Exemple de configuration de l'authentification IEEE 802.1x avec Catalyst 6500/6000 exécutant Cisco IOS

Contenu

Introduction

Ce document explique comment configurer le 802.1x d'IEEE sur un Catalyst 6500/6000 que cela exécute dans le mode natif (une image logicielle simple de Cisco IOS® pour l'engine de superviseur et le MSFC) et un serveur de Service RADIUS (Remote Authentication Dial-In User Service) pour l'authentification et l'affectation VLAN.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir connaissance des sujets suivants :

- Guide d'installation pour le Cisco Secure ACS pour Windows 4.1
- Guide utilisateur pour le Cisco Secure Access Control Server 4.1
- Fonctionnement de RADIUS
- Commutation de Catalyst et guide de déploiement ACS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Catalyst 6500 qui exécute le Logiciel Cisco IOS version 12.2(18)SXF sur l'engine de superviseur**Remarque:** Vous avez besoin prendre en charge de Logiciel Cisco IOS version 12.1(13)E ou plus tard l'authentification basée sur port de 802.1x.
- Cet exemple utilise le Cisco Secure Access Control Server (ACS) 4.1 en tant que serveur de RAYON.**Remarque:** Un serveur de RAYON doit être spécifié avant que vous activiez le 802.1x sur le commutateur.
- Clients PC qui prend en charge l'authentification de 802.1x**Remarque:** Cet exemple utilise des clients de Microsoft Windows XP.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

La norme de 802.1x d'IEEE définit un client-serveur - le protocole basé de contrôle d'accès et d'authentification qui limite les périphériques non autorisés de se connecter à un RÉSEAU LOCAL par les ports publiquement accessibles. le 802.1x contrôle l'accès au réseau en créant deux Points d'accès virtuels distincts à chaque port. Un Point d'accès est un port incontrôlé ; l'autre est un port commandé. Tout le trafic par le port unique est disponible aux deux Points d'accès. le 802.1x authentifie chaque périphérique d'utilisateur qui est connecté à un port de commutateur et assigne le port à un VLAN avant qu'il fasse disponible tous les services qui sont offerts par le commutateur ou le RÉSEAU LOCAL. Jusqu'à ce que le périphérique soit authentifié, le contrôle d'accès de 802.1x permet seulement Extensible Authentication Protocol au-dessus du trafic du RÉSEAU LOCAL (EAPOL) par le port auquel le périphérique est connecté. Après l'authentification est réussie, le trafic normal peut traverser le port.

Remarque: Si le commutateur reçoit des paquets EAPOL du port qui n'est pas configuré pour l'authentification de 802.1x ou si le commutateur ne prend en charge pas l'authentification de 802.1x, alors les paquets EAPOL sont lâchés et ne sont expédiés à aucun périphérique en amont.

Configurez

Dans cette section, vous êtes présenté avec les informations pour configurer la fonction décrite de 802.1x dans ce document.

Cette configuration requiert les étapes suivantes :

- Configurez le commutateur de Catalyst pour l'authentification de 802.1x.

- Configurez le serveur de RAYON.
- Configurez les clients PC pour utiliser l'authentification de 802.1x.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

- Serveur de RAYON — Exécute l'authentification réelle du client. Le serveur de RAYON valide l'identité du client et informe le commutateur si le client est autorisé à accéder au RÉSEAU LOCAL et à commuter des services. Ici, le serveur de RAYON est configuré pour l'authentification et l'affectation VLAN.
- Commutateur — Contrôle l'accès physique au réseau basé sur l'état d'authentification du client. Le commutateur agit en tant qu'intermédiaire (proxy) entre le client et le serveur de RAYON. Il demande les informations d'identité du client, vérifie ces informations avec le serveur de RAYON, et transmet par relais une réponse au client. Ici, le commutateur de Catalyst 6500 est également configuré comme serveur DHCP. Le soutien d'authentification de 802.1x du protocole DHCP (DHCP) permet au serveur DHCP pour assigner les adresses IP aux classes différentes d'utilisateurs finaux en ajoutant l'identité de l'utilisateur authentifiée dans le processus de découverte DHCP.
- Clients — Les périphériques (postes de travail) ces demande l'accès au RÉSEAU LOCAL et aux services de commutateur et répond aux demandes du commutateur. Ici, PC 1 4 sont les clients qui demandent un accès au réseau authentifié. PC 1 et 2 utilisent le même laisser-passer de connexion qui est dans le VLAN 2. De même, PC 3 et 4 utilisent un laisser-passer de connexion pour des clients PC VLAN 3. sont configurés pour atteindre l'adresse IP d'un serveur DHCP.

