

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK**

TRANQUILITY IP LLC,

Plaintiff,

v.

BELDEN INC.,

Defendant.

C.A. No. 22-cv-05213

JURY TRIAL DEMANDED

PATENT CASE

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Tranquility IP LLC files this Original Complaint for Patent Infringement against Belden 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 Belden Inc. (“Defendant”) is a corporation with a place of business at 19-02 Whitestone Expressway, Suite 305, Whitestone, NY 11357. Defendant has a registered agent at Corporation Service Company, 80 State Street, Albany, NY 12207.

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 New York Long-Arm Statute, due at least to

its business in this forum, including at least a portion of the infringements alleged herein at 19-02 Whitestone Expressway, Suite 305, Whitestone, NY 11357.

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 New York. 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 New York. 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 New York. Defendant has committed such purposeful acts and/or transactions in New York 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 maintains a place of business at 19-02 Whitestone Expressway, Suite 305, Whitestone, NY 11357. 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 New York, 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 Belden Classic Switch Software 9.0 (“Accused Instrumentality”) (e.g., <https://www.belden.com/products/industrial-networking-cybersecurity/software-solutions/device-software/classic-switch-software/classic-switch-software-9-0-mach102-l2p>).

15. Upon information and belief, the Accused Instrumentality is used in 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.

BELDEN

Products
Markets
Partners
Solutions
Resources
Support



Overview
Specifications
Resources

Classic Switch Software 9.0 - MACH102 (L2P)

Classic Software 9 for the MACH102 L2P

The Classic Switch Software provides a range of functions normally found in backbone systems used in office networks. This includes comprehensive management, diagnostics and filter functions, various redundancy features, security mechanisms and real-time applications. All relevant software files can be downloaded from the "Documents " tab



Classic Switch Software - 9.0

Data Sheet ▾

Request Quote

(E.g., <https://www.belden.com/products/industrial-networking-cybersecurity/software-solutions/device-software/classic-switch-software/classic-switch-software-9-0-mach102-l2p>).

Security	IP-based Port Security, MAC-based Port Security, <u>Port-based Access Control with 802.1X</u>, Guest/unauthenticated VLAN, RADIUS VLAN Assignment, Multi-Client Authentication per Port, <u>MAC Authentication Bypass</u>, Access to Management restricted by VLAN, HTTPS Certificate Management, Restricted Management Access, Appropriate Use Banner, SNMP Logging, Local User Management, Remote Authentication via RADIUS
---	--

(E.g., <https://www.belden.com/products/industrial-networking-cybersecurity/software-solutions/device-software/classic-switch-software/classic-switch-software-9-0-mach102-l2p>).

2.6 **802.1X Port Authentication**

The 802.1X Port Authentication provides you with the following dialogs:

- ▶ “802.1X Global Configuration”
- ▶ “802.1X Port Configuration”
- ▶ “802.1X Port Clients”
- ▶ “802.1X Port Statistics”

The port-based network access control is a method described in norm IEEE 802.1X to protect IEEE 802 networks from unauthorized access. The protocol controls the access on a port by authenticating and authorizing a terminal device that is connected to this port of the device.

The 802.1X Port Authentication function requires that you configure a RADIUS Server for authentication and authorization. The authentication and authorization are carried out by the authenticator, in this case the device. The device authenticates the supplicant (the querying device, e.g. a PC), which means that it permits the access to the services it provides (e.g. access to the network to which the device is connected), or else refuses it. In the process, the device accesses an external authentication server (RADIUS server), which checks the authentication data of the supplicant. The device exchanges the authentication data with the supplicant via the Extensible Authentication Protocol over LANs (EAPOL), and with the RADIUS server via the RADIUS protocol.

