three required devices to perform user authentication at the port level:

Supplicant: The client device wanting to access the network.

Authenticator: The device that passes the authentication messages to the authentication server and acts on the response returned from the server. It can enable or disable the port to which the supplicant is connected based on the authentication server feedback.

Authentication server: A server that authenticates the supplicant upon receiving its credentials. RADIUS is commonly used as the authentication server.

*Figure 2 - **IEEE802.1X components and protocols***

AUTHENTICATION PROCESS

The steps below show how a RADIUS server authenticates a supplicant:

1. Once the supplicant is connected to the ethernet switch, it will send an EAP-Start message.
2. The Switch sends an identity request message to the supplicant.
   The authentication process can also start from this step if an EAP-Start request is not received. The Switch will periodically send an identity request message.
3. The supplicant sends an EAP-Response that contains the username.

4. The Switch uses a RADIUS message to send the username to the authentication server.
5. The supplicant and the authentication server will exchange multiple messages to authenticate the supplicant. These messages will depend on the method and encapsulation of EAP used. Common EAP types are EAP-TLS and PEAP-MSCHAPv2.
6. If the supplicant is successfully authenticated, the authentication server sends an EAP-Success to the Switch (Authenticator).
7. The Switch will send an EAP-Success to the supplicant and change the stat of the port to authorized. The supplicant has access to the network.

CONFIGURATION STEPS

This section describes the configuration steps required to implement IEEE802.1X with the PEAP-MSCHAPv2 authentication method.

The configuration details are defined in the image below.

*Figure 3 - **Configuration details***

RAPTOR CONFIGURATION

The RAPTOR configuration requires five steps:

1. Configure the RADIUS server IP address and secret preshared key.
   iS5comm(config)# radius-server host 192.168.10.251 key password
2. Enable 802.1x authentication on the switch.
   iS5comm(config)# dot1x system-auth-control
3. Configure the RAPTOR to use RADIUS server remote authentication method for all ports.
   iS5comm(config)# aaa authentication dot1x default group radius
4. Enable 802.1x authentication on port level
   iS5comm(config)# interface gi 0/1
   iS5comm(config-if)# dot1x port-control auto

*Figure 4 - **RAPTOR Configuration***

```
iS5comm(config)#
iS5comm(config)# radius-server host 192.168.10.251 key password
iS5comm(config)# dot1x system-auth-control
iS5comm(config)# aaa authentication dot1x default group radius
iS5comm(config)# interface gi 0/1
iS5comm(config-if)# dot1x port-control auto
iS5comm(config-if)# end
iS5comm#
iS5comm#
```

FreeRADIUS CONFIGURATION

FreeRADIUS installation is out of the scope of this application note. The installation steps can be found in the FreeRADIUS Technical Guide.

https://networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf

Three steps are needed to configure FreeRADIUS:

1. **Client creation**

   Use a text editor such as VIM or NANO to edit the client.conf file.

   Add the RAPTOR as a client of the RADIUS server.

   The secret preshared password is used to encrypt the password when sent from the Switch. Therefore, a strong secret key should be used. The secret “password” in this example is used for simplicity.

*Figure 5 - **Client.conf file configuration***

```
 GNU nano 4.8                  /etc/freeradius/3.0/clients.conf
#

#
#  Each client has a "short name" that is used to distinguish it from
#  other clients.
#
#  In version 1.x, the string after the word "client" was the IP
#  address of the client.  In 2.0, the IP address is configured via
#  the "ipaddr" or "ipv6addr" fields.  For compatibility, the 1.x
#  format is still accepted.
#
client RAPTOR {
        ipaddr = 192.168.10.1
        secret = password
}
```

2. User creation

Use a text editor such as VIM or NANO to edit the user file.

Define the supplicant access credentials. RADIUS will compare the access credentials sent by the Switch with the credentials stored in this file.

