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 PAP fournit une méthode simple pour qu'un noeud distant établisse son identité utilisant une prise de contact bi-directionnelle. Après établissement de la liaison PPP la phase est complète, une paire de nom d'utilisateur et mot de passe est à plusieurs reprises envoyée par le noeud distant à travers le lien (en texte clair) jusqu'à ce que l'authentification soit reconnue, ou jusqu'à ce que la connexion est terminée.
- Le PAP n'est pas un protocole d'authentification sécurisé. Des mots de passe sont envoyés à travers le lien en texte clair et il n'y a aucune protection contre des attaques de lecture ou de test et erreur. Le noeud distant est aux commandes de la fréquence et de la synchronisation des tentatives de procédure de connexion.

Pour plus d'informations sur l'authentification de PPP de dépannage (utilisant le PAP ou le CHAP), référez-vous à l'authentification de PPP de dépannage (CHAP ou PAP) pour un organigramme complet et pas à pas pour dépanner la phase d'authentification de PPP. Pour plus d'informations

sur dépanner toutes les phases de PPP (LCP, authentification, NCP), référez-vous à l'organigramme de dépannage de PPP de document pour un organigramme complet pour le dépannage pas à pas de tous les phases relatives de PPP et paramètres négociés.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

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 utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Le CHAP est considéré plus sécurisé parce que le mot de passe utilisateur n'est jamais envoyé à travers la connexion. Pour plus d'informations sur le CHAP, référez-vous à comprendre et à configurer l'authentification de PPP CHAP.

En dépit de ses défauts, le PAP peut être utilisé dans les environnements suivants :

- Grandes bases installées d'applications clientes qui ne prennent en charge pas le CHAP
- Incompatibilités entre les réalisations de différent constructeur du CHAP
- Situations où un mot de passe de plaintext doit être disponible pour simuler une procédure de connexion au serveur distant

Unidirectionnel contre l'authentification bidirectionnelle

Comme avec la plupart des types d'authentification, le PAP prend en charge l'authentification bidirectionnelle (bi-directionnel) et unidirectionnelle (d'une manière). Avec l'authentification unidirectionnelle, seulement 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 Authentifier-demande (AUTHENTIC-REQ) et reçoit une Authentifier-reconnaissance (AUTHENTIC-ACK) ou l'authentifie-Non reconnu (AUTHENTIC-NAK). Ceux-ci peuvent être vus avec la commande de debug ppp authentication. Un exemple de ceci mettent au point au client est affiché 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 verrions seulement les deux premiers mettre au point des lignes.

Commandes de configuration

Il y a trois commandes exigées pour l'authentification PAP normale décrite ci-dessous :

authentification PAP [callin] de ppp

Le routeur que la commande de l'authentification PAP de ppp est configurée en fonction emploiera le PAP pour vérifier l'identité de l'autre côté (pair). Ceci signifie que l'autre côté (pair) doit le présenter est nom d'utilisateur/mot de passe au périphérique local pour la vérification.

L'option callin indique que le routeur que la commande de callin de l'authentification PAP de ppp est configurée en fonction authentifiera seulement l'autre côté pendant un appel entrant. Pour un appel sortant, il n'authentifiera pas l'autre côté. Ceci signifie que le routeur initiant l'appel n'a pas besoin d'une demande pour l'authentification (AUTHENTIC-REQ) de l'autre côté

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

Type d'authentification	Client (appelant)	NAS (appelé)
Unidirectionnel	callin de l'authentification PAP de ppp	authentification PAP de ppp
Bidirectionnel	authentification PAP de ppp	authentification PAP de ppp

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

C'est le nom d'utilisateur et mot de passe utilisé par le routeur local pour authentifier le pair de PPP. Quand le pair envoie son nom d'utilisateur et mot de passe PAP, le routeur local vérifiera si ce nom d'utilisateur et mot de passe sont configurés localement. S'il y a une concordance réussie, le pair est authentifié.

Remarque: La fonction de la commande de nom d'utilisateur pour le PAP est différente que sa fonction pour le CHAP. Avec le CHAP, ce nom d'utilisateur et mot de passe sont utilisés pour générer la réponse au défi, mais le PAP l'emploie seulement pour vérifier qu'un nom d'utilisateur et mot de passe entrant sont valide.

Pour l'authentification à sens unique, cette commande est seulement exigée sur le routeur appelé. Pour l'authentification bi-directionnelle cette commande est nécessaire des deux côtés.

<password> de mot de passe de <username> de ppp pap sent-username

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

Si vous utilisez l'authentification à sens unique, cette commande est seulement nécessaire sur le routeur initiant l'appel. Pour l'authentification bi-directionnelle cette commande doit être configurée des deux côtés.

