IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS

TRANQUILITY IP LLC, Plaintiff, v.	C.A. No. 6:22-cv-1012 **JURY TRIAL DEMANDED**
SCHNEIDER ELECTRIC USA, INC., Defendant.	**PATENT CASE**

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Tranquility IP LLC files this Original Complaint for Patent Infringement against Schneider Electric USA, Inc., and would respectfully show the Court as follows:

I. THE PARTIES

1. Plaintiff Tranquility IP LLC ("Tranquility" or "Plaintiff") is a Texas limited liability company having an address at 7548 Preston Rd, Suite 141 PMB 1114, Frisco, TX 75034.

2. On information and belief, Defendant Schneider Electric USA, Inc., ("Defendant") has a place of business at 9101 Burnet Road, Ste. 202, Austin, TX 78758. Defendant has a registered agent at Corporation Service Company, 211 E. 7th Street, Suite 620, Austin, TX 78701.

II. JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction of such action under 28 U.S.C. §§ 1331 and 1338(a).

4. On information and belief, Defendant is subject to this Court's specific and general personal jurisdiction, pursuant to due process and the Texas Long-Arm Statute, due at least to its business in this forum, including at least a portion of the infringements alleged herein, at 9101 Burnet Road, Ste. 202, Austin, TX 78758 and 4305 N. Garfield, Suite 246, Midland, TX, 79705.

5. Without limitation, on information and belief, within this state, Defendant has used the patented inventions thereby committing, and continuing to commit, acts of patent infringement alleged herein. In addition, on information and belief, Defendant has derived revenues from its infringing acts occurring within Texas. Further, on information and belief, Defendant is subject to the Court's general jurisdiction, including from regularly doing or soliciting business, engaging in other persistent courses of conduct, and deriving substantial revenue from goods and services provided to persons or entities in Texas. Further, on information and belief, Defendant is subject to the Court's personal jurisdiction at least due to its sale of products and/or services within Texas. Defendant has committed such purposeful acts and/or transactions in Texas such that it reasonably should know and expect that it could be haled into this Court as a consequence of such activity.

6. Venue is proper in this district under 28 U.S.C. § 1400(b). On information and belief, Defendant has businesses in this district at 9101 Burnet Road, Ste. 202 Austin, TX 78758 and 4305 N. Garfield, Suite 246, Midland, TX, 79705. On information and belief, from and within this District Defendant has committed at least a portion of the infringements at issue in this case.

7. For these reasons, personal jurisdiction exists and venue is proper in this Court under 28 U.S.C. § 1400(b).

III. COUNT I
(PATENT INFRINGEMENT OF UNITED STATES PATENT NO. 8,272,037)

8. Plaintiff incorporates the above paragraphs herein by reference.

9. On September 18, 2012, United States Patent No. 8,272,037 ("the '037 Patent") was duly and legally issued by the United States Patent and Trademark Office. The '037 Patent is titled "Flexible WLAN Access Point Architecture Capable of Accommodating Different User Devices." A true and correct copy of the '037 Patent is attached hereto as Exhibit A and incorporated herein by reference.

10. Plaintiff is the assignee of all right, title and interest in the '037 patent, including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the '037 Patent. Accordingly, Plaintiff possesses the exclusive right and standing to prosecute the present action for infringement of the '037 Patent by Defendant.

11. The invention in the '037 Patent relates to the field of controlling access by a mobile terminal to a WLAN by accommodating for the particular capabilities of each mobile terminal and selecting accordingly the optimum available authentication mechanism. (*Id.* at col. 1:17-23).

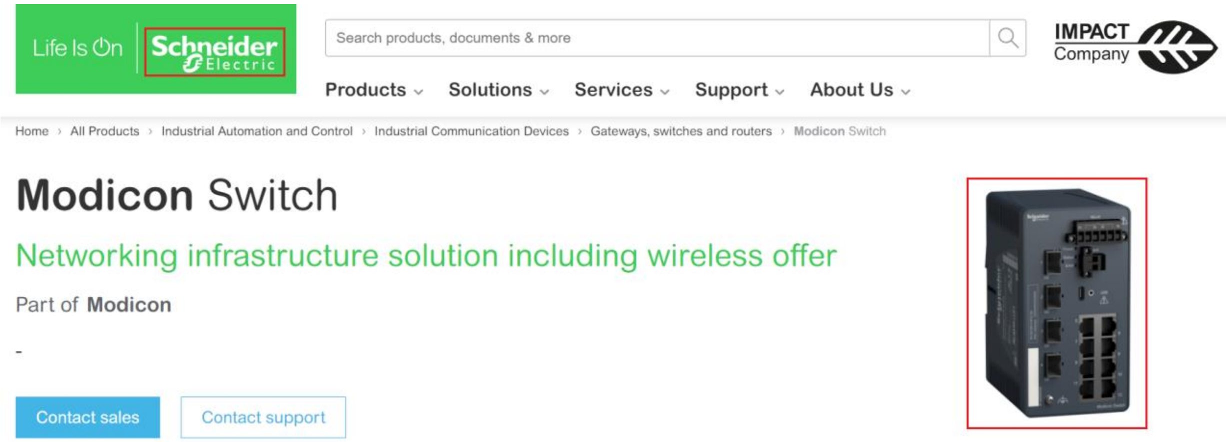
12. The context of the patented invention in the '037 Patent is wireless local area networks ("WLAN") employing the IEEE 802.1X architecture with an access point that provides access for mobile devices to other networks, such as hardwired local area and global networks such as the Internet. (*Id.* at col. 1:27-31). Because a public WLAN is relatively easy and low cost to implement and operate, it is an ideal access mechanism through which mobile wireless communication devices can exchange packet with an external entity. (*Id.* at col. 1:38-43). WLAN technology has resulted in publicly available hotspots (such as at cafes, restaurants, and libraries) where a mobile device (such as your mobile phone or laptop computer) can access the Internet through an access point associated with a WLAN. (*Id.* at col. 1:32-38). However, such a public deployment can compromise security unless there are adequate means for identification and authentication of connected devices. (*Id.* at col. 1:43-46).

13. When a mobile device incorporating an IEEE 802.1X protocol ("IEEE 802.1X client") attempts to access a public WLAN or hotspot, the IEEE 802.1X client would begin the authentication process according to its current machine configurations. (*Id.* at col. 1:47-51). After authentication occurs, the public WLAN opens a secure data channel to a mobile communications device to protect the privacy of data passing between the WLAN and the device. (*Id.* at col. 1:51-

54). Although many manufacturers of WLAN equipment have adopted the IEEE 802.1X protocol for deployed equipment, other devices using WLAN may use other protocols such as may be provided by wired electronic privacy ("WEP"). (*Id.* at col. 1:54-58). Unfortunately, the IEEE 802.1X protocol was designed with a private LAN access as its usage model so the protocol does not provide certain features necessary for a public WLAN environment. (*Id.* at col. 1:60-64). For example, the IEEE 802.1X protocol does not have a sophisticated mechanism for interacting with users. (*Id.* at col. 1:65-col. 2:1). The access point can only send simple messages to the client using electronic access point notification. (*Id.* at col. 2:1-3). This may be sufficient for an enterprise setting but would be insufficient for a public hotspot. (*Id.* at col. 2:3-5). A public hotspot should therefore be able to accommodate different client and operator capabilities, based on which the WLAN should have the ability to select different authentication mechanism. (*Id.* at col. 2:25-28). The prior art does not sufficiently address how the systems would provide such capabilities. (*Id.* at col. 2:28-31). The invention in the '037 patent seeks to address the variation in authentication mechanisms by providing a method for controlling the access of a terminal device in a WLAN environment by determining whether a terminal device uses an IEEE 802.1X protocol. (*Id.* at col. 2:43-46).

14. **Direct Infringement.** Upon information and belief, Defendant has been directly infringing at least claims 9, 10, and 11 of the '037 patent in Texas, and elsewhere in the United States, by performing actions comprising at least performing the claimed method of controlling access by a user terminal in a wireless local area network by determining whether the user terminal uses an IEEE 802.1X protocol using at least the Schneider Electric Modicon MCSESM Switch ("Accused Instrumentality") (*e.g.*, https://www.se.com/us/en/product-range/584-modicon-switch/?parent-subcategory-id=2420&filter=business-1-industrial-automation-and-control).

15. Upon information and belief, the Accused Instrumentality discloses a method for controlling access by a user terminal (*e.g.*, user equipment) in a wireless local area network by determining whether the user terminal utilizes an IEEE 802.1x protocol. IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. The Accused Instrumentality determines whether the UE supports the IEEE 802.1x protocol by sending an EAP request and waits for response from the UE. If UE responds by authenticating itself using credentials before time out, then it is 802.1x compliant otherwise not.



Home › All Products › Industrial Automation and Control › Industrial Communication Devices › Gateways, switches and routers › Modicon Switch

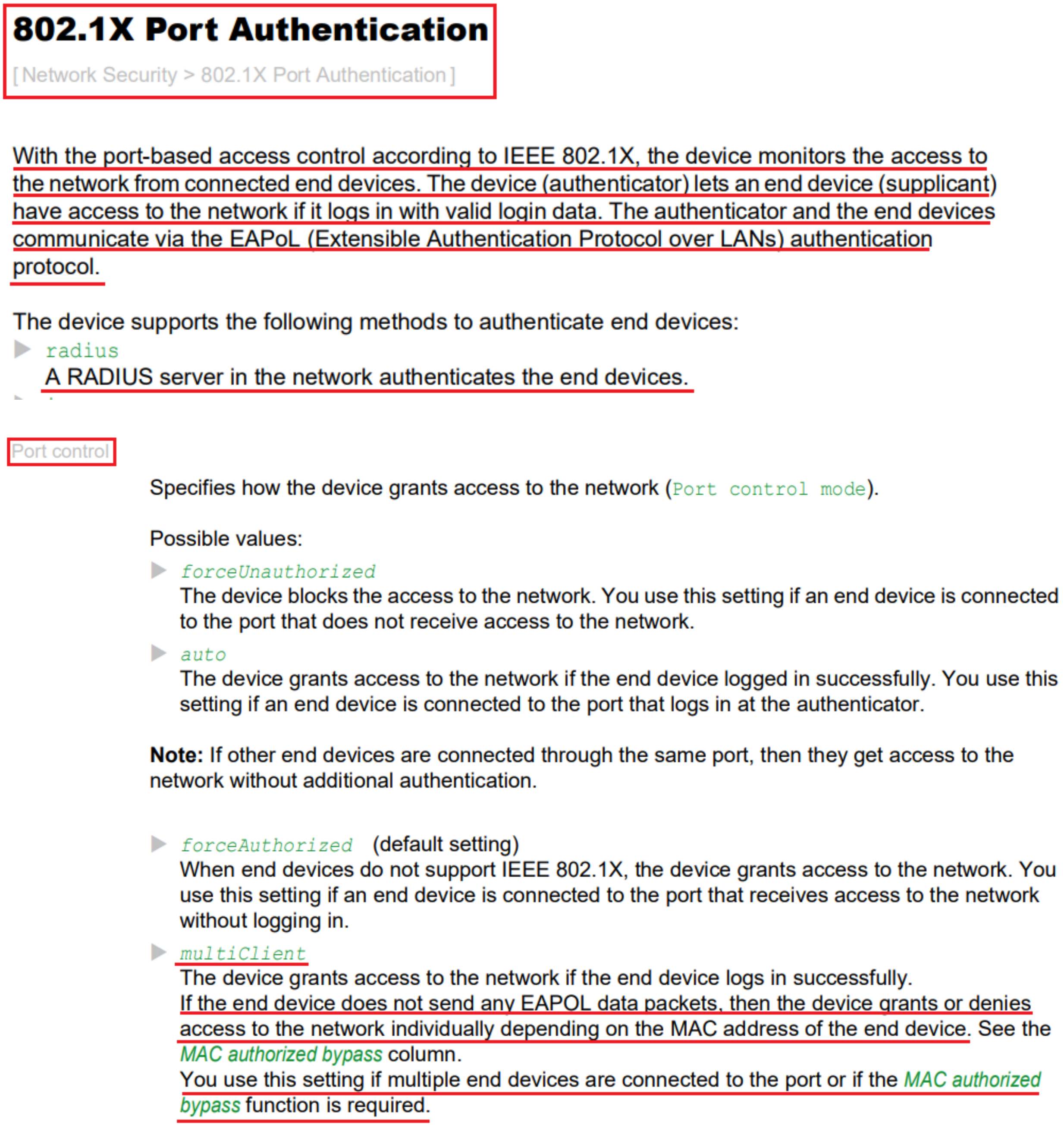
Modicon Switch

Networking infrastructure solution including wireless offer

Part of Modicon

-

(*E.g.*, https://www.se.com/us/en/product-range/584-modicon-switch/?parent-subcategory-id=2420&filter=business-1-industrial-automation-and-control).



