Présentation et configuration de l'authentification PPP CHAP

Contenu

Introduction

Le protocole d'authentification CHAP (Challenge Handshake Authentication Protocol) (défini dans RFC 1994) vérifie l'identité de l'homologue au moyen d'un dialogue à trois. Les étapes exécutées par le protocole CHAP sont les suivantes :

1. Une fois la phase LCP (Link Control Protocol) terminée et le protocole CHAP négocié entre les deux périphériques, l'authentificateur envoie un message de défi à l'homologue.
2. L'homologue répond avec une valeur calculée via une fonction de hachage irréversible (MD5 - Message Digest 5).
3. L'authentificateur contrôle la réponse en la comparant à son propre calcul de la valeur de hachage prévue. Si les valeurs correspondent, l'authentification est réussie. Dans le cas contraire, la connexion prend fin.

Cette méthode d'authentification s'appuie sur un « secret » connu seulement de l'authentificateur et de l'homologue. Le secret n'est pas envoyé via la liaison. Bien que l'authentification soit seulement à sens unique, vous pouvez négocier le protocole CHAP dans les deux directions, avec l'aide du même secret défini pour l'authentification mutuelle.

Pour plus d'informations sur les avantages et les inconvénients du protocole CHAP, reportez-vous à RFC 1994 .

Conditions préalables

Conditions requises

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

- Comment activer PPP sur l'interface à l'aide de la commande **encapsulation ppp** .
- Résultats de la commande **debug ppp negotiation** . Pour plus d'informations, reportez-vous à Comprendre les sorties de la commande debug ppp negotiation.
- Capacité de dépannage lorsque la phase LCP (Link Control Protocol) n'est pas à l'état Open (Ouvert). Cela est dû au fait que la phase d'authentification PPP ne commence qu'une fois la phase LCP terminée et l'état défini comme Open (Ouvert). Si la commande **debug ppp negotiation** n'indique pas que la phase LCP est ouverte, vous devez résoudre ce problème avant de pouvoir poursuivre.

Remarque: Ce document ne traite pas du protocole MS-CHAP (version 1 ou version 2). Pour plus d'informations sur MS-CHAP, reportez-vous aux documents intitulés MS-CHAP Support (Support MS-CHAP) et MSCHAP version 2 .

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

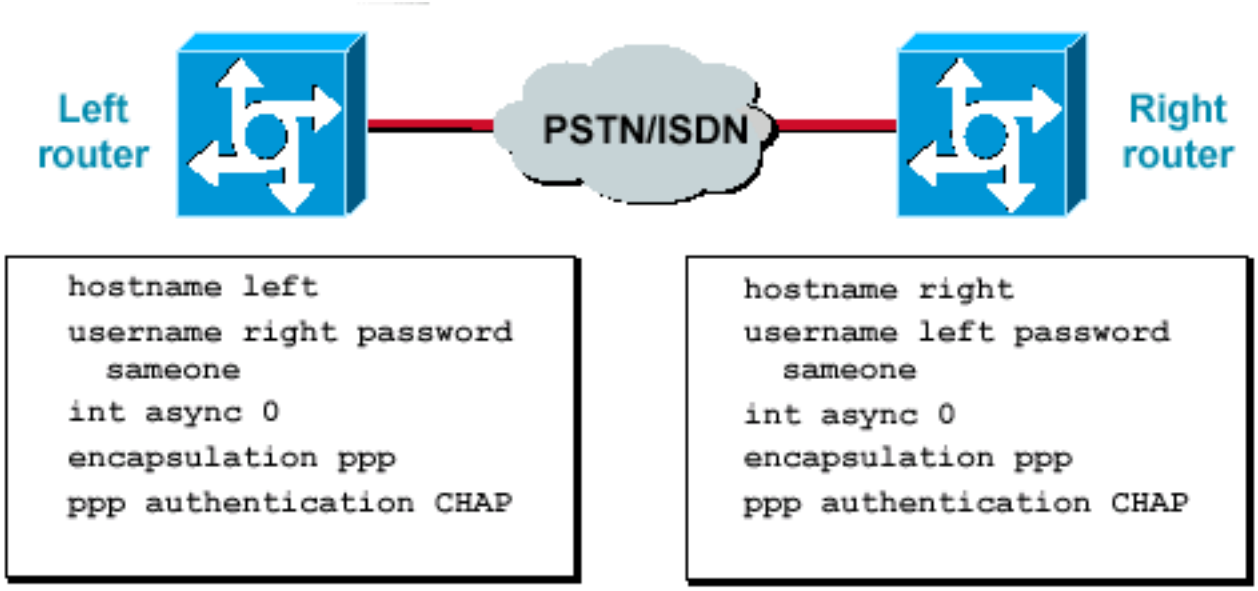
Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Configuration de CHAP

