

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

TRANQUILITY IP LLC,

Plaintiff,

v.

KONTRON AMERICA, INCORPORATED,

Defendants.

CASE NO.

PATENT CASE

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Tranquility IP LLC files this Original Complaint for Patent Infringement against Kontron America, Incorporated, 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 Kontron America, Incorporated, (“Defendant”) is a corporation organized and existing under the laws of Delaware. Defendant has a registered agent at The Corporation Trust Company, Corporation Trust Center, 1209 Orange St, Wilmington, DE 19801.

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 Delaware Long-Arm Statute, due at least to

its business in this forum, including at least a portion of the infringements alleged herein. Furthermore, Defendant is subject to this Court's specific and general personal jurisdiction because Defendant is a Delaware corporation.

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 Delaware. 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 Delaware. 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 Delaware. Defendant has committed such purposeful acts and/or transactions in Delaware 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 is incorporated in Delaware. Under the patent venue analysis, Defendant resides only in this District. 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).

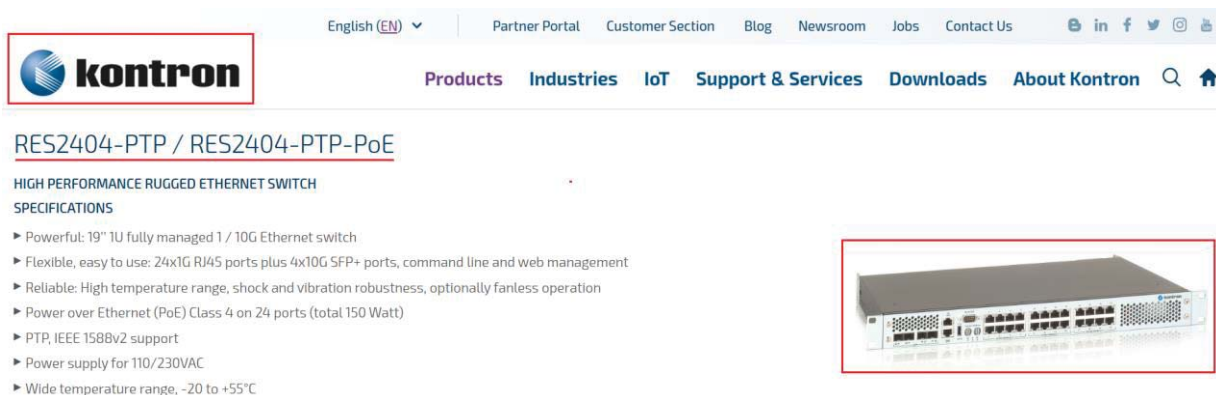
12. The context of the patented invention in the ‘037 Patent is wireless local area networks (“WLAN”) employing the IEEE 802.1X architecture with an access point that provides access for mobile devices to other networks, such as hardwired local area and global networks such as the Internet. (*Id.* at 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 Delaware, 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 Kontron Rugged Ethernet Switch (“Accused Instrumentality”) (e.g., <https://www.kontron.com/en/products/res2404-ptp-res2404-ptp-poe/p148574>).

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.



English (EN) Partner Portal Customer Section Blog Newsroom Jobs Contact Us


kontron Products Industries IoT Support & Services Downloads About Kontron

RES2404-PTP / RES2404-PTP-PoE

HIGH PERFORMANCE RUGGED ETHERNET SWITCH

SPECIFICATIONS

- ▶ Powerful: 19" 1U fully managed 1 / 10G Ethernet switch
- ▶ Flexible, easy to use: 24x1G RJ45 ports plus 4x10G SFP+ ports, command line and web management
- ▶ Reliable: High temperature range, shock and vibration robustness, optionally fanless operation
- ▶ Power over Ethernet (PoE) Class 4 on 24 ports (total 150 Watt)
- ▶ PTP, IEEE 1588v2 support
- ▶ Power supply for 110/230VAC
- ▶ Wide temperature range, -20 to +55°C



(E.g., <https://www.kontron.com/en/products/res2404-ptp-res2404-ptp-poe/p148574>).

Ethernet/Bridging	Link aggregation (IEEE 802.3ad)
	Classic and rapid spanning tree algorithms(IEEE 802.1D, IEEE 802.1w)
	Multiple Spanning Tree (IEEE 802.5)
	Quality Of Service on all ports (IEEE 802.1p)
	Full Duplex operation and flow control on all ports (IEEE 802.3x)
	Static MAC filtering
	Port Authentication (IEEE 802.1X)
	Auto negotiation of speeds and operational mode on all external copper GE interfaces as well as on all base fabric interfaces

A maximum of five Accounting Method lists can be created for each exec and commands type.