802.1X Port Authentication

[Network Security > 802.1X Port Authentication]

With the port-based access control according to IEEE 802.1X, the device monitors the access to the network from connected end devices. The device (authenticator) lets an end device (supplicant) have access to the network if it logs in with valid login data. The authenticator and the end devices communicate via the EAPoL (Extensible Authentication Protocol over LANs) authentication protocol.

The device supports the following methods to authenticate end devices:

- `radius`
  A RADIUS server in the network authenticates the end devices.

Port control

Specifies how the device grants access to the network (`Port control mode`).

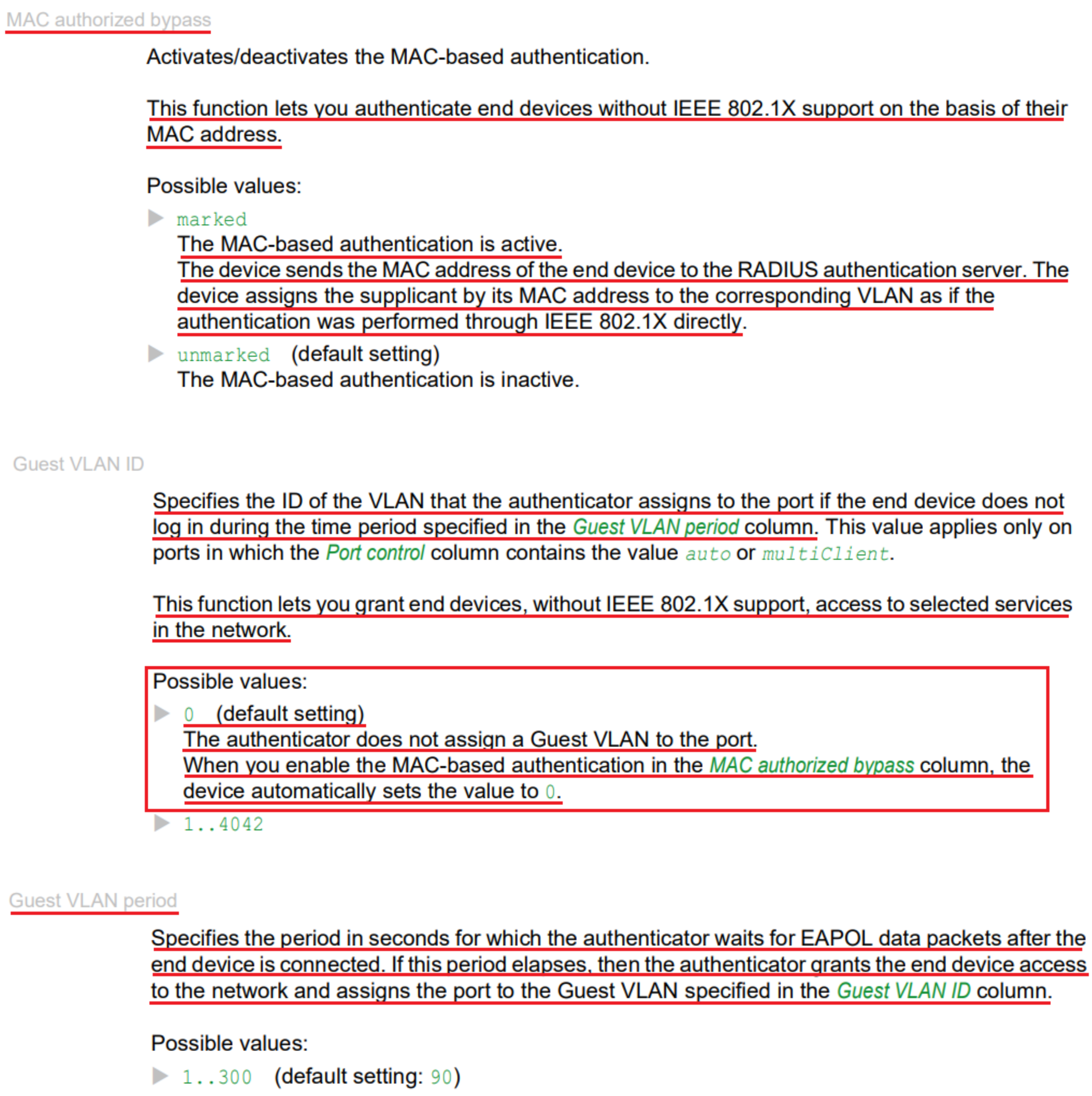
Possible values:

- *`forceUnauthorized`*
  The device blocks the access to the network. You use this setting if an end device is connected to the port that does not receive access to the network.
- *`auto`*
  The device grants access to the network if the end device logged in successfully. You use this setting if an end device is connected to the port that logs in at the authenticator.

Note: If other end devices are connected through the same port, then they get access to the network without additional authentication.

- *`forceAuthorized`* (default setting)
  When end devices do not support IEEE 802.1X, the device grants access to the network. You use this setting if an end device is connected to the port that receives access to the network without logging in.
- *`multiClient`*
  The device grants access to the network if the end device logs in successfully.
  If the end device does not send any EAPOL data packets, then the device grants or denies access to the network individually depending on the MAC address of the end device. See the *MAC authorized bypass* column.
  You use this setting if multiple end devices are connected to the port or if the *MAC authorized bypass* function is required.

(*E.g.*, https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=QGH5908401-01.pdf&p_Doc_Ref=QGH59084&_ga=2.187119082.331813519.1662528344-1610863410.1660293470).



MAC authorized bypass

Activates/deactivates the MAC-based authentication.

This function lets you authenticate end devices without IEEE 802.1X support on the basis of their MAC address.

Possible values:

- `marked`
  The MAC-based authentication is active.
  The device sends the MAC address of the end device to the RADIUS authentication server. The device assigns the supplicant by its MAC address to the corresponding VLAN as if the authentication was performed through IEEE 802.1X directly.
- `unmarked` (default setting)
  The MAC-based authentication is inactive.

Guest VLAN ID

Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not log in during the time period specified in the *Guest VLAN period* column. This value applies only on ports in which the *Port control* column contains the value `auto` or `multiClient`.

This function lets you grant end devices, without IEEE 802.1X support, access to selected services in the network.

Possible values:

- `0` (default setting)
  The authenticator does not assign a Guest VLAN to the port.
  When you enable the MAC-based authentication in the *MAC authorized bypass* column, the device automatically sets the value to `0`.
- `1..4042`

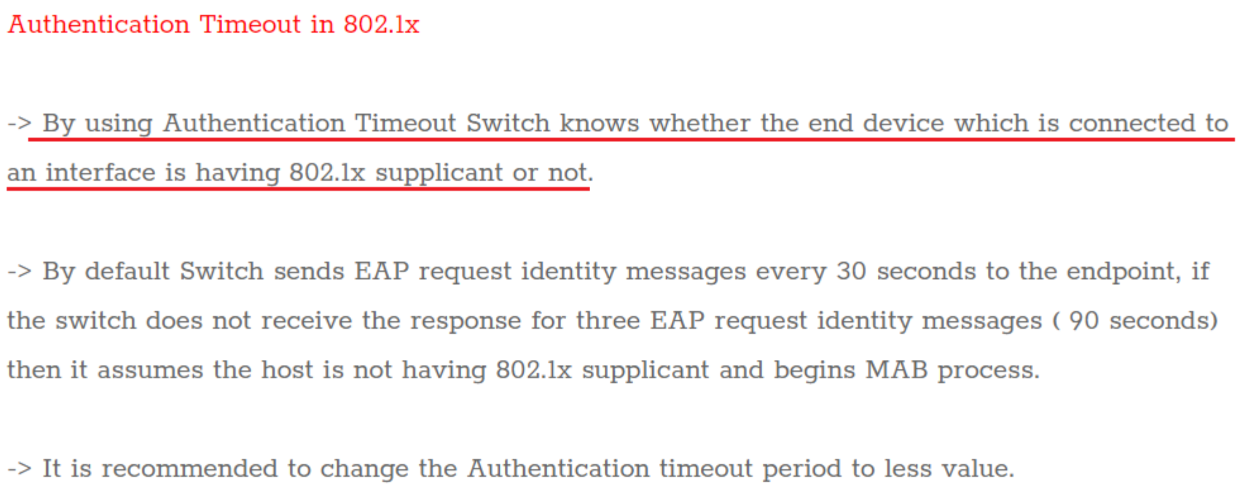
Guest VLAN period

Specifies the period in seconds for which the authenticator waits for EAPOL data packets after the end device is connected. If this period elapses, then the authenticator grants the end device access to the network and assigns the port to the Guest VLAN specified in the *Guest VLAN ID* column.

Possible values:

- `1..300` (default setting: `90`)

(*E.g.*, https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=QGH5908401-01.pdf&p_Doc_Ref=QGH59084&_ga=2.187119082.331813519.1662528344-1610863410.1660293470).