La procédure de configuration du protocole CHAP est assez simple. Par exemple, supposons que vous ayez deux routeurs (un routeur gauche et un routeur droit) connectés au sein d'un réseau, comme l'illustre la Figure 1.

Les Routeurs du deux de d'â de figure 1 se sont connectés à travers un réseau



Pour configurer l'authentification CHAP, exécutez la procédure suivante :

1. Sur interface, émettez la commande **encapsulation ppp** .
2. Activez l'utilisation de l'authentification CHAP sur les deux Routeurs à l'aide de la commande **ppp authentication chap** .
3. Configurez les noms d'utilisateurs et les mots de passe. Pour cela, émettez la commande **username username password password** , où *username* correspond au nom d'hôte de l'homologue. Vérifiez les points suivants :Les mots de passe doivent être identiques aux deux extrémités.Le nom et le mot de passe du routeur doivent être rigoureusement identiques, parce qu'ils distinguent les majuscules et les minuscules.**Remarque:** Par défaut, le routeur utilise son nom d'hôte pour s'identifier à l'homologue. Cependant, ce nom d'utilisateur CHAP peut être modifié à l'aide de la commande **ppp chap hostname** . Pour plus d'informations, reportez-vous aux commandes PPP Authentication Using the ppp chap hostname et ppp authentication chap callin .

Authentification à sens unique et bi-directionnelle

CHAP est défini comme une méthode d'authentification à sens unique. Cependant, vous pouvez utiliser CHAP dans les deux directions pour créer une authentification bi-directionnelle. Par conséquent, avec le protocole CHAP bi-directionnel, un dialogue à trois distinct est lancé par chaque côté.

Par défaut, dans l'implémentation CHAP Cisco, la partie appelée doit authentifier l'appelant (à moins que l'authentification ne soit complètement arrêtée). Par conséquent, une authentification à sens unique lancée par la partie appelée constitue l'authentification minimum possible. Cependant, l'appelant peut également vérifier l'identité de la partie appelée, et ceci a comme conséquence une authentification bi-directionnelle.

L'authentification à sens unique est souvent requise quand vous vous connectez à des périphériques non-Cisco.

Pour l'authentification à sens unique, configurez la commande **ppp authentication chap callin** sur le routeur appelant.

Le tableau 1 indique à quel moment vous devez configurer l'option callin.

de d'â du tableau 1 quand configurer l'option callin

Type d'authentification	Client (appelant)	NAS (appelé)
Unidirectionnel	ppp authentication chap callin	ppp authentication chap
Bi-directionnel	ppp authentication chap	ppp authentication chap

Pour plus d'informations sur la mise en oeuvre de l'authentification unidirectionnelle, reportez-vous aux commandes PPP Authentication using the ppp chap hostname et ppp authentication chap callin.