Configurez le commutateur de Catalyst pour l'authentification de 802.1x

Cette configuration de commutateur témoin inclut :

- Comment activer l'authentification de 802.1x sur des ports FastEthernets.
- Comment connecter un serveur de RAYON au VLAN 10 derrière le port FastEthernet 3/1.
- Une configuration du serveur DHCP pour deux groupes IP, un pour des clients dans le VLAN 2 et l'autre pour des clients dans le VLAN 3.
- Routage inter-VLAN pour avoir la Connectivité entre les clients après authentification.

Référez-vous aux instructions et aux restrictions basées sur port d'authentification de 802.1x pour les instructions sur la façon dont configurer l'authentification de 802.1x.

Remarque: Assurez-vous que le serveur de RAYON se connecte toujours derrière un port autorisé.

Catalyst 6500

```
Router#configure terminal Enter configuration commands,
one per line. End with CNTL/Z. Router(config)#hostname
Cat6K !--- Sets the hostname for the switch.
Cat6K(config)#vlan 2 Cat6K(config-vlan)#name VLAN2
Cat6K(config-vlan)#vlan 3 Cat6K(config-vlan)#name VLAN3
!--- VLAN should be existing in the switch for a
successful authentication. Cat6K(config-vlan)#vlan 10
Cat6K(config-vlan)#name RADIUS_SERVER !--- This is a
```

```
dedicated VLAN for the RADIUS server. Cat6K(config-
vlan)#exit Cat6K(config-if)#interface fastEthernet3/1
Cat6K(config-if)#switchport Cat6K(config-if)#switchport
mode access Cat6K(config-if)#switchport access vlan 10
Cat6K(config-if)#no shut !--- Assigns the port connected
to the RADIUS server to VLAN 10. !--- Note:- All the
active access ports are in VLAN 1 by default.
Cat6K(config-if)#exit Cat6K(config)#dot1x system-auth-
control !--- Globally enables 802.1x.
Cat6K(config)#interface range fastEthernet3/2-48
Cat6K(config-if-range)#switchport Cat6K(config-if-
range)#switchport mode access Cat6K(config-if-
range)#dot1x port-control auto Cat6K(config-if-range)#no
shut !--- Enables 802.1x on all the FastEthernet
interfaces. Cat6K(config-if-range)#exit
Cat6K(config)#aaa new-model !--- Enables AAA.
Cat6K(config)#aaa authentication dot1x default group
radius !--- Method list should be default. Otherwise
dot1x does not work. Cat6K(config)#aaa authorization
network default group radius !--- You need authorization
for dynamic VLAN assignment to work with RADIUS.
Cat6K(config)#radius-server host 172.16.1.1 !--- Sets
the IP address of the RADIUS server.
Cat6K(config)#radius-server key cisco !--- The key must
match the key used on the RADIUS server.
Cat6K(config)#interface vlan 10 Cat6K(config-if)#ip
address 172.16.1.2 255.255.255.0 Cat6K(config-if)#no
shut !--- This is used as the gateway address in RADIUS
server !--- and also as the client identifier in the
RADIUS server. Cat6K(config-if)#interface vlan 2
Cat6K(config-if)#ip address 172.16.2.1 255.255.255.0
Cat6K(config-if)#no shut !--- This is the gateway
address for clients in VLAN 2. Cat6K(config-
if)#interface vlan 3 Cat6K(config-if)#ip address
172.16.3.1 255.255.255.0 Cat6K(config-if)#no shut !---
This is the gateway address for clients in VLAN 3.
Cat6K(config-if)#exit Cat6K(config)#ip dhcp pool
vlan2_clients Cat6K(dhcp-config)#network 172.16.2.0
255.255.255.0 Cat6K(dhcp-config)#default-router
172.16.2.1 !--- This pool assigns ip address for clients
in VLAN 2. Cat6K(dhcp-config)#ip dhcp pool vlan3_clients
Cat6K(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.3.1 !--- This
pool assigns ip address for clients in VLAN 3.
Cat6K(dhcp-config)#exit Cat6K(config)#ip dhcp excluded-
address 172.16.2.1 Cat6K(config)#ip dhcp excluded-
address 172.16.3.1 Cat6K(config-if)#end Cat6K#show vlan
VLAN Name Status Ports ---- ----------------------------
---- --------- ------------------------------ 1 default
active Fa3/2, Fa3/3, Fa3/4, Fa3/5 Fa3/6, Fa3/7, Fa3/8,
Fa3/9 Fa3/10, Fa3/11, Fa3/12, Fa3/13 Fa3/14, Fa3/15,
Fa3/16, Fa3/17 Fa3/18, Fa3/19, Fa3/20, Fa3/21 Fa3/22,
Fa3/23, Fa3/24, Fa3/25 Fa3/26, Fa3/27, Fa3/28, Fa3/29
Fa3/30, Fa3/31, Fa3/32, Fa3/33 Fa3/34, Fa3/35, Fa3/36,
Fa3/37 Fa3/38, Fa3/39, Fa3/40, Fa3/41 Fa3/42, Fa3/43,
Fa3/44, Fa3/45 Fa3/46, Fa3/47, Fa3/48 2 VLAN2 active 3
VLAN3 active 10 RADIUS_SERVER active Fa3/1 1002 fddi-
default act/unsup 1003 token-ring-default act/unsup 1004
fddinet-default act/unsup 1005 trnet-default act/unsup
!--- Output suppressed. !--- All active ports are in
VLAN 1 (except 3/1) before authentication.
```

