Authentification de la gamme 5760/3850 WLC PEAP avec l'exemple de configuration de Microsoft NPS

ID de document : 117684

Mis à jour : Mai 05, 2014

Contribué par Surendra BG, ingénieur TAC Cisco.

Produits connexes

- Contrôleurs LAN de radio de gamme Cisco 5700
- Service RADIUS (Remote Authentication Dial-In User Service)

Contenu

Introduction

Ce document décrit comment configurer le Protected Extensible Authentication Protocol (PEAP) avec l'authentification de la version 2 (MS-CHAP v2) de Microsoft Challenge Handshake Authentication Protocol sur un déploiement Sans fil du RÉSEAU LOCAL d'Access convergé par Cisco (WLAN) avec le policy server de réseau Microsoft (NPS) en tant que serveur de RAYON.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de ces thèmes avant que vous tentiez la configuration décrite dans ce document :

- Installation de base de version 2008 de Microsoft Windows
- Cisco a convergé l'installation de contrôleur WLAN d'Access

Assurez-vous que ces exigences sont répondues avant que vous tentiez cette configuration :

- Installez le système d'exploitation de version 2008 de Microsoft Windows Server (OS) sur chacun des serveurs dans le laboratoire de test.
- Mettez à jour tous les packs de services.
- Installez les contrôleurs et le Point d'accès léger (recouvrements).
- Configurez les dernières mises à jour logicielles.

> Remarque: Pour l'installation initiale et les informations de configuration pour Cisco a convergé des contrôleurs WLAN d'Access, se rapporte à l'article de Cisco d'exemple de configuration de commutateur du contrôleur CT5760 et du Catalyst 3850.

Composants utilisés

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

- Version 3.3.2 de contrôleur WLAN de gamme Cisco 5760 (local de câblage de nouvelle génération (NGWC))
- RECOUVREMENT de gamme Cisco 3602
- Microsoft Windows XP avec le suppliant d'Intel PROset
- Serveur de version 2008 de Microsoft Windows qui exécute NPS avec des rôles de contrôleur de domaine
- Commutateur de gamme Cisco Catalyst 3560

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

Les utilisations PEAP transportent la Sécurité de niveau (TLS) afin de créer un canal chiffré entre un client authentifiant PEAP, tel qu'un ordinateur portable sans fil, et un authentificateur PEAP, tel que Microsoft NPS ou n'importe quel serveur de RAYON. Le PEAP ne spécifie pas une méthode d'authentification mais fournit la Sécurité supplémentaire pour d'autres protocoles d'authentification extensible (eap), comme EAP-MS-CHAP v2, qui peut fonctionner par le canal Tls-chiffré qui est fourni par PEAP. La procédure d'authentification PEAP se compose de deux phases principales.

Première phase PEAP : La Manche Tls-chiffrée

Les associés de client sans fil avec le Point d'accès (AP). Une association d'IEEE 802.11-based fournit un système ouvert ou une authentification principale partagée avant qu'une association sécurisée soit créée entre le client et l'AP. Après que l'association d'IEEE 802.11-based soit avec succès établie entre le client et l'AP, la session de TLS est étée en pourparlers avec AP.

Après l'authentification est avec succès terminée entre le client sans fil et le NPS, la session de TLS est négociée entre le client et le NPS. La clé qui est dérivée dans cette négociation est utilisée afin de chiffrer toute la transmission ultérieure.

Deuxième phase PEAP : communication authentifiée d'EAP

La transmission d'EAP, qui inclut la négociation d'EAP, se produit à l'intérieur de du canal de TLS qui est créé par PEAP dans la première phase de la procédure d'authentification PEAP. Le NPS authentifie le client sans fil avec EAP-MS-CHAP v2. Le RECOUVREMENT et les messages en avant de contrôleur seulement entre le client sans fil et le serveur de RAYON. Le contrôleur WLAN (WLC) et le RECOUVREMENT ne peuvent pas déchiffrer les messages parce que le WLC n'est pas le point final de TLS.

Voici l'ordre de message de RAYON pour une tentative réussie d'authentification, où l'utilisateur fournit les qualifications basées sur mot de passe valides avec PEAP-MS-CHAP v2 :

1. Le NPS envoie un message de demande d'identité au client :
   `EAP-Request/Identity`
2. Le client répond avec un message de réponse d'identité :
   `EAP-Response/Identity`
3. Le NPS envoie un message de défi MS-CHAP v2 :
   `EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge)`
4. Le client répond avec un défi et la réponse MS-CHAP v2 :
   `EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response)`
5. Le NPS répond avec un paquet de succès MS-CHAP v2 quand le serveur authentifie avec succès le client :
   `EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success)`
6. Le client répond avec un paquet de succès MS-CHAP v2 quand le client authentifie avec succès le serveur :
   `EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success)`
7. Le NPS envoie une Eap-type-longueur-valeur (TLV) qui indique l'authentification réussie.
8. Le client répond avec un message de réussite d'état EAP-TLV.
9. Le serveur se termine l'authentification et envoie un message d'Eap-succès en texte brut. Si

des VLAN sont déployés pour l'isolation du client, les attributs VLAN sont inclus dans ce message.

Configurez

Employez cette section afin de configurer le PEAP avec l'authentification MS-CHAP v2 sur un déploiement d'Access convergé par Cisco WLC avec Microsoft NPS en tant que serveur de RAYON.

Diagramme du réseau

Dans cet exemple, le serveur de version 2008 de Microsoft Windows exécute ces rôles :

- Contrôleur de domaine pour le domaine de **wireless.com**
- Serveur de Système de noms de domaine (DNS)
- Serveur d'Autorité de certification (CA)
- NPS afin d'authentifier les utilisateurs de sans fil
- Répertoire actif (AD) afin de mettre à jour la base de données utilisateur

Le serveur se connecte au réseau câblé par un commutateur de la couche 2 (L2), comme affiché. Les WLC et le RECOUVREMENT enregistré se connectent également au réseau par le commutateur L2.

Les clients sans fil emploient l'accès protégé par Wi-Fi 2 (WPA2) - authentification PEAP-MS-CHAP v2 afin de se connecter au réseau Sans fil.

Configurations

La configuration qui est décrite dans cette section est terminée dans deux étapes :

1. Configurez la gamme 5760/3850 WLC avec le CLI ou le GUI.

2. Configurez le serveur de version 2008 de Microsoft Windows pour NPS, le contrôleur de domaine, et les comptes d'utilisateur sur l'AD.

Configurez Access convergé WLCs avec le CLI

Terminez-vous ces étapes afin de configurer le WLAN pour le client requis VLAN et le tracer à la liste de méthode d'authentification avec le CLI :

> Remarque: Assurez-vous que le **système de dot1x contrôle authentique** est activé sur le WLC, ou le dot1x ne fonctionne pas.

1. Activez la caractéristique de **nouveau modèle d'AAA**.

2. Configurez le serveur de RAYON.

3. Ajoutez le serveur dans le groupe de serveurs.

4. Tracez le groupe de serveurs à la liste de méthode.

5. Tracez la liste de méthode au WLAN.

```
aaa new-model
!
!
aaa group server radius Microsoft_NPS
 server name Microsoft_NPS
!
aaa authentication dot1x Microsoft_NPS group Microsoft_NPS aaa authorization network
Microsoft_NPS group Microsoft_NPS
radius server Microsoft_NPS
 address ipv4 10.104.208.96 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 10
 key Cisco123 wlan Microsoft_NPS 8 Microsoft_NPS
 client vlan VLAN0020
 no exclusionlist
 security dot1x authentication-list Microsoft_NPS
 session-timeout 1800
 no shutdown
```

Configurez Access convergé WLCs avec le GUI

Terminez-vous ces étapes afin de configurer Access convergé WLCs avec le GUI :

1. Activez le **dot1x system-auth-control** :

2. Naviguez vers la **configuration** > la **Sécurité** > l'**AAA** afin d'ajouter le serveur de RAYON :

3. Naviguez vers le **RAYON > les serveurs**, cliquez sur New, et mettez à jour l'adresse IP du serveur de RAYON avec le secret partagé. Le secret partagé devrait apparier le secret partagé qui est aussi bien configuré sur le serveur de RAYON.

   Après que vous configuriez le serveur de RAYON, l'onglet de serveur devrait ressembler à ceci :

4. Configurez un groupe de serveurs et un **rayon** choisi pour le type de groupe. Puis, ajoutez le serveur de RAYON que vous avez créé dans l'étape précédente :

Le groupe de serveurs devrait ressembler à ceci après la configuration :

5. **Le dot1x** choisi pour le type de liste de méthode d'authentification et le **groupe** pour le groupe tapent. Puis, tracez le groupe de serveurs que vous avez configuré dans l'étape précédente :

   La liste de méthode d'authentification devrait ressembler à ceci après la configuration :

6. **Réseau** choisi pour le type et le **groupe de** liste d'authorization method pour le type de groupe. Puis, tracez le groupe de serveurs que vous avez configuré dans l'étape précédente :

   La liste d'authorization method devrait ressembler à ceci après la configuration :

7. Naviguez **pour configurer > radio** et cliquer sur le **WLAN** tableau configurez un nouveau WLAN auquel les utilisateurs peuvent se connecter et devenir authentifiés par le serveur de Microsoft NPS avec l'authentification EAP :

   L'onglet de la Sécurité L2 devrait ressembler à ceci après la configuration :

8. Tracez la liste de méthode que vous avez configurée dans les étapes précédentes. Ceci aide à authentifier le client au serveur correct.

Configuration sur le serveur de version 2008 de Microsoft Windows

Cette section décrit une configuration complète du serveur de version 2008 de Microsoft Windows. La configuration est terminée dans six étapes :

1. Configurez le serveur comme contrôleur de domaine.
2. Installez et configurez le serveur en tant que serveur CA.
3. Installez le NPS.

4. Installez un certificat.

5. Configurez le NPS pour l'authentification PEAP.

6. Ajoutez les utilisateurs à l'AD.

Configurez le serveur de Microsoft Windows 2008 comme contrôleur de domaine

Terminez-vous ces étapes afin de configurer le serveur de version 2008 de Microsoft Windows comme contrôleur de domaine :

1. Naviguez **pour commencer > gestionnaire du serveur > rôles > ajouter des rôles**.

2. Cliquez sur **Next** (Suivant).

3. Cochez la case de **services de domaine de Répertoire actif** et cliquez sur Next.

4. Passez en revue l'**introduction aux services de domaine de Répertoire actif** et cliquez sur Next.

5. Le clic **installent** afin de commencer le processus d'installation.

   L'installation poursuit et se termine.

6. Cliquez sur **étroitement cet assistant et lancez l'assistant d'installation de services de domaine de Répertoire actif (dcpromo.exe) afin de** continuer l'installation et la configuration de l'AD.

7. Cliquez sur Next afin d'exécuter l'**assistant d'installation de services de domaine de Répertoire actif**.

8. Examinez les informations sur la **compatibilité du système d'exploitation** et cliquez sur Next.

9. Cliquez sur la **création un nouveau domaine dans une nouvelle** case d'option de **forêt** et cliquez sur Next **afin de créer un nouveau domaine.**

10. Écrivez le plein nom DNS pour le nouveau domaine (**wireless.com** dans cet exemple) et cliquez sur Next.

11. Sélectionnez le **niveau fonctionnel de forêt** pour votre domaine et cliquez sur Next.

12. Sélectionnez le **niveau fonctionnel de domaine** pour votre domaine et cliquez sur Next.

13. Cochez la case de **serveur DNS** et cliquez sur Next.

14. Cliquez sur **oui** quand la fenêtre externe d'**assistant d'installation de services de domaine de Répertoire actif** apparaît afin de créer une nouvelle zone dans les DN pour le domaine.

15. Sélectionnez les répertoires que vous voulez que l'AD l'utilise pour des fichiers et clique sur Next.

16. Entrez le mot de passe administrateur et cliquez sur Next.

17. Passez en revue vos sélections et cliquez sur Next.

    Le montant d'installation.

18. Cliquez sur Finish **afin de fermer l'assistant.**

19. Redémarrez le serveur pour que les modifications les prennent effet.

Installez et configurez le serveur de version 2008 de Microsoft Windows en tant que serveur CA

Le PEAP avec EAP-MS-CHAP v2 valide le serveur de RAYON basé sur le certificat qui est présent sur le serveur. Supplémentaire, le certificat de serveur doit être délivré par un public CA qui est de confiance par l'ordinateur client. C'est-à-dire, le certificat de CA public existe déjà dans le répertoire d'Autorité de certification racine approuvée sur la mémoire de certificat d'ordinateur client.

Terminez-vous ces étapes afin de configurer le serveur de version 2008 de Microsoft Windows en tant que serveur CA qui fournit le certificat au NPS :

1. Naviguez **pour commencer > gestionnaire du serveur > rôles > ajouter des rôles**.

2. Cliquez sur **Next** (Suivant).

3. Cochez la case de **services de certificat de Répertoire actif** et cliquez sur Next.

4. Passez en revue l'**introduction aux services de certificat de Répertoire actif** et cliquez sur Next.

5. Cochez la case d'**autorité de certification** et cliquez sur Next.

6. Cliquez sur la case d'option d'**entreprise** et cliquez sur Next.

7. Cliquez sur la case d'option de la **racine CA** et cliquez sur Next.

8. Cliquez sur la **création une nouvelle** case d'option de **clé privée** et cliquez sur Next.

9. Cliquez sur Next dans le **chiffrement configurant pour la** fenêtre **CA**.

10. Cliquez sur Next afin de recevoir le **nom commun pour ce** nom par défaut **CA**.

11. Sélectionnez la durée pour laquelle le certificat de CA est valide et cliquez sur Next.

12. Cliquez sur Next afin de recevoir l'emplacement par défaut d'**emplacement de base de données de certificat**.

13. Passez en revue la configuration et le clic **installent** afin de commencer les **services de certificat de Répertoire actif**.

14. Après que l'installation soit terminée, **fin de** clic.

Installez le NPS sur le serveur de version 2008 de Microsoft Windows

> Remarque: Avec l'installation qui est décrite dans cette section, le NPS est utilisé pendant qu'un serveur de RAYON afin d'authentifier les clients sans fil avec l'authentification PEAP.

Terminez-vous ces étapes afin d'installer et configurer le NPS sur le serveur de version 2008 de Microsoft Windows :

1. Naviguez **pour commencer > gestionnaire du serveur > rôles > ajouter des rôles**.

2. Cliquez sur **Next** (Suivant).

3. Cochez la case de **politique réseau et de services d'accès** et cliquez sur Next.

4. Passez en revue l'**introduction à la politique réseau et aux services d'accès** et cliquez sur Next.

5. Cochez la case de **serveur de politique réseau** et cliquez sur Next.

6. Passez en revue la confirmation et le clic **installent**.

   Après que l'installation soit complète, un écran semblable à ceci devrait apparaître :

7. Cliquez sur **Fermer**.

Installez un certificat

Terminez-vous ces étapes afin d'installer le certificat d'ordinateur pour le NPS :

1. Cliquez sur le **début**, entrez dans le Microsoft Management Console (MMC), et l'appuyez sur **entrent**.
2. Naviguez **pour classer > ajout/suppression SNAP-dans**.
3. Choisissez les **Certificats** et cliquez sur Add.
4. Cliquez sur la case d'option de **compte d'ordinateur** et cliquez sur Next.
5. Cliquez sur la case d'option d'**ordinateur local** et cliquez sur Finish.
6. Cliquez sur OK afin de retourner au MMC.
7. Développez les **Certificats (ordinateur local)** et les répertoires **personnels**, et cliquez sur les **Certificats**.
8. Cliquez avec le bouton droit l'espace blanc dans le certificat de CA, et choisissez **tous les tâches > certificat de demande nouveau**.

9. Cliquez sur **Next** (Suivant).

10. Cliquez sur la case de **contrôleur de domaine**, et le clic **s'inscrivent**.

    Remarque: Si l'authentification client échoue en raison d'une erreur de certificat d'EAP, alors assurez-vous que toutes les cases sont vérifiées cette page d'**inscription de certificat** avant que vous clic **vous inscriviez**. Ceci crée approximativement trois Certificats.

11. Cliquez sur Finish une fois que le certificat est installé.

    Le certificat NPS est maintenant installé.

12. Assurez cette **authentification client, authentification de serveur** apparaît dans la colonne de buts visés pour le certificat.

Configurez le service de serveur de politique réseau pour l'authentification PEAP-MS-CHAP v2

Terminez-vous ces étapes afin de configurer le NPS pour l'authentification :

1. Naviguez **pour commencer > les outils d'administration** > le **serveur de politique réseau**.
2. Cliquez avec le bouton droit **NPS (gens du pays)** et choisissez le **serveur de registre dans le Répertoire actif**.
3. Cliquez sur **OK**.
4. Cliquez sur **OK**.
5. Ajoutez le WLC en tant que client d'Authentification, autorisation et comptabilité (AAA) sur le NPS.
6. Développez les **clients RADIUS et les serveurs**. Cliquez avec le bouton droit les **clients RADIUS** et choisissez le **nouveau client RADIUS** :

7. Écrivez un nom (**WLC** dans cet exemple), l'adresse IP de Gestion du WLC (**10.105.135.178** dans cet exemple), et un secret partagé.

   Remarque: Le même secret partagé est utilisé afin de configurer le WLC.

8. Cliquez sur OK afin de retourner à l'écran précédent.

9. Créez une nouvelle politique réseau pour les utilisateurs de sans fil. Développez les **stratégies**, cliquez avec le bouton droit les **politiques réseau**, et choisissez **nouveau** :

10. Écrivez un nom de stratégie pour cette règle (**PEAP** dans cet exemple) et cliquez sur Next.

11. Afin de configurer cette stratégie pour permettre seulement les utilisateurs Sans fil de domaine, ajoutez ces trois conditions et cliquez sur Next :

12. Cliquez sur la case d'option **autorisation d'accès** Afin d'accorder les tentatives de connexion qui apparient cette stratégie et cliquent sur Next.

13. Désactivez tout les **moins des méthodes d'authentification sécurisées** :

14. Cliquez sur Add, sélectionnez **Microsoft :** Le type **protégé d'**EAP de l'**EAP (PEAP)**, et cliquent sur OK **afin d'activer le PEAP.**

15. **Microsoft** choisi **: L'EAP protégé (PEAP)** et cliquent sur Edit. Assurez-vous que le certificat précédent-créé de contrôleur de domaine est sélectionné dans la liste déroulante émise par certificat et cliquez sur l'**ok**.

16. Cliquez sur **Next** (Suivant).

17. Cliquez sur **Next** (Suivant).

18. Cliquez sur **Next** (Suivant).

19. Cliquez sur **Finish** (Terminer).

    Remarque: Personne à charge sur vos besoins, vous pourriez devoir configurer des **stratégies de demande de connexion** sur le NPS afin de permettre le profil PEAP ou la stratégie.

Ajoutez les utilisateurs à l'Active Directory

Remarque: Dans cet exemple, la base de données utilisateur est mise à jour sur l'AD.

Terminez-vous ces étapes afin d'ajouter des utilisateurs à la base de données d'AD :

1. Naviguez **pour commencer** > des **outils d'administration** > des **utilisateurs et des ordinateurs de Répertoire actif**.

2. Dans l'arborescence de la console d'utilisateurs et d'ordinateurs de Répertoire actif, développez le domaine, cliquez avec le bouton droit les **utilisateurs** et **nouveau**, et choisissez l'**utilisateur**.

3. Dans le nouvel objet - La boîte de dialogue d'utilisateur, écrivent le nom de l'utilisateur de sans fil. Cet exemple utilise **Client1** dans le domaine de prénom et **Client1** dans le nom de connexion d'utilisateur mettent en place. Cliquez sur **Next** (Suivant).

4. Dans le nouvel objet - La boîte de dialogue d'utilisateur, entrent un mot de passe de votre choix dans les domaines de mot de passe et de confirmation du mot de passe. Décochez l'**utilisateur doit changer le mot de passe à la prochaine** case de **connexion** et cliquer sur Next.

5. Dans le nouvel objet - La boîte de dialogue d'utilisateur, cliquent sur Finish.

6. Répétez les étapes 2 à 4 afin de créer des comptes d'utilisateur supplémentaires.

Vérifiez

Terminez-vous ces étapes afin de vérifier votre configuration :

1. Recherchez l'identification d'ensemble de services (SSID) sur la machine cliente.

2. Assurez-vous que le client est connecté avec succès :

Dépannez

> Remarque: Cisco recommande que vous employiez des suivis afin de dépanner les questions Sans fil. Des suivis sont enregistrés dans la mémoire tampon circulaire et ne sont pas processeur intensif.

Permettez à ces suivis afin d'obtenir les **logs L2 authentiques** :

- **le niveau groupe-radio-sécurisé de set trace mettent au point**
- **MAC groupe-radio-sécurisé 0017.7C2F.B69A de filtre de set trace**

Permettez à ces suivis afin d'obtenir les **événements d'AAA de dot1x** :

- **l'AAA du set trace wcm-dot1x de niveau mettent au point**
- **MAC 0017.7C2F.B69A de filtre d'AAA du set trace wcm-dot1x**

Permettez à ces suivis afin de recevoir les **événements DHCP** :

- **les événements DHCP de set trace de niveau mettent au point**
- **MAC 0017.7C2F.B69A de filtre d'événements DHCP de set trace**

Permettez à ces suivis afin de désactiver les suivis et effacer la mémoire tampon :

- **les système-filtrer-suivis de contrôle de set trace effacent**
- **par défaut de niveau d'AAA du set trace wcm-dot1x**
- **filtre d'AAA du set trace wcm-dot1x aucun**
- **par défaut groupe-radio-sécurisé de niveau de set trace**
- **filtre groupe-radio-sécurisé de set trace aucun**

Écrivez les système-filtrer-**suivis de show trace** commandent afin de visualiser les suivis :

```
[04/23/14 21:27:51.963 IST 1 8151] 0017.7c2f.b69a Adding mobile on LWAPP AP
 1caa.076f.9e10 (0)
[04/23/14 21:27:51.963 IST 2 8151] 0017.7c2f.b69a Local Policy:  Created MSCB
 Just AccessVLAN = 0 and SessionTimeout  is 0 and apfMsTimeout is 0

[04/23/14 21:27:51.963 IST 8 8151] 0017.7c2f.b69a Local Policy:Setting local
 bridging VLAN  name VLAN0020 and VLAN ID  20
```

[04/23/14 21:27:51.963 IST 9 8151] 0017.7c2f.b69a Applying WLAN ACL policies
to client
[04/23/14 21:27:51.963 IST a 8151] 0017.7c2f.b69a No Interface ACL used for
Wireless client in WCM(NGWC)
[04/23/14 21:27:51.963 IST b 8151] 0017.7c2f.b69a Applying site-specific IPv6
override for station 0017.7c2f.b69a - vapId 8, site 'test',
interface 'VLAN0020'
[04/23/14 21:27:51.963 IST c 8151] 0017.7c2f.b69a Applying local bridging
Interface Policy for station 0017.7c2f.b69a - vlan 20,
interface 'VLAN0020'
[04/23/14 21:27:51.963 IST d 8151] 0017.7c2f.b69a
**** Inside applyLocalProfilingPolicyAction ****

04/23/14 21:27:51.963 IST f 8151] 0017.7c2f.b69a Local Profiling Values :
isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
sessionTimeout=0, isSessionTORecdInDelete = 0 ProtocolMap = 0 ,
applyPolicyAtRun= 0
[04/23/14 21:27:51.963 IST 10 8151] 0017.7c2f.b69a ipv4ACL = [],
ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[**04/23/14 21:27:51.963 IST 11 8151] 0017.7c2f.b69a STA - rates (4):**
130 132 139 150 0 0 0 0 0 0 0 0 0 0 0 0
[04/23/14 21:27:51.963 IST 12 8151] 0017.7c2f.b69a STA - rates (12):
130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
[04/23/14 21:27:51.963 IST 13 8151] 0017.7c2f.b69a Processing RSN IE type 48,
length 20 for mobile 0017.7c2f.b69a
[04/23/14 21:27:51.963 IST 14 8151] 0017.7c2f.b69a Received RSN IE with 0
PMKIDsfrom mobile 0017.7c2f.b69a

[04/23/14 21:27:51.964 IST 1b 8151] 0017.7c2f.b69a **Change state to AUTHCHECK**
(2) last state START (0)

[04/23/14 21:27:51.964 IST 1c 8151] 0017.7c2f.b69a Change state to 8021X_REQD
(3) last state AUTHCHECK (2)

[04/23/14 21:27:51.964 IST 25 8151] 0017.7c2f.b69a apfProcessAssocReq
(apf_80211.c:6272) **Changing state for mobile 0017.7c2f.b69a on AP**
1caa.076f.9e10 from Associated to Associated

[04/23/14 21:27:51.971 IST 26 8151] 0017.7c2f.b69a 1XA: Initiating
authentication
[04/23/14 21:27:51.971 IST 27 8151] 0017.7c2f.b69a 1XA: Setting reauth
timeout to 1800 seconds
[04/23/14 21:27:51.971 IST 28 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 0

[04/23/14 21:27:51.971 IST 29 8151] 0017.7c2f.b69a 1XA: Allocated uid 40
[04/23/14 21:27:51.971 IST 2a 8151] 0017.7c2f.b69a 1XA: **Calling Auth Mgr**
to authenticate client 4975000000003e uid 40
[04/23/14 21:27:51.971 IST 2b 8151] 0017.7c2f.b69a 1XA: **Session Start from**
wireless client

[04/23/14 21:27:51.971 IST 2c 8151] 0017.7c2f.b69a Session Manager Call Client
4975000000003e, uid 40, capwap id 7ae8c000000013,Flag 0, Audit-Session ID
0a6987b25357e2ff00000028, **method list Microsoft_NPS**, policy name (null)

[04/23/14 21:27:51.971 IST 2d 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca3] Session start request from Client[1] for 0017.7c2f.b69a
(method: Dot1X, method list: Microsoft_NPS, aaa id: 0x00000028), policy
[04/23/14 21:27:51.971 IST 2e 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca3] - client iif_id: 4975000000003E, session ID:
0a6987b25357e2ff00000028 for 0017.7c2f.b69a

```
[04/23/14 21:27:51.972 IST 43 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting !EAP_RESTART on Client 0x22000025
[04/23/14 21:27:51.972 IST 44 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:enter connecting state
[04/23/14 21:27:51.972 IST 45 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025: restart connecting
[04/23/14 21:27:51.972 IST 46 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting RX_REQ on Client 0x22000025
[04/23/14 21:27:51.972 IST 47 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025: authenticating state entered
[04/23/14 21:27:51.972 IST 48 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:connecting authenticating action
[04/23/14 21:27:51.972 IST 49 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting AUTH_START for 0x22000025
[04/23/14 21:27:51.972 IST 4a 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:entering request state
[04/23/14 21:27:51.972 IST 4b 291] ACCESS-METHOD-DOT1X-NOTF:
 [0017.7c2f.b69a, Ca3] Sending EAPOL packet
[04/23/14 21:27:51.972 IST 4c 291] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Platform changed src mac  of EAPOL packet
[04/23/14 21:27:51.972 IST 4d 291] ACCESS-METHOD-DOT1X-NOTF:
 [0017.7c2f.b69a, Ca3] Sending out EAPOL packet
[04/23/14 21:27:51.972 IST 4e 291] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] EAPOL packet sent to client 0x22000025


[04/23/14 21:27:52.112 IST 7d 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[04/23/14 21:27:52.112 IST 7e 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:52.112 IST 7f 211] AAA SRV(00000000): Authen method=SERVER_GROUP
 Microsoft_NPS
[04/23/14 21:27:52.112 IST 80 211] AAA SRV(00000000): Selecting SG = DIAMETER
[04/23/14 21:27:52.113 IST 81 186] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Queuing an EAPOL pkt on Authenticator Q
[04/23/14 21:27:52.113 IST 82 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting EAPOL_EAP for 0x22000025
[04/23/14 21:27:52.278 IST 83 220] AAA SRV(00000000): protocol reply
 GET_CHALLENGE_RESPONSE for Authentication
[04/23/14 21:27:52.278 IST 84 220] AAA SRV(00000000): Return Authentication
 status=GET_CHALLENGE_RESPONSE
[04/23/14 21:27:52.278 IST 85 291] ACCESS-METHOD-DOT1X-DEB:[0017.7c2f.b69a,Ca3]
 Posting EAP_REQ for 0x22000025
```

Voici le reste de l'EAP sorti :

```
[04/23/14 21:27:54.690 IST 12b 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:54.690 IST 12c 211] AAA SRV(00000000): Authen
 method=SERVER_GROUP Microsoft_NPS
[04/23/14 21:27:54.690 IST 12d 211] AAA SRV(00000000): Selecting SG =
 DIAMETER
[04/23/14 21:27:54.694 IST 12e 220] AAA SRV(00000000): protocol reply PASS
 for Authentication
[04/23/14 21:27:54.694 IST 12f 220] AAA SRV(00000000): Return Authentication
 status=PASS
[04/23/14 21:27:54.694 IST 130 189] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Received an EAP Success


[04/23/14 21:27:54.695 IST 186 8151] 0017.7c2f.b69a Starting key exchange with
 mobile - data forwarding is disabled
[04/23/14 21:27:54.695 IST 187 8151] 0017.7c2f.b69a 1XA: Sending EAPOL message
 to mobile, WLAN=8 AP WLAN=8
[04/23/14 21:27:54.706 IST 188 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL
 message (len 121) from mobile
```

```
[04/23/14 21:27:54.706 IST 189 8151] 0017.7c2f.b69a 1XA: Received EAPOL-Key
 from mobile
[04/23/14 21:27:54.706 IST 18a 8151] 0017.7c2f.b69a 1XK: Received EAPOL-key in
 PTK_START state (msg 2) from mobile
[04/23/14 21:27:54.706 IST 18b 8151] 0017.7c2f.b69a 1XK: Stopping retransmission
 timer
[04/23/14 21:27:54.706 IST 18c 8151] 0017.7c2f.b69a 1XA: Sending EAPOL message
 to mobile, WLAN=8 AP WLAN=8
[04/23/14 21:27:54.717 IST 18d 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL
 message (len 99) from mobile
[04/23/14 21:27:54.717 IST 18e 8151] 0017.7c2f.b69a 1XA: Received EAPOL-Key
 from mobile
[04/23/14 21:27:54.717 IST 18f 8151] 0017.7c2f.b69a 1XK: Received EAPOL-key in
 PTKINITNEGOTIATING state (msg 4) from mobile
[04/23/14 21:27:54.717 IST 190 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 1

[04/23/14 21:27:54.717 IST 191 8151] 0017.7c2f.b69a 1XK: Key exchange complete
 - updating PEM
[04/23/14 21:27:54.717 IST 192 8151] 0017.7c2f.b69a apfMs1xStateInc
[04/23/14 21:27:54.717 IST 193 8151] 0017.7c2f.b69a Change state to
 L2AUTHCOMPLETE (4) last state 8021X_REQD (3)


[04/23/14 21:27:58.277 IST 1df 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:27:58.277 IST 1e0 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:28:05.279 IST 1e1 269] DHCPD: Adding binding to hash tree
[04/23/14 21:28:05.279 IST 1e2 269] DHCPD: DHCPOFFER notify setup address
 20.20.20.5 mask 255.255.255.0


[04/23/14 21:28:05.306 IST 1f4 8151] 0017.7c2f.b69a Change state to RUN (20)
 last state DHCP_REQD (7)
```


Cisco relatif prennent en charge des discussions de la Communauté

Mis à jour : Mai 05, 2014
ID de document : 117684