Commandes et options de configuration de CHAP

Le tableau 2 répertorie les commandes et les options CHAP :

Le CHAP de de d'â du tableau 2 commande et des options

Commande	Description
ppp authentication {chap / *ms-chap* / *ms-chap-v2* / *eap* /pap} [callin]	Cette commande permet d'activer l'authentification locale de l'homologue PPP distant à l'aide du protocole spécifié.
ppp chap hostname username	Cette commande permet de définir un nom d'hôte CHAP propre à une interface spécifique. Pour plus d'informations, reportez-vous aux commandes PPP Authentication Using the ppp chap hostname et ppp authentication chap callin .
ppp chap password password	Cette commande permet de définir un mot de passe CHAP propre à une interface spécifique.
ppp direction callin	Cette commande permet de forcer une direction d'appel. Utilisez cette commande lorsqu'un routeur ne sait pas si l'appel est entrant ou

/ légende / dédié	sortant (par exemple, quand il est connecté dos à dos ou via des lignes louées alors que l'unité de service d'unité CSU ou de données (CSU/DSU), ou encore l'adaptateur terminal RNIS (TA) sont configurés pour le mode numérotation).
ppp chap refuse [callin]	Cette commande permet de désactiver l'authentification par un homologue (elle est activée par défaut). Avec cette commande, l'authentification CHAP est désactivée pour tous les appels, ce qui signifie que toutes les tentatives effectuées par l'homologue pour forcer l'utilisateur à s'authentifier via CHAP sont refusées. L'option callin spécifie que le routeur doit refuser de répondre aux défis d'authentification CHAP envoyés par l'homologue, mais que l'homologue doit continuer à répondre aux défis CHAP envoyés par le routeur.
ppp chap wait	Cette commande spécifie que le visiteur doit au préalable s'authentifier (cette commande est activée par défaut). Cette commande spécifie que le router ne s'authentifiera à un homologue qui demande une authentification CHAP qu'une fois que ce dernier se sera lui-même authentifié auprès du routeur.
ppp max-bad-auth value	Cette commande spécifie le nombre autorisé de tentatives d'authentification (la valeur par défaut est 0). Cette commande permet de configurer une interface point à point qui ne se réinitialise pas immédiatement après un échec d'authentification, mais qui spécifie un nombre autorisé de nouvelles tentatives d'authentification.
ppp chap splitnames	Cette commande cachée permet d'utiliser différents noms d'hôte pour un défi et une réponse CHAP (la valeur par défaut est désactivée).
ppp chap ignoreus	Cette commande cachée ignore les défis CHAP avec le nom local (la valeur par défaut est activée).

Exemple de transaction

Les diagrammes de cette section illustrent la série d'événements qui se produit pendant une authentification CHAP entre deux routeurs. Ceux-ci ne représentent pas les messages réels présents dans les résultats de la commande **debug ppp negotiation** . Pour plus d'informations, reportez-vous à Comprendre les sorties de la commande debug ppp negotiation.