Only the default Accounting Method list can be created for DOT1X. There is no provision to create more.

The same list-name can be used for both exec and commands accounting type

AAA Accounting for commands with RADIUS as the accounting method is not supported.

Start-stop or None are the only supported record types for DOT1X accounting. Start-stop enables accounting and None disables accounting.

RADIUS is the only accounting method type supported for DOT1X accounting.

4.15.13 **dot1x mac-auth-bypass**

If the 802.1X mode on the interface is mac-based, you can optionally use this command to enable MAC Authentication Bypass (MAB) on an interface. MAB is a supplemental authentication mechanism that allows 802.1X unaware clients – such as printers, fax machines, and some IP phones – to authenticate to the network using the client MAC address as an identifier.

Default	disabled
Format	dot1x mac-auth-bypass
Mode	Interface Config

4.15.22 authentication order

This command sets the order of authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method is unsuccessful or timed out, the next method is attempted.

Each method can only be entered once. Ordering is only possible between 802.1x and MAB. Captive portal can be configured either as a stand-alone method or as the last method in the order.

Format	authentication order {dot1x [mab [captive-portal] captive-portal] mab [dot1x [captive-portal] captive-portal] captive-portal}
Mode	Interface Config

(E.g., [https://www.kontron.com/download/download?filename=/downloads/manuals/res-esc-
ptp/res-ptp-poe-cli-reference-manual-v1.0.pdf&product=148574](https://www.kontron.com/download/download?filename=/downloads/manuals/res-esc-
ptp/res-ptp-poe-cli-reference-manual-v1.0.pdf&product=148574)).

<u>Dot1x Statistics</u>	<ul style="list-style-type: none">• <u>EAPOL Frames Transmitted - The number of EAPOL frames of any type that have been transmitted by this authenticator.</u>• <u>EAPOL Start Frames Received - The number of valid EAPOL start frames that have been received by this authenticator.</u>
--------------------------------	---

(E.g., <https://www.kontron.com/download/download?filename=/downloads/manuals/res-esc-ntp/res-ntp-poe-cli-reference-manual-v1.0.pdf&product=148574>),

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.

(Id.).

16. Upon information and belief, the Accused Instrumentality discloses an access point (e.g., 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 Address Bypass or MAB) compatible with the user terminal.

Ethernet/Bridging	Link aggregation (IEEE 802.3ad)
	Classic and rapid spanning tree algorithms(IEEE 802.1D, IEEE 802.1w)
	Multiple Spanning Tree (IEEE 802.5)
	Quality Of Service on all ports (IEEE 802.1p)
	Full Duplex operation and flow control on all ports (IEEE 802.3x)
	Static MAC filtering
	Port Authentication (IEEE 802.1X)
	Auto negotiation of speeds and operational mode on all external copper GE interfaces as well as on all base fabric interfaces

A maximum of five Accounting Method lists can be created for each exec and commands type.

Only the default Accounting Method list can be created for DOT1X. There is no provision to create more.

The same list-name can be used for both exec and commands accounting type

AAA Accounting for commands with RADIUS as the accounting method is not supported.

Start-stop or None are the only supported record types for DOT1X accounting. Start-stop enables accounting and None disables accounting.

RADIUS is the only accounting method type supported for DOT1X accounting.

4.15.13 **dot1x mac-auth-bypass**

If the 802.1X mode on the interface is mac-based, you can optionally use this command to enable MAC Authentication Bypass (MAB) on an interface. MAB is a supplemental authentication mechanism that allows 802.1X unaware clients – such as printers, fax machines, and some IP phones – to authenticate to the network using the client MAC address as an identifier.

Default	disabled
Format	dot1x mac-auth-bypass
Mode	Interface Config

4.15.22 authentication order

This command sets the order of authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method is unsuccessful or timed out, the next method is attempted.

Each method can only be entered once. Ordering is only possible between 802.1x and MAB. Captive portal can be configured either as a stand-alone method or as the last method in the order.

Format	authentication order {dot1x [mab [captive-portal] captive-portal] mab [dot1x [captive-portal] captive-portal] captive-portal}
Mode	Interface Config

(E.g., https://www.kontron.com/download/download?filename=/downloads/manuals/u/userguide_res2404-ptp-poe_rev1.1_2020-08-18.pdf&product=148574).