Authentication Timeout in 802.1x

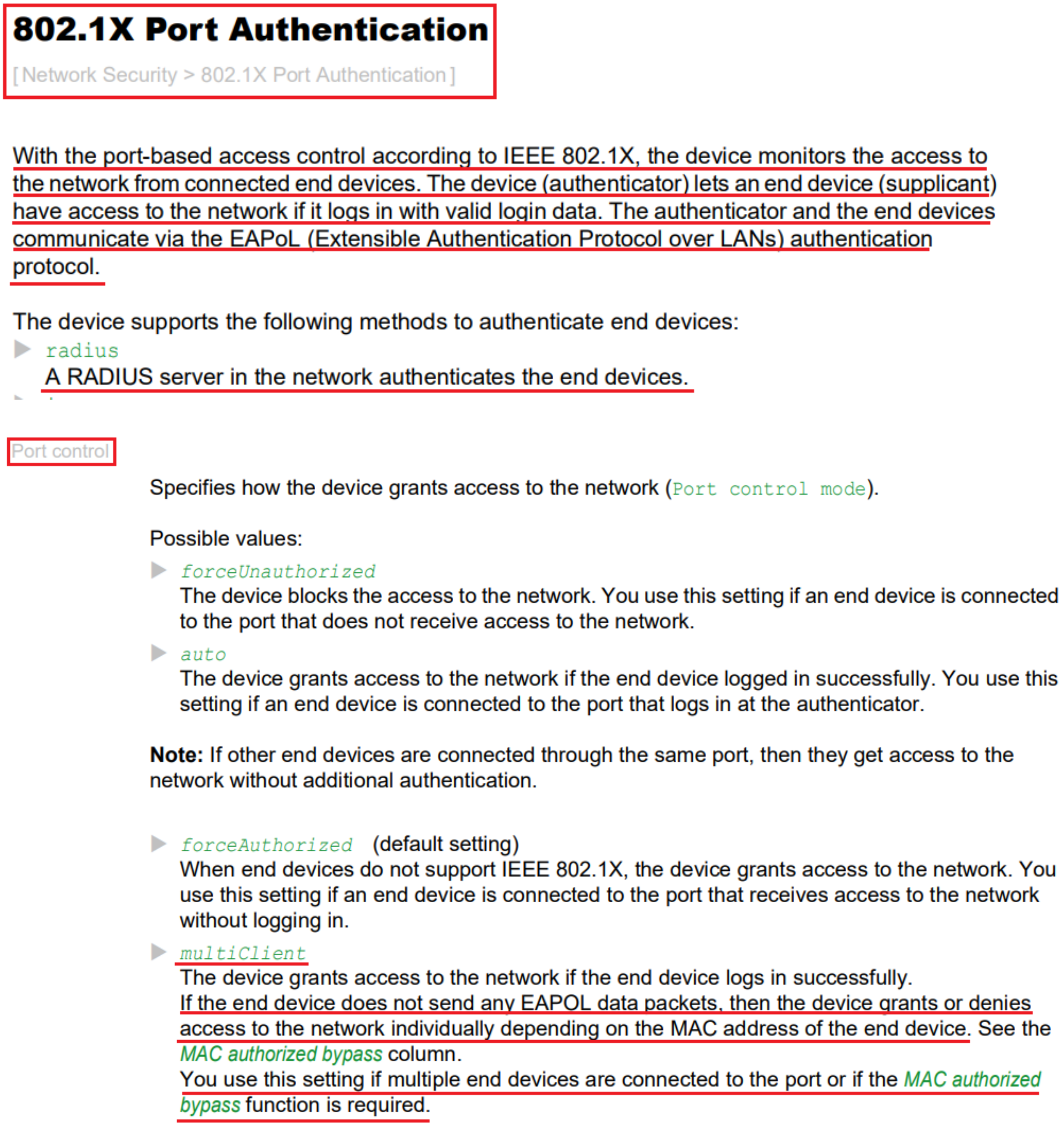
-> By using Authentication Timeout Switch knows whether the end device which is connected to an interface is having 802.1x supplicant or not.

-> By default Switch sends EAP request identity messages every 30 seconds to the endpoint, if the switch does not receive the response for three EAP request identity messages (90 seconds) then it assumes the host is not having 802.1x supplicant and begins MAB process.

-> It is recommended to change the Authentication timeout period to less value.

(*E.g.*, https://www.kareemccie.com/2017/01/mac-authentication-bypass.html).

16. Upon information and belief, the Accused Instrumentality discloses an access point (*e.g.*, authenticator) communicating to the user terminal (*e.g.*, user equipment) a request (*e.g.*, EAPoL request) to identify (*e.g.*, to identify whether UE is a supplicant or not), and if the user terminal utilizes an IEEE 802.1x protocol, acknowledging the request to identify (*e.g.*, when UE supports 802.1x, it authenticates itself using credentials), otherwise the access point determining that the user terminal is not IEEE 802.1x compliant and selecting an authentication mechanism (*e.g.*, Mac Address Bypass or MAB) compatible with the user terminal.



802.1X Port Authentication

[Network Security > 802.1X Port Authentication]

With the port-based access control according to IEEE 802.1X, the device monitors the access to the network from connected end devices. The device (authenticator) lets an end device (supplicant) have access to the network if it logs in with valid login data. The authenticator and the end devices communicate via the EAPoL (Extensible Authentication Protocol over LANs) authentication protocol.

The device supports the following methods to authenticate end devices:

- `radius`
  A RADIUS server in the network authenticates the end devices.

Port control

Specifies how the device grants access to the network (`Port control mode`).

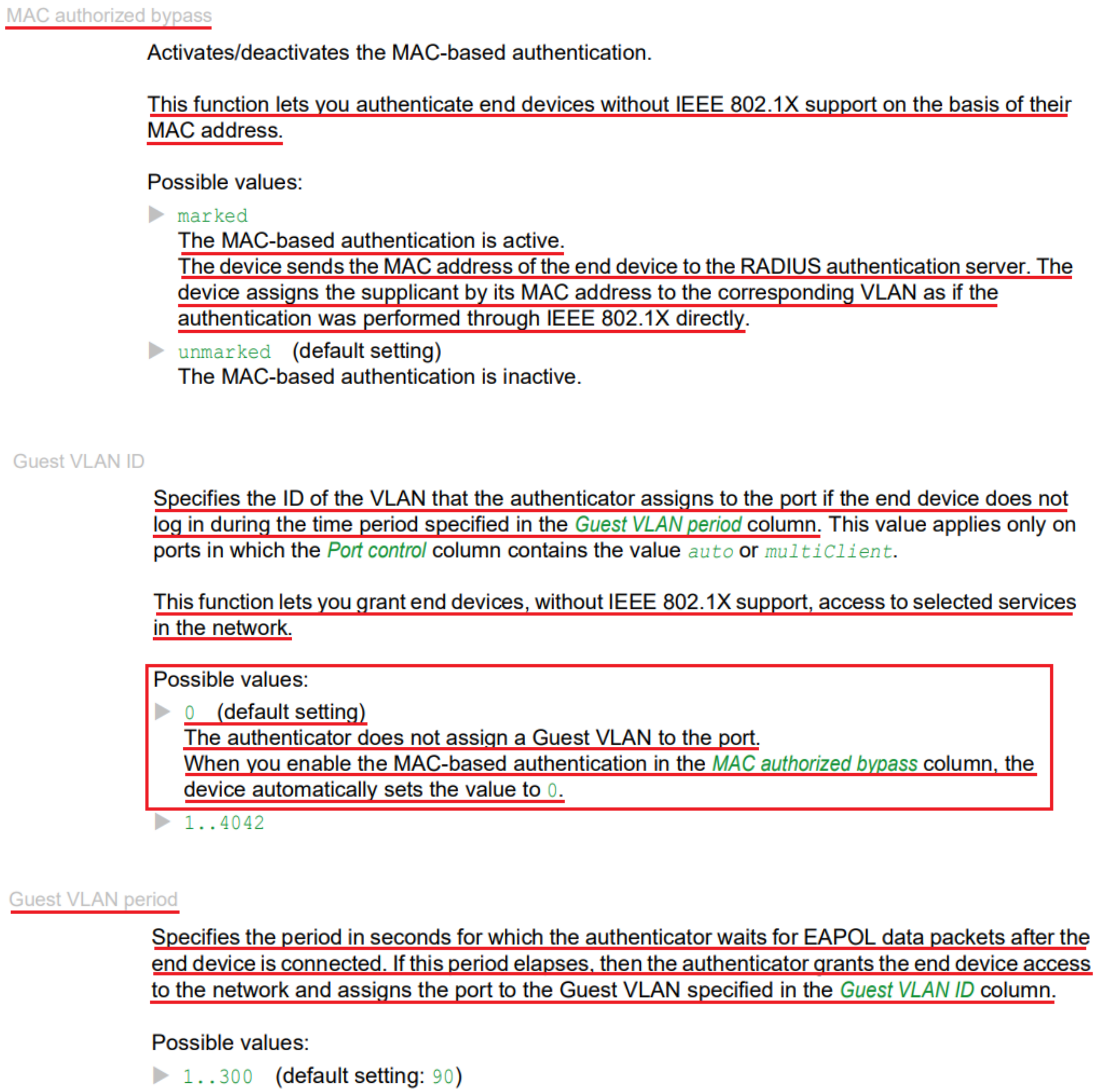
Possible values:

- *`forceUnauthorized`*
  The device blocks the access to the network. You use this setting if an end device is connected to the port that does not receive access to the network.
- *`auto`*
  The device grants access to the network if the end device logged in successfully. You use this setting if an end device is connected to the port that logs in at the authenticator.

Note: If other end devices are connected through the same port, then they get access to the network without additional authentication.

- *`forceAuthorized`* (default setting)
  When end devices do not support IEEE 802.1X, the device grants access to the network. You use this setting if an end device is connected to the port that receives access to the network without logging in.
- *`multiClient`*
  The device grants access to the network if the end device logs in successfully.
  If the end device does not send any EAPOL data packets, then the device grants or denies access to the network individually depending on the MAC address of the end device. See the *MAC authorized bypass* column.
  You use this setting if multiple end devices are connected to the port or if the *MAC authorized bypass* function is required.

(*E.g.*, https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=QGH5908401-01.pdf&p_Doc_Ref=QGH59084&_ga=2.187119082.331813519.1662528344-1610863410.1660293470).



MAC authorized bypass

Activates/deactivates the MAC-based authentication.

This function lets you authenticate end devices without IEEE 802.1X support on the basis of their MAC address.

Possible values:

- `marked`
  The MAC-based authentication is active.
  The device sends the MAC address of the end device to the RADIUS authentication server. The device assigns the supplicant by its MAC address to the corresponding VLAN as if the authentication was performed through IEEE 802.1X directly.
- `unmarked` (default setting)
  The MAC-based authentication is inactive.

Guest VLAN ID

Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not log in during the time period specified in the *Guest VLAN period* column. This value applies only on ports in which the *Port control* column contains the value `auto` or `multiClient`.

This function lets you grant end devices, without IEEE 802.1X support, access to selected services in the network.

Possible values:

- `0` (default setting)
  The authenticator does not assign a Guest VLAN to the port.
  When you enable the MAC-based authentication in the *MAC authorized bypass* column, the device automatically sets the value to `0`.
- `1..4042`

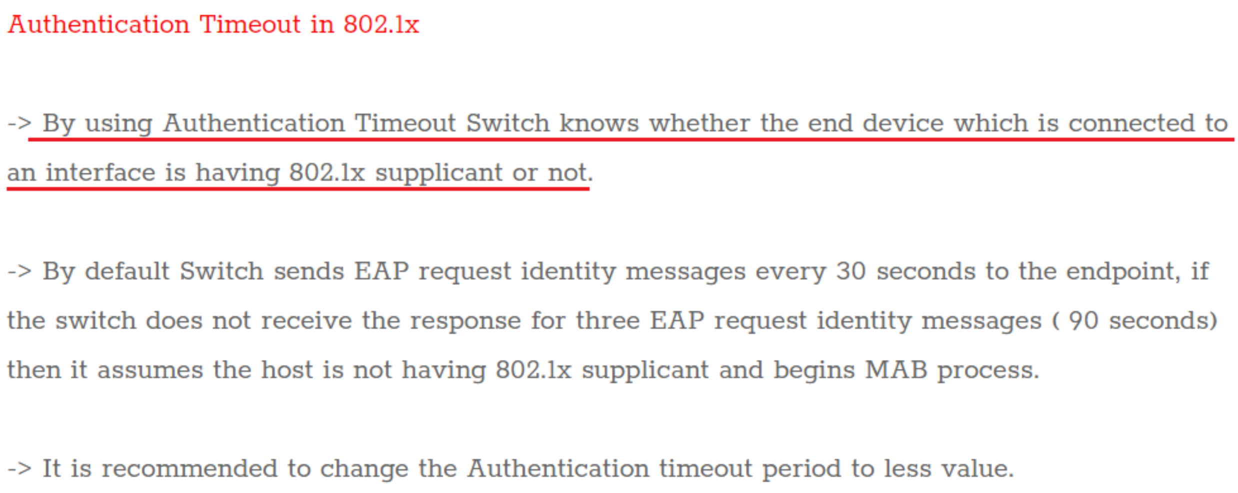
Guest VLAN period

Specifies the period in seconds for which the authenticator waits for EAPOL data packets after the end device is connected. If this period elapses, then the authenticator grants the end device access to the network and assigns the port to the Guest VLAN specified in the *Guest VLAN ID* column.

Possible values:

- `1..300` (default setting: `90`)

(*E.g.*, https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=QGH5908401-01.pdf&p_Doc_Ref=QGH59084&_ga=2.187119082.331813519.1662528344-1610863410.1660293470).