Appel

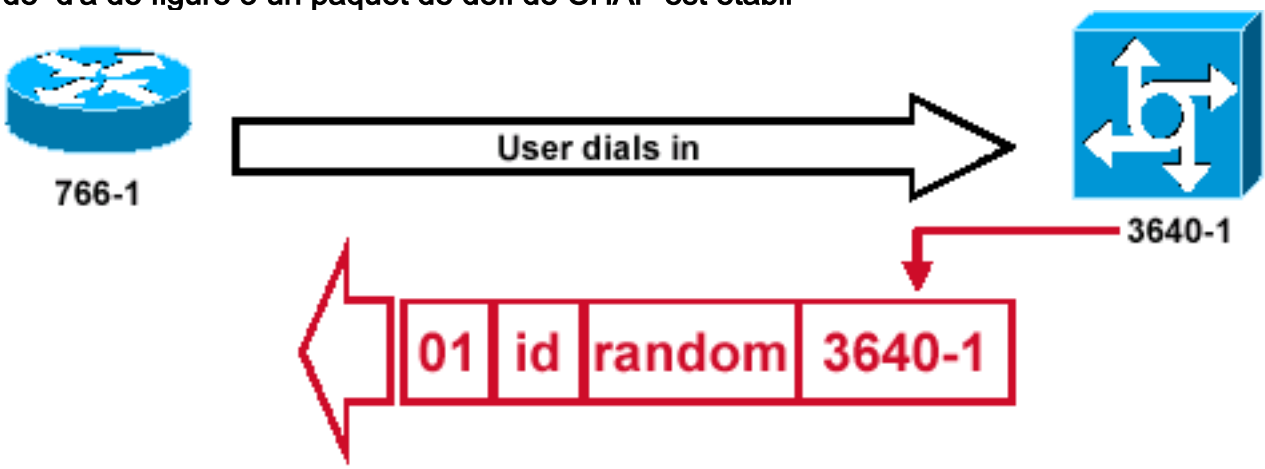
de d'â de figure 2 que l'appel entre

La Figure 2 illustre les étapes suivantes :

1. L'appel entre au niveau de 3640-1. L'interface entrante est configurée à l'aide de la commande **ppp authentication chap** .
2. LCP négocie CHAP et MD5. Pour plus d'informations sur la façon de déterminer ces éléments, reportez-vous à Comprendre les sorties de la commande debug ppp negotiation.
3. Un défi CHAP entre 3640-1 et le routeur appelant est requis pour cet appel.

Défi

Le de d'â de figure 3 un paquet de défi de CHAP est établi

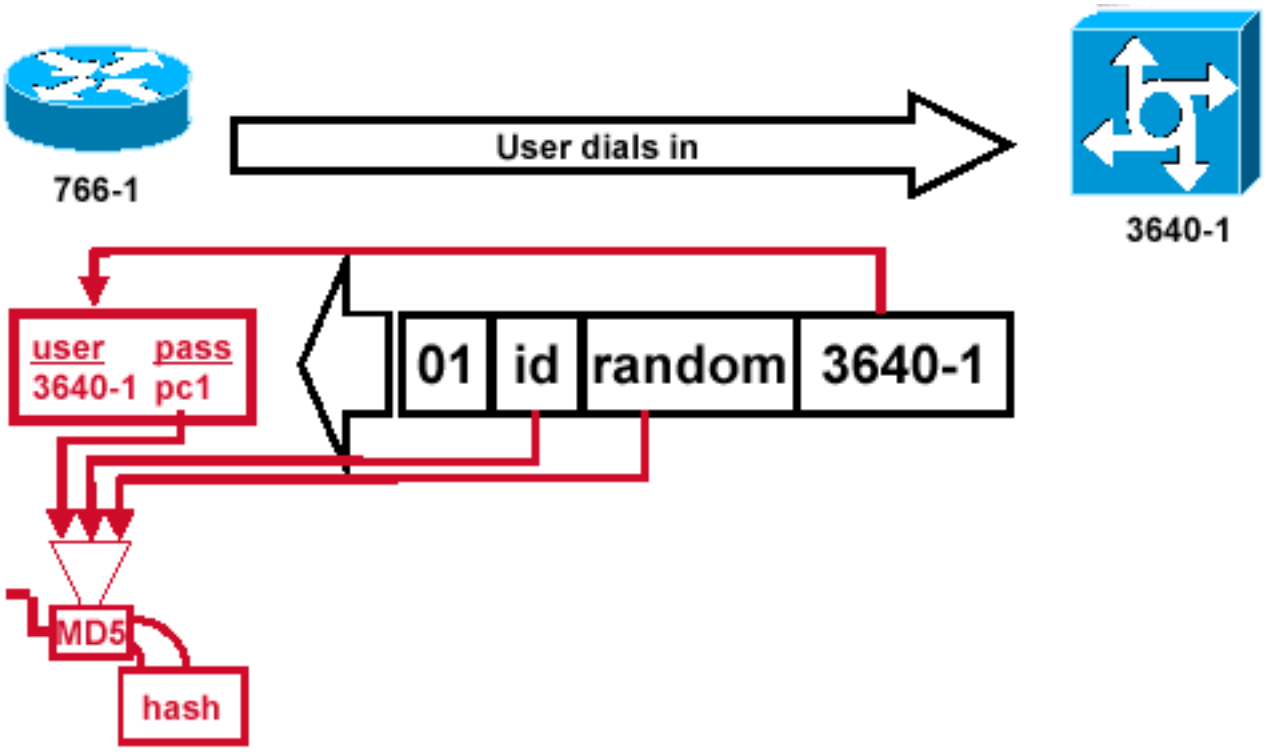


La figure 3 illustre ces étapes dans le cadre de l'authentification CHAP entre les deux routeurs :

1. Un paquet de défi CHAP se construit avec les caractéristiques suivantes :01 = identificateur de type de paquet de défi.ID = nombre séquentiel qui identifie le défi.random = un nombre raisonnablement aléatoire produit par le routeur.3640-1 = le nom d'authentification de l'initiateur du défi.
2. L'ID et les valeurs aléatoires sont gardés sur le routeur appelé.
3. Le paquet de défi est envoyé au routeur appelant. La liste des défis exceptionnels est mise à jour.

Réponse

Réception de de d'â de figure 4 et traitement de MD5 du paquet de défi du pair

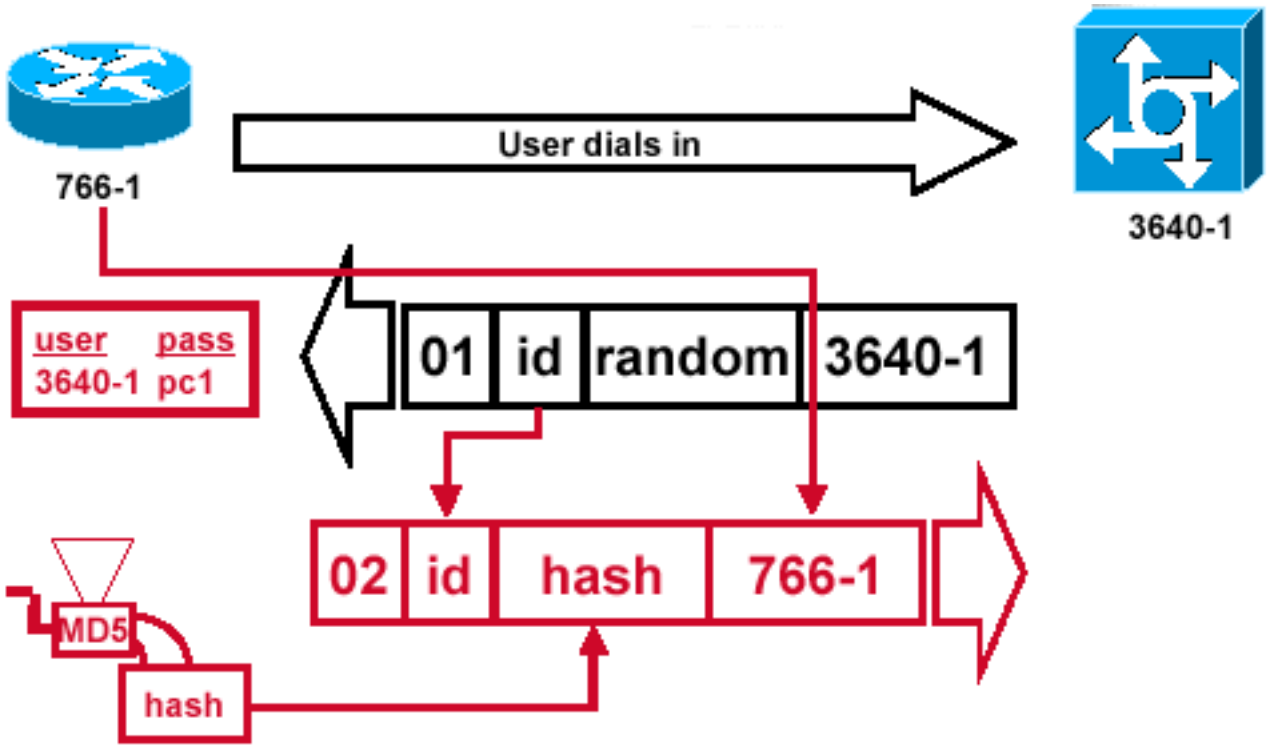


La figure 4 illustre la façon dont le paquet de défi envoyé par l'homologue est reçu et traité (MD5). Le routeur traite router le paquet de défi CHAP entrant de cette façon :

1. La valeur d'ID est introduite dans le générateur d'informations parasites de MD5.
2. La valeur aléatoire est introduite dans le générateur d'informations parasites de MD5.
3. Le nom 3640-1 est utilisé pour rechercher le mot de passe. Le routeur recherche une