Configuration et dépannage du protocole PAP (Password Authentication Protocol) pour PPP

Contenu

Introduction

Le protocole point-à-point (PPP) prend en charge actuellement deux protocoles d'authentification : Le protocole d'authentification PAP (Password Authentication Protocol) et le protocole d'authentification CHAP (Challenge Handshake Authentication Protocol). Chacun des deux sont spécifiés dans la spécification RFC 1334 et sont pris en charge sur les interfaces synchrones et asynchrones.

- Le protocole PAP fournit une méthode simple permettant à un noeud distant d'établir son identité à l'aide d'une connexion en deux étapes. Une fois la phase d'établissement de la liaison PPP terminée, une paire de nom d'utilisateur et de mot de passe est envoyée à plusieurs reprises par le noeud distant sur la liaison (en texte clair) jusqu'à ce que l'authentification soit reconnue ou jusqu'à ce que la connexion soit interrompue.
- Le protocole PAP n'est pas un protocole d'authentification sécurisé. Les mots de passe sont envoyés sur le lien en texte clair et il n'y a aucune protection contre la lecture ou les attaques

par essais et erreurs. Le noeud distant contrôle la fréquence et la durée des tentatives de connexion.

Pour plus d'informations sur le dépannage de l'authentification PPP (à l'aide du protocole PAP ou CHAP), référez-vous à Dépannage de l'authentification PPP (CHAP ou PAP) pour un organigramme détaillé et détaillé pour le dépannage de la phase d'authentification PPP. Pour plus d'informations sur le dépannage de toutes les phases PPP (LCP, Authentification, NCP), reportez-vous au document PPP Troubleshooting FlowChart pour un organigramme complet pour le dépannage pas à pas de toutes les phases PPP associées et des paramètres négociés.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

Conventions

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

Informations générales

Le protocole CHAP est considéré comme étant plus sécurisé car le mot de passe utilisateur n'est jamais envoyé sur la connexion. Pour plus d'informations sur CHAP, référez-vous à Comprendre et configurer l'authentification PPP CHAP.

Malgré ses défauts, le protocole PAP peut être utilisé dans les environnements suivants :

- Une vaste base installée d'applications clientes qui ne prennent pas en charge CHAP
- Incompatibilités entre les implémentations de différents fournisseurs de CHAP
- Situations dans lesquelles un mot de passe en clair doit être disponible pour simuler une connexion sur l'hôte distant

Authentification Bidirectionnelle Vs Unidirectionnelle

Comme pour la plupart des types d'authentification, PAP prend en charge l'authentification bidirectionnelle (bidirectionnelle) et unidirectionnelle (unidirectionnelle). Avec l'authentification unidirectionnelle, seul le côté recevant l'appel (NAS) authentifie le côté distant (client). Le client distant n'authentifie pas le serveur.

Avec l'authentification bidirectionnelle, chaque côté envoie indépendamment une demande d'authentification (AUTH-REQ) et reçoit soit un AUTH-ACK (Authenticate-AcKnowledge), soit AUTH-NAK (Authenticate-Not Acknowledged). Celles-ci peuvent être vues avec la commande debug ppp authentication. Un exemple de ce débogage au niveau du client est présenté ci-

dessous :

```
*Mar  6 19:18:53.322: BR0:1 PAP: O AUTH-REQ id 7 len 18 from "PAPUSER"
 ! --- Outgoing PAP AUTH-REQ. We are sending out our username (PAPUSER)and password ! --- to the
NAS. The NAS will verify that the username/password is correct. *Mar 6 19:18:53.441: BR0:1 PAP:
I AUTH-ACK id 7 Len 5
! --- Incoming AUTH-ACK. ! --- The NAS verified the username and password and responded with an
AUTH-ACK. ! --- One-way authentication is complete at this point. *Mar 6 19:18:53.445: BR0:1
PAP: I AUTH-REQ id 1 Len 14 from "NAS"
 ! --- Incoming AUTH-REQ from the NAS. This means we now verify the identity of the NAS. *Mar 6
19:18:53.453: BR0:1 PAP: Authenticating peer NAS
! --- Performing a lookup for the username (NAS) and password. *Mar 6 19:18:53.457: BR0:1 PAP: O
AUTH-ACK id 1 Len 5
! --- Outgoing AUTH-ACK. ! --- We have verified the username/password of the NAS and responded
with an AUTH-ACK. ! --- Two-way authentication is complete.
```

Dans la sortie de débogage ci-dessus, l'authentification était bidirectionnelle. Cependant, si l'authentification unidirectionnelle avait été configurée, nous ne verrions que les deux premières lignes de débogage.

