# Contenu



# Introduction

Ce document décrit la procédure pour dépanner des authentifications sur les Commutateurs qui utilisent les services basés sur identité de réseau (IBNS)

# Conditions préalables

## Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Engine de gestion d'identité (ISE)
- Concepts de 802.1X d'IEEE (dot1x)
- Dérivation d'authentification MAC (MAB)

## Composants utilisés

Les informations dans ce document sont basées sur des ces logiciel et versions de matériel mais pas lmited à :

- Cisco commutent - C3750X-48PF-S avec IOS 15.2.1E3(ED)
- Engine 2.1 de gestion d'identité

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

# Informations générales

IBNS 2.0 est une engine de nouvelle stratégie qui remplace l'authentique-gestionnaire traditionnel.

Il est équipé d'un ensemble de capacités améliorées qui offrent la configuration souple avec le langage commun de stratégie de classification de Cisco (C3PL). A maintenant appelé le gestionnaire de session d'Access, IBNS 2.0 donne à des administrateurs des options de configurer des stratégies et des actions basées sur des conditions et des événements spécifiques de point final. Au lieu des conditions régulières, C3PL est utilisé pour définir les conditions d'authentification, des paramètres et les actions. Pour plus d'informations sur IBNS 2.0, suivez le lien donné dans la section Informations connexes.

Il y a différents types de cartes de stratégie qui sont utilisées pour différents buts. Ce paragraphe se concentre sur le type d'abonné. Il y a trois sections dans une carte de stratégie à noter.

- Section d'événement
- Section de classe
- Section d'action

Ils suivent l'**événement > la classe > l'action de** hiérarchie**.** Quand une carte de stratégie est appliquée à une interface, tous les événements définis dans la carte de stratégie sont évalués. Basé sur l'événement actuel, la mesure appropriée définie dans la carte de stratégie est appliquée au niveau d'interface.

Une fois que l'événement est apparié, il y a une option d'évaluer les classes basées sur l'événement/méthode/résultat de l'authentification/d'autorisation. Les résultats de ces classes peuvent être **TOUJOURS EXÉCUTENT** ou ont appelé dans les class map supplémentaires.

Dans la section d'action, les importantes actions qui peuvent être incluses sont :

- Spécifiez une méthode d'authentification avec une priorité
- Spécifiez une liste de méthode d'authentification pour une méthode d'authentification particulière
- Spécifiez une liste d'authorization method pour une méthode d'authentification
- Spécifiez le nombre de relances
- Remplacez les données existantes d'authntication/autorisation par de nouvelles données d'authentification/autorisation
- Autorisation de force
- Force Unauthorization
- Lancez un modèle de service

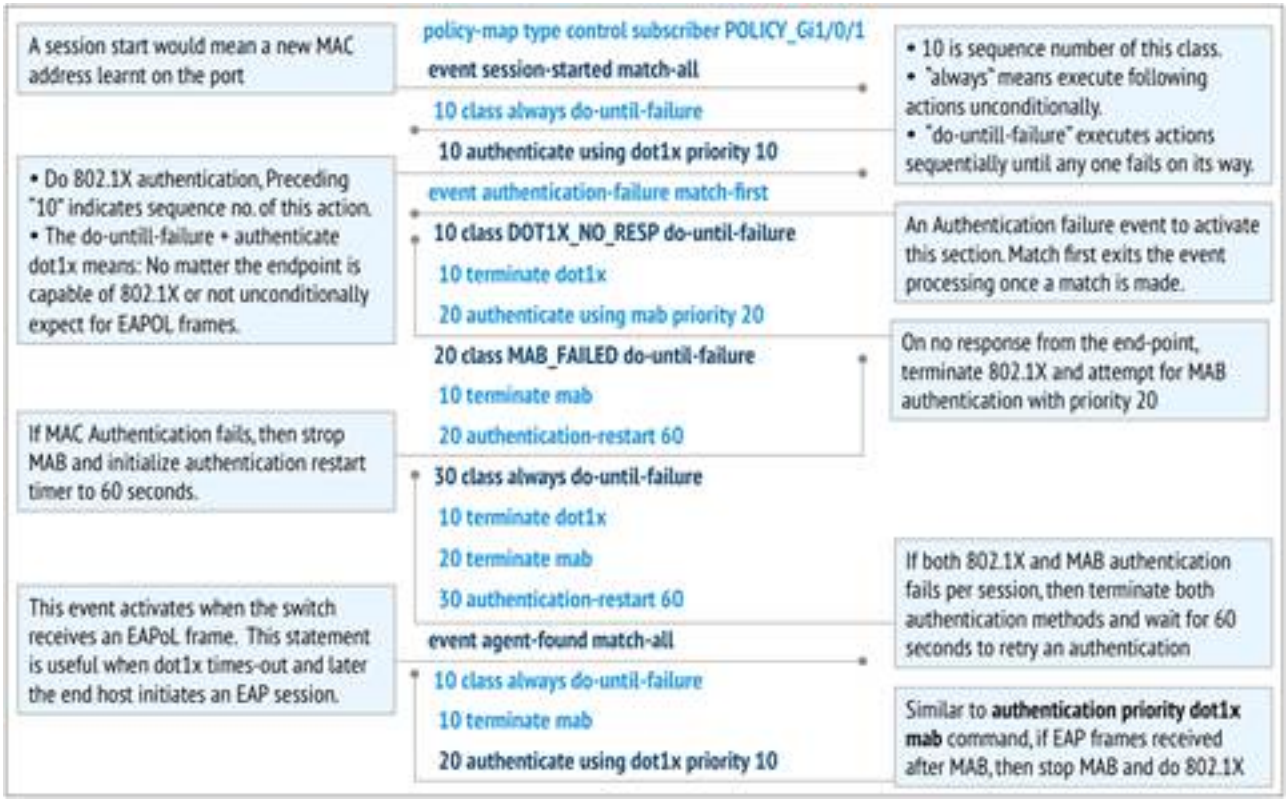
Dans les Commutateurs traditionnels IOS, il n'y avait aucune option de s'appliquer une particularité de liste de méthode à une session authentifiée. IBNS 2.0 fournit cette capacité utilisant des service-modèles. Le modèle de service est configuré localement sur le commutateur et l'autorisation réussie appliquée de session de courrier. Il y a également une option de pousser le modèle de service exigé d'un serveur d'AAA.