entrée correspondant au nom d'utilisateur dans le défi. Dans cet exemple, il recherche :`username 3640-1 password pc1`
4. Le mot de passe est introduit dans le générateur d'informations parasites de MD5.Le résultat est le défi à sens unique MD5 CHAP qui est renvoyé dans la réponse CHAP.

Réponse (suite)

Le de d'â de figure 5 le paquet de réponse de CHAP envoyé à l'authentificateur est établi.



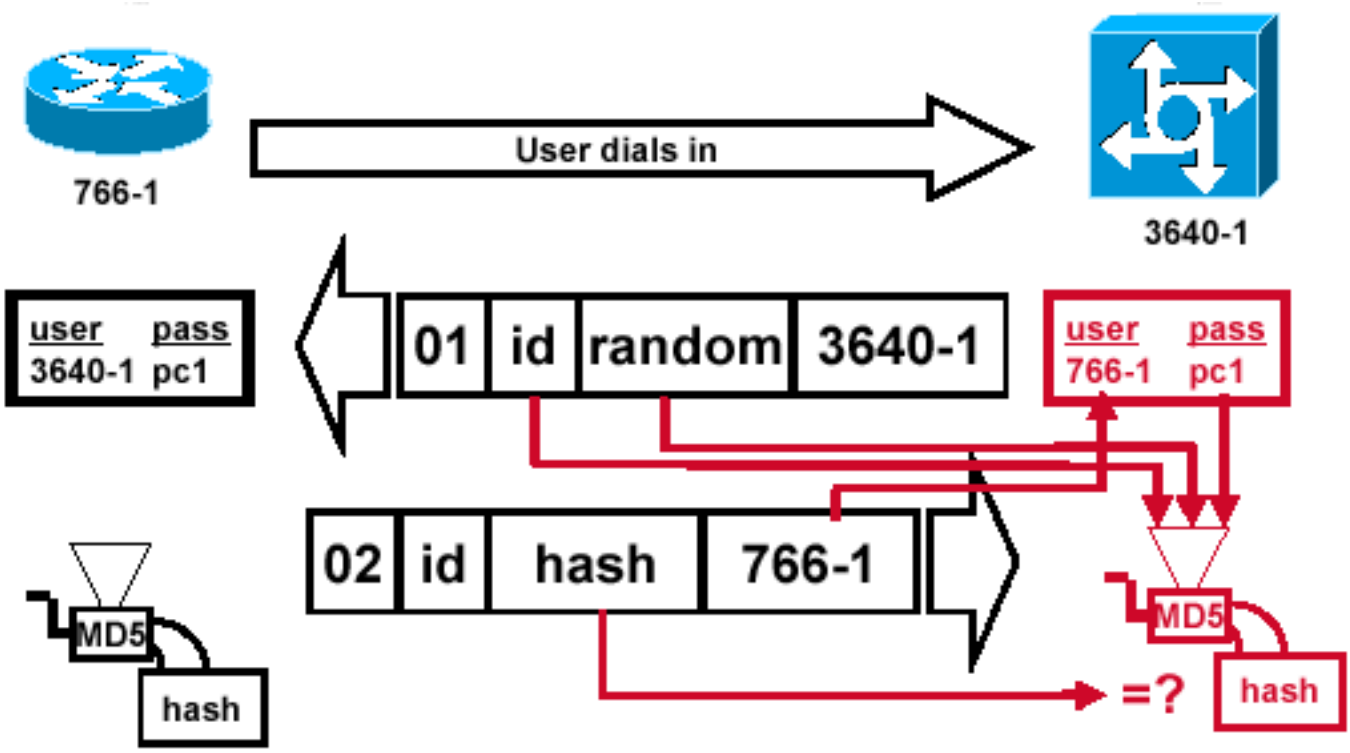
La figure 5 illustre la façon dont le paquet de réponse CHAP envoyé à l'authentificateur est élaboré. Ce diagramme montre ces étapes :