Authentication Timeout in 802.1x

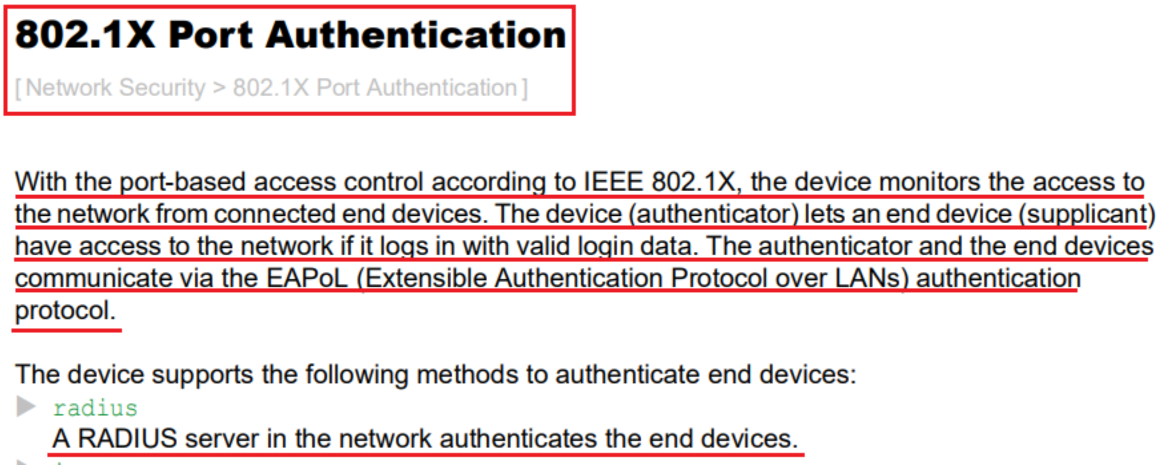
-> By using Authentication Timeout Switch knows whether the end device which is connected to an interface is having 802.1x supplicant or not.

-> By default Switch sends EAP request identity messages every 30 seconds to the endpoint, if the switch does not receive the response for three EAP request identity messages (90 seconds) then it assumes the host is not having 802.1x supplicant and begins MAB process.

-> It is recommended to change the Authentication timeout period to less value.

(*E.g.*, https://www.kareemccie.com/2017/01/mac-authentication-bypass.html).

17. Upon information and belief, the Accused Instrumentality is used in a method performing the step of the access point determines that the user terminal is not IEEE 802.1x compliant when it does not receive an extensible authentication protocol identity (*e.g.*, response to the EAPoL request) response packet after a timeout value.



802.1X Port Authentication

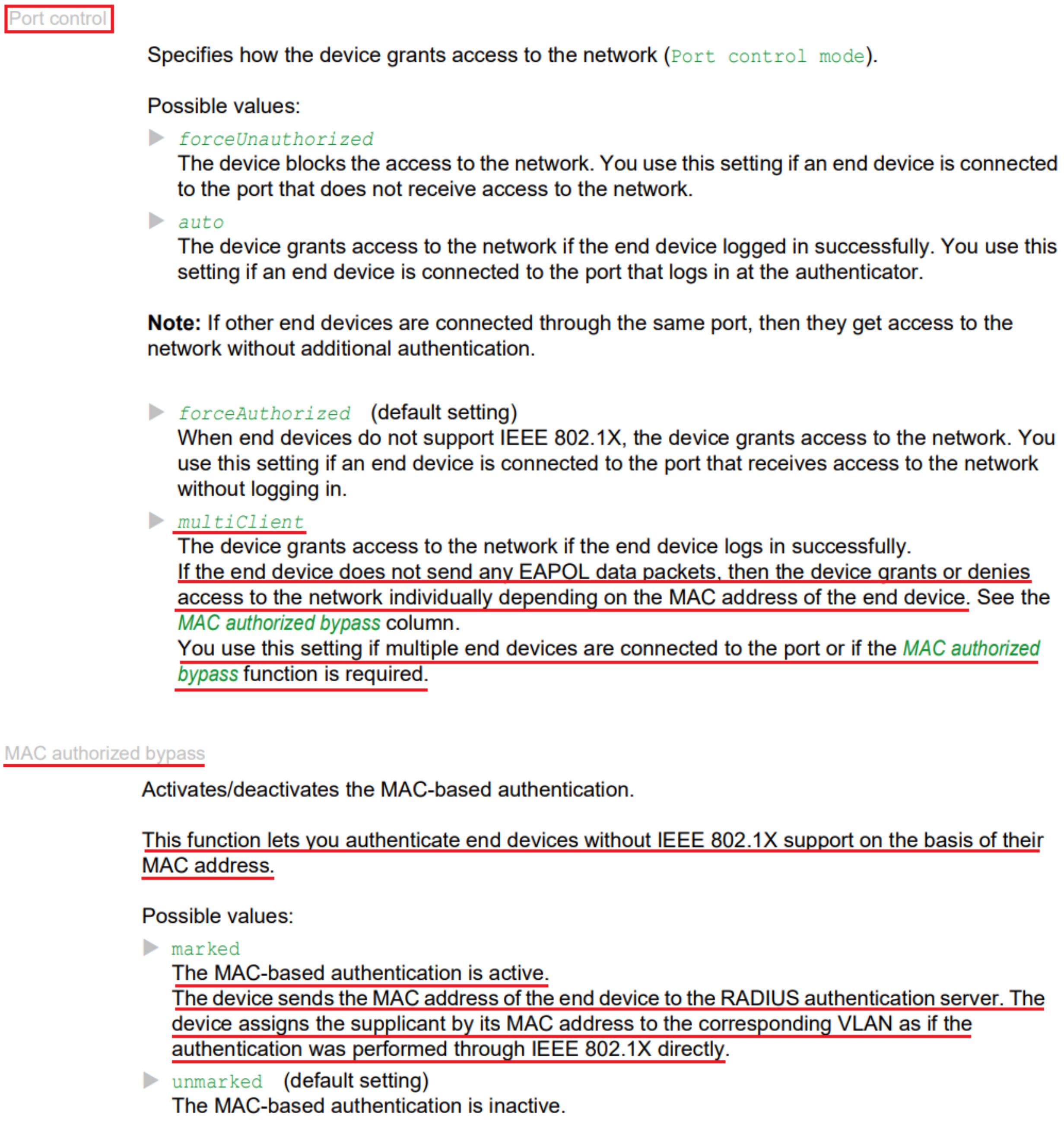
[Network Security > 802.1X Port Authentication]

With the port-based access control according to IEEE 802.1X, the device monitors the access to the network from connected end devices. The device (authenticator) lets an end device (supplicant) have access to the network if it logs in with valid login data. The authenticator and the end devices communicate via the EAPoL (Extensible Authentication Protocol over LANs) authentication protocol.

The device supports the following methods to authenticate end devices:

▶ radius
A RADIUS server in the network authenticates the end devices.

(*E.g.*, https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=QGH5908401-01.pdf&p_Doc_Ref=QGH59084&_ga=2.187119082.331813519.1662528344-1610863410.1660293470).



Port control

Specifies how the device grants access to the network (`Port control mode`).

Possible values:

- *forceUnauthorized*
  The device blocks the access to the network. You use this setting if an end device is connected to the port that does not receive access to the network.
- *auto*
  The device grants access to the network if the end device logged in successfully. You use this setting if an end device is connected to the port that logs in at the authenticator.

Note: If other end devices are connected through the same port, then they get access to the network without additional authentication.

- *forceAuthorized* (default setting)
  When end devices do not support IEEE 802.1X, the device grants access to the network. You use this setting if an end device is connected to the port that receives access to the network without logging in.
- *multiClient*
  The device grants access to the network if the end device logs in successfully.
  If the end device does not send any EAPOL data packets, then the device grants or denies access to the network individually depending on the MAC address of the end device. See the *MAC authorized bypass* column.
  You use this setting if multiple end devices are connected to the port or if the *MAC authorized bypass* function is required.

MAC authorized bypass

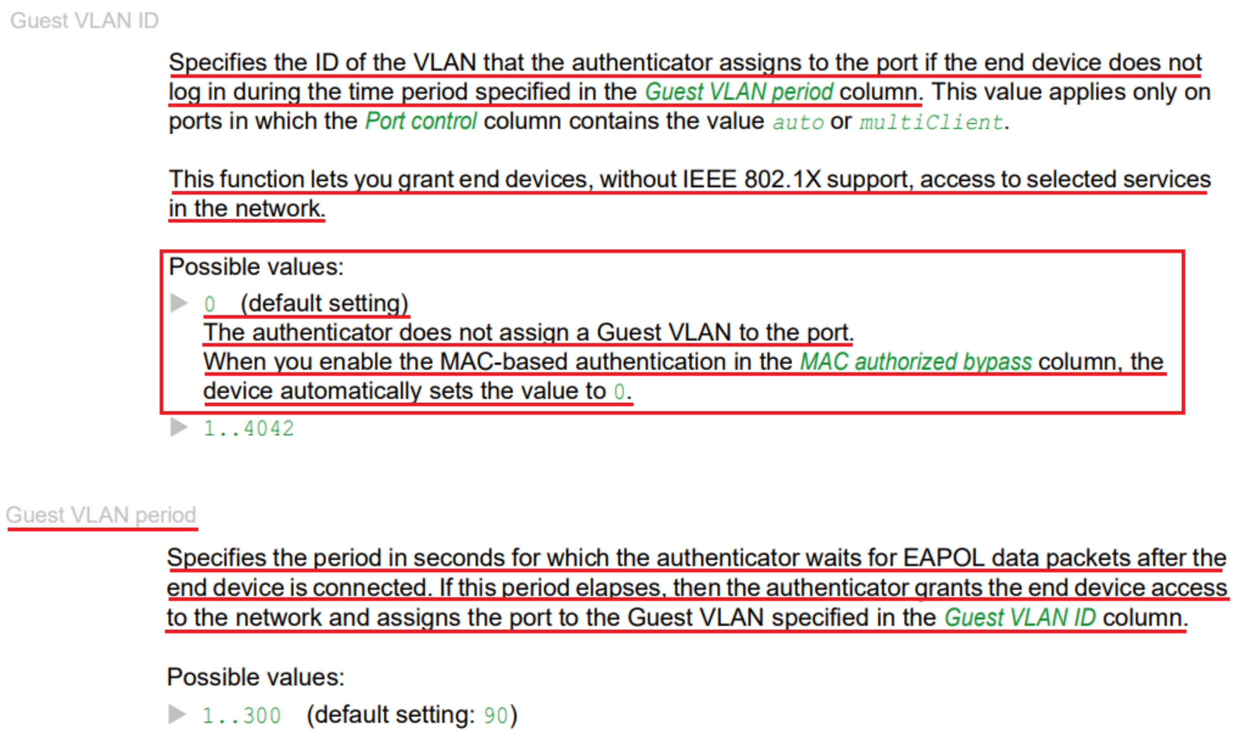
Activates/deactivates the MAC-based authentication.

This function lets you authenticate end devices without IEEE 802.1X support on the basis of their MAC address.

Possible values:

- `marked`
  The MAC-based authentication is active.
  The device sends the MAC address of the end device to the RADIUS authentication server. The device assigns the supplicant by its MAC address to the corresponding VLAN as if the authentication was performed through IEEE 802.1X directly.
- `unmarked` (default setting)
  The MAC-based authentication is inactive.

(*E.g.*, https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=QGH5908401-01.pdf&p_Doc_Ref=QGH59084&_ga=2.187119082.331813519.1662528344-1610863410.1660293470).



Guest VLAN ID

Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not log in during the time period specified in the *Guest VLAN period* column. This value applies only on ports in which the *Port control* column contains the value `auto` or `multiClient`.

This function lets you grant end devices, without IEEE 802.1X support, access to selected services in the network.

