

Contenu

[Introduction](#)

[Informations générales](#)

[Configuration](#)

[Dépannez](#)

[Bogues](#)

Introduction

Ce document décrit comment dépanner le CPU/MÉMOIRE élevé dû au cadre de Protocole EAP (Extensible Authentication Protocol) et au gestionnaire d'Authentification, autorisation et comptabilité (AAA). Ceci est vu sur les Commutateurs qui utilisent l'authentification dot1x/mab.

Informations générales

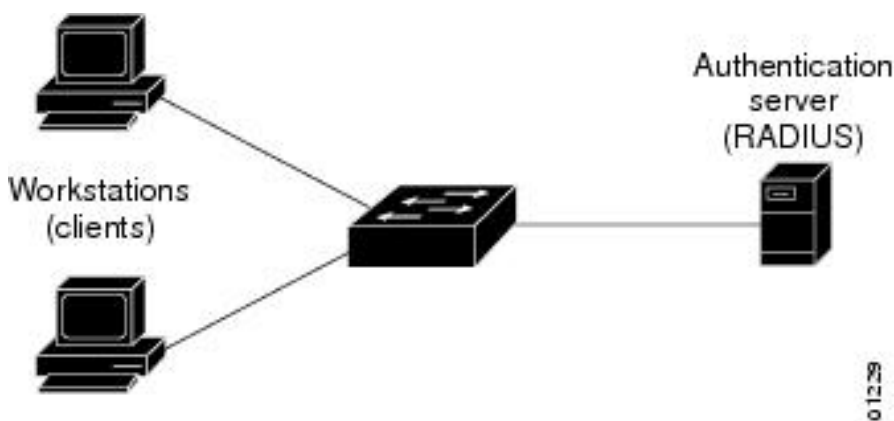
Le gestionnaire authentique de Cisco IOS traite des demandes d'authentification de réseau et impose des stratégies d'autorisation indépendamment de la méthode d'authentification. Le gestionnaire authentique met à jour des données opérationnelles pour toutes les tentatives, authentications, autorisations, et déconnexions basées sur port de connexion réseau et, des servir de gestionnaire de session.

Le commutateur agit en tant qu'intermédiaire (proxy) entre le client et le serveur d'authentification, il demande les informations d'identité du client, vérifie ces informations avec le serveur d'authentification, et transmet par relais une réponse au client. Le commutateur inclut le client RADIUS, qui encapsule et désencapsule les trames d'EAP et interagit avec le serveur d'authentification.

Configuration

Cette section affiche un commutateur de Cisco qui fait l'authentification MAB/DOT1X (MAC AuthenticationBypass).

Vous devriez comprendre les concepts du contrôle d'accès au réseau basé sur port et avoir une compréhension de la façon configurer le contrôle d'accès au réseau basé sur port sur votre plateforme de Cisco. Cette image illustre les postes de travail qui ont l'authentification dot1x/MAB.



C'est d'une configuration d'échantillon :

Dépannez

Les Commutateurs qui utilisent l'authentification dot1x/MAB ont parfois les pics élevés de CPU/MÉMOIRE dus au cadre d'EAP et au gestionnaire d'AAA. Ceci peut affecter la production puisque des demandes d'authentification sont abandonnées.

Afin de résoudre ceci, ces étapes sont recommandées :

Étape 1. Sélectionnez la commande de **tri CPU de show proc** afin de vérifier l'utilisation du CPU élevée sur le commutateur et s'assurer que le cadre d'EAP et les processus maître authentiques ont le plus à trafic intense suivant les indications de cet exemple :

Étape 2. Vérifiez l'utilisation de mémoire sur le commutateur pour des processus comme le gestionnaire et le RAYON authentiques avec la commande de **mémoire UC de processus d'exposition** suivant les indications de cet exemple.

Étape 3. Si vous faites face à l'utilisation de ressource élevée sur le commutateur, vous pourriez voir les logs suivants pour les échecs d'authentification comme affichés :

Sélectionnez la commande de **show logging**.

Étape 4. Placez le temporisateur d'authentifier à nouveau à une valeur supérieure (par exemple, 3600 secondes) afin de s'assurer que vous n'authentifiez pas fréquemment pour les clients, qui augmente de ce fait le chargement sur le commutateur.

Afin de valider la configuration sélectionnez la commande de **<interface-name> d'interface de passage d'exposition** :

Étape 5. Déterminez combien de sessions sont vues pour des processus MAB/dot1x, parce que parfois un nombre élevé de sessions authentifiées peut également mener à la CPU de haute. Afin de vérifier le nombre de sessions actives, sélectionnez ces commandes :

Étape 6. Afin de vérifier les bogues de version et de potentiel, sélectionnez la commande de **show version**.

Si la bogue n'est pas répertoriée dans les « bogues » sectionnent, ouvrent une valise avec le centre d'assistance technique (TAC) et reliez tous les logs des étapes 1 5.

Bogues

CPU de la fuite de mémoire [CSCus46997](#) et de la haute dans la piste d'hôte IP et le gestionnaire authentique

Le Catalyst 2960 [CSCtz06177](#) A peut exécuter le bas sur la mémoire.

Le cadre de l'EAP [CSCty49762](#) et sous-titre de l'AttrL d'AAA utilise toute la mémoire de processus

Conseil : Pour d'autres détails, référez-vous aux id de bogue Cisco [CSCus46997](#), [CSCtz06177](#) et [CSCty49762](#).