1. Le paquet de réponse est assemblé à partir de ces composants :02 = Identificateur de type de paquet de réponse CHAP.ID = Copié du paquet de défi.hash = La sortie du générateur d'informations parasites de MD5 (l'information hachée du paquet de défi).766-1 = Le nom d'authentification de ce périphérique. Il est requis pour que l'homologue recherche le nom d'utilisateur et le mot de passe requis pour vérifier l'identité (ceci est expliqué plus en détails dans la section Vérification de CHAP).
2. Le paquet de réponse est alors envoyé à l'initiateur du défi.

Vérification de CHAP

Cette section fournit des astuces sur la méthode de vérification de votre configuration.

Le de d'â de figure 6 le challengeur traite le paquet de réponse

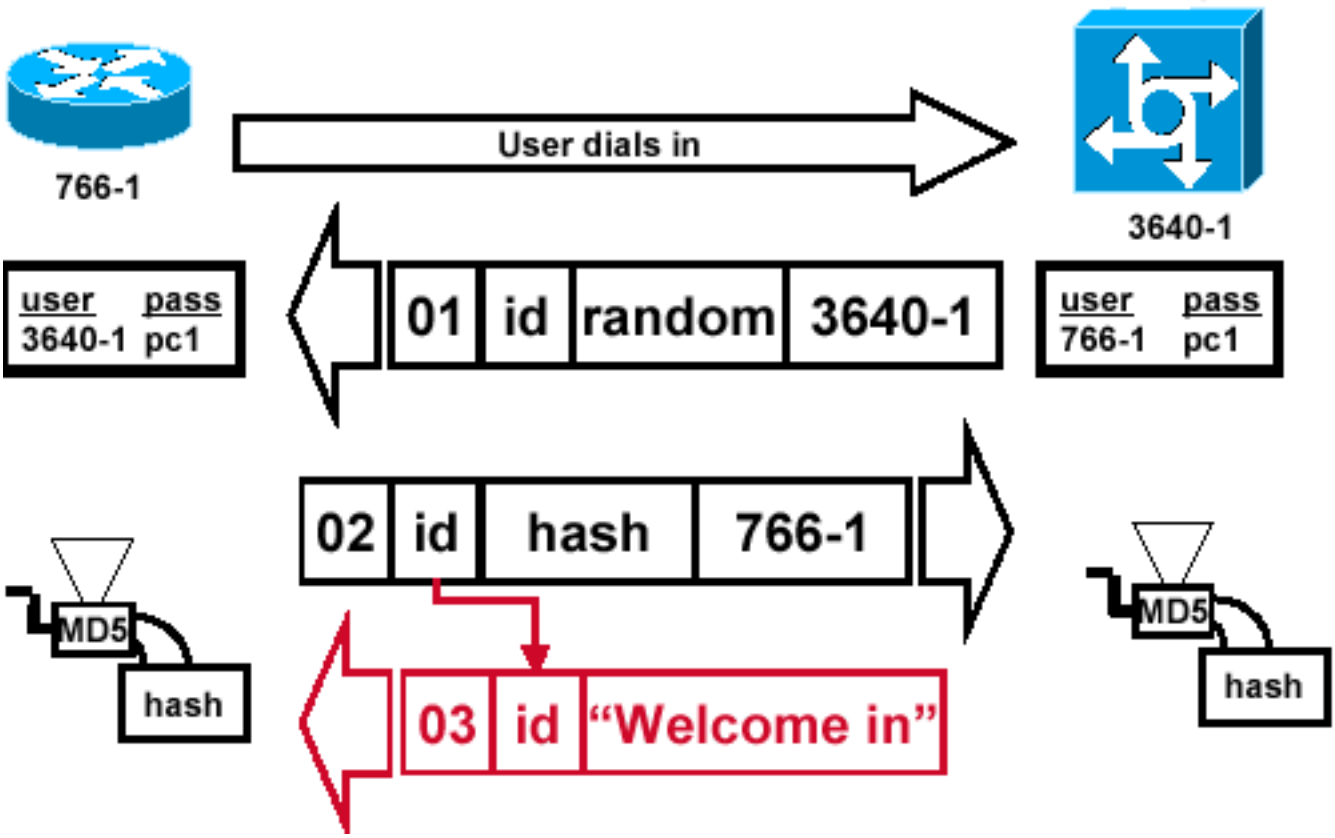


La figure 6 montre comment l'initiateur du défi traite le paquet de réponse. Voici les étapes de traitement du paquet de réponse CHAP (sur l'authentificateur) :

1. L'ID est utilisé pour rechercher le paquet initial de défi.
2. La valeur d'ID est introduite dans le générateur d'informations parasites de MD5.
3. La valeur aléatoire de défi initiale est introduite dans le générateur d'informations parasites de MD5.
4. Le nom 766-1 est utilisé pour rechercher le mot de passe à partir de l'une des sources suivantes :Base de données locale de noms d'utilisateur et de mots de passe.Serveur RADIUS ou TACACS+.
5. Le mot de passe est introduit dans le générateur d'informations parasites de MD5.
6. La valeur d'informations parasites reçue dans le paquet de réponse est alors comparée à la valeur d'informations parasites calculée de MD5. L'authentification CHAP réussit si les valeurs d'informations parasites calculées et reçues correspondent.

Résultat

Le message de succès de de d'â de figure 7 est envoyé au routeur appelant



La figure 7 illustre le message de succès envoyé au routeur appelant. Cela implique les étapes suivantes :

1. Si l'authentification aboutit, un paquet de succès CHAP est construit à partir de ces composants :03 = Type de message de succès CHAP.ID = Copié du paquet de réponse.le de d'inâ d'accueil de de d'â est simplement un message texte qui fournit une explication utilisateur-accessible en lecture.
2. Si l'authentification échoue, un paquet d'échec CHAP est construit à partir de ces composants :04 = Type de message d'échec CHAP.ID = Copié du paquet de réponse.le de de failureâ d'authentification de de d'â ou tout autre message texte, cela fournit une explication utilisateur-accessible en lecture.
3. Le paquet de succès ou d'échec est alors envoyé au routeur appelant.**Remarque:** Cet exemple illustre une authentification à sens unique. Dans une authentification bi-directionnelle, ce processus complet est répété. Dans ce cas toutefois, c'est le routeur appelant qui lance le défi initial.

Dépannage de CHAP

Pour plus d'informations sur le dépannage, reportez-vous à Dépannage de l'authentification PPP .

Informations connexes

- Présentation de la sortie de négociation de débogage ppp
- Troubleshooting PPP Authentication (Dépannage de l'authentification PPP)
- Authentification PPP par le biais des commandes ppp chap hostname et ppp authentication chap callin

- Accès aux pages d'assistance technologique
- Support technique - Cisco Systems