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

Parameter	Meanings	Possible values	Default setting
Port Control	Setting for the port access control.	► ForceAuthorized: Access is also available for all clients without authentication. ► ForceUnauthorized: Access is blocked for all clients, even for clients with authentication. ► auto: Access to the port depends on the result of the authentication. ► macBased: Behavior like for auto. Access is also available for clients with a MAC address which the client uses in the course of authentication.	ForceAuthorized
Note: ► In the ForceAuthorized, ForceUnauthorized and auto modes the Switch opens or blocks the port for all clients. Use these modes if you are connecting a single client to the Switch. ► In the macBased mode the Switch <u>authenticates the clients based on the individual MAC addresses and allows or blocks their data traffic separately.</u> Use this mode if you want to use multi-client authentication or the "MAC Authentication Bypass" function.			

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

<u>Guest VLAN ID</u>	<u>ID of a VLAN that the Switch assigns to the port, if:</u>	0 - 4094	0
-	▶ <u>the 802.1X protocol is active on the port and the port control is set to <i>auto</i> or <i>macBased</i>,</u> ▶ <u>a client wants to receive data traffic and EAPOL frames from the client fail to appear, i.e. the client does not support the 802.1X protocol.</u> The Switch: ▶ switches the port to the authenticated state, ▶ allows data traffic, ▶ but only to the guest VLAN. Specify a guest VLAN ID if you want to allow devices without 802.1X support access to a guest VLAN. Note: ▶ Use only as a guest VLAN a VLAN that you have set up statically in the Switch. ▶ However, if a client connects via 802.1X and his authentication fails, then the Switch only gives him access to the <u>unauthenticated VLAN.</u> ▶ When you activate the MAC Authorized Bypass (MAB) function, the device automatically sets the guest VLAN ID to 0.	With a VLAN ID of 0, the Switch blocks the data traffic because it denies a VLAN setup with this ID.	

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

Parameter	Meaning	Possible values	Default setting
MAC Authorized Bypass Enable	<u>The Switch makes authenticated access available via MAB, if:</u> ▶ <u>You have set the "Port Control" to macBased,</u> ▶ <u>a device wants to receive data traffic employing a particular known MAC address,</u> ▶ <u>this device does not authenticate itself via 802.1X and</u> ▶ <u>the RADIUS server recognizes the MAC addresses authorized to access.</u> <u>The Switch:</u> ▶ <u>waits for the guest VLAN interval to elapse in order to do this,</u> ▶ <u>then sends a query to the RADIUS server and in doing so uses the MAC address as the user name and the password.</u> <u>Activate this function, if:</u> ▶ <u>you want to allow particular devices normal access,</u> ▶ <u>however these devices do not support 802.1X.</u>	On Off	Off
Guest VLAN Period	<u>Time that the Switch waits for EAPOL frames after connecting a device on this port in order to determine whether it supports the 802.1X protocol.</u> <u>If this time elapses, the Switch only provides access to the guest VLAN for the device connected.</u>	1 - 300 s	90 s

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

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 is used in a method performing the step of an access point (e.g., authenticator or switch) 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 Authentication Bypass or MAB) compatible with the user terminal.

Security

IP-based Port Security, MAC-based Port Security, Port-based Access Control with 802.1X, Guest/unauthenticated VLAN, RADIUS VLAN Assignment, Multi-Client Authentication per Port, MAC Authentication Bypass, Access to Management restricted by VLAN, HTTPS Certificate Management, Restricted Management Access, Appropriate Use Banner, SNMP Logging, Local User Management, Remote Authentication via RADIUS

(E.g., <https://www.belden.com/products/industrial-networking-cybersecurity/software-solutions/device-software/classic-switch-software/classic-switch-software-9-0-mach102-l2p>).

2.6 802.1X Port Authentication

The 802.1X Port Authentication provides you with the following dialogs:

- ▶ “802.1X Global Configuration”
- ▶ “802.1X Port Configuration”
- ▶ “802.1X Port Clients”
- ▶ “802.1X Port Statistics”

The port-based network access control is a method described in norm IEEE 802.1X to protect IEEE 802 networks from unauthorized access. The protocol controls the access on a port by authenticating and authorizing a terminal device that is connected to this port of the device.