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus

d'informations sur les commandes utilisées dans cette section.

Configurez le serveur de RAYON

Le serveur de RAYON est configuré avec une adresse IP statique de 172.16.1.1/24. Terminez-vous ces étapes afin de configurer le serveur de RAYON pour un client d'AAA :

1. Cliquez sur Network Configuration sur la fenêtre de gestion ACS afin de configurer un client d'AAA.
2. Cliquez sur Add l'**entrée** sous la section de clients d'AAA.
3. Configurez l'adresse Internet de client d'AAA, l'adresse IP, la clé secrète partagée et le type d'authentification en tant que :Adresse Internet de client d'AAA = nom de hôte du commutateur (**Cat6K**).Adresse IP de client d'AAA = adresse IP d'interface de gestion du commutateur (**172.16.1.2**).Secret partagé = RAYON clé configuré sur le commutateur (**Cisco**).Authentifiez utilisant = **IETF de RAYON**.**Remarque:** Pour l'exécution correcte, la clé secrète partagée doit être identique sur le client d'AAA et l'ACS. Les clés distinguent les majuscules et minuscules.
4. Cliquez sur Submit **+ appliquez** pour apporter ces modifications efficaces, comme indiqué dans cet exemple :

Terminez-vous ces étapes afin de configurer le serveur de RAYON pour l'authentification, le VLAN et l'affectation d'adresse IP.

Deux noms d'utilisateur doivent être créés séparément pour les clients qui se connectent au VLAN 2 aussi bien que pour le VLAN 3. Ici, un utilisateur **user_vlan2** pour les clients qui se connectent à un VLAN 2 et à un utilisateur différent **user_vlan3** pour les clients qui se connectent au VLAN 3 sont créés à cet effet.

Remarque: Ici, la configuration utilisateur est affichée pour les clients qui se connectent au VLAN 2 seulement. Pour les utilisateurs qui se connectent au VLAN 3, suivez la même procédure.