Possible values:

- `0` (default setting)
  The authenticator does not assign a Guest VLAN to the port.
  When you enable the MAC-based authentication in the *MAC authorized bypass* column, the device automatically sets the value to `0`.
- `1..4042`

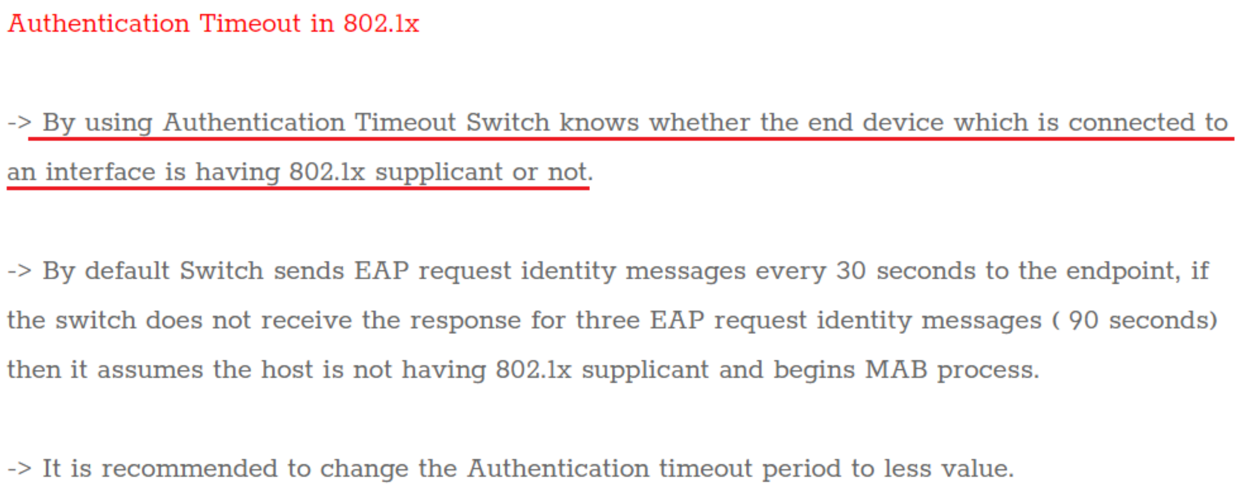
Guest VLAN period

Specifies the period in seconds for which the authenticator waits for EAPOL data packets after the end device is connected. If this period elapses, then the authenticator grants the end device access to the network and assigns the port to the Guest VLAN specified in the *Guest VLAN ID* column.

Possible values:

- `1..300` (default setting: `90`)

(*E.g.*, https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=QGH5908401-01.pdf&p_Doc_Ref=QGH59084&_ga=2.187119082.331813519.1662528344-1610863410.1660293470).



Authentication Timeout in 802.1x

-> By using Authentication Timeout Switch knows whether the end device which is connected to an interface is having 802.1x supplicant or not.

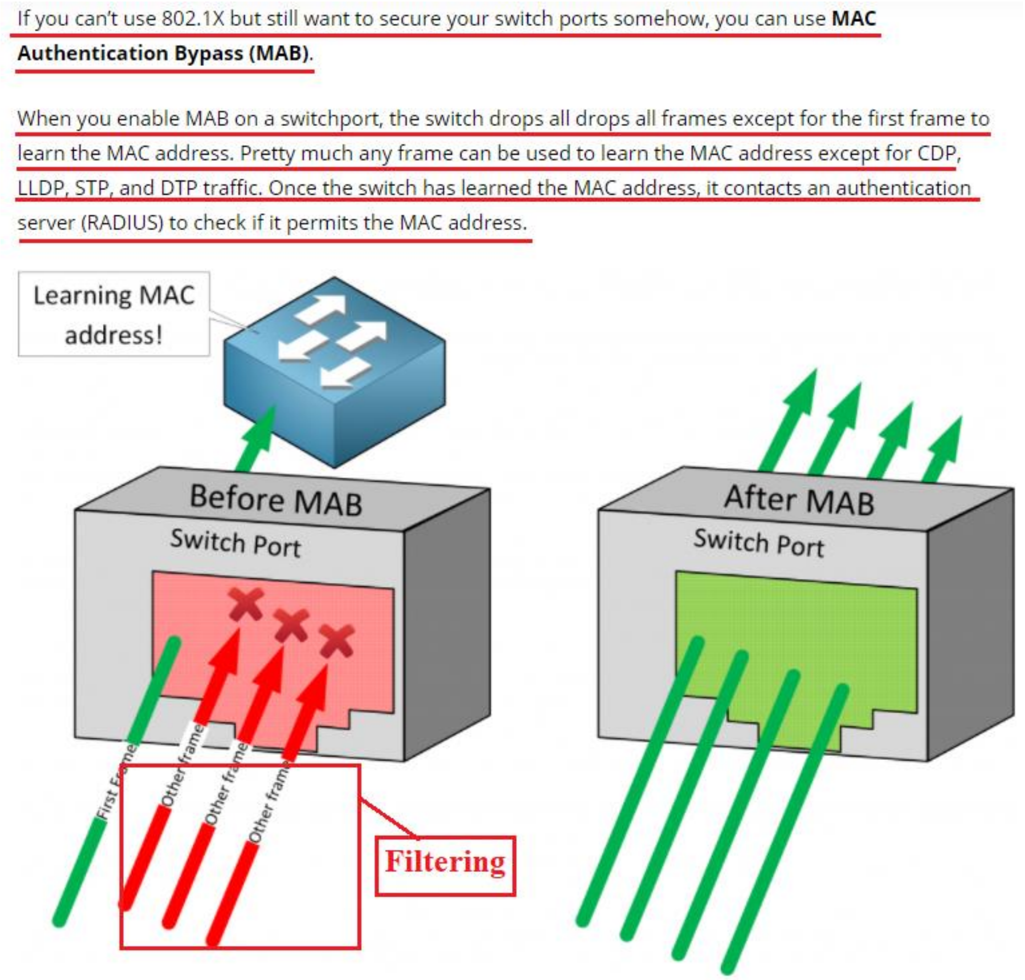
-> By default Switch sends EAP request identity messages every 30 seconds to the endpoint, if the switch does not receive the response for three EAP request identity messages (90 seconds) then it assumes the host is not having 802.1x supplicant and begins MAB process.

-> It is recommended to change the Authentication timeout period to less value.

(*E.g.*, https://www.kareemccie.com/2017/01/mac-authentication-bypass.html).

18. Upon information and belief, the Accused Instrumentality is used in a method performing the step of the access point detects if the user terminal is not IEEE 802.1x compliant,

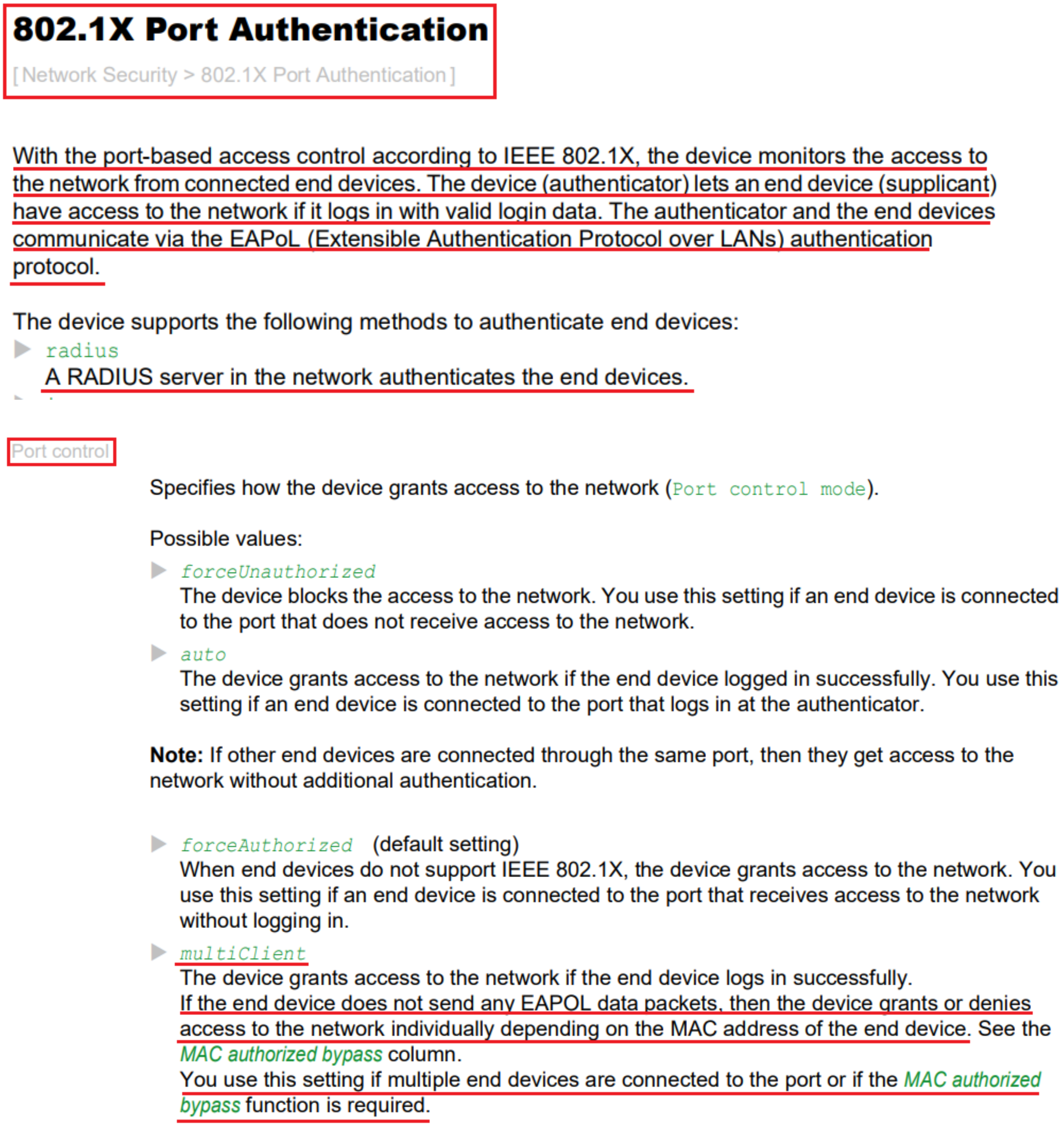
then configuring an internet protocol packet filter (*e.g.*, switch drops all the frames except the first frame to learn the MAC address) and redirecting a user request to a local server (*e.g.*, authentication server).



If you can't use 802.1X but still want to secure your switch ports somehow, you can use **MAC Authentication Bypass (MAB)**.

When you enable MAB on a switchport, the switch drops all drops all frames except for the first frame to learn the MAC address. Pretty much any frame can be used to learn the MAC address except for CDP, LLDP, STP, and DTP traffic. Once the switch has learned the MAC address, it contacts an authentication server (RADIUS) to check if it permits the MAC address.

(*E.g.*, https://www.kareemccie.com/2017/01/mac-authentication-bypass.html).



802.1X Port Authentication

[Network Security > 802.1X Port Authentication]

With the port-based access control according to IEEE 802.1X, the device monitors the access to the network from connected end devices. The device (authenticator) lets an end device (supplicant) have access to the network if it logs in with valid login data. The authenticator and the end devices communicate via the EAPoL (Extensible Authentication Protocol over LANs) authentication protocol.

The device supports the following methods to authenticate end devices:

- `radius`
  A RADIUS server in the network authenticates the end devices.

Port control

Specifies how the device grants access to the network (`Port control mode`).