Dot1x Statistics	<ul style="list-style-type: none"> • <u>EAPOL Frames Transmitted - The number of EAPOL frames of any type that have been transmitted by this authenticator.</u> • <u>EAPOL Start Frames Received - The number of valid EAPOL start frames that have been received by this authenticator.</u>
-------------------------	--

(E.g., https://www.kontron.com/download/download?filename=/downloads/manuals/u/userguide_res2404-ptp-poe_rev1.1_2020-08-18.pdf&product=148574).

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 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.

Ethernet/Bridging	Link aggregation (IEEE 802.3ad)
	Classic and rapid spanning tree algorithms(IEEE 802.1D, IEEE 802.1w)
	Multiple Spanning Tree (IEEE 802.5)
	Quality Of Service on all ports (IEEE 802.1p)
	Full Duplex operation and flow control on all ports (IEEE 802.3x)
	Static MAC filtering
	Port Authentication (IEEE 802.1X)
	Auto negotiation of speeds and operational mode on all external copper GE interfaces as well as on all base fabric interfaces

(E.g., https://www.kontron.com/download/download?filename=/downloads/manuals/u/userguide_res2404-ptp-poe_rev1.1_2020-08-18.pdf&product=148574).

A maximum of five Accounting Method lists can be created for each exec and commands type.

Only the default Accounting Method list can be created for DOT1X. There is no provision to create more.

The same list-name can be used for both exec and commands accounting type

AAA Accounting for commands with RADIUS as the accounting method is not supported.

Start-stop or None are the only supported record types for DOT1X accounting. Start-stop enables accounting and None disables accounting.

RADIUS is the only accounting method type supported for DOT1X accounting.

4.15.13 dot1x mac-auth-bypass

If the 802.1X mode on the interface is mac-based, you can optionally use this command to enable MAC Authentication Bypass (MAB) on an interface. MAB is a supplemental authentication mechanism that allows 802.1X unaware clients – such as printers, fax machines, and some IP phones – to authenticate to the network using the client MAC address as an identifier.

Default disabled
Format dot1x mac-auth-bypass
Mode Interface Config

4.15.22 authentication order

This command sets the order of authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method is unsuccessful or timed out, the next method is attempted.

Each method can only be entered once. Ordering is only possible between 802.1x and MAB. Captive portal can be configured either as a stand-alone method or as the last method in the order.

Format authentication order {dot1x [mab [captive-portal] | captive-portal] | mab [dot1x [captive-portal] | captive-portal] | captive-portal}

Mode Interface Config

Dot1x Statistics

- EAPOL Frames Transmitted - The number of EAPOL frames of any type that have been transmitted by this authenticator.
- EAPOL Start Frames Received - The number of valid EAPOL start frames that have been received by this authenticator.

(E.g., https://www.kontron.com/download/download?filename=/downloads/manuals/u/userguide_res2404-ptp-poe_rev1.1_2020-08-18.pdf&product=148574).

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.

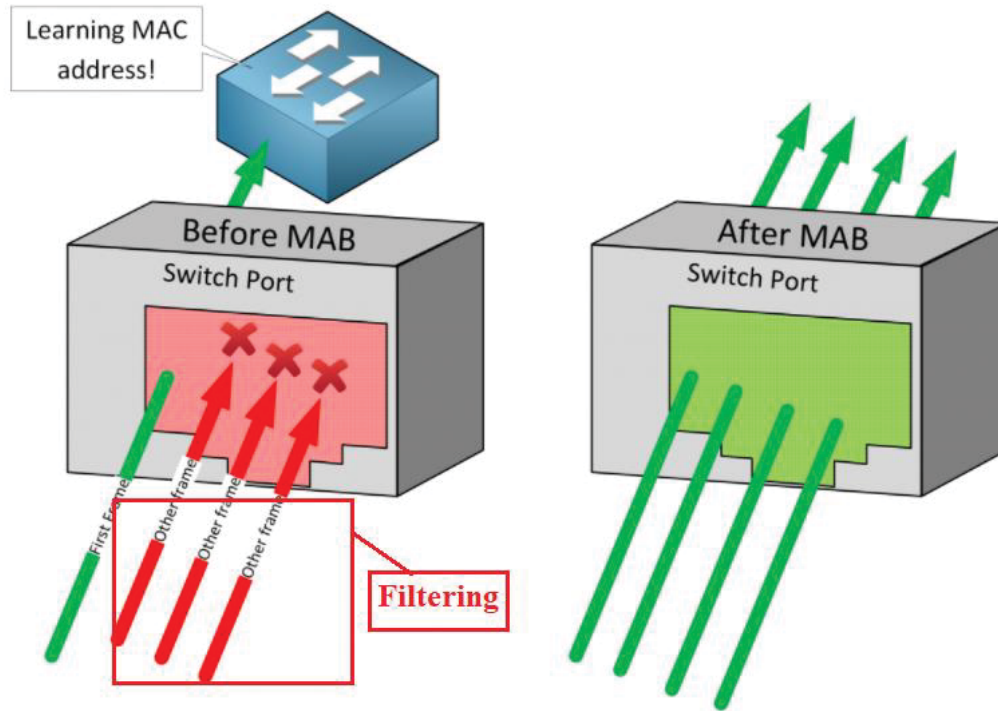
(e.g., <https://www.kareemccie.com/2017/01/mac-authentication-bypass.html>).