1. Afin d'ajouter et configurer des utilisateurs, cliquez sur User Setup et définissez le nom d'utilisateur et le mot de passe.
2. Définissez l'affectation d'adresse IP de client comme **assignée par le client pool d'AAA**. Écrivez le nom du groupe d'adresse IP configuré sur le commutateur pour les clients VLAN 2.**Remarque:** Sélectionnez cette option et introduisez le nom de client ip pool d'AAA dans la case, seulement si cet utilisateur doit faire assigner l'adresse IP par un groupe d'adresse IP configuré sur le client d'AAA.
3. Définissez les attributs **64** et **65 de l'**Internet Engineering Task Force (IETF).Assurez-vous que les balises des valeurs sont placés à **1**, comme indiqué dans cet exemple. Le Catalyst ignore n'importe quelle balise autre que 1. afin d'affecter un utilisateur à une particularité VLAN, vous devez également définir l'attribut **81** avec un *nom* VLAN ou le *nombre* VLAN qui correspondent.**Remarque:** Si vous utilisez le *nom* VLAN, il devrait être exactement même que celui configuré dans le commutateur.**Remarque:** Pour plus d'informations sur ces attributs IETF, référez-vous à RFC 2868 : Attributs RADIUS pour le support de Protocol de tunnel .**Remarque:** En configuration initiale du serveur ACS, les attributs RADIUS IETF peuvent pour afficher dans l'**installation utilisateur**. Afin d'activer des attributs IETF dans des écrans de configuration utilisateur, choisissez la **configuration d'interface > le RAYON (IETF)**. Puis, le contrôle attribue **64**, **65**, et **81** dans les colonnes d'utilisateur et de groupe.**Remarque:** Si vous ne définissez pas l'attribut **81** IETF et le port est un port de

commutateur dans le mode d'accès, le client a l'affectation à l'accès VLAN du port. Si vous avez défini l'attribut **81** pour l'affectation dynamique VLAN et le port est un port de commutateur dans le mode d'accès, vous devez émettre le **rayon de groupe par défaut d'aaa authorization network de** commande sur le commutateur. Cette commande assigne le port au VLAN que le serveur de RAYON fournit. Autrement, le 802.1x déplace le port à l'état AUTORISÉ après authentification de l'utilisateur ; mais le port est toujours dans le par défaut VLAN du port, et la Connectivité peut échouer. Si vous avez défini l'attribut **81**, mais vous ont configuré le port pendant qu'un port conduit, refus d'accès se produit. Affichages de ce message d'erreur :

```
%DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE:
RADIUS attempted to assign a VLAN to Dot1x port FastEthernet3/4 whose
VLAN cannot be assigned.
```

Configurez les clients PC pour utiliser l'authentification de 802.1x

Cet exemple est spécifique au Protocole EAP (Extensible Authentication Protocol) de Microsoft Windows XP au-dessus du client du RÉSEAU LOCAL (EAPOL) :

1. Choisissez le **début > le panneau de configuration > les connexions réseau**, puis cliquez avec le bouton droit sur votre **connexion au réseau local** et choisissez Properties.
2. Vérifiez l'**icône d'exposition dans la zone de notification une fois connecté** sous l'onglet Général.
3. Sous l'onglet d'authentification, **authentification de 802.1x d'IEEE d'enable de** contrôle **pour ce réseau**.
4. Placez le type d'EAP à **MD5-Challenge**, comme indiqué dans cet exemple :

Terminez-vous ces étapes pour configurer les clients pour obtenir l'adresse IP d'un serveur DHCP.

1. Choisissez le **début > le panneau de configuration > les connexions réseau**, puis cliquez avec le bouton droit sur votre **connexion au réseau local** et choisissez Properties.
2. Sous l'onglet **General**, cliquez sur **Internet Protocol (TCP/IP)**, puis sur **Properties**.
3. Choisissez **Obtain an IP address automatically**.

Vérifiez

Clients PC

Si vous avez correctement complété la configuration, les clients PC affiche une demande instantanée pour entrer un nom d'utilisateur et un mot de passe.