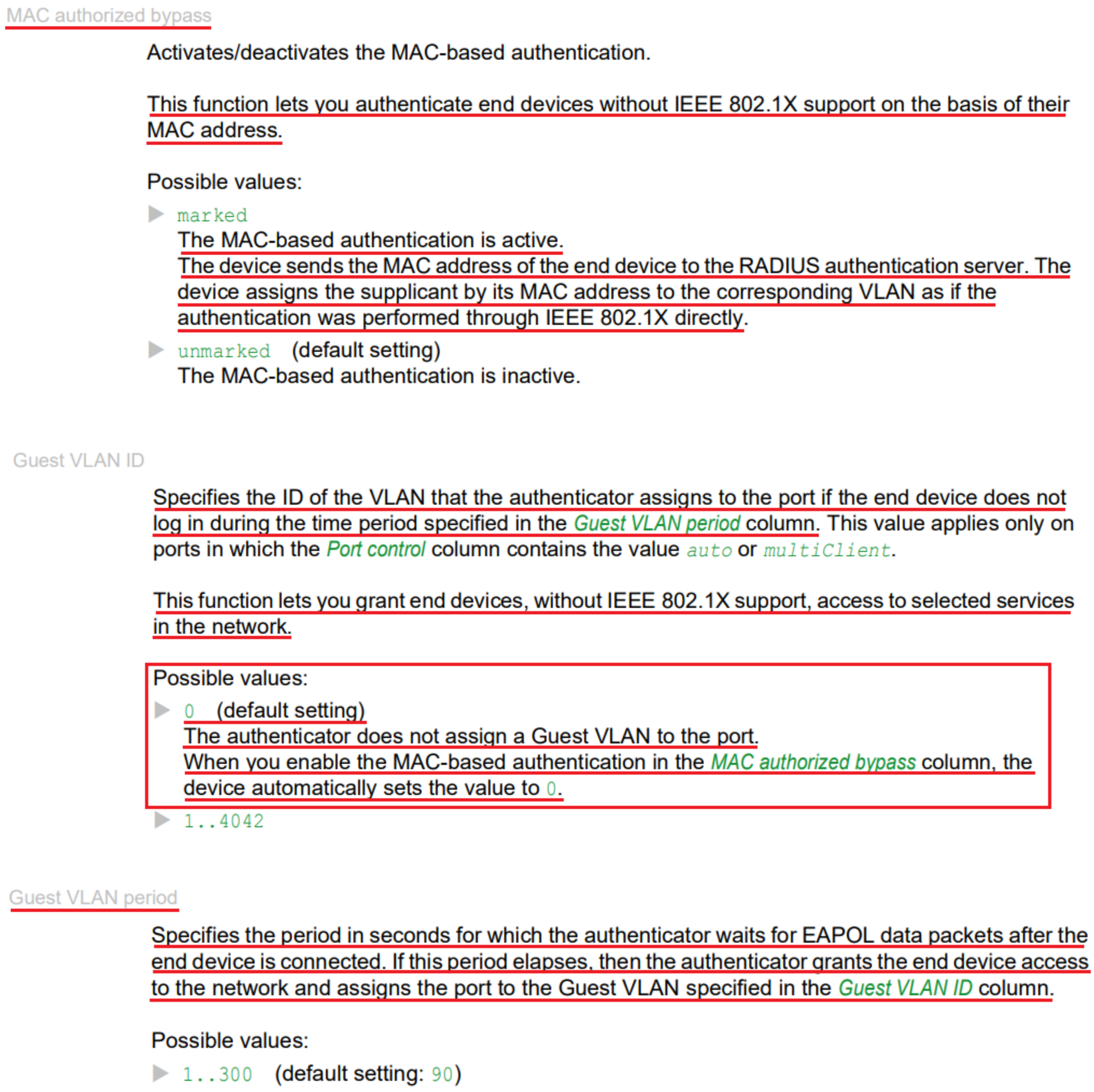
Possible values:

- *`forceUnauthorized`*
  The device blocks the access to the network. You use this setting if an end device is connected to the port that does not receive access to the network.
- *`auto`*
  The device grants access to the network if the end device logged in successfully. You use this setting if an end device is connected to the port that logs in at the authenticator.

Note: If other end devices are connected through the same port, then they get access to the network without additional authentication.

- *`forceAuthorized`* (default setting)
  When end devices do not support IEEE 802.1X, the device grants access to the network. You use this setting if an end device is connected to the port that receives access to the network without logging in.
- *`multiClient`*
  The device grants access to the network if the end device logs in successfully.
  If the end device does not send any EAPOL data packets, then the device grants or denies access to the network individually depending on the MAC address of the end device. See the *MAC authorized bypass* column.
  You use this setting if multiple end devices are connected to the port or if the *MAC authorized bypass* function is required.

(*E.g.*, https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=QGH5908401-01.pdf&p_Doc_Ref=QGH59084&_ga=2.187119082.331813519.1662528344-1610863410.1660293470).



MAC authorized bypass

Activates/deactivates the MAC-based authentication.

This function lets you authenticate end devices without IEEE 802.1X support on the basis of their MAC address.

Possible values:

- marked
  The MAC-based authentication is active.
  The device sends the MAC address of the end device to the RADIUS authentication server. The device assigns the supplicant by its MAC address to the corresponding VLAN as if the authentication was performed through IEEE 802.1X directly.
- unmarked (default setting)
  The MAC-based authentication is inactive.

Guest VLAN ID

Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not log in during the time period specified in the *Guest VLAN period* column. This value applies only on ports in which the *Port control* column contains the value `auto` or `multiClient`.

This function lets you grant end devices, without IEEE 802.1X support, access to selected services in the network.

Possible values:

- 0 (default setting)
  The authenticator does not assign a Guest VLAN to the port.
  When you enable the MAC-based authentication in the *MAC authorized bypass* column, the device automatically sets the value to 0.
- 1..4042

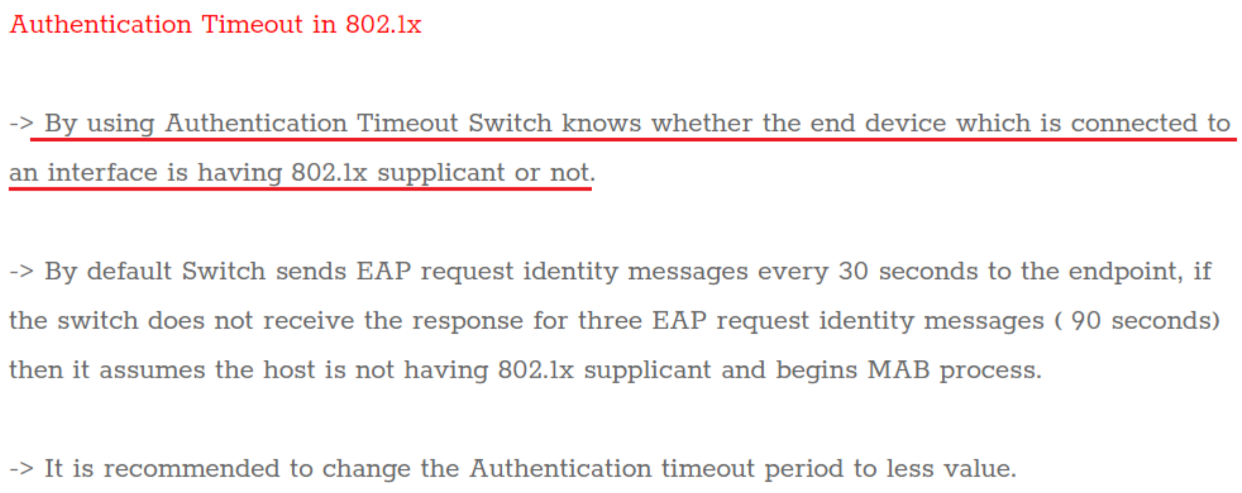
Guest VLAN period

Specifies the period in seconds for which the authenticator waits for EAPOL data packets after the end device is connected. If this period elapses, then the authenticator grants the end device access to the network and assigns the port to the Guest VLAN specified in the *Guest VLAN ID* column.

Possible values:

- 1..300 (default setting: 90)

(*E.g.*, https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name =QGH5908401-01.pdf&p_Doc_Ref=QGH59084&_ga=2.187119082.331813519.1662528344-1610863410.1660293470).



Authentication Timeout in 802.1x

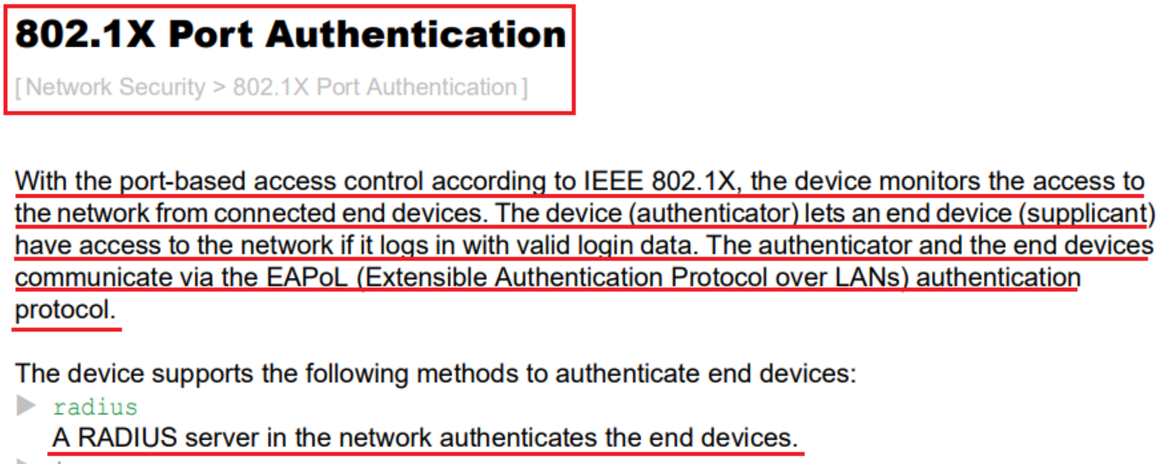
-> By using Authentication Timeout Switch knows whether the end device which is connected to an interface is having 802.1x supplicant or not.

-> By default Switch sends EAP request identity messages every 30 seconds to the endpoint, if the switch does not receive the response for three EAP request identity messages (90 seconds) then it assumes the host is not having 802.1x supplicant and begins MAB process.

-> It is recommended to change the Authentication timeout period to less value.

(*E.g.*, https://www.kareemccie.com/2017/01/mac-authentication-bypass.html).

19. Upon information and belief, the Accused Instrumentality is used in a method performing the step of the access point transitions (*e.g.*, from normal 802.1x authentication protocol after time out) to a state corresponding to browser based authentication (*e.g.*, authentication using RADIUS protocol via MAB) protocol if the user terminal is not IEEE 802.1x compliant.