18. Upon information and belief, the Accused Instrumentality is used in a method performing the 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://networklessons.com/cisco/ccie-routing-switching-written/mac-authentication-bypass-mab>).

Ethernet/Bridging	Link aggregation (IEEE 802.3ad)
	Classic and rapid spanning tree algorithms(IEEE 802.1D, IEEE 802.1w)
	Multiple Spanning Tree (IEEE 802.5)
	Quality Of Service on all ports (IEEE 802.1p)
	Full Duplex operation and flow control on all ports (IEEE 802.3x)
	Static MAC filtering
	Port Authentication (IEEE 802.1X)
	Auto negotiation of speeds and operational mode on all external copper GE interfaces as well as on all base fabric interfaces

(E.g., https://www.kontron.com/download/download?filename=/downloads/manuals/u/userguide_res2404-ptp-poe_rev1.1_2020-08-18.pdf&product=148574).

A maximum of five Accounting Method lists can be created for each exec and commands type.

Only the default Accounting Method list can be created for DOT1X. There is no provision to create more.

The same list-name can be used for both exec and commands accounting type

AAA Accounting for commands with RADIUS as the accounting method is not supported.

Start-stop or None are the only supported record types for DOT1X accounting. Start-stop enables accounting and None disables accounting.

RADIUS is the only accounting method type supported for DOT1X accounting.

4.15.13 dot1x mac-auth-bypass

If the 802.1X mode on the interface is mac-based, you can optionally use this command to enable MAC Authentication Bypass (MAB) on an interface. MAB is a supplemental authentication mechanism that allows 802.1X unaware clients – such as printers, fax machines, and some IP phones – to authenticate to the network using the client MAC address as an identifier.

Default	disabled
Format	dot1x mac-auth-bypass
Mode	Interface Config

4.15.22 authentication order

This command sets the order of authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method is unsuccessful or timed out, the next method is attempted.

Each method can only be entered once. Ordering is only possible between 802.1x and MAB. Captive portal can be configured either as a stand-alone method or as the last method in the order.

Format	authentication order {dot1x [mab [captive-portal] captive-portal] mab [dot1x [captive-portal] captive-portal] captive-portal}
Mode	Interface Config

Dot1x Statistics	<ul style="list-style-type: none"> <u>EAPOL Frames Transmitted - The number of EAPOL frames of any type that have been transmitted by this authenticator.</u> <u>EAPOL Start Frames Received - The number of valid EAPOL start frames that have been received by this authenticator.</u>
-------------------------	--

(E.g., https://www.kontron.com/download/download?filename=/downloads/manuals/u/userguide_res2404-ptp-poe_rev1.1_2020-08-18.pdf&product=148574).

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 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.

A maximum of five Accounting Method lists can be created for each exec and commands type.

Only the default Accounting Method list can be created for DOT1X. There is no provision to create more.

The same list-name can be used for both exec and commands accounting type

AAA Accounting for commands with RADIUS as the accounting method is not supported.

Start-stop or None are the only supported record types for DOT1X accounting. Start-stop enables accounting and None disables accounting.

RADIUS is the only accounting method type supported for DOT1X accounting.

(E.g., https://www.kontron.com/download/download?filename=/downloads/manuals/u/userguide_res2404-ptp-poe_rev1.1_2020-08-18.pdf&product=148574).

4.15.13 **dot1x mac-auth-bypass**

If the 802.1X mode on the interface is mac-based, you can optionally use this command to enable MAC Authentication Bypass (MAB) on an interface. MAB is a supplemental authentication mechanism that allows 802.1X unaware clients – such as printers, fax machines, and some IP phones – to authenticate to the network using the client MAC address as an identifier.

Default	disabled
Format	dot1x mac-auth-bypass
Mode	Interface Config

4.15.22 authentication order

This command sets the order of authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method is unsuccessful or timed out, the next method is attempted.

Each method can only be entered once. Ordering is only possible between 802.1x and MAB. Captive portal can be configured either as a stand-alone method or as the last method in the order.

Format	authentication order {dot1x [mab [captive-portal] captive-portal] mab [dot1x [captive-portal] captive-portal] captive-portal}
Mode	Interface Config

Dot1x Statistics	<ul style="list-style-type: none"> • <u>EAPOL Frames Transmitted - The number of EAPOL frames of any type that have been transmitted by this authenticator.</u> • <u>EAPOL Start Frames Received - The number of valid EAPOL start frames that have been received by this authenticator.</u>
-------------------------	--

(E.g., https://www.kontron.com/download/download?filename=/downloads/manuals/u/userguide_res2404-ptp-poe_rev1.1_2020-08-18.pdf&product=148574).

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.

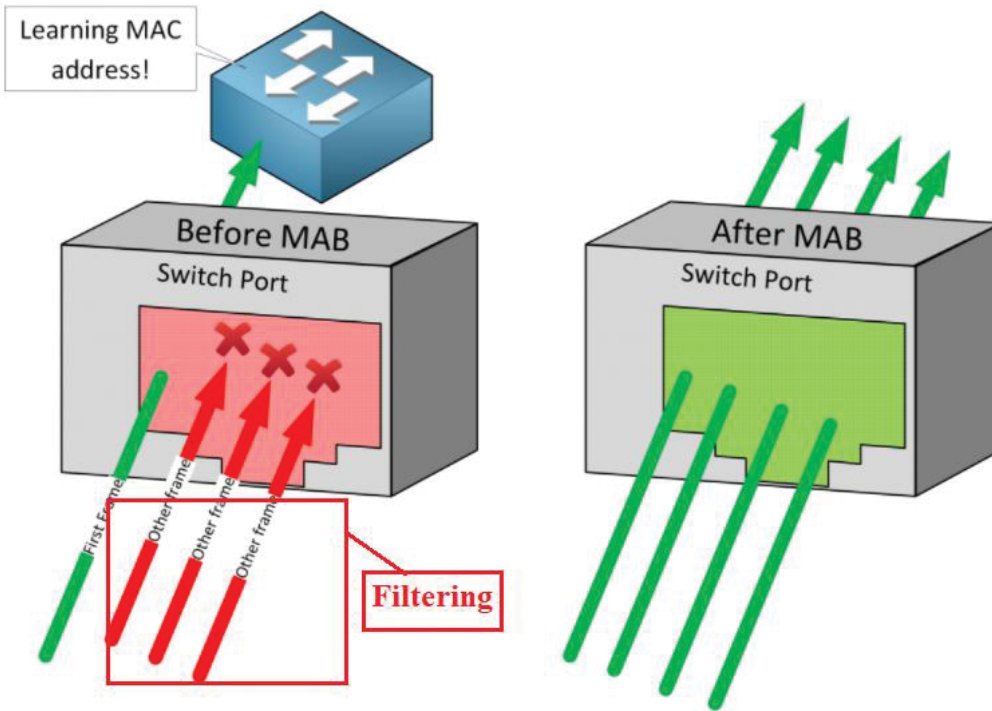
-> By default Switch sends EAP request identity messages every 30 seconds to the endpoint, if the switch does not receive the response for three EAP request identity messages (90 seconds) then it assumes the host is not having 802.1x supplicant and begins MAB process.

-> 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>).

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.

Dated: September 30, 2022

Respectfully submitted,

OF COUNSEL:

David R. Bennett

DIRECTION IP LAW

PO Box 14184

Chicago IL 60614-0184

Tel: (312) 291-1667

dbennett@directionip.com

By: /s/ David W. deBruin

David W. deBruin (DE # 4846)

NAPOLI SHKOLNIK LLC

919 North Market Street

Suite 1801

Wilmington DE 19801-3033

Tel: (302) 330-8025

DdeBruin@NapoliLaw.com

Attorneys for Plaintiff

Tranquility IP LLC