1. Cliquez sur en fonction la demande, que cet exemple affiche :Affichages de fenêtre d'entrée d'un nom d'utilisateur et de mot de passe.
2. Entrez le nom d'utilisateur et le mot de passe.**Remarque:** Dans PC 1 et 2, écrivez les identifiants utilisateurs VLAN 2 et dans PC 3 et 4 écrivez les identifiants utilisateurs VLAN 3.
3. Si message d'erreur n'apparaît pas, vérifiez la Connectivité avec les méthodes habituelles, telles que l'accès traversant des ressources de réseau et avec le **ping**. Cette sortie est de PC 1, et affiche un **ping** réussi à PC 4 :Si cette erreur apparaît, vérifiez que le nom d'utilisateur et le mot de passe sont corrects :

Catalyst 6500

Si le mot de passe et le nom d'utilisateur semblent être corrects, vérifiez l'État du port de 802.1x sur le commutateur.

1. Recherchez un état de port qui indique AUTORISÉ.`Cat6K#show dot1x Sysauthcontrol = Enabled Dot1x Protocol Version = 1 Dot1x Oper Controlled Directions = Both Dot1x Admin Controlled Directions = Both Cat6K#show dot1x interface fastEthernet 3/2 AuthSM State = AUTHENTICATED BendSM State = IDLE PortStatus = AUTHORIZED MaxReq = 2 MultiHosts = Enabled Port Control = Auto QuietPeriod = 60 Seconds Re-authentication = Disabled ReAuthPeriod = 3600 Seconds ServerTimeout = 30 Seconds SuppTimeout = 30 Seconds TxPeriod = 30 Seconds Cat6K#show dot1x interface fastEthernet 3/4 AuthSM State = AUTHENTICATED BendSM State = IDLE PortStatus = AUTHORIZED MaxReq = 2 MultiHosts = Enabled Port Control = Auto QuietPeriod = 60 Seconds Re-authentication = Disabled ReAuthPeriod = 3600 Seconds ServerTimeout = 30 Seconds SuppTimeout = 30 Seconds TxPeriod = 30 Seconds Cat6K#show dot1x interface fastEthernet 3/1 Default Dot1x Configuration Exists for this interface FastEthernet3/1 AuthSM State = FORCE AUTHORIZED BendSM State = IDLE PortStatus = AUTHORIZED MaxReq = 2 MultiHosts = Disabled PortControl = Force Authorized QuietPeriod = 60 Seconds Re-authentication = Disabled ReAuthPeriod = 3600 Seconds ServerTimeout = 30 Seconds SuppTimeout = 30 Seconds TxPeriod = 30 Seconds` Vérifiez l'état VLAN après l'authentification réussie.`Cat6K#show vlan VLAN Name Status Ports ---- -------------------------------- --------- ------------------------------- - 1 default active Fa3/6, Fa3/7, Fa3/8, Fa3/9, Fa3/10, Fa3/11, Fa3/12, Fa3/13, Fa3/14, Fa3/15, Fa3/16, Fa3/17, Fa3/18, Fa3/19, Fa3/20, Fa3/21, Fa3/22, Fa3/23, Fa3/24, Fa3/25, Fa3/26, Fa3/27, Fa3/28, Fa3/29, Fa3/30, Fa3/31, Fa3/32, Fa3/33, Fa3/34, Fa3/35, Fa3/36, Fa3/37, Fa3/38, Fa3/39, Fa3/40, Fa3/41, Fa3/42, Fa3/43, Fa3/44, Fa3/45, Fa3/46, Fa3/47, Fa3/48 2 VLAN2 active Fa3/2, Fa3/3 3 VLAN3 active Fa3/4, Fa3/5 10 RADIUS_SERVER active Fa3/1 1002 fddi-default act/unsup 1003 token-ring-default act/unsup 1004 fddinet-default act/unsup 1005 trnet-default act/unsup !--- Output suppressed.`
2. Vérifiez l'état de liaison DHCP du après l'authentification réussie.`Router#show ip dhcp binding IP address Hardware address Lease expiration Type 172.16.2.2 0100.1636.3333.9c Mar 04 2007 06:35 AM Automatic 172.16.2.3 0100.166F.3CA3.42 Mar 04 2007 06:43 AM Automatic 172.16.3.2 0100.145e.945f.99 Mar 04 2007 06:50 AM Automatic 172.16.3.3 0100.1185.8D9A.F9 Mar 04 2007 06:57 AM Automatic` L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Dépannez

