Flexible Authentication Order, Priority, and Failed Authentication

Introduction

Flexible authentication (FlexAuth) is a set of features that allows IT administrators to configure the sequence and priority of IEEE 802.1X, MAC authentication bypass (MAB), and switch-based web authentication (local WebAuth). Before changing the default order and priority of these authentication methods, however, you should understand the potential consequences of those changes.

By default, a Cisco® switch always attempts IEEE 802.1X authentication before MAB. With FlexAuth, you can change the order so that MAB is attempted before IEEE 802.1X authentication. The first consequence of changing the default order is that all endpoints, including endpoints that can perform IEEE 802.1X authentication, will be subject to MAB, which may result in significant additional authentication traffic on the network.

Changing the default order of authentication also affects other FlexAuth features. The rest of this document discusses the potential effects on the following features: authentication priority, authentication failure handling, and WebAuth. Table 1 summarizes the commands that will be discussed.

Table 1. FlexAuth Feature Quick Reference

FlexAuth Commands	Purpose
switch(config-if)# authentication order [dot1x | mab] | {webauth}	(Optional) Sets the order of authentication methods used on a port
switch(config-if)# authentication priority [dot1x | mab] | {webauth}	(Optional) Sets the priority of the authentication methods
Fallback Authentication Methods	**Purpose**
switch(config-if)# authentication event fail action [next-method | authorize vlan VLAN]	(Optional) Specifies the behavior when authentication fails: either the next configured authentication method is attempted or the port is authorized for the specified VLAN

The features discussed in this document are supported in the Cisco IOS® Software releases listed in Table 2.

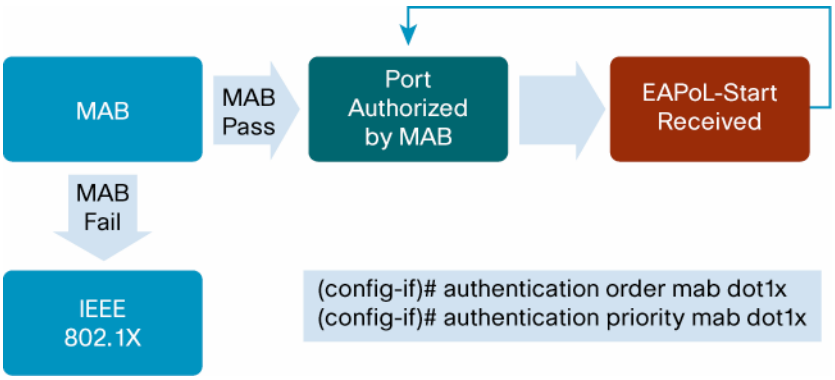
Table 2. Table 2 Supported Platforms and Cisco IOS Software Releases

Cisco Catalyst® Platforms	Cisco IOS Software Release
Cisco Catalyst 6500 Series Switches	Cisco IOS Software Release 12.2(33)SXI
Cisco Catalyst 4500 Series Switches	Cisco IOS Software Release 12.2(50)SG
Cisco Catalyst 3750, 3560, and 2960 Series Switches.	Cisco IOS Software Release 12.2(50)SE

Case 1: Order MAB Dot1x with Default Priority

Currently, by default, the priority changes when the order is changed. If MAB is configured as the first authentication method, then MAB will have priority over all other authentication methods. Therefore, if the port is configured to attempt MAB before IEEE 802.1X authentication, then, by default, any device that passes MAB will never be allowed to pass IEEE 802.1X authentication. Figure 1 summarizes the behavior when the order (and consequently, the priority) is changed.

Figure 1. Order MAB Dot1x, Priority MAB Dot1x

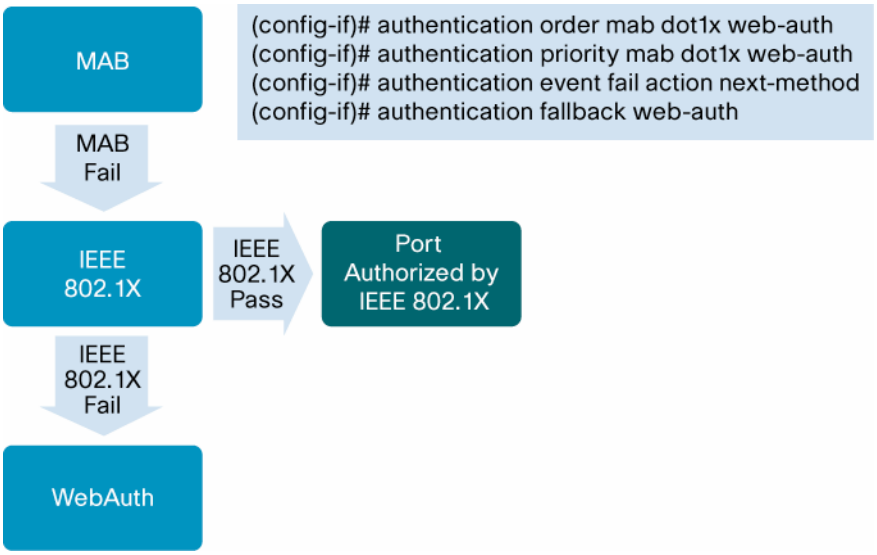


As Figure 1 illustrates, if an endpoint needs to perform IEEE 802.1X authentication, then it must fail MAB. Consequently, its MAC address must not be in the databases that are checked for MAB. In addition, the authentication, authorization, and accounting (AAA) server should not have a policy that allows unknown MAC addresses to pass MAB (for example, for a dynamic guest VLAN assignment).

Another use case that must be addressed is what happens when IEEE 802.1X fails. You can configure either of two mutually exclusive options for IEEE 802.1X failure handling on the switch: continue to the next authentication method (next-method) or authorize for a specific VLAN (the authorization failure [auth-fail] VLAN). The deployment requirements for each of these options are discussed here.

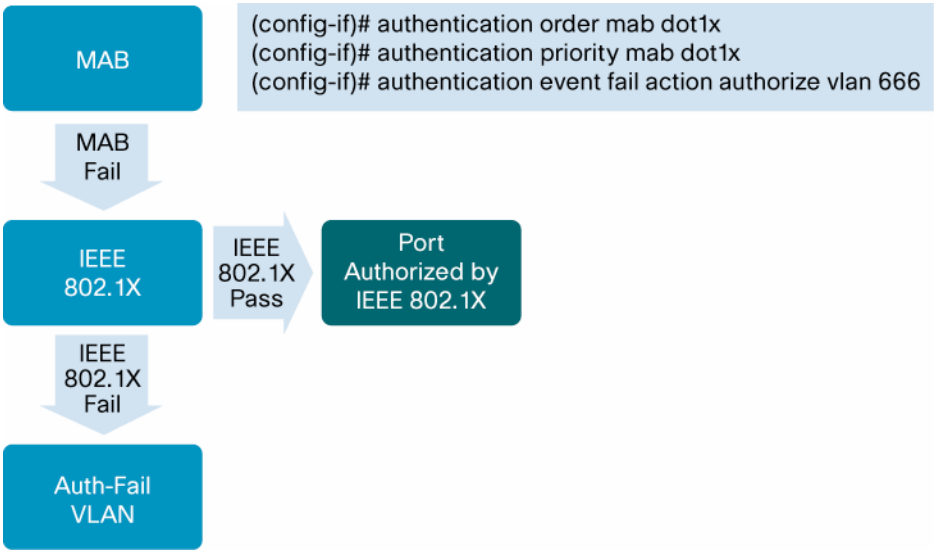
If next-method is configured and a third authentication method (for example, WebAuth) is not enabled, then the switch will return to the first method (MAB). MAB will fail again, IEEE 802.1X authentication will fail again, and the device will never get any kind of access. This limitation means that MAB cannot be used to remediate known devices that fail IEEE 802.1X authentication (for example, an employee PC with an expired certificate). Therefore, for IEEE 802.1X authentication failures, use next-method only if WebAuth is configured on the switch. Figure 2 summarizes the configuration and behavior when next-method is used to handle IEEE 802.1X authentication failures.

Figure 2. IEEE 802.1X Failure Handling Option 1: Next-Method WebAuth



The other option for the IEEE 802.1X authentication failure use case is to put devices that fail IEEE 802.1X authentication in the auth-fail VLAN. Figure 3 shows the authentication flow for this configuration.

Figure 3. IEEE 802.1X Failure Handling Option 2: Auth-Fail VLAN



Be aware that the only way to get out of the auth-fail VLAN is reauthentication initiated from the switch, through an Extensible Authentication Protocol over LAN Logoff (EAPoL-Logoff) command from the supplicant, or through a link down or up event. Note that if you do perform reauthentication, reauthentication always returns to the first method (MAB).[1]

In summary, there are three points to remember if MAB precedes IEEE 802.1X authentication in both order and priority:

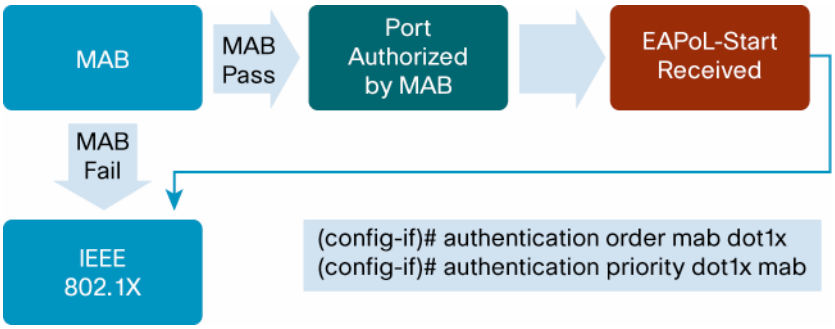
- Make sure that all devices that perform IEEE 802.1X authentication are *not* in your MAC address database and that your policy never returns an access-accept event for unknown MAC addresses. IEEE 802.1X devices must fail MAB if they are to perform IEEE 802.1X authentication. As a consequence, many MAB failure records will be generated in the course of normal operation.
- Use next-method for IEEE 802.1X failure handing only if local WebAuth is configured.
- If the next method is not local WebAuth, the only option for granting access after IEEE 802.1X authentication failure is the auth-fail VLAN.

Case 2: Order MAB Dot1x and Priority Dot1x MAB

If you change the order so that MAB comes before IEEE 802.1X authentication and change the default priority so that IEEE 802.1X authentication precedes MAB, then every device in the network will still be subject to MAB, but devices that pass MAB can subsequently go through IEEE 802.1X authentication. This approach enables a scenario in which devices can get partial access (to get an IP address, begin a PXE boot, etc.) after successful MAB, and then get full access after successful IEEE 802.1X authentication. In this case, you can have IEEE 802.1X devices in your MAB database. Figure 4 illustrates this behavior.

[1] Some platforms may support the Cisco AVPair attribute termination-action-modifier=1, which instructs the switch to retry only the last authentication method.

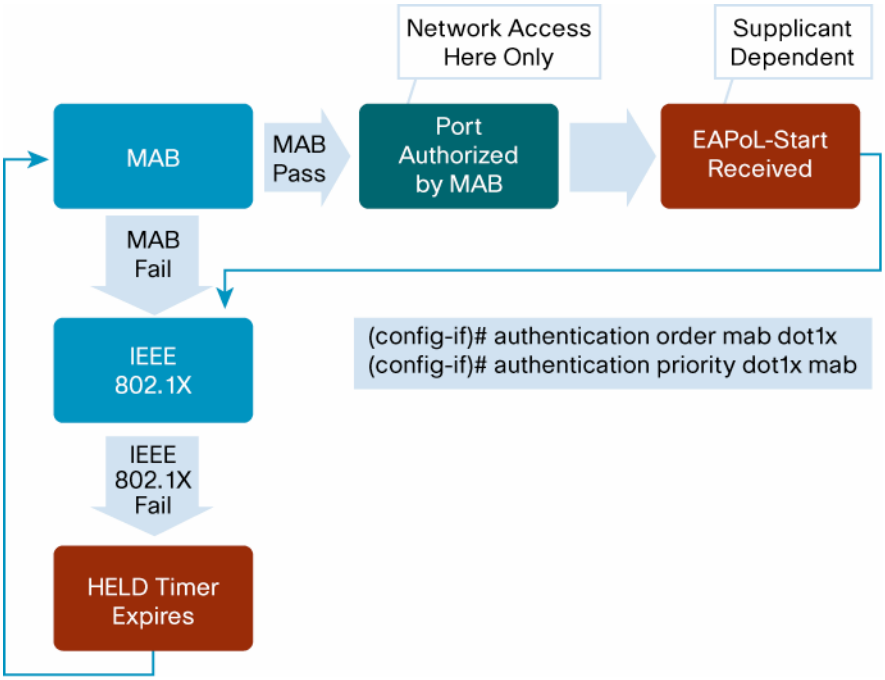
Figure 4. Order MAB Dot1x, Priority Dot1x MAB



Special consideration must be paid to what happens if a device fails IEEE 802.1X authentication after successful MAB. First, the device will have temporary network access between the time MAB succeeds and IEEE 802.1X authentication fails. What happens next depends on the configured event-fail behavior.

If next-method is configured and a third authentication method (such as WebAuth) is not enabled, then the switch will return to the first method (MAB) after the held period. MAB will succeed, and the device will again have temporary access until and unless the supplicant tries to authenticate again. This behavior is supplicant dependent. Some supplicants will give up on IEEE 802.1X authentication after some number of failures, and some may continue forever. If the supplicant stops attempting IEEE 802.1X authentication altogether, then the device will eventually end up with MAB-authorized access. If the supplicant continues to attempt IEEE 802.1X authentication, then the device will have intermittent access as it cycles between successful MAB and failed IEEE 802.1X authentication (Figure 5).

Figure 5. Intermittent Access Loop



To avoid this potential loop, you need to specify an authentication failure behavior. As before, the two options are next-method with local WebAuth and the auth-fail VLAN.

If next-method failure handling and local WebAuth are both configured and if the supplicant retries IEEE 802.1X authentication during or after WebAuth, then IEEE 802.1X authentication will not start again, regardless of the status

of WebAuth. This behavior occurs because after IEEE 802.1X authentication fails, local WebAuth ignores EAPoL-Start commands from the supplicant.

If the auth-fail VLAN is configured, endpoints that fail IEEE 802.1X authentication after successful MAB will be placed in the auth-fail VLAN, and no other methods will be attempted. Since EAPoL-Start commands are ignored in the auth-fail VLAN, the supplicant's behavior will not change the authorization state of the port. Again, the only way to get out of the auth-fail VLAN is reauthentication from the switch, through an EAPoL-Logoff command from the supplicant, or through a link down or up event.

In summary, three points to remember if MAB precedes IEEE 802.1X authentication in order but IEEE 802.1X authentication has priority:

- IEEE 802.1X–capable endpoints can be in the MAC address database.
- Using next-method for IEEE 802.1X authentication failure handling without local WebAuth can lead to unpredictable behavior and intermittent network access (as described earlier, with MAB cycling to IEEE 802.1X authentication failure).
- For deterministic behavior upon IEEE 802.1X authentication failure after successful MAB, use the auth-fail VLAN or local WebAuth.

Conclusion

Changing the default order of authentication affects the behavior of the system in multiple ways. Before making this change, be sure to address the concerns described in Table 3.

Table 3. Points to Consider

Effect	Resolution
All devices will be subject to MAB	Plan for increased control-plane traffic.
Authentication priority affects MAB	If MAB has priority, IEEE 802.1X–capable devices must fail MAB. If IEEE 802.1X authentication has priority, IEEE 802.1X–capable devices may pass or fail MAB.
MAB cannot be used as a next method for IEEE 802.1X authentication failures	Use next-method with WebAuth or the auth-fail VLAN.

For More Information

http://www.cisco.com/go/ibns

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C27-573287-00 12/09