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.

Le 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.

Composants utilisés

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

- Version de logiciel 11.2 ou ultérieures de Cisco IOS®

Théorie générale

L'authentification PAP implique une prise de contact bi-directionnelle où le nom d'utilisateur et mot de passe sont envoyés à travers le lien en texte clair ; par conséquent, l'authentification PAP n'assure aucune protection contre la lecture et raye le reniflement.

L'authentification CHAP, d'autre part, vérifie périodiquement l'identité du noeud distant utilisant une connexion en trois étapes. Après que le lien de PPP soit établi, l'hôte envoie un message de « défi » au noeud distant. Le noeud distant répond avec une valeur calculée utilisant une fonction de hachage irréversible. L'hôte vérifie la réponse contre son propre calcul de la valeur de hachage prévue. Si les valeurs s'assortissent, l'authentification est reconnue ; autrement, la connexion est terminée.

Configurez

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

Remarque: Pour trouver les informations complémentaires sur les commandes utilisées dans ce document, utilisez l'utilitaire de recherche de commande IOS

Configurer l'authentification CHAP unidirectionnelle

Quand deux périphériques utilisent normalement l'authentification CHAP, chaque côté envoie un défi auquel l'autre côté répond et est authentifié par le provocateur. Chacun dégrossit authentifie un un autre indépendamment. Si vous voulez opérer avec les Routeurs de non-Cisco qui ne prennent en charge pas l'authentification par le routeur ou le périphérique appelant, vous devez utiliser la commande de **callin de CHAP d'authentification de ppp**. Quand en utilisant l'**authentication command de ppp** avec le mot clé de **callin**, le serveur d'accès authentifiera seulement le périphérique distant si le périphérique distant initiait l'appel (par exemple, si le périphérique distant « appelé dans »). Dans ce cas, l'authentification est spécifiée aux appels (reçus) entrants seulement.

Configurant un nom d'utilisateur différent du nom du routeur

Quand un routeur de Cisco de distant se connecte à Cisco ou à un routeur central de non-Cisco

d'un contrôle administratif différent, d'un fournisseur de services Internet (ISP), ou d'un rotary des Routeurs centraux, il est nécessaire de configurer un nom d'utilisateur d'authentification qui est différent de l'adresse Internet. Dans cette situation, l'adresse Internet du routeur n'est pas fournie ou est différente aux heures différentes (rotary). En outre, le nom d'utilisateur et mot de passe qui est alloué par l'ISP peut ne pas être l'adresse Internet de routeur distant. Dans une telle situation, la commande de **ppp chap hostname** est utilisée de spécifier un nom d'utilisateur alternatif qui sera utilisé pour l'authentification.

Par exemple, considérez une situation où les plusieurs périphériques distants introduisent dans un lieu d'exploitation principal. Utilisant l'authentification CHAP normale, le nom d'utilisateur (qui serait l'adresse Internet) de chaque périphérique distant et un secret partagé doivent être configurés sur le routeur central. Dans ce scénario, la configuration du routeur central peut obtenir prolongé et encombrant pour gérer ; cependant, si les périphériques distants les utilisent un nom d'utilisateur qui est différent de leur adresse Internet ceci peut être évité. Le lieu d'exploitation principal peut être configuré avec un nom d'utilisateur simple et un secret partagé qui peuvent être utilisés pour authentifier de plusieurs clients entrant.

Diagramme du réseau

Si le routeur 1 initie un appel au Router2, le Router2 défierait le routeur 1, mais le routeur 1 ne contesterait pas le Router2. Ceci se produit parce que la commande de **callin de CHAP d'authentification de ppp** est configurée sur le routeur 1. C'est un exemple d'une authentification unidirectionnelle.

Dans cette installation, la commande du **ppp chap hostname alias-r1** est configurée sur des utilisations du routeur 1 du routeur 1. "alias-r1" en tant que son adresse Internet pour l'authentification CHAP au lieu de "r1." que le map name de numéroteur de Router2 devrait apparier le ppp chap hostname du routeur 1's ; autrement, 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 configuration

Veuillez se référer aux nombres au-dessous de ce graphique pour des explications :

1. Dans cet exemple, le routeur 1 initie l'appel. Puisque le routeur 1 est configuré avec la commande de **callin de CHAP d'authentification de ppp**, elle ne conteste pas l'appelant, qui est Router2.
2. Quand le Router2 reçoit l'appel, il conteste l'authentification de 1par de routeur. Par défaut pour cette authentification, l'adresse Internet du routeur est utilisée pour s'identifier. Si la commande de *nom de* **ppp chap hostname** est configurée, un routeur emploie le nom au lieu de l'adresse Internet pour s'identifier. Dans cet exemple, le défi est étiqueté pendant qu'il provient "r2."
3. Le routeur 1 reçoit le défi et les aspects du routeur 2's dans sa base de données locale pour le nom d'utilisateur "r2."
4. Le routeur 1 trouve le mot de passe de "r2", qui est « Cisco. » Le routeur 1 utilise ce mot de passe et le défi du Router2 comme des paramètres d'entrée de la fonction d'informations parasites de MD5. La valeur de hachage est générée.
5. Le routeur 1 envoie la valeur de sortie d'informations parasites au Router2. Ici, puisque la commande de **ppp chap hostname** est configurée pendant que "alias-r1," la réponse est étiqueté en tant que provenir "alias-r1."
6. Le Router2 reçoit la réponse et recherche le nom d'utilisateur de "alias-r1" dans sa base de données locale pour le mot de passe.
7. Découvertes de Router2 que le mot de passe pour "alias-r1" est « Cisco. » Le Router2 utilise le mot de passe et le défi envoyés plus tôt au routeur 1 comme des paramètres d'entrée pour la fonction d'informations parasites de MD5. La fonction d'informations parasites génère une valeur de hachage.
8. Le Router2 compare la valeur de hachage qu'il a générée et celle elle reçoit du routeur 1.
9. Puisque les paramètres d'entrée (défi et mot de passe) sont identiques, la valeur de hachage est même ayant pour résultat une authentification réussie.

Vérifiez

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

Dépannez

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

Avant de tenter des commandes de débogage l'unes des, voir s'il vous plaît les informations importantes sur des commandes de debug

Exemple de sortie de débogage

Être suit sortie témoin de la commande de **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 de PPP pour le réseau d'étendu
- Compréhension de l'authentification de PPP et de PPP
- Les informations de debug RNIS