

Dépannage des clients 802.1X sur le contrôleur LAN sans fil Catalyst 9800 : Modification de la version Eapol/802.1X

Table des matières

Introduction

Ce document décrit comment aider à connecter d'anciens clients sans fil IoT qui ne prennent pas en charge les versions 802.1X plus récentes.

Exigences

Composants utilisés

Il est basé sur le contrôleur LAN sans fil Catalyst 9800 exécutant n'importe quelle version de Cisco IOS® XE 17.x.

Contexte

Le protocole 802.1X a jusqu'à présent 3 versions. 802.1X-2001 est la version 1, 802.1X-2004 est la version 2, 802.1X-2010 et toutes les révisions ultérieures utilisent l'identifiant de la version 3.

La norme IEEE indique très clairement que chaque périphérique doit annoncer sa version maximale prise en charge, puis convenir d'une version commune, car toutes les versions sont rétrocompatibles.

Le WLC Catalyst 9800 annonce 802.1X et Eapol version 3.

Dans de nombreux cas, le client sans fil répond avec la version 1 de 802.1X et l'authentification peut continuer à utiliser l'implémentation de la version 1, par exemple.

Cependant, certains clients IoT plus anciens s'attendent à voir une version 802.1X spécifique à l'autre extrémité et ne tolèrent pas de voir une version plus récente qu'ils ne comprennent pas. C'est une violation de la norme. Cependant, il est parfois difficile de mettre à jour votre appareil IoT et vous devez l'utiliser. Il est donc possible d'ajuster la version 802.1X sur le contrôleur pour faire ces clients.

Il n'y a pas de bonnes raisons de modifier cette version à moins d'avoir des preuves que vous êtes confronté à ce problème avec un ensemble spécifique de clients !

Vérifiez que vous rencontrez ce problème

Voici un exemple de trace radioactive active où le contrôleur annonce la version 3 mais le client répond avec raison avec une version inférieure et l'authentification peut continuer :

```
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Posting RESTART on Client
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Entering init state
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Entering idle state
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Posting !AUTH_ABORT on Client
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Entering restart state
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Resetting the client 0xD8000002
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Override cfg - MAC <MAC> - profile (
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Override cfg - SuppTimeout 30s, ReAu
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Sending create new context event to
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Posting !EAP_RESTART on Client
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Enter connecting state
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Restart connecting
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Posting RX_REQ on Client
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Authenticating state entered
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Connecting authenticating action
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Entering request state
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Setting EAPOL eth-type to 0x888e, de
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [0000.0000.0000:capwap_9000002c] Sending out EAPOL packet
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] Sent EAPOL packet - Version : 3,EAPOL
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] EAP Packet - REQUEST, ID : 0x1
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [0000.0000.0000:unknown] Pkt body: 01 01 00 05 01
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] EAPOL packet sent to client
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>] Received EAPOL packet - Version : 1,EAPOL Type : EAP
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [<MAC>:capwap_9000002c] EAP Packet - RESPONSE, ID : 0x1
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [0000.0000.0000:unknown] Pkt body: 02 01 00 0c 01 34 34 37 3
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [0000.0000.0000:capwap_9000002c] Queuing an EAPOL pkt on Aut
{wncd_x_R0-0}{1}: [dot1x] [25076]: (info): [0000.0000.0000:capwap_9000002c] Dequeued pkt: CODE = 2,TYPE
```

(...) RADIUS authentication follows

Une sortie de non-fonctionnement semble similaire jusqu'à ce que le message de demande d'identité EAP envoyé par le WLC/AP et que le client ne réponde à rien.

Modification de la version Eapol/802.1X

```
WLC#show dot1x all
Sysauthcontrol          Disabled
Dot1x Protocol Version      3
WLC#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
WLC(config)#service internal
WLC(config)#dot1x eapol version 2
WLC(config)#exit
WLC#show dot1x all
Sysauthcontrol          Disabled
Dot1x Protocol Version      2
```


À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.