The 802.1X Port Authentication function requires that you configure a RADIUS Server for authentication and authorization. The authentication and authorization are carried out by the authenticator, in this case the device. The device authenticates the supplicant (the querying device, e.g. a PC), which means that it permits the access to the services it provides (e.g. access to the network to which the device is connected), or else refuses it. In the process, the device accesses an external authentication server (RADIUS server), which checks the authentication data of the supplicant. The device exchanges the authentication data with the supplicant via the Extensible Authentication Protocol over LANs (EAPOL), and with the RADIUS server via the RADIUS protocol.

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

Parameter	Meanings	Possible values	Default setting
Port Control	Setting for the port access control.	► ForceAuthorized: Access is also available for all clients without authentication. ► ForceUnauthorized: Access is blocked for all clients, even for clients with authentication. ► auto: Access to the port depends on the result of the authentication. ► macBased: Behavior like for auto. Access is also available for clients with a MAC address which the client uses in the course of authentication.	ForceAuthorized
Note: ► In the ForceAuthorized, ForceUnauthorized and auto modes the Switch opens or blocks the port for all clients. Use these modes if you are connecting a single client to the Switch. ► In the macBased mode the Switch <u>authenticates the clients based on the individual MAC addresses and allows or blocks their data traffic separately.</u> Use this mode if you want to use multi-client authentication or the "MAC Authentication Bypass" function.			

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

<u>Guest VLAN ID</u>	<u>ID of a VLAN that the Switch assigns to the port, if:</u>	0 - 4094	0
-	▶ <u>the 802.1X protocol is active on the port and the port control is set to <i>auto</i> or <i>macBased</i>,</u> ▶ <u>a client wants to receive data traffic and EAPOL frames from the client fail to appear, i.e. the client does not support the 802.1X protocol.</u> The Switch: ▶ switches the port to the authenticated state, ▶ allows data traffic, ▶ but only to the guest VLAN. Specify a guest VLAN ID if you want to allow devices without 802.1X support access to a guest VLAN. Note: ▶ Use only as a guest VLAN a VLAN that you have set up statically in the Switch. ▶ However, if a client connects via 802.1X and his authentication fails, then the Switch only gives him access to the <u>unauthenticated VLAN.</u> ▶ When you activate the MAC Authorized Bypass (MAB) function, the device automatically sets the guest VLAN ID to 0.	With a VLAN ID of 0, the Switch blocks the data traffic because it denies a VLAN setup with this ID.	

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

Parameter	Meaning	Possible values	Default setting
MAC Authorized Bypass Enable	<u>The Switch makes authenticated access available via MAB, if:</u> ▶ <u>You have set the "Port Control" to macBased,</u> ▶ <u>a device wants to receive data traffic employing a particular known MAC address,</u> ▶ <u>this device does not authenticate itself via 802.1X and</u> ▶ <u>the RADIUS server recognizes the MAC addresses authorized to access.</u> <u>The Switch:</u> ▶ <u>waits for the guest VLAN interval to elapse in order to do this,</u> ▶ <u>then sends a query to the RADIUS server and in doing so uses the MAC address as the user name and the password.</u> <u>Activate this function, if:</u> ▶ <u>you want to allow particular devices normal access,</u> ▶ <u>however these devices do not support 802.1X.</u>	On Off	Off
Guest VLAN Period	<u>Time that the Switch waits for EAPOL frames after connecting a device on this port in order to determine whether it supports the 802.1X protocol.</u> <u>If this time elapses, the Switch only provides access to the guest VLAN for the device connected.</u>	1 - 300 s	90 s

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

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.

Security

IP-based Port Security, MAC-based Port Security, Port-based Access Control with 802.1X, Guest/unauthenticated VLAN, RADIUS VLAN Assignment, Multi-Client Authentication per Port, MAC Authentication Bypass, Access to Management restricted by VLAN, HTTPS Certificate Management, Restricted Management Access, Appropriate Use Banner, SNMP Logging, Local User Management, Remote Authentication via RADIUS

(E.g., <https://www.belden.com/products/industrial-networking-cybersecurity/software-solutions/device-software/classic-switch-software/classic-switch-software-9-0-mach102-l2p>).