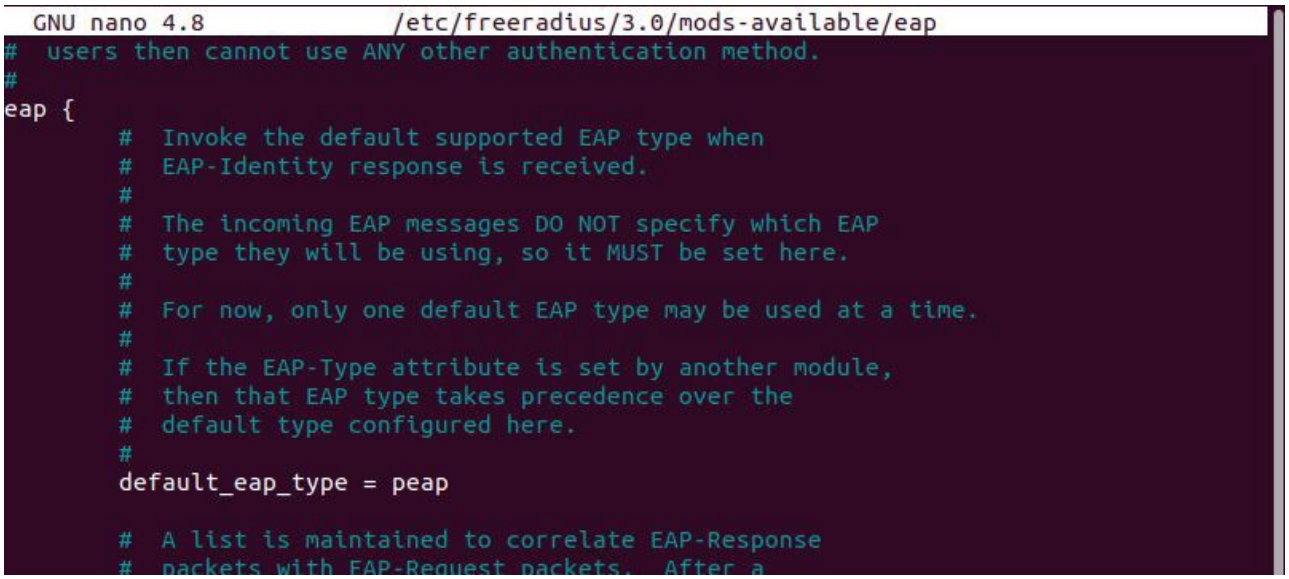
Create user bob with the password “Tech!123”.

*Figure 6 - **User file configuration***

3. Configure the EAP file

Use a text editor such as VIM or NANO to edit the file. Set the default EAP type to PEAP.

Figure 7



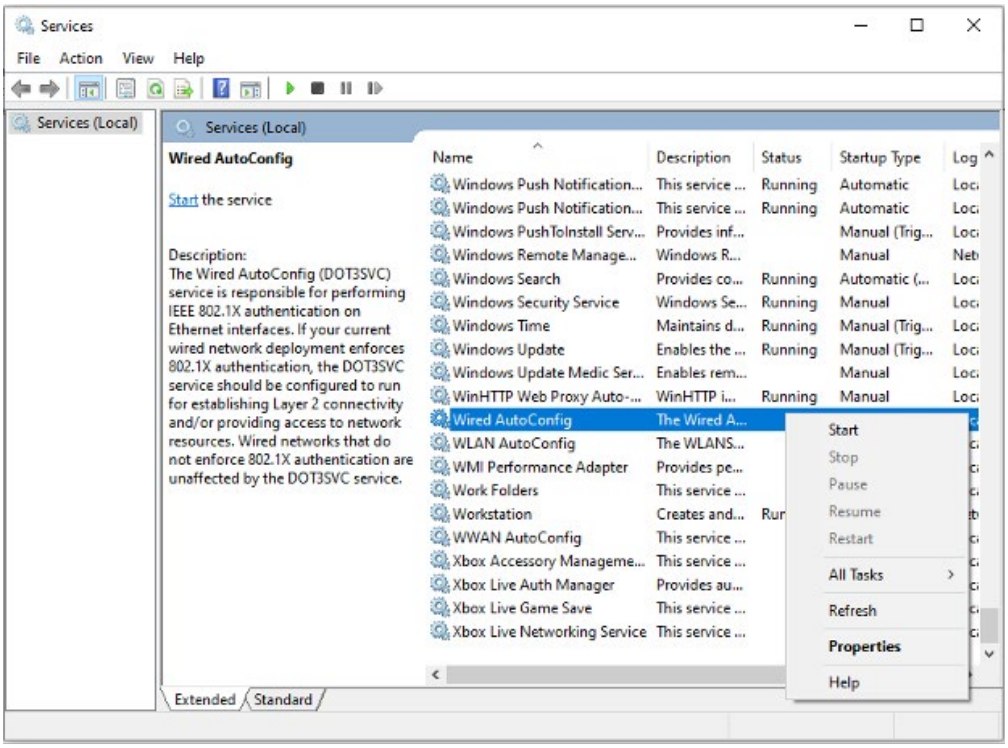
802.1X ACTIVATION ON WINDOWS 10

The steps needed to configure 802.1X are as follows.