Collectez la sortie de ces commandes de **débogage** afin de dépanner :

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **événements de debug dot1x** — Active l'élimination des imperfections des déclarations d'impression gardées par le drapeau d'événement de dot1x.`Cat6K#debug dot1x events Dot1x events debugging is on Cat6K# !--- Debug output for PC 1 connected to Fa3/2. 00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 14 00:13:36: dot1x-ev:Couldn't Find a process thats already handling the request for this id 3 00:13:36: dot1x-ev:Inserted the request on to list of pending requests. Total requests = 1 00:13:36: dot1x-ev:Found a free slot at slot: 0 00:13:36: dot1x-ev:AAA Client process spawned at slot: 0 00:13:36: dot1x-ev:AAA Client-process processing Request Interface= Fa3/2, Request-Id = 14, Length = 15 00:13:36: dot1x-ev:The Interface on which we got this AAA Request is FastEthernet3/2 00:13:36: dot1x-ev:MAC Address is 0016.3633.339c 00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:13:36: dot1x-ev:going to send to backend on SP, length = 6 00:13:36: dot1x-ev:Sent to Bend 00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 15 00:13:36: dot1x-ev:Found a process thats already handling therequest for this id 12 00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 6 00:13:36: dot1x-`

ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:13:36: dot1x-ev:going to send to backend on SP, length = 31 00:13:36: dot1x-ev:Sent to Bend 00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 16 00:13:36: dot1x-ev:Found a process thats already handling therequest for this id 13 **00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 32 00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS 00:13:36: dot1x-ev:Vlan name = VLAN2** 00:13:37: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 16 EAP pkt len = 4 00:13:37: dot1x-ev:The process finished processing the request will pick up any pending requests from the queue Cat6K# Cat6K# *!--- Debug output for PC 3 connected to Fa3/4.* 00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 8 00:19:58: dot1x-ev:Couldn't Find a process thats already handling the request for this id 1 00:19:58: dot1x-ev:Inserted the request on to list of pending requests. Total requests = 1 00:19:58: dot1x-ev:Found a free slot at slot: 0 00:19:58: dot1x-ev:AAA Client process spawned at slot: 0 00:19:58: dot1x-ev:AAA Client-process processing Request Interface= Fa3/4, Request-Id = 8, Length = 15 **00:19:58: dot1x-ev:The Interface on which we got this AAA Request is FastEthernet3/4** 00:19:58: dot1x-ev:MAC Address is 0014.5e94.5f99 00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:19:58: dot1x-ev:going to send to backend on SP, length = 6 00:19:58: dot1x-ev:Sent to Bend 00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 9 00:19:58: dot1x-ev:Found a process thats already handling therequest for this id 10 00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 6 00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:19:58: dot1x-ev:going to send to backend on SP, length = 31 00:19:58: dot1x-ev:Sent to Bend 00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 10 00:19:58: dot1x-ev:Found a process thats already handling therequest for this id 11 **00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 32 00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS 00:19:58: dot1x-ev:Vlan name = 3** 00:19:58: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 10 EAP pkt len = 4 00:19:58: dot1x-ev:The process finished processing the request will pick up any pending requests from the queue Cat6K#