2.6 802.1X Port Authentication

The 802.1X Port Authentication provides you with the following dialogs:

- ▶ “802.1X Global Configuration”
- ▶ “802.1X Port Configuration”
- ▶ “802.1X Port Clients”
- ▶ “802.1X Port Statistics”

The port-based network access control is a method described in norm IEEE 802.1X to protect IEEE 802 networks from unauthorized access. The protocol controls the access on a port by authenticating and authorizing a terminal device that is connected to this port of the device.

The 802.1X Port Authentication function requires that you configure a RADIUS Server for authentication and authorization. The authentication and authorization are carried out by the authenticator, in this case the device. The device authenticates the supplicant (the querying device, e.g. a PC), which means that it permits the access to the services it provides (e.g. access to the network to which the device is connected), or else refuses it. In the process, the device accesses an external authentication server (RADIUS server), which checks the authentication data of the supplicant. The device exchanges the authentication data with the supplicant via the Extensible Authentication Protocol over LANs (EAPOL), and with the RADIUS server via the RADIUS protocol.

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

Parameter	Meanings	Possible values	Default setting
Port Control	Setting for the port access control.	► ForceAuthorized: Access is also available for all clients without authentication. ► ForceUnauthorized: Access is blocked for all clients, even for clients with authentication. ► auto: Access to the port depends on the result of the authentication. ► macBased: Behavior like for auto. Access is also available for clients with a MAC address which the client uses in the course of authentication.	ForceAuthorized
Note: ► In the ForceAuthorized, ForceUnauthorized and auto modes the Switch opens or blocks the port for all clients. Use these modes if you are connecting a single client to the Switch. ► In the macBased mode the Switch <u>authenticates the clients based on the individual MAC addresses and allows or blocks their data traffic separately.</u> Use this mode if you want to use multi-client authentication or the "MAC Authentication Bypass" function.			

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

<u>Guest VLAN ID</u>	<u>ID of a VLAN that the Switch assigns to the port, if:</u>	0 - 4094	0
-	▶ <u>the 802.1X protocol is active on the port and the port control is set to <i>auto</i> or <i>macBased</i>,</u> ▶ <u>a client wants to receive data traffic and EAPOL frames from the client fail to appear, i.e. the client does not support the 802.1X protocol.</u> The Switch: ▶ switches the port to the authenticated state, ▶ allows data traffic, ▶ but only to the guest VLAN. Specify a guest VLAN ID if you want to allow devices without 802.1X support access to a guest VLAN. Note: ▶ Use only as a guest VLAN a VLAN that you have set up statically in the Switch. ▶ However, if a client connects via 802.1X and his authentication fails, then the Switch only gives him access to the <u>unauthenticated VLAN.</u> ▶ When you activate the MAC Authorized Bypass (MAB) function, the device automatically sets the guest VLAN ID to 0.	With a VLAN ID of 0, the Switch blocks the data traffic because it denies a VLAN setup with this ID.	

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

Parameter	Meaning	Possible values	Default setting
MAC Authorized Bypass Enable	<u>The Switch makes authenticated access available via MAB, if:</u> ▶ <u>You have set the "Port Control" to macBased,</u> ▶ <u>a device wants to receive data traffic employing a particular known MAC address,</u> ▶ <u>this device does not authenticate itself via 802.1X and</u> ▶ <u>the RADIUS server recognizes the MAC addresses authorized to access.</u> <u>The Switch:</u> ▶ <u>waits for the guest VLAN interval to elapse in order to do this,</u> ▶ <u>then sends a query to the RADIUS server and in doing so uses the MAC address as the user name and the password.</u> <u>Activate this function, if:</u> ▶ <u>you want to allow particular devices normal access,</u> ▶ <u>however these devices do not support 802.1X.</u>	On Off	Off
Guest VLAN Period	<u>Time that the Switch waits for EAPOL frames after connecting a device on this port in order to determine whether it supports the 802.1X protocol.</u> <u>If this time elapses, the Switch only provides access to the guest VLAN for the device connected.</u>	1 - 300 s	90 s

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

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.

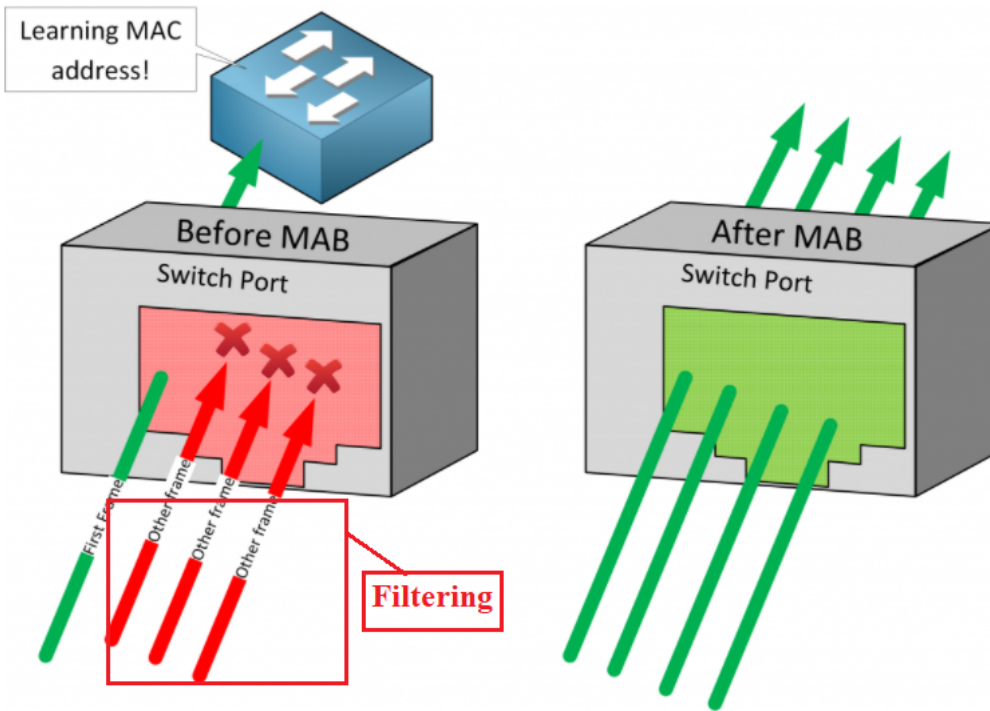
-> It is recommended to change the Authentication timeout period to less value.

(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 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#:~:text=Once%20the%20switch%20has%20learned,you%20can%20with%20802.1X.>).

Security

IP-based Port Security, MAC-based Port Security, Port-based Access Control with 802.1X, Guest/unauthenticated VLAN, RADIUS VLAN Assignment, Multi-Client Authentication per Port, MAC Authentication Bypass, Access to Management restricted by VLAN, HTTPS Certificate Management, Restricted Management Access, Appropriate Use Banner, SNMP Logging, Local User Management, Remote Authentication via RADIUS

(E.g., <https://www.belden.com/products/industrial-networking-cybersecurity/software-solutions/device-software/classic-switch-software/classic-switch-software-9-0-mach102-l2p>).

2.6 802.1X Port Authentication

The 802.1X Port Authentication provides you with the following dialogs:

- ▶ “802.1X Global Configuration”
- ▶ “802.1X Port Configuration”
- ▶ “802.1X Port Clients”
- ▶ “802.1X Port Statistics”

The port-based network access control is a method described in norm IEEE 802.1X to protect IEEE 802 networks from unauthorized access. The protocol controls the access on a port by authenticating and authorizing a terminal device that is connected to this port of the device.