802.1X Port Authentication

[Network Security > 802.1X Port Authentication]

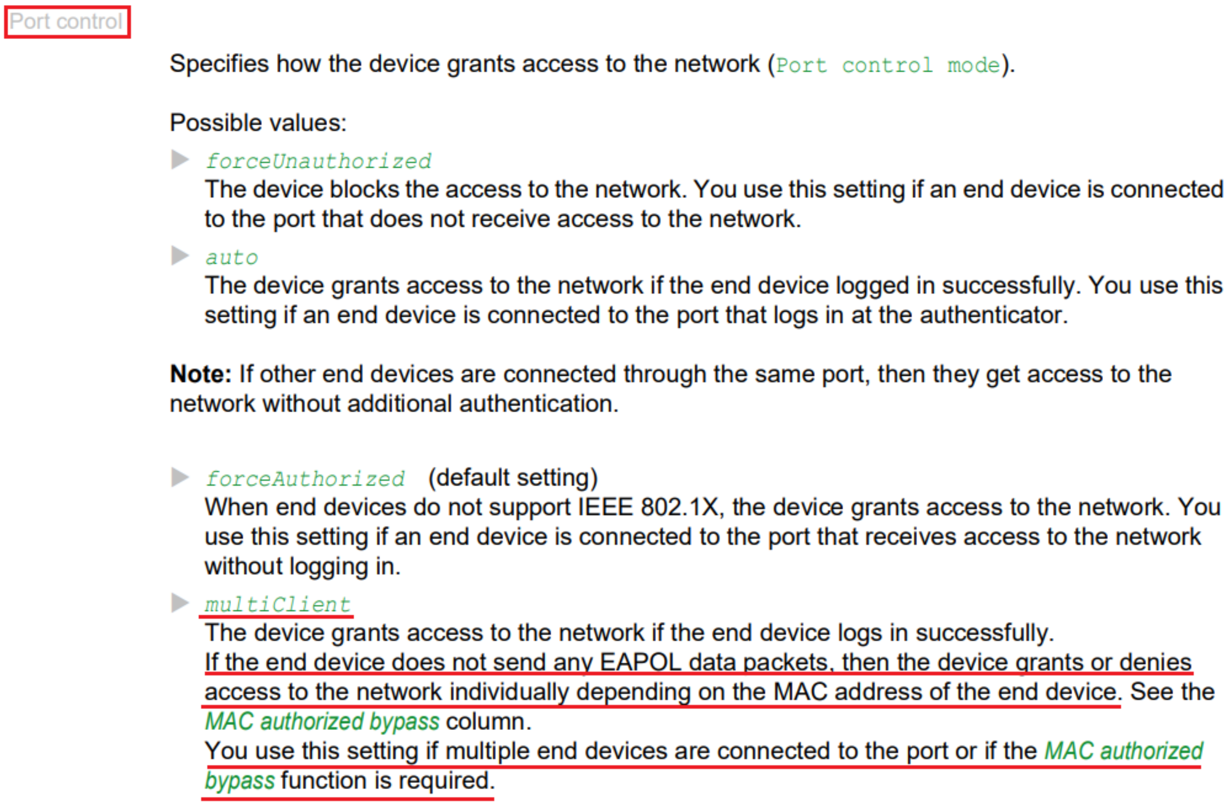
With the port-based access control according to IEEE 802.1X, the device monitors the access to the network from connected end devices. The device (authenticator) lets an end device (supplicant) have access to the network if it logs in with valid login data. The authenticator and the end devices communicate via the EAPoL (Extensible Authentication Protocol over LANs) authentication protocol.

The device supports the following methods to authenticate end devices:

▶ radius

A RADIUS server in the network authenticates the end devices.

(*E.g.*, https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=QGH5908401-01.pdf&p_Doc_Ref=QGH59084&_ga=2.187119082.331813519.1662528344-1610863410.1660293470).



Port control

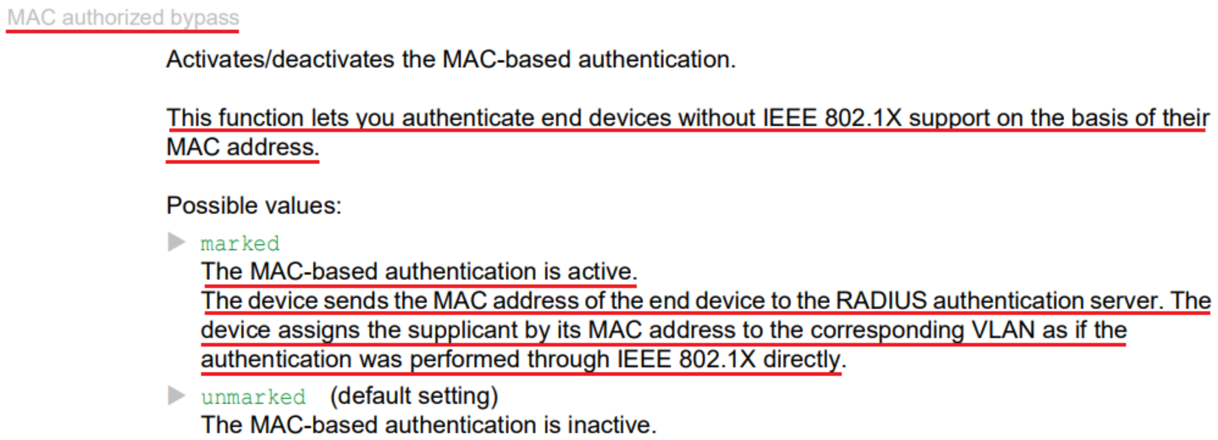
Specifies how the device grants access to the network (Port control mode).

Possible values:

- forceUnauthorized
  The device blocks the access to the network. You use this setting if an end device is connected to the port that does not receive access to the network.
- auto
  The device grants access to the network if the end device logged in successfully. You use this setting if an end device is connected to the port that logs in at the authenticator.

Note: If other end devices are connected through the same port, then they get access to the network without additional authentication.

- forceAuthorized (default setting)
  When end devices do not support IEEE 802.1X, the device grants access to the network. You use this setting if an end device is connected to the port that receives access to the network without logging in.
- multiClient
  The device grants access to the network if the end device logs in successfully.
  If the end device does not send any EAPOL data packets, then the device grants or denies access to the network individually depending on the MAC address of the end device. See the *MAC authorized bypass* column.
  You use this setting if multiple end devices are connected to the port or if the *MAC authorized bypass* function is required.



MAC authorized bypass

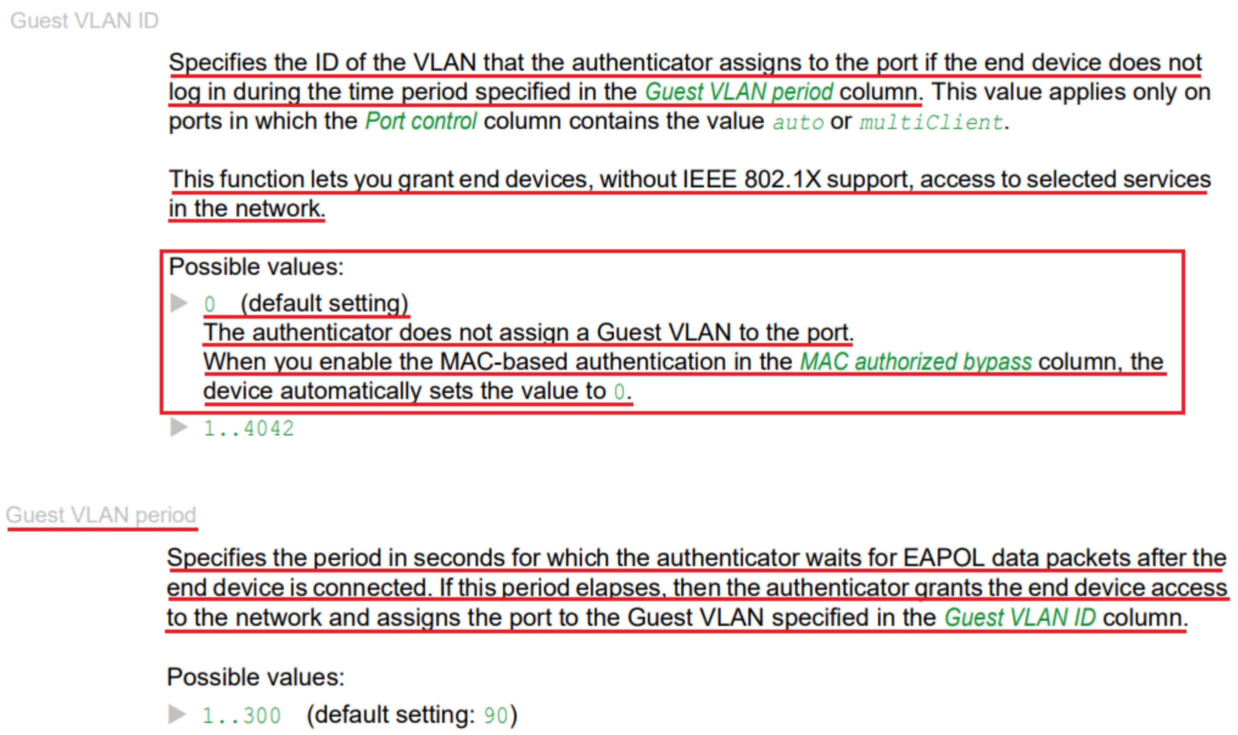
Activates/deactivates the MAC-based authentication.

This function lets you authenticate end devices without IEEE 802.1X support on the basis of their MAC address.

Possible values:

- marked
  The MAC-based authentication is active.
  The device sends the MAC address of the end device to the RADIUS authentication server. The device assigns the supplicant by its MAC address to the corresponding VLAN as if the authentication was performed through IEEE 802.1X directly.
- unmarked (default setting)
  The MAC-based authentication is inactive.

(*E.g.*, https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=QGH5908401-01.pdf&p_Doc_Ref=QGH59084&_ga=2.187119082.331813519.1662528344-1610863410.1660293470).



Guest VLAN ID

Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not log in during the time period specified in the *Guest VLAN period* column. This value applies only on ports in which the *Port control* column contains the value `auto` or `multiClient`.

This function lets you grant end devices, without IEEE 802.1X support, access to selected services in the network.

Possible values:

- `0` (default setting)
  The authenticator does not assign a Guest VLAN to the port.
  When you enable the MAC-based authentication in the *MAC authorized bypass* column, the device automatically sets the value to `0`.
- `1..4042`

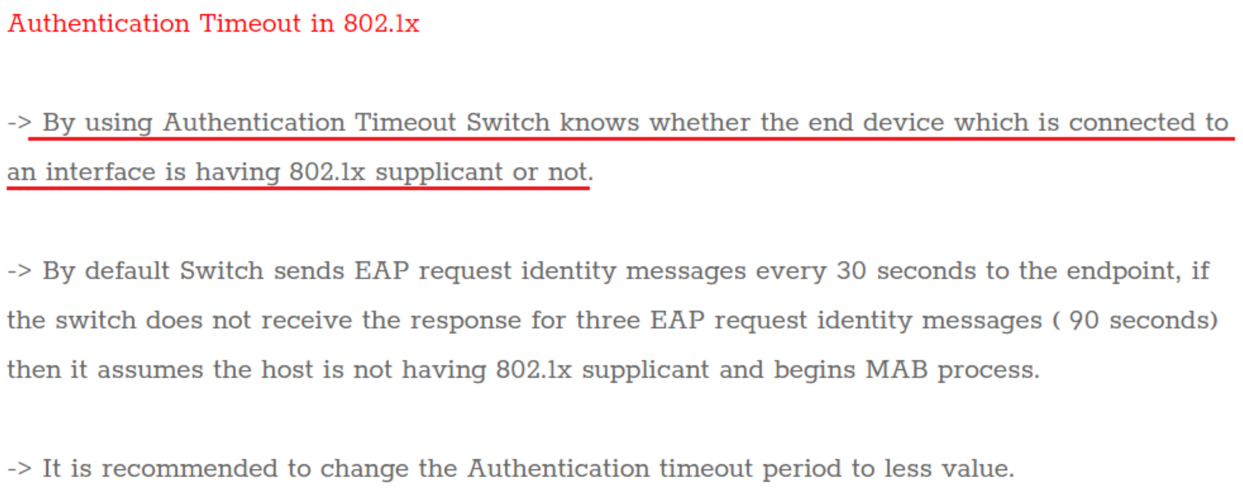
Guest VLAN period

Specifies the period in seconds for which the authenticator waits for EAPOL data packets after the end device is connected. If this period elapses, then the authenticator grants the end device access to the network and assigns the port to the Guest VLAN specified in the *Guest VLAN ID* column.

Possible values:

- `1..300` (default setting: `90`)

(*E.g.*, https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=QGH5908401-01.pdf&p_Doc_Ref=QGH59084&_ga=2.187119082.331813519.1662528344-1610863410.1660293470).