L'attribut RADIUS qui est utilisé pour faire la même chose est *abonné : nom de service = <name du template> de service.* Dans l'engine de gestion d'identité (ISE), vous pouvez nommer le profil

d'autorisation exactement les mêmes en date du service-modèle local configuré sur le commutateur et cocher la case de *modèle de service*. Ce profil d'autorisation avec n'importe quel autre profil d'autorisation peut être poussé comme résultat d'autorisation.

Dans l'état de résultat d'autorisation, il y a des Cisco-POIDs du commerce-paires nommées *abonné : nom de service = <name du template> de service*. Ce indiacates qu'on a annoncé le swich pour appliquer ce modèle de service pour cette session.

Voici une image qui affiche la signification précise de chaque entité d'une carte de stratégie d'échantillon.




# Configurez

Configuration d'AAA

Configuration du serveur RADIUS

Configuration de policy-map

Configuration de class map

Configuration d'interface

# Dépannez

La meilleure manière de dépanner est de comparer les logs fonctionnants et les logs non-travaillants. De cette façon, l'étape précise à laquelle le processus est allée mal est connue. Il y a quelques uns met au point qui est nécessaire pour être activé dépanner des questions mab/dot1x. Voici les commandes d'activer ceux met au point.

- **debug aaa authentication**
- **debug aaa authorization**
- mettez au point le mab tout
- debug dot1x tout
- **debug radius**

Voici les logs fonctionnants avec le dot1x et le mab activé en même temps.

### mettez au point le mab tout

### debug dot1x tout

Puisque le dot1x a beaucoup d'échanges de message en raison des négociations de protocole, des échanges de certificat et ainsi de suite, non toutes les logs de débogage ont été mentionnés ici. L'écoulement des événements dans la commande dans laquelle ils sont censés se produire et leur correspondance mettent au point des logs ont été documentés ici.

### debug radius

Puisqu'il y a sort de messages d'EAP, les paquets RADIUS ont envoyé au serveur et reçu soyez également plus. Non chaque authentification de dot1x finit avec sur l'Access-demande. Par conséquent les logs affichés ici sont ceux qui sont importants et car l'écoulement disparaît.

### debug aaa authentication/autorisation

debug aaa authentication et informations utiles d'expositions d'autorisation de debug aaa pendant la diverses authentification/authorizations method. Dans ce cas, c'est seulement une ligne simple spécifiant la liste de méthode étant utilisée.

Ceci affiche si les méthodes d'authentification l'unes des sont indisponibles/non activées.

La procédure pour dépanner CWA/Posture/DACLs etc., est identique que celle des Commutateurs traditionnels IOS. La vérification de configuration est la première étape dans le dépannage. Assurez que la configuration répond aux exigences. Si la configuration de la carte de stratégie, class map est jusqu'à la marque, alors des problèmes de debugg si, en peuvent être très faciles. Pour d'autres détails sur la configuration utilisant IBNS 2.0, référez-vous la section Informations connexes.

## Informations connexes

- Guide de déploiement IBNS 2.0