The 802.1X Port Authentication function requires that you configure a RADIUS Server for authentication and authorization. The authentication and authorization are carried out by the authenticator, in this case the device. The device authenticates the supplicant (the querying device, e.g. a PC), which means that it permits the access to the services it provides (e.g. access to the network to which the device is connected), or else refuses it. In the process, the device accesses an external authentication server (RADIUS server), which checks the authentication data of the supplicant. The device exchanges the authentication data with the supplicant via the Extensible Authentication Protocol over LANs (EAPOL), and with the RADIUS server via the RADIUS protocol.

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

Parameter	Meanings	Possible values	Default setting
Port Control	Setting for the port access control.	► ForceAuthorized: Access is also available for all clients without authentication. ► ForceUnauthorized: Access is blocked for all clients, even for clients with authentication. ► auto: Access to the port depends on the result of the authentication. ► macBased: Behavior like for auto. Access is also available for clients with a MAC address which the client uses in the course of authentication.	ForceAuthorized
Note: ► In the ForceAuthorized, ForceUnauthorized and auto modes the Switch opens or blocks the port for all clients. Use these modes if you are connecting a single client to the Switch. ► In the macBased mode the Switch <u>authenticates the clients based on the individual MAC addresses and allows or blocks their data traffic separately.</u> Use this mode if you want to use multi-client authentication or the "MAC Authentication Bypass" function.			

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

<u>Guest VLAN ID</u>	<u>ID of a VLAN that the Switch assigns to the port, if:</u>	0 - 4094	0
-	▶ <u>the 802.1X protocol is active on the port and the port control is set to <i>auto</i> or <i>macBased</i>,</u> ▶ <u>a client wants to receive data traffic and EAPOL frames from the client fail to appear, i.e. the client does not support the 802.1X protocol.</u> The Switch: ▶ switches the port to the authenticated state, ▶ allows data traffic, ▶ but only to the guest VLAN. Specify a guest VLAN ID if you want to allow devices without 802.1X support access to a guest VLAN. Note: ▶ Use only as a guest VLAN a VLAN that you have set up statically in the Switch. ▶ However, if a client connects via 802.1X and his authentication fails, then the Switch only gives him access to the <u>unauthenticated VLAN.</u> ▶ When you activate the MAC Authorized Bypass (MAB) function, the device automatically sets the guest VLAN ID to 0.	With a VLAN ID of 0, the Switch blocks the data traffic because it denies a VLAN setup with this ID.	

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

Parameter	Meaning	Possible values	Default setting
MAC Authorized Bypass Enable	<u>The Switch makes authenticated access available via MAB, if:</u> ▶ <u>You have set the "Port Control" to macBased,</u> ▶ <u>a device wants to receive data traffic employing a particular known MAC address,</u> ▶ <u>this device does not authenticate itself via 802.1X and</u> ▶ <u>the RADIUS server recognizes the MAC addresses authorized to access.</u> <u>The Switch:</u> ▶ <u>waits for the guest VLAN interval to elapse in order to do this,</u> ▶ <u>then sends a query to the RADIUS server and in doing so uses the MAC address as the user name and the password.</u> <u>Activate this function, if:</u> ▶ <u>you want to allow particular devices normal access,</u> ▶ <u>however these devices do not support 802.1X.</u>	On Off	Off
Guest VLAN Period	<u>Time that the Switch waits for EAPOL frames after connecting a device on this port in order to determine whether it supports the 802.1X protocol.</u> <u>If this time elapses, the Switch only provides access to the guest VLAN for the device connected.</u>	1 - 300 s	90 s

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

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.

Security

IP-based Port Security, MAC-based Port Security, <u>Port-based Access Control with 802.1X</u> , Guest/unauthenticated VLAN, RADIUS VLAN Assignment, Multi-Client Authentication per Port, <u>MAC Authentication Bypass</u> , Access to Management restricted by VLAN, HTTPS Certificate Management, Restricted Management Access, Appropriate Use Banner, SNMP Logging, Local User Management, Remote Authentication via RADIUS

(E.g., <https://www.belden.com/products/industrial-networking-cybersecurity/software-solutions/device-software/classic-switch-software/classic-switch-software-9-0-mach102-l2p>).