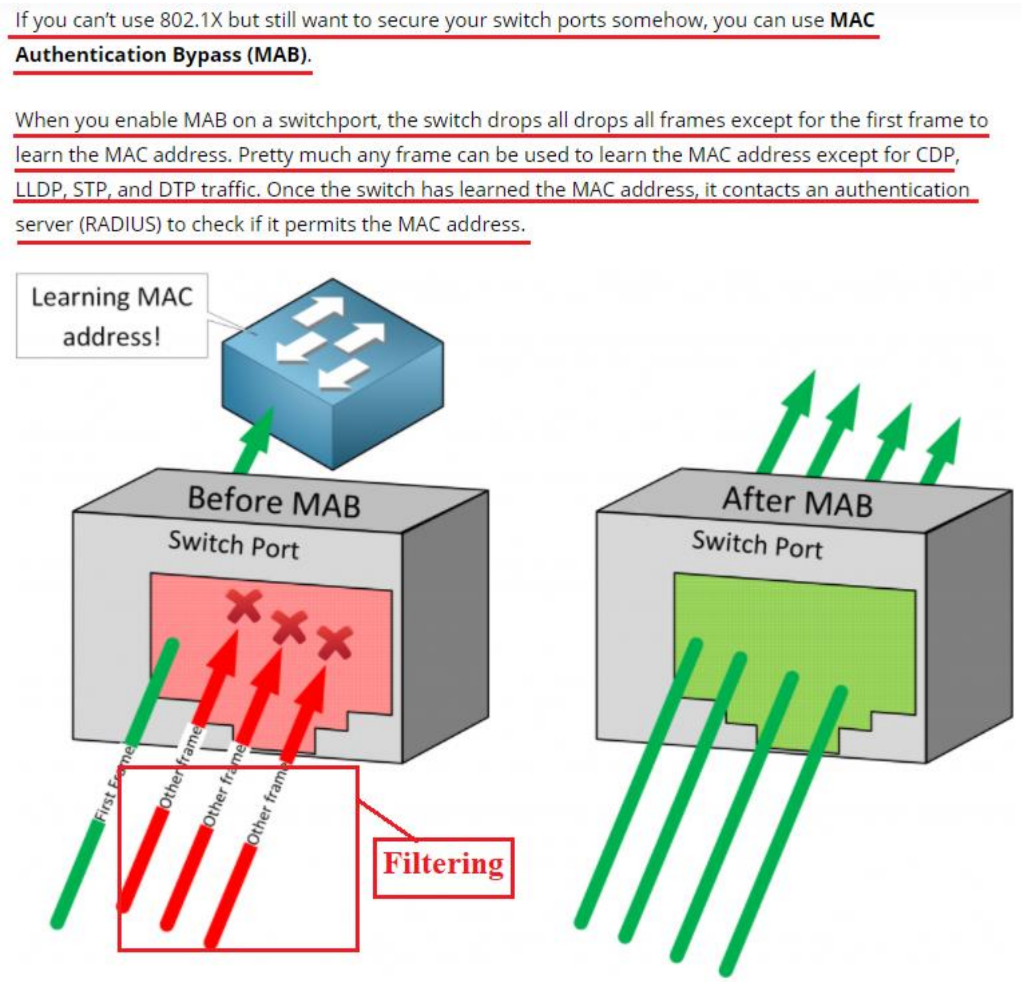
Authentication Timeout in 802.1x

-> By using Authentication Timeout Switch knows whether the end device which is connected to an interface is having 802.1x supplicant or not.

-> By default Switch sends EAP request identity messages every 30 seconds to the endpoint, if the switch does not receive the response for three EAP request identity messages (90 seconds) then it assumes the host is not having 802.1x supplicant and begins MAB process.

-> It is recommended to change the Authentication timeout period to less value.

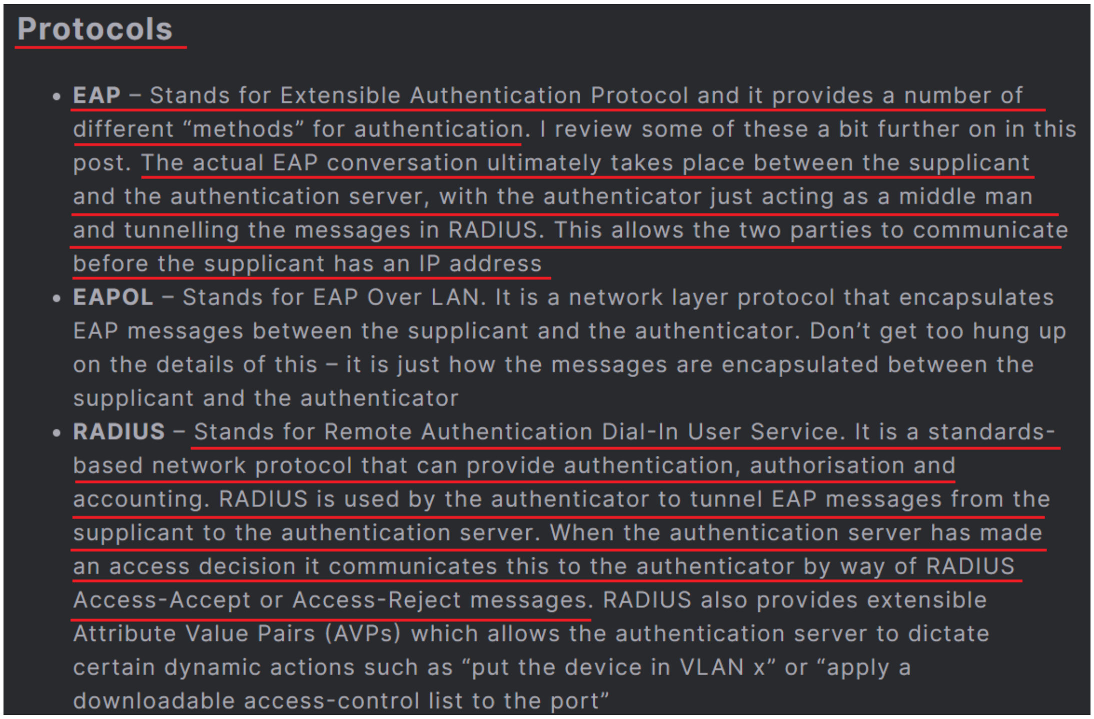
(*E.g.*, https://www.kareemccie.com/2017/01/mac-authentication-bypass.html).



If you can't use 802.1X but still want to secure your switch ports somehow, you can use **MAC Authentication Bypass (MAB)**.

When you enable MAB on a switchport, the switch drops all drops all frames except for the first frame to learn the MAC address. Pretty much any frame can be used to learn the MAC address except for CDP, LLDP, STP, and DTP traffic. Once the switch has learned the MAC address, it contacts an authentication server (RADIUS) to check if it permits the MAC address.

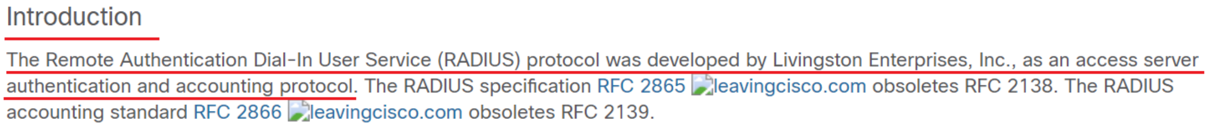
(*E.g.*, https://networklessons.com/cisco/ccie-routing-switching-written/mac-authentication-bypass-mab).



Protocols

- **EAP** – Stands for Extensible Authentication Protocol and it provides a number of different "methods" for authentication. I review some of these a bit further on in this post. The actual EAP conversation ultimately takes place between the supplicant and the authentication server, with the authenticator just acting as a middle man and tunnelling the messages in RADIUS. This allows the two parties to communicate before the supplicant has an IP address
- **EAPOL** – Stands for EAP Over LAN. It is a network layer protocol that encapsulates EAP messages between the supplicant and the authenticator. Don't get too hung up on the details of this – it is just how the messages are encapsulated between the supplicant and the authenticator
- **RADIUS** – Stands for Remote Authentication Dial-In User Service. It is a standards-based network protocol that can provide authentication, authorisation and accounting. RADIUS is used by the authenticator to tunnel EAP messages from the supplicant to the authentication server. When the authentication server has made an access decision it communicates this to the authenticator by way of RADIUS Access-Accept or Access-Reject messages. RADIUS also provides extensible Attribute Value Pairs (AVPs) which allows the authentication server to dictate certain dynamic actions such as "put the device in VLAN x" or "apply a downloadable access-control list to the port"

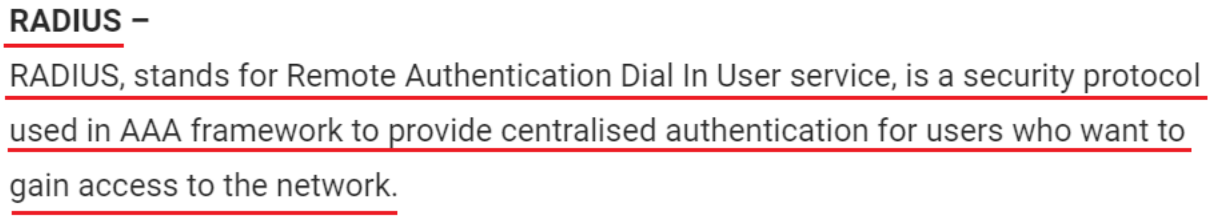
(*E.g.*, https://mikeguy.co.uk/posts/2018/06/understanding-nac-802.1x-and-mab/).



Introduction

The Remote Authentication Dial-In User Service (RADIUS) protocol was developed by Livingston Enterprises, Inc., as an access server authentication and accounting protocol. The RADIUS specification RFC 2865 leavingcisco.com obsoletes RFC 2138. The RADIUS accounting standard RFC 2866 leavingcisco.com obsoletes RFC 2139.

(*E.g.*, https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html).



RADIUS –

RADIUS, stands for Remote Authentication Dial In User service, is a security protocol used in AAA framework to provide centralised authentication for users who want to gain access to the network.

(*E.g.*, https://www.geeksforgeeks.org/radius-protocol/).

20. Defendant's customers also infringe claims 9,10, and 11 of the '037 patent by using or performing the claimed method using the Accused Instrumentality as described above. Furthermore, Defendant advertises, markets, and offers for sale the Accused Instrumentality to its

customers for use in a system in a manner that, as described above, infringes claims 9,10, and 11 of the ‘037 patent. Exemplary materials are cited above.

21. Plaintiff has been damaged as a result of Defendant’s infringing conduct. Defendant is thus liable to Plaintiff for damages in an amount that adequately compensates Plaintiff for such Defendant’s infringement of the ‘037 patent, *i.e.*, in an amount that by law cannot be less than would constitute a reasonable royalty for the use of the patented technology, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

22. The asserted claims of the ‘037 Patent are method claims to which the marking requirements are not applicable. To the extent required, Plaintiff has therefore complied with the marking statute.

IV. JURY DEMAND

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

V. PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court find in its favor and against Defendant, and that the Court grant Plaintiff the following relief:

a. Judgment that one or more claims of United States Patent No. 8,272,037 have been infringed, either literally and/or under the doctrine of equivalents, by Defendant;

b. Judgment that Defendant account for and pay to Plaintiff all damages to and costs incurred by Plaintiff because of Defendant’s infringing activities and other conduct complained of herein;

c. That Plaintiff be granted pre-judgment and post-judgment interest on the damages caused by Defendant’s infringing activities and other conduct complained of herein;

d. That Plaintiff be granted such other and further relief as the Court may deem just and proper under the circumstances.

September 28, 2022

DIRECTION IP LAW

/s/ David R. Benneтт

David R. Bennett
Direction IP Law
P.O. Box 14184
Chicago, IL 60614-0184
(312) 291-1667
dbennett@directionip.com

Attorney for Plaintiff Tranquility IP LLC