1. Activate 802.1X

802.1X is not enabled by default in Windows. The service Wired autoConfig must be enabled.

Figure 8 - 802.1X service activation



2. Configure 802.1X

802.1X can be activated and configured in the network interface card settings.

Figure 9 - NIC settings

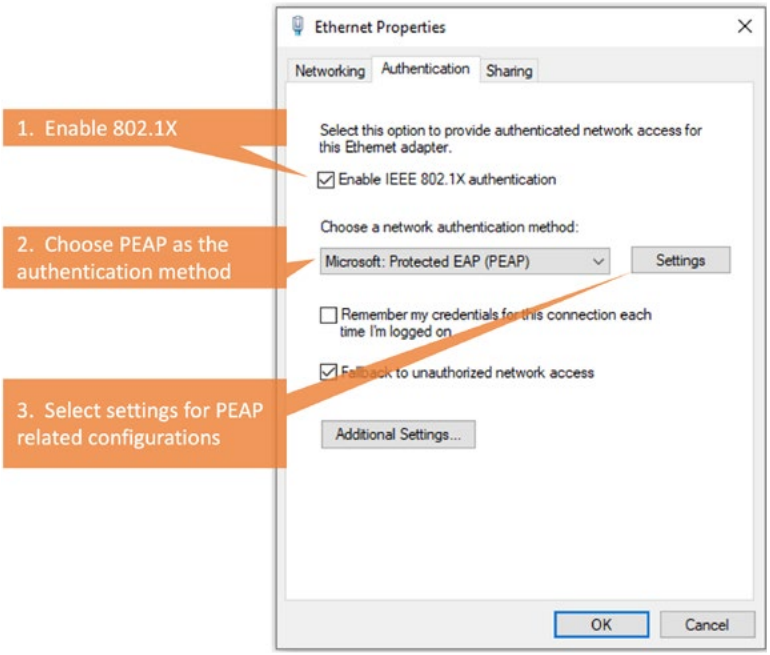


*Figure 10 - **NIC PEAP authentication settings***

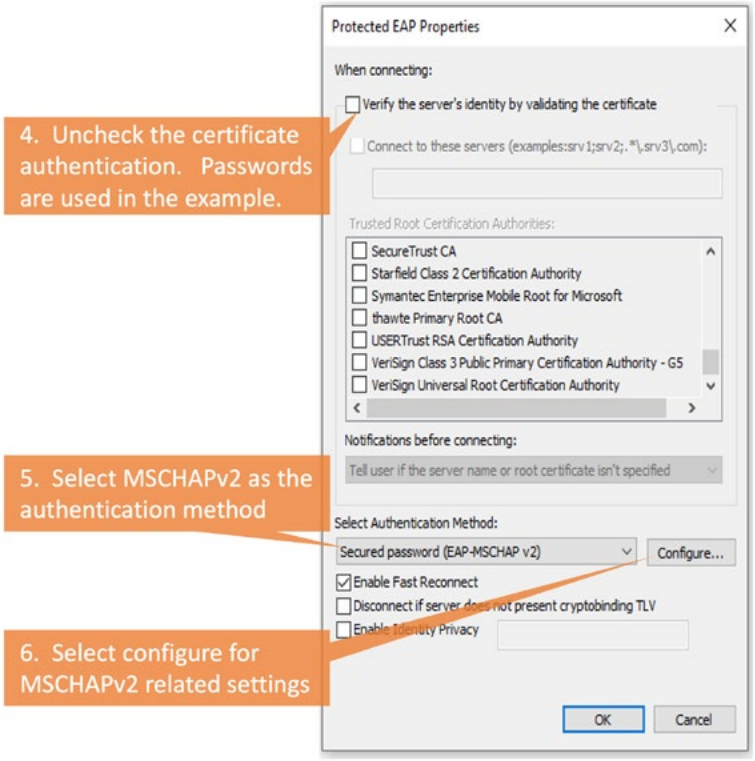
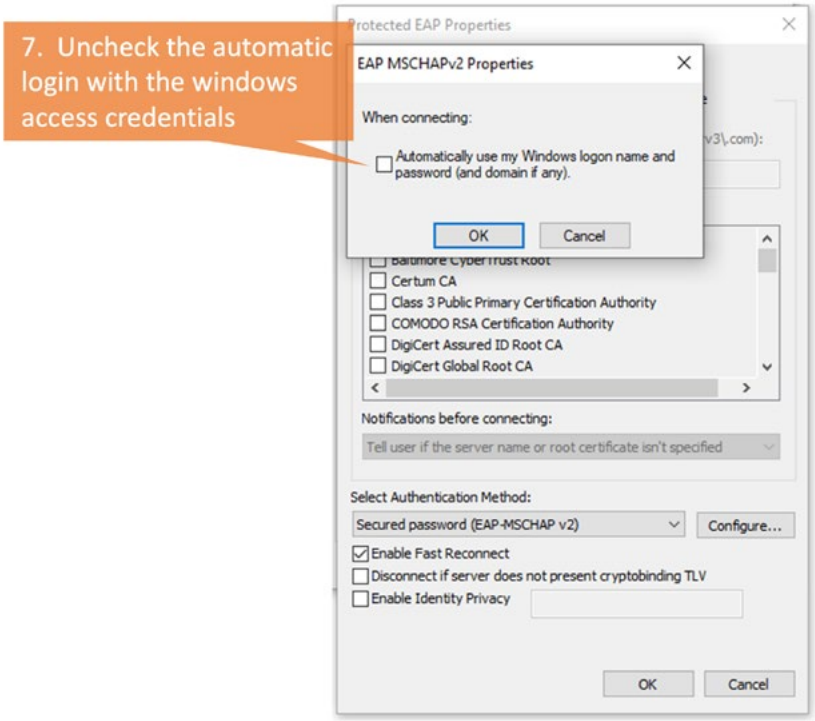
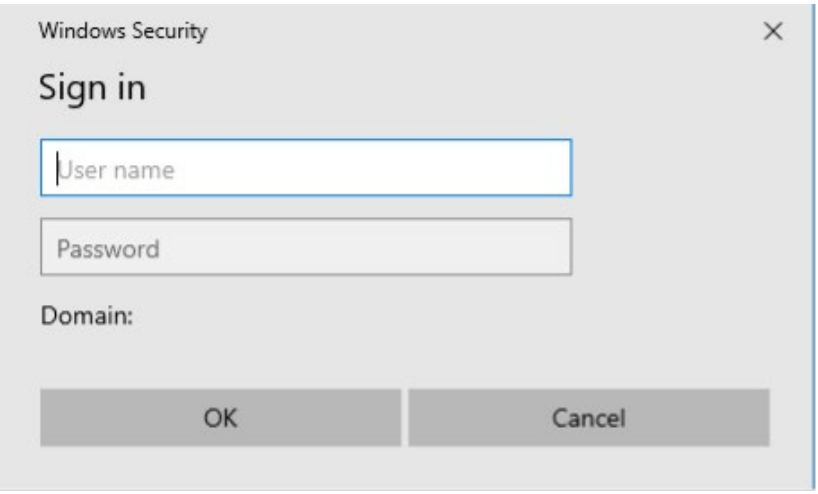


*Figure 11 - **MSCHAPv2 settings***



If 802.1X is configured on an interface, users will be required to enter a username and password to access the network.

Figure 12 - ***Access credentials required***



CONCLUSION

802.1X is a well know and commonly used protocol to implement port access control. 802.1X provides additional visibility and security by authenticating any user who requires network services. this application note has described how 802.1X can restrict and allow access to users after authentication and detailed the configuration steps needed to implement 802.1X with PEAP-MSCHAPv2 with RAPTOR.

ABOUT iS5 COMMUNICATIONS INC.

iS5 Communications Inc. (“iS5Com”) is a global provider of integrated services and solutions, and manufacturer of intelligent Industrial Ethernet products. Our products are designed to meet the stringent demand requirements of utility sub-stations, roadside transportation, rail, and industrial applications. iS5Com’s services and products are key enablers of advanced technology implementation such as the Smart Grid, Intelligent Transportation Systems, Intelligent Oil Field, and Internet of Things. All products have the ability to transmit data efficiently without the loss of any packets under harsh environments and EMI conditions.

iS5 COMMUNICATIONS

SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

For more information, visit: is5com.com

toll free: +1-844-520-0588 | fax: +1-289-401-5206 | info@is5com.com
technical support: +1-844-475-8324 | support@is5com.com
Address: 5895 Ambler Dr, Mississauga, ON L4W 5B7