Commandes de configuration

Trois commandes sont requises pour l'authentification PAP normale décrite ci-dessous :

ppp authentication pap [callin]

Le routeur sur lequel la commande ppp authentication pap est configurée utilise PAP pour vérifier l'identité de l'autre côté (homologue). Cela signifie que l'autre côté (homologue) doit présenter son nom d'utilisateur/mot de passe au périphérique local pour vérification.

L'option **callin** indique au routeur que la commande ppp authentication pap callin est configurée sur authentifiera uniquement l'autre côté lors d'un appel entrant. Pour un appel sortant, il n'authentifiera pas l'autre côté. Cela signifie que le routeur qui lance l'appel ne nécessite pas de demande d'authentification (AUTH-REQ) de l'autre côté

Le tableau suivant indique quand configurer l'option **callin** :

Type d'authentification	Client (appelant)	NAS (appelé)
Unidirectionnel	ppp authentication pap callin	ppp authentication pap
Bidirectionnel	ppp authentication pap	ppp authentication pap

username <nom d'utilisateur> password <mot de passe>

Il s’agit du nom d’utilisateur et du mot de passe utilisés par le routeur local pour authentifier l’homologue PPP. Lorsque l’homologue envoie son nom d’utilisateur et son mot de passe PAP, le routeur local vérifie si ce nom d’utilisateur et ce mot de passe sont configurés localement. S'il y a correspondance réussie, l'homologue est authentifié.

Remarque : La fonction de la commande username pour PAP est différente de celle de CHAP. Avec CHAP, ce nom d'utilisateur et ce mot de passe sont utilisés pour générer la réponse à la demande, mais PAP ne l'utilise que pour vérifier qu'un nom d'utilisateur et un mot de passe entrants sont valides.

Pour l'authentification unidirectionnelle, cette commande n'est requise que sur le routeur appelé. Pour l'authentification bidirectionnelle, cette commande est nécessaire des deux côtés.

PPP pap sent-username <nom d'utilisateur> password <mot de passe>

Active l'authentification PAP sortante. Le routeur local utilise le nom d'utilisateur et le mot de passe spécifiés par la commande ppp pap sent-username pour s'authentifier sur un périphérique distant. L'autre routeur doit avoir ce même nom d'utilisateur/mot de passe configuré à l'aide de la commande **username** décrite ci-dessus.

Si vous utilisez l'authentification unidirectionnelle, cette commande n'est nécessaire que sur le routeur qui lance l'appel. Pour l'authentification bidirectionnelle, cette commande doit être configurée des deux côtés.

Exemple de configuration

Les sections de configuration suivantes présentent les commandes PAP nécessaires pour un scénario d'authentification unidirectionnelle.

Remarque : Seules les sections pertinentes de la configuration sont affichées.

Configuration côté appelant (client)

```
interface BRI0
! --- BRI interface for the dialout. ip address negotiated encapsulation ppp
! --- Use PPP encapsulation. This command is a required for PAP. dialer string 3785555 class 56k
! --- Number to dial for the outgoing connection. dialer-group 1 isdn switch-type basic-ni isdn
spid1 51299611110101 9961111 isdn spid2 51299622220101 9962222  ppp authentication pap callin
! --- Use PAP authentication for incoming calls. ! --- The callin keyword has made this a one-
way authentication scenario. ! --- This router (client) will not request that the peer (server)
authenticate ! --- itself back to the client. ppp pap sent-username PAPUSER password 7
```

```
! --- Permit outbound authentication of this router (client) to the peer. ! --- Send a PAP AUTH-
REQ packet to the peer with the username PAPUSER and password. ! --- The peer must have the
username PAPUSER and password configured on it.
```

Configuration côté réception (serveur)

```
username PAPUSER password 0 cisco
! --- Username PAPUSER is the same as the one sent by the client. ! --- Upon receiving the AUTH-
REQ packet from the client, we will verify that the ! --- username and password match the one
configured here. interface Serial0:23 ! --- This is the D-channel for the PRI on the access
server receiving the call. ip unnumbered Ethernet0 no ip directed-broadcast  encapsulation ppp
! --- Use PPP encapsulation. This command is a required for PAP. dialer-group 1 isdn switch-type
```

```
primary-ni isdn incoming-voice modem peer default ip address pool default fair-queue 64 256 0
ppp authentication pap
! --- Use PAP authentication for incoming calls. ! --- This router (server) will request that
the peer authenticate itself to us. ! --- Note: the callin option is not used as this router is
not initiating the call.
```

Sorties de débogage

Pour déboguer un problème PPP PAP, utilisez les commandes debug ppp negotiation et debug ppp authentication. Il y a deux problèmes principaux auxquels vous devez faire attention :

1. Les deux parties sont-elles d'accord pour dire que PAP est la méthode d'authentification ?
2. Si oui, l'authentification PAP réussit-elle ?

Reportez-vous aux débogages ci-dessous pour obtenir des informations sur la façon de répondre correctement à ces questions. En outre, référez-vous à Comprendre le résultat de la négociation de débogage ppp pour une explication de toutes les différentes lignes de débogage avec leur signification relative au cours des différentes phases PPP, y compris l'authentification PPP. Ce document est utile pour déterminer rapidement la cause des échecs de négociation PPP. Pour plus d'informations sur le dépannage de l'authentification PPP (à l'aide du protocole PAP ou CHAP), référez-vous à Dépannage de l'authentification PPP (CHAP ou PAP) pour un organigramme détaillé et détaillé pour le dépannage de la phase d'authentification PPP.

Débogage côté appelant (client) pour une authentification PAP unidirectionnelle réussie

```
maui-soho-01#show debug
PPP:
  PPP authentication debugging is on
  PPP protocol negotiation debugging is on
maui-soho-01#ping 172.22.53.144

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.53.144, timeout is 2 seconds:

*Mar  6 21:33:26.412: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
*Mar  6 21:33:26.432: BR0:1 PPP: Treating connection as a callout
*Mar  6 21:33:26.436: BR0:1 PPP: Phase is ESTABLISHING, Active Open [0 sess, 0 load]
*Mar  6 21:33:26.440: BR0:1 PPP: No remote authentication for call-out
! --- The client will not authenticate the server for an outgoing call. ! --- Remember this is a
one-way authentication example. *Mar 6 21:33:26.444: BR0:1 LCP: O CONFREQ [Closed] id 82 Len 10
*Mar  6 21:33:26.448: BR0:1 LCP:    MagicNumber 0x2F1A7C63 (0x05062F1A7C63)
! --- Outgoing CONFREQ (CONFigure-REQuest). ! --- Notice that we do not specify an
authentication method, ! --- since only the peer will authenticate us. *Mar 6 21:33:26.475:
BR0:1 LCP: I CONFREQ [REQsent] id 13 Len 14
*Mar  6 21:33:26.479: BR0:1 LCP:    AuthProto PAP (0x0304C023)
! --- Incoming LCP CONFREQ (Configure-Request) indicating that ! --- the peer(server) wishes to
use PAP. *Mar 6 21:33:26.483: BR0:1 LCP: MagicNumber 0x3DBEE95B (0x05063DBEE95B) *Mar 6
21:33:26.491: BR0:1 LCP: O CONFACK [REQsent] id 13 Len 14
*Mar  6 21:33:26.495: BR0:1 LCP:    AuthProto PAP (0x0304C023)
! --- This shows the outgoing LCP CONFACK (CONFigure-ACKnowledge) indicating that ! --- the
client can do PAP. *Mar 6 21:33:26.499: BR0:1 LCP: MagicNumber 0x3DBEE95B (0x05063DBEE95B) *Mar
6 21:33:26.511: BR0:1 LCP: I CONFACK [ACKsent] id 82 Len 10 *Mar 6 21:33:26.515: BR0:1 LCP:
MagicNumber 0x2F1A7C63 (0x05062F1.A7C63) *Mar 6 21:33:26.519: BR0:1 LCP: State is Open
! --- This shows LCP negotiation is complete. *Mar 6 21:33:26.523: BR0:1 PPP: Phase is
AUTHENTICATING, by the peer [0 sess, 0 load]
! --- The PAP authentication (by the peer) begins. *Mar 6 21:33:26.531: BR0:1 PAP: O AUTH-REQ id
20 Len 18 from "PAPUSER"
```

```
 ! --- The client sends out a PAP AUTH-REQ with username PAPUSER. ! --- This username is
configured with the ppp pap sent-username command. *Mar 6 21:33:26.555: BR0:1 PAP: I AUTH-ACK id
20 Len 5
! --- The Peer responds with a PPP AUTH-ACK, indicating that ! --- it has successfully
authenticated the client.
```

Débogage côté appelé (serveur) pour une authentification PAP unidirectionnelle réussie

```
maui-nas-06#show debug
PPP:
  PPP authentication debugging is on
  PPP protocol negotiation debugging is on
maui-nas-06#
*Jan  3 14:07:57.872: %LINK-3-UPDOWN: Interface Serial0:4, changed state to up
*Jan  3 14:07:57.876: Se0:4 PPP: Treating connection as a callin
! --- Since the connection is incoming, we will authenticate the client. *Jan 3 14:07:57.876:
Se0:4 PPP: Phase is ESTABLISHING, Passive Open *Jan 3 14:07:57.876: Se0:4 LCP: State is Listen
*Jan 3 14:07:58.120: Se0:4 LCP: I CONFREQ [Listen] id 83 Len 10 *Jan 3 14:07:58.120: Se0:4 LCP:
MagicNumber 0x2F319828 (0x05062F319828) *Jan 3 14:07:58.124: Se0:4 LCP: O CONFREQ [Listen] id 13
Len 14
*Jan  3 14:07:58.124: Se0:4 LCP:    AuthProto PAP (0x0304C023)
! --- Outgoing CONFREQ (Configure-Request) ! --- use PAP for the peer authentication. *Jan 3
14:07:58.124: Se0:4 LCP: MagicNumber 0x3DD5D5B9 (0x05063DD5D5B9) *Jan 3 14:07:58.124: Se0:4 LCP:
O CONFACK [Listen] id 83 Len 10 *Jan 3 14:07:58.124: Se0:4 LCP: MagicNumber 0x2F319828
(0x05062F319828) *Jan 3 14:07:58.172: Se0:4 LCP: I CONFACK [ACKsent] id 13 Len 14
*Jan  3 14:07:58.172: Se0:4 LCP:    AuthProto PAP (0x0304C023)
! --- This shows the incoming LCP CONFACK (Configure-Acknowledge) indicating that ! --- the
client can do PAP. *Jan 3 14:07:58.172: Se0:4 LCP: MagicNumber 0x3DD5D5B9 (0x05063DD5D5B9) *Jan
3 14:07:58.172: Se0:4 LCP: State is Open *Jan 3 14:07:58.172: Se0:4 PPP: Phase is
AUTHENTICATING, by this end
! --- The PAP authentication (by this side) begins. *Jan 3 14:07:58.204: Se0:4 PAP: I AUTH-REQ
id 21 Len 18 from "PAPUSER"
! --- Incoming AUTH-REQ from the peer. This means we must now verify ! --- the identity of the
peer. *Jan 3 14:07:58.204: Se0:4 PPP: Phase is FORWARDING *Jan 3 14:07:58.204: Se0:4 PPP: Phase
is AUTHENTICATING *Jan 3 14:07:58.204: Se0:4 PAP: Authenticating peer PAPUSER
! --- Performing a lookup for the username (PAPUSER) and password. *Jan 3 14:07:58.208: Se0:4
PAP: O AUTH-ACK id 21 Len 5 ! --- This shows the outgoing AUTH-ACK. ! --- We have verified the
username and password and responded with an AUTH-ACK. ! --- One-way authentication is complete.
```

Dépannage du protocole PAP

Lors du dépannage du protocole PAP, répondez aux mêmes questions que dans la section Sortie de débogage :

1. Les deux parties sont-elles d'accord pour dire que PAP est la méthode d'authentification ?
2. Si oui, l'authentification PAP réussit-elle ?

Pour plus d'informations sur le dépannage de l'authentification PPP (à l'aide du protocole PAP ou CHAP), référez-vous à Dépannage de l'authentification PPP (CHAP ou PAP) pour un organigramme détaillé et détaillé pour le dépannage de la phase d'authentification PPP.

Les deux parties ne sont pas d'accord sur le protocole PAP comme protocole d'authentification

Dans certaines configurations, vous pouvez observer que les deux côtés ne sont pas d'accord sur PAP comme protocole d'authentification ou plutôt sur CHAP (lorsque vous vouliez PAP). Procédez comme suit pour résoudre ces problèmes :

1. Vérifiez que le routeur recevant l'appel possède l'une des commandes d'authentification suivantes

```
ppp authentication pap
       or
ppp authentication pap chap
       or
ppp authentication chap pap
```

2. Vérifiez que la fonction ppp authentication pap callin est configurée sur le routeur qui effectue l'appel.
3. Vérifiez que la commande **ppp pap sent-username *username* password *password*** du côté appelant est correctement configurée, où le nom d'utilisateur et le mot de passe correspondent à celui configuré sur le routeur récepteur.
4. Configurez la commande **ppp chap refuser** en mode de configuration d'interface sur le routeur appelant.Par défaut, les routeurs Cisco acceptent CHAP comme protocole d'authentification. Dans une situation où le client souhaite faire PAP mais que le serveur d'accès peut faire PAP ou CHAP (**ppp authentication chap pap** configuré), la commande **ppp chap deny** peut être utilisée pour forcer le client à accepter PAP comme protocole d'authentification.

```
maui-soho-01(config)#interface BRI 0
maui-soho-01(config-if)#ppp chap refuse
```

L'authentification PAP n'a pas réussi

Si les deux parties conviennent du protocole d'authentification PAP, mais que la connexion PAP échoue, il s'agit probablement d'un problème de nom d'utilisateur/mot de passe.

1. Vérifiez que la commande **ppp pap sent-username *username* password *password*** du côté appelant est correctement configurée, où le nom d'utilisateur et le mot de passe correspondent à celui configuré sur le routeur récepteur.
2. Pour l'authentification bidirectionnelle, vérifiez que le côté récepteur dispose de la commande **ppp pap sent-username *username* password *password*** correctement configurée, où le nom d'utilisateur et le mot de passe correspondent à celui configuré sur le routeur appelant.Lors de l'authentification bidirectionnelle, si la commande **ppp pap sent-username *username* password password *password*** n'était pas présente sur le routeur récepteur et que le client PPP tente de forcer le serveur à s'authentifier à distance, le résultat de **debug ppp negotiation** (ou **debug ppp authentication**) indique
   ```
   *Jan  3 16:47:20.259: Se0:1 PAP: Failed request for PAP credentials.  Username maui-nas-06
   ```
   Ce message d'erreur indique un problème de configuration et pas nécessairement une faille de sécurité.
3. 3. Vérifiez que le nom d'utilisateur et le mot de passe correspondent à celui configuré dans la commande **ppp pap sent-username nom d'*utilisateur* mot de passe *mot de passe*** sur l'homologue.Si elles ne correspondent pas, vous voyez ce message :
   ```
   *Jan  3 17:18:57.559: Se0:3 PAP: I AUTH-REQ id 25 Len 18 from "PAPUSER"
   *Jan  3 17:18:57.559: Se0:3 PPP: Phase is FORWARDING
   *Jan  3 17:18:57.559: Se0:3 PPP: Phase is AUTHENTICATING
   *Jan  3 17:18:57.559: Se0:3 PAP: Authenticating peer PAPUSER
   *Jan  3 17:18:57.559: Se0:3 PAP: O AUTH-NAK id 25 Len 32 msg is
    "Password validation failure"
   ! --- This is an outgoing AUTH-NAK. This means that the mismatch occurred ! --- on this
   ```

```
router. Verify that the username and password configured locally is ! --- identical to that
on the peer.
```

Informations connexes

- Configuration de l'authentification
- Organigramme du dépannage PPP
- Dépannage de l'authentification PPP (CHAP ou PAP)
- Présentation de la sortie de négociation de débogage ppp
- Authentification PPP par le biais des commandes ppp chap hostname et ppp authentication chap callin
- Technologie d'accès commuté : Présentation et explications
- Support et documentation techniques - Cisco Systems