Contents

Introduction

This document describes the procedure to troubleshoot authentications on switches which use Identity-Based Networking Services (IBNS)

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Service Engine (ISE)
- IEEE 802.1X concepts (dot1X)
- MAC Authentication Bypass (MAB)

Components Used

The information in this document is based on these software and hardware versions but not lmited to:

- Cisco Switch - C3750X-48PF-S with IOS 15.2.1E3(ED)
- Identity Service Engine 2.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

IBNS 2.0 is a new policy engine which replaces the traditional auth-manager. It is equipped with a set of enhanced capabilities which offer flexible configuration with the Cisco Common

Classification Policy Language (C3PL). Now called the Access Session Manager, IBNS 2.0 gives administrators options to configure policies and actions based on specific conditions and endpoint events. Instead of regular conditions, C3PL is used to define the authentication conditions, parameters and the actions. For more information on IBNS 2.0, follow the link given in the Related Information section.

There are different types of policy maps that are used for various purposes. This paragraph focuses on subscriber type. There are three sections in a policy map to be noted.

- Event section
- Class section
- Action section

They follow the hierarchy **Event > Class > Action.** When a policy map is applied to an interface, all events defined in the policy map are evaluated. Based upon the current event, the appropriate action defined in the policy map is applied at the interface level.

Once the event is matched, there is an option to evaluate the classes based on the event/method/result of the authentication/authorization. The results of these classes can be **ALWAYS EXECUTE** or called in additional class maps.

In the action section, the important actions that can be included are:

- Specify an authentication method with a priority
- Specify an authentication method list for a particular authentication method
- Specify an authorization method list for an authentication method
- Specify number of retries
- Replace the existing authntication/authorization data with new authentication/authorization data
- Force Authorization
- Force Unauthorization
- Activate a service template

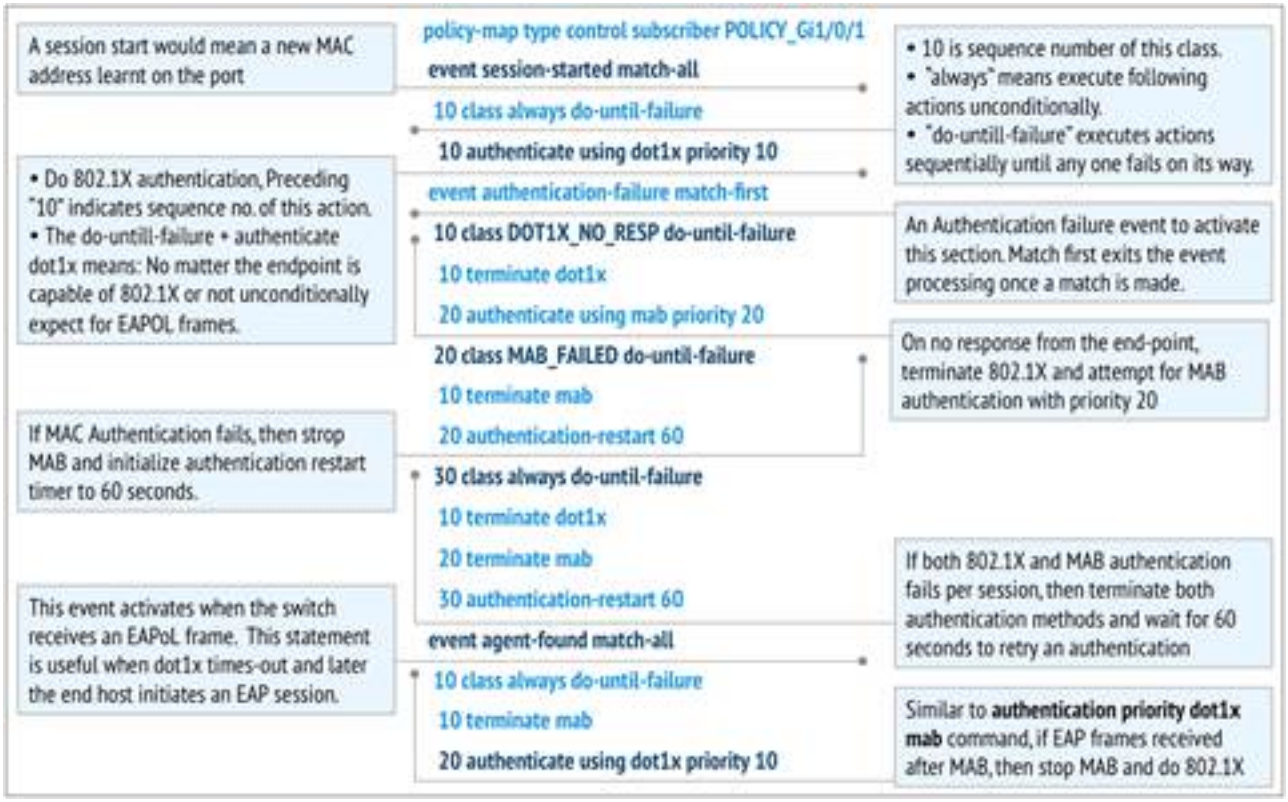
In the traditional IOS Switches, there was no option to apply a method list specific to a authenticated session. IBNS 2.0 provides this capability using a service-templates. The service template is configured locally on the switch and applied post successful session authorization. There is also an option to push the required service template from a AAA server.

The radius attribute that is used to do the same is *subscriber:service-name = <name of the service template>.* In Identity Serice Engine (ISE), you can name the authorization profile exactly the same as of the local service-template configured on the switch and check the *Service Template* check box. This authorization profile along with any other authorization profile can be pushed as an authorization result.

In the authorization result report, there is a Cisco-AV-Pair named *subscriber:service-name* =

<name of the service template> . This indiacates that the swich has been notified to apply that service template for that session.

Here is a picture which shows the exact meaning of every entity of a sample policy map.



Configure

AAA configuration

RADIUS server configuration

Policy map configuration

Class maps configuration

Interface configuration

Troubleshoot

The best way to troubleshoot is to compare the working logs and the non-working logs. This way, the exact step at which the process went wrong is known. There are a few debugs which are needed to be enabled to troubleshoot mab/dot1x issues. Here are the commands to enable those debugs.

- debug aaa authentication
- debug aaa authorization
- debug mab all
- debug dot1x all
- debug radius

Here are the working logs with dot1x and mab enabled at the same time.

debug mab all

debug dot1x all

Since dot1x has a lot of message exchanges because of the protocol negotiations, certificate exchanges and so on, not all the debug logs have been mentioned here. The flow of events in the order in which they are supposed to occur and their corresponding debug logs have been documented here.

debug radius

Since there are lot of EAP messages,RADIUS packets sent to the server and received will also be more. Not every dot1x authentication finishes off with on Access-Request. Hence the logs shown here are the ones that are important and as the flow goes.

debug aaa authentication/authorization

debug aaa authentication and debug aaa authorization shows useful information during various authentication/authorization methods. In this case, It is only a single line specifying the method list being used.

This shows if any of the authentication methods are unavailable/not enabled.

The procedure to troubleshoot CWA/Posture/DACLs etc., is the same as that of the traditional IOS switches. Configuration verification is the first step in troubleshooting. Ensure the configuration meets the requirements. If the configuration of the policy map, class map is upto the mark, then debugg problems if any, can be very easy. For further details on configuration using IBNS 2.0, refer the Related Information section.

Related Information

- IBNS 2.0 Deployment Guide