- **debug radius** — Affiche des informations associée avec le RAYON.Cat6K#**debug radius** Radius protocol debugging is on Cat6K# *!--- Debug output for PC 1 connected to Fa3/2.* 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 85 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 17 172.16.1.1:1812, Access-Request, len 85 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 79 17 0201000F 00:13:36: Attribute 80 18 CCEE4889 00:13:36: RADIUS: Received from id 17 172.16.1.1:1812, Access-Challenge, len 79 00:13:36: Attribute 79 8 010D0006 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80 18 C883376B 00:13:36: RADIUS: EAP-login: length of eap packet = 6 00:13:36: RADIUS: EAP-login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 109 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 18 172.16.1.1:1812, Access-Request, len 109 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 8 020D0006 00:13:36: Attribute 80 18 15582484 00:13:36: RADIUS: Received from id 18 172.16.1.1:1812, Access-Challenge, len 104 00:13:36: Attribute 79 33 010E001F 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80 18 0643D234 00:13:36: RADIUS: EAP-login: length of eap packet = 31 00:13:36: RADIUS: EAP-login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 135 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 19 172.16.1.1:1812, Access-Request, len 135 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 34 020E0020 00:13:36: Attribute 80 18 E8A61751 00:13:36: RADIUS: Received from id 19 172.16.1.1:1812, Access-Accept, len 124 00:13:36: Attribute 64 6 0100000D 00:13:36: Attribute 65 6 01000006 00:13:36: Attribute 81 8 01564C41 00:13:36: Attribute 88 15 766C616E 00:13:36: Attribute 8 6 FFFFFFFE 00:13:36: Attribute 79 6 030E0004 00:13:36: Attribute 25 39 43495343 00:13:36: Attribute 80 18 11A7DD44 00:13:36: RADIUS: EAP-login: length of eap packet = 4 Cat6K# Cat6K# *!--- Debug output for PC 3 connected to Fa3/4.* 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 85 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 11 172.16.1.1:1812, Access-Request, len 85 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 79 17 0201000F 00:19:58: Attribute 80 18

```
0001AC52 00:19:58: RADIUS: Received from id 11 172.16.1.1:1812, Access-Challenge, len 79
00:19:58: Attribute 79 8 010B0006 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80
18 23B9C9E7 00:19:58: RADIUS: EAP-login: length of eap packet = 6 00:19:58: RADIUS: EAP-
login: got challenge from radius 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS:
Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius
packet = 109 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 12
172.16.1.1:1812, Access-Request, len 109 00:19:58: Attribute 4 6 AC100201 00:19:58:
Attribute 61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8
00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 79 8 020B0006 00:19:58: Attribute 80
18 F4C8832E 00:19:58: RADIUS: Received from id 12 172.16.1.1:1812, Access-Challenge, len 104
00:19:58: Attribute 79 33 010C001F 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80
18 45472A93 00:19:58: RADIUS: EAP-login: length of eap packet = 31 00:19:58: RADIUS: EAP-
login: got challenge from radius 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS:
Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius
packet = 135 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 13
172.16.1.1:1812, Access-Request, len 135 00:19:58: Attribute 4 6 AC100201 00:19:58:
Attribute 61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8
00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 79 34 020C0020 00:19:58: Attribute 80
18 37011E8F 00:19:58: RADIUS: Received from id 13 172.16.1.1:1812, Access-Accept, len 120
00:19:58: Attribute 64 6 0100000D 00:19:58: Attribute 65 6 01000006 00:19:58: Attribute 81 4
0133580F 00:19:58: Attribute 88 15 766C616E 00:19:58: Attribute 8 6 FFFFFFFE 00:19:58:
Attribute 79 6 030C0004 00:19:58: Attribute 25 39 43495343 00:19:58: Attribute 80 18
F5520A95 00:19:58: RADIUS: EAP-login: length of eap packet = 4 Cat6K#
```

Informations connexes

- Exemple de configuration de l'authentification IEEE 802.1x avec Catalyst 6500/6000 exécutant CatOS
- Instructions pour le déploiement du Cisco Secure ACS pour des serveurs de Windows Nt/2000 dans un environnement de commutateur Cisco Catalyst
- RFC 2868 : Attributs RADIUS pour le support de Protocol de tunnel
- Configurer l'authentification basée sur port de 802.1X d'IEEE
- Support pour les produits LAN
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems