Authentification PPP par le biais des commandes ppp chap hostname et ppp authentication chap callin

Contenu

Introduction

La négociation PPP implique plusieurs étapes telles que la négociation du protocole de contrôle de liaison (LCP), l'authentification, et la négociation de protocole de contrôle de réseau (NCP). Si les deux côtés ne peuvent pas convenir des bons paramètres, alors la connexion est terminée. Une fois le lien établi, les deux côtés s'authentifient utilisant le protocole d'authentification convenu pendant la négociation LCP. L'authentification doit être réussie avant de commencer la négociation NCP.

PPP prend en charge deux protocoles d’authentification : Le protocole d'authentification PAP (Password Authentication Protocol) et le protocole d'authentification CHAP (Challenge Handshake Authentication Protocol).

Conditions préalables

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions

utilisées pour les conseils techniques de Cisco.

Conditions requises

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- Logiciel Cisco IOS® version 11.2 ou ultérieure

Théorie générale

L'authentification PAP implique une connexion en deux étapes où le nom d'utilisateur et le mot de passe sont envoyés sur la liaison en texte clair ; par conséquent, l'authentification PAP ne fournit aucune protection contre la lecture et l'analyse de ligne.

L'authentification CHAP, en revanche, vérifie périodiquement l'identité du noeud distant à l'aide d'une connexion en trois étapes. Une fois la liaison PPP établie, l'hôte envoie un message de confirmation au noeud distant. Le noeud distant répond avec une valeur calculée à l'aide d'une fonction de hachage unidirectionnel. L'hôte compare la réponse à son propre calcul de la valeur de hachage attendue. Si les valeurs correspondent, l'authentification est reconnue; dans le cas contraire, la connexion prend fin.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'outil de recherche de commandes IOS

Configuration de l'authentification CHAP unidirectionnelle

Lorsque deux périphériques utilisent normalement l'authentification CHAP, chaque côté envoie un défi auquel l'autre côté répond et est authentifié par le demandeur. Chaque partie s'authentifie indépendamment l'une de l'autre. Si vous voulez utiliser des routeurs non-Cisco qui ne prennent pas en charge l'authentification par le routeur ou le périphérique appelant, vous devez utiliser la commande **ppp authentication chap callin**. Lors de l'utilisation de la commande **ppp authentication** avec le mot clé **callin**, Access Server authentifiera le périphérique distant uniquement si le périphérique distant a initié l'appel (par exemple, si le périphérique distant a appelé). Dans ce cas, l'authentification est spécifiée sur les appels entrants (reçus) uniquement.

Configuration d'un nom d'utilisateur différent du nom du routeur

Lorsqu'un routeur Cisco distant se connecte à un routeur central Cisco ou non Cisco d'un contrôle administratif différent, à un fournisseur d'accès à Internet (FAI) ou à un routeur de routeurs

centraux, il est nécessaire de configurer un nom d'utilisateur d'authentification différent du nom d'hôte. Dans ce cas, le nom d'hôte du routeur n'est pas fourni ou est différent à des moments différents (rotatif). En outre, le nom d'utilisateur et le mot de passe attribués par le FAI peuvent ne pas correspondre au nom d'hôte du routeur distant. Dans une telle situation, la commande **ppp chap hostname** est utilisée pour spécifier un autre nom d'utilisateur qui sera utilisé pour l'authentification.

Par exemple, considérez une situation dans laquelle plusieurs périphériques distants se connectent à un site central. En utilisant l'authentification CHAP normale, le nom d'utilisateur (qui serait le nom d'hôte) de chaque périphérique distant et un secret partagé doivent être configurés sur le routeur central. Dans ce scénario, la configuration du routeur central peut devenir longue et lourde à gérer ; cependant, si les périphériques distants utilisent un nom d'utilisateur différent de leur nom d'hôte, cela peut être évité. Le site central peut être configuré avec un nom d'utilisateur unique et un secret partagé qui peuvent être utilisés pour authentifier plusieurs clients de numérotation.

Diagramme du réseau

Si le routeur 1 lance un appel vers le routeur 2, le routeur 2 conteste le routeur 1, mais le routeur 1 ne conteste pas le routeur 2. Cela se produit car la commande **ppp authentication chap callin** est configurée sur le routeur 1. Ceci est un exemple d'authentification unidirectionnelle.

Dans cette configuration, la commande **ppp chap hostname alias-r1** est configurée sur le routeur 1. Le routeur 1 utilise « alias-r1 » comme nom d'hôte pour l'authentification CHAP au lieu de « r1 ». Le nom de la carte de numérotation du routeur 2 doit correspondre au nom d'hôte ppp chap du routeur 1 ; sinon, deux canaux B sont établis, un pour chaque direction.

Configurations

Routeur 1

```
!
 isdn switch-type basic-5ess
 !
 hostname r1
 !
 username r2 password 0 cisco
 ! -- Hostname of other router and shared secret !
interface BRI0/0 ip address 20.1.1.1 255.255.255.0 no ip
directed-broadcast encapsulation ppp dialer map ip
20.1.1.2 name r2 broadcast 5772222
  dialer-group 1
  isdn switch-type basic-5ess
  ppp authentication chap callin
 ! -- Authentication on incoming calls only  ppp chap
hostname alias-r1
 ! -- Alternate CHAP hostname ! access-list 101 permit
```

```
ip any any dialer-list 1 protocol ip list 101 !
```

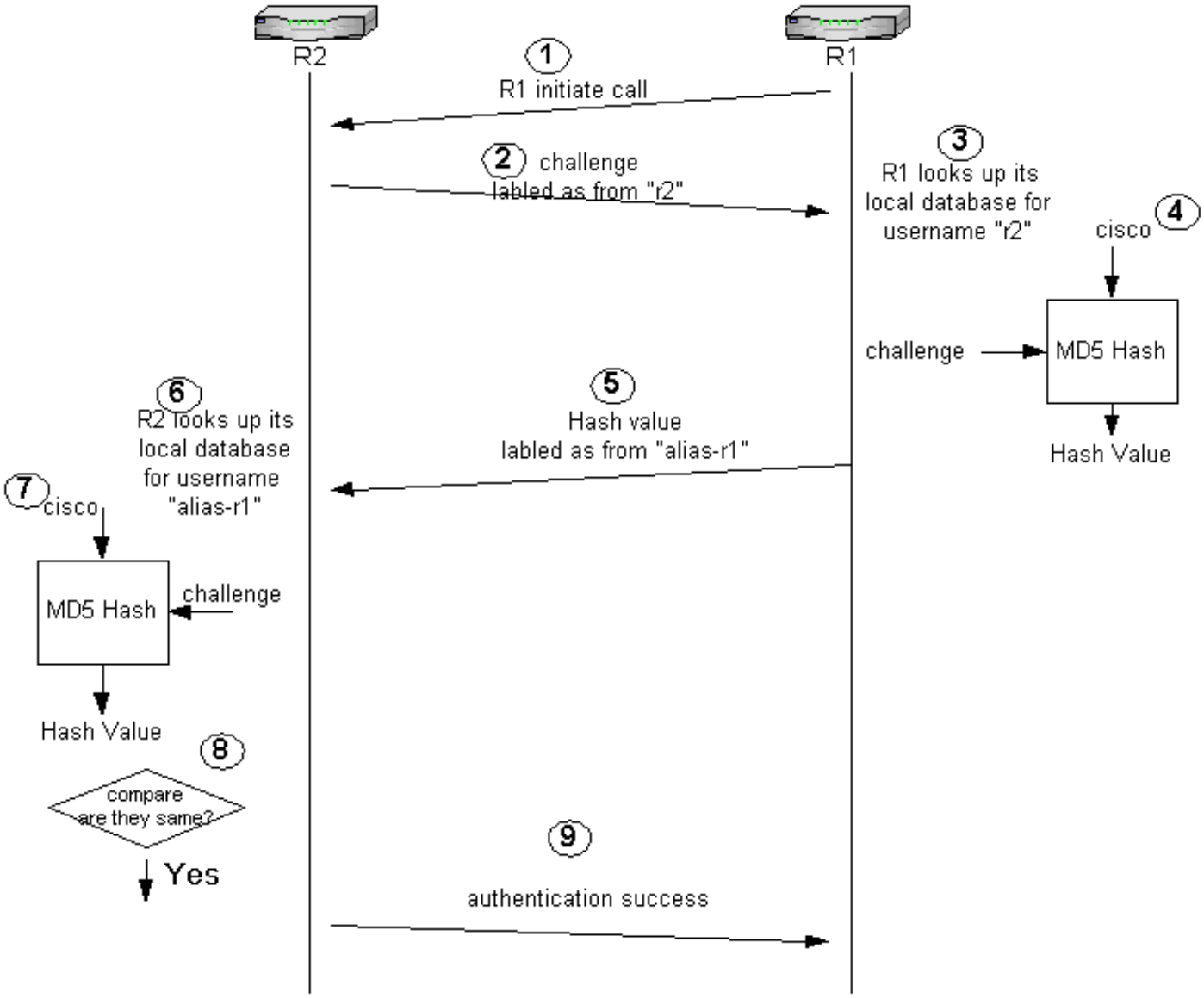
Routeur 2

```
!
 isdn switch-type basic-5ess
 !
 hostname r2
 !
 username alias-r1 password 0 cisco
  ! -- Alternate CHAP hostname and shared secret. ! --
The username must match the one in the ppp chap hostname
! -- command on the remote router.

 !
 interface BRI0/0
  ip address 20.1.1.2 255.255.255.0
  no ip directed-broadcast
  encapsulation ppp
  dialer map ip 20.1.1.1 name
  alias-r1 broadcast 5771111
   ! -- Dialer map name matches alternate hostname
"alias-r1". dialer-group 1 isdn switch-type basic-5ess
ppp authentication chap ! access-list 101 permit ip any
any dialer-list 1 protocol ip list 101 !
```

Explication de la configuration

Veuillez consulter les chiffres ci-dessous pour obtenir des explications :



1. Dans cet exemple, le routeur 1 lance l'appel. Puisque le routeur 1 est configuré avec la commande **ppp authentication chap callin**, il ne conteste pas l'appelant, qui est le routeur 2.
2. Lorsque le routeur 2 reçoit l'appel, il le conteste pour l'authentification. Par défaut pour cette authentification, le nom d'hôte du routeur est utilisé pour s'identifier. Si la commande **ppp chap hostname *name*** est configurée, un routeur utilise le nom à la place du nom d'hôte pour s'identifier. Dans cet exemple, le défi est étiqueté comme venant de « r2 ».
3. Le routeur 1 reçoit le défi du routeur 2 et recherche dans sa base de données locale le nom d'utilisateur « r2 ».
4. Le routeur 1 recherche le mot de passe « r2 », qui est « cisco ». Le routeur 1 utilise ce mot de passe et le défi du routeur 2 comme paramètres d'entrée de la fonction de hachage MD5. La valeur de hachage est générée.
5. Le routeur 1 envoie la valeur de sortie de hachage au routeur 2. Ici, puisque la commande **ppp chap hostname** est configurée comme « alias-r1 », la réponse est étiquetée comme provenant de « alias-r1. »
6. Le routeur 2 reçoit la réponse et recherche le nom d'utilisateur « alias-r1 » dans sa base de données locale pour le mot de passe.
7. Le routeur 2 trouve que le mot de passe de « alias-r1 » est « cisco ». Le routeur 2 utilise le mot de passe et la demande de confirmation envoyée précédemment au routeur 1 comme paramètres d'entrée pour la fonction de hachage MD5. La fonction de hachage génère une valeur de hachage.

8. Le routeur 2 compare la valeur de hachage qu'il a générée et celle qu'il reçoit du routeur 1.
9. Puisque les paramètres d'entrée (défi et mot de passe) sont identiques, la valeur de hachage est identique, ce qui donne une authentification réussie.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Avant d'essayer l'une des commandes debug, consultez Informations importantes sur les commandes debug

Exemple de sortie de débogage

Voici un exemple de sortie de la commande **debug ppp authentication** :

Routeur 1

```
r1#ping 20.1.1.2

 Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 20.1.1.2, timeout is 2 seconds:

  *Mar 1 20:06:27.179: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
  *Mar 1 20:06:27.183: %ISDN-6-CONNECT:
  Interface BRI0/0:1 is now connected to 5772222
  *Mar 1 20:06:27.187: BR0/0:1 PPP: Treating connection as a callout
  *Mar 1 20:06:27.223: BR0/0:1 CHAP: I CHALLENGE id 57 len 23 from "r2"
   ! -- Received a CHAP challenge from other router (r2) *Mar 1 20:06:27.223: BR0/0:1 CHAP:
Using alternate hostname alias-r1
  ! -- Using alternate hostname configured with ! -- ppp chap hostname command *Mar 1
20:06:27.223: BR0/0:1 CHAP: O RESPONSE id 57 Len 29 from "alias-r1" ! -- Sending response from
"alias-r1" ! -- which is the alternate hostname for r1 *Mar 1 20:06:27.243: BR0/0:1 CHAP: I
SUCCESS id 57 Len 4 ! -- Received CHAP authentication is successful ! -- Note that r1 is not
challenging r2 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 36/38/40 ms r1#
*Mar 1 20:06:28.243: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to
up r1# *Mar 1 20:06:33.187: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5772222 r2
```

Routeur 2

```
r2#

  20:05:20: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
  20:05:20: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5771111
  20:05:20: BR0/0:1 PPP: Treating connection as a callin
  20:05:21: BR0/0:1 CHAP: O CHALLENGE id 57 Len 23 from "r2"
  ! -- r2 is sending out a challenge 20:05:21: BR0/0:1 CHAP: I RESPONSE id 57 Len 29 from
"alias-r1"
 ! -- Received a response from alias-r1, ! -- which is the alternate hostname on r1 20:05:21:
BR0/0:1 CHAP: O SUCCESS id 57 Len 4 ! -- Sending out CHAP authentication is successful 20:05:22:
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to up 20:05:26: %ISDN-6-
CONNECT: Interface BRI0/0:1 is now connected to 5771111 alias-r1
```

Informations connexes

- Commandes PPP pour les réseaux étendus
- Comprendre l'authentification PPP et PPP
- Informations de débogage RNIS