2.6 802.1X Port Authentication

The 802.1X Port Authentication provides you with the following dialogs:

- ▶ “802.1X Global Configuration”
- ▶ “802.1X Port Configuration”
- ▶ “802.1X Port Clients”
- ▶ “802.1X Port Statistics”

The port-based network access control is a method described in norm IEEE 802.1X to protect IEEE 802 networks from unauthorized access. The protocol controls the access on a port by authenticating and authorizing a terminal device that is connected to this port of the device.

The 802.1X Port Authentication function requires that you configure a RADIUS Server for authentication and authorization. The authentication and authorization are carried out by the authenticator, in this case the device. The device authenticates the supplicant (the querying device, e.g. a PC), which means that it permits the access to the services it provides (e.g. access to the network to which the device is connected), or else refuses it. In the process, the device accesses an external authentication server (RADIUS server), which checks the authentication data of the supplicant. The device exchanges the authentication data with the supplicant via the Extensible Authentication Protocol over LANs (EAPOL), and with the RADIUS server via the RADIUS protocol.

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

Parameter	Meanings	Possible values	Default setting
Port Control	Setting for the port access control.	► ForceAuthorized: Access is also available for all clients without authentication. ► ForceUnauthorized: Access is blocked for all clients, even for clients with authentication. ► auto: Access to the port depends on the result of the authentication. ► macBased: Behavior like for auto. Access is also available for clients with a MAC address which the client uses in the course of authentication.	ForceAuthorized
Note: ► In the ForceAuthorized, ForceUnauthorized and auto modes the Switch opens or blocks the port for all clients. Use these modes if you are connecting a single client to the Switch. ► In the macBased mode the Switch <u>authenticates the clients based on the individual MAC addresses and allows or blocks their data traffic separately.</u> Use this mode if you want to use multi-client authentication or the "MAC Authentication Bypass" function.			

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

<u>Guest VLAN ID</u>	<u>ID of a VLAN that the Switch assigns to the port, if:</u>	0 - 4094	0
-	▶ <u>the 802.1X protocol is active on the port and the port control is set to <i>auto</i> or <i>macBased</i>,</u> ▶ <u>a client wants to receive data traffic and EAPOL frames from the client fail to appear, i.e. the client does not support the 802.1X protocol.</u> The Switch: ▶ switches the port to the authenticated state, ▶ allows data traffic, ▶ but only to the guest VLAN. Specify a guest VLAN ID if you want to allow devices without 802.1X support access to a guest VLAN. Note: ▶ Use only as a guest VLAN a VLAN that you have set up statically in the Switch. ▶ However, if a client connects via 802.1X and his authentication fails, then the Switch only gives him access to the <u>unauthenticated VLAN.</u> ▶ When you activate the MAC Authorized Bypass (MAB) function, the device automatically sets the guest VLAN ID to 0.	With a VLAN ID of 0, the Switch blocks the data traffic because it denies a VLAN setup with this ID.	

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

Parameter	Meaning	Possible values	Default setting
MAC Authorized Bypass Enable	<u>The Switch makes authenticated access available via MAB, if:</u> ▶ <u>You have set the "Port Control" to macBased,</u> ▶ <u>a device wants to receive data traffic employing a particular known MAC address,</u> ▶ <u>this device does not authenticate itself via 802.1X and</u> ▶ <u>the RADIUS server recognizes the MAC addresses authorized to access.</u> <u>The Switch:</u> ▶ <u>waits for the guest VLAN interval to elapse in order to do this,</u> ▶ <u>then sends a query to the RADIUS server and in doing so uses the MAC address as the user name and the password.</u> <u>Activate this function, if:</u> ▶ <u>you want to allow particular devices normal access,</u> ▶ <u>however these devices do not support 802.1X.</u>	On Off	Off
Guest VLAN Period	<u>Time that the Switch waits for EAPOL frames after connecting a device on this port in order to determine whether it supports the 802.1X protocol.</u> <u>If this time elapses, the Switch only provides access to the guest VLAN for the device connected.</u>	1 - 300 s	90 s

(E.g., https://www.doc.hirschmann.com/pdf/ManualCollection_Classic_L2P_09000_en.pdf).

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.

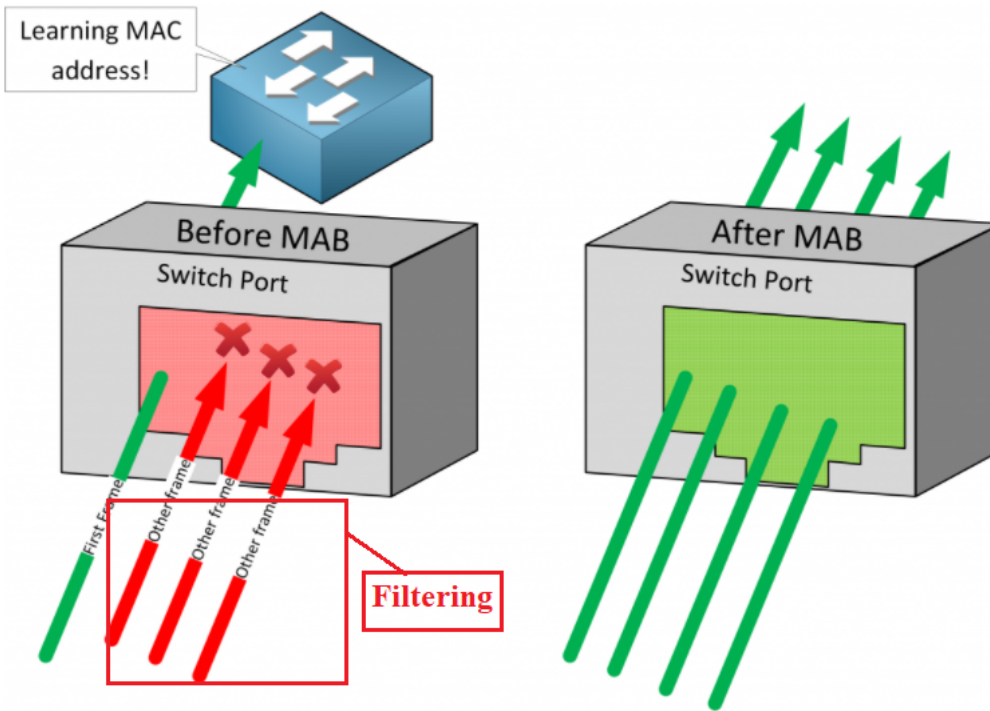
-> By default Switch sends EAP request identity messages every 30 seconds to the endpoint, if the switch does not receive the response for three EAP request identity messages (90 seconds) then it assumes the host is not having 802.1x supplicant and begins MAB process.

-> 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 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#:~:text=Once%20the%20switch%20has%20learned,you%20can%20with%20802.1X.\).](https://networklessons.com/cisco/ccie-routing-switching-written/mac-authentication-bypass-mab#:~:text=Once%20the%20switch%20has%20learned,you%20can%20with%20802.1X.).)

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.

August 31, 2022

LOAKNAUTH LAW, P.C.

OF COUNSEL:

David R. Bennett
(*pro hac vice* to be filed)
Direction IP Law
P.O. Box 14184
Chicago, IL 60614-0184
(312) 291-1667
dbennett@directionip.com

/s/ Nicholas Loaknauth
Nicholas Loaknauth
Loaknauth Law, P.C.
1460 Broadway
New York, NY 10036
(212) 641-0745
nick@loaknauthlaw.com

Attorneys for Plaintiff Tranquility IP LLC