Exemple de configuration

Les sections de configuration suivantes affichent les commandes nécessaires PAP pour un scénario d'authentification d'une manière.

Remarque: Seulement les sections afférentes de la configuration sont affichées.

Configuration de 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 <deleted>! --- 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 de 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 mettre au point une question du PPP PAP utilisez le debug ppp negotiation et les commandes de debug ppp authentication. Il y a deux problèmes principaux pour lesquels vous devez observer :

1. Les deux côtés conviennent-ils que le PAP est la méthode d'authentification ?
2. Si oui, l'authentification PAP réussit-elle ?

Référez-vous au met au point ci-dessous pour les informations sur la façon dont répondre correctement aux ces questions. En outre, référez-vous s'il vous plaît compréhension derrière le debug ppp negotiation sorti pour une explication de toutes les différentes lignes de mise en point

avec leur signification relative pendant les différentes phases de PPP, y compris l'authentification de PPP. Ce document est utile en déterminant rapidement la cause des pannes de négociation PPP. Pour plus d'informations sur l'authentification de PPP de dépannage (utilisant le PAP ou le CHAP), référez-vous à l'authentification de PPP de dépannage (CHAP ou PAP) pour un organigramme complet et pas à pas pour dépanner la phase d'authentification de PPP.

Le côté appelant (client) mettent au point pour une authentification PAP à sens unique réussie

```
maui-soho-01#show debugPPP:  PPP authentication debugging is on  PPP protocol negotiation
debugging is onmaui-soho-01#ping 172.22.53.144Type 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.
```

Side appelé (serveur) mettent au point pour une authentification PAP à sens unique réussie

```
maui-nas-06#show debugPPP:  PPP authentication debugging is on  PPP protocol negotiation
debugging is onmaui-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 PAP

Le pour le dépannage PAP, répondent aux mêmes questions affichées dans la section de sortie de débogage :

1. Les deux côtés conviennent-ils que le PAP est la méthode d'authentification ?
2. Si oui, l'authentification PAP réussit-elle ?

Pour plus d'informations sur l'authentification de PPP de dépannage (utilisant le PAP ou le CHAP), référez-vous à l'authentification de PPP de dépannage (CHAP ou PAP) pour un organigramme complet et pas à pas pour dépanner la phase d'authentification de PPP.

Les deux côtés ne conviennent pas sur le PAP comme protocole d'authentification

Dans certaine configuration vous pouvez observer que les deux côtés ne conviennent pas sur le PAP car le protocole d'authentification ou conviennent à la place sur le CHAP (quand vous avez voulu le PAP). Employez les étapes suivantes pour dépanner de telles questions :

1. Vérifiez que le routeur recevant l'appel a une des authentications command suivantes`ppp authentication pap` or `ppp authentication pap chap` or `ppp authentication chap pap`
2. Vérifiez que le routeur faisant l'appel fait configurer le callin de l'authentification PAP de ppp.
3. Vérifiez que le côté appelant fait configurer correctement le password password de nom d'utilisateur de **ppp pap sent-username de** commande, où la correspondance de nom d'utilisateur et mot de passe celle a configuré sur le routeur récepteur.
4. Configurez les **ppp chap refuse de** commande dans le mode de configuration d'interface sur le routeur appelant.Les Routeurs de Cisco, par défaut, recevront le CHAP comme protocole d'authentification. Dans une situation où le client souhaite faire le PAP mais le serveur d'accès peut faire PAP ou CHAP (CHAP PAP d'authentification de ppp configuré), la commande de **ppp chap refuse** peut être utilisée pour forcer le client pour recevoir le PAP comme protocole d'authentification.`maui-soho-01(config)#interface BRI 0maui-soho-01(config-if)#ppp chap refuse`

L'authentification PAP ne réussit pas

Si les deux côtés conviennent sur le PAP pendant que le protocole d'authentification, mais la connexion PAP échoue, il est le plus susceptible une question de nom d'utilisateur/mot de passe.

1. Vérifiez que le côté appelant fait configurer correctement le **password password de** *nom d'utilisateur de* **ppp pap sent-username de** commande, où la correspondance de nom d'utilisateur et mot de passe celle a configuré sur le routeur récepteur.
2. Pour l'authentification bi-directionnelle, vérifiez que le côté réception fait configurer correctement le **password password de** *nom d'utilisateur de* **ppp pap sent-username de** commande, où la correspondance de nom d'utilisateur et mot de passe celle a configuré sur le routeur appelant.En faire l'authentification bi-directionnelle, si le **password password de** *nom d'utilisateur de* **ppp pap sent-username de** commande n'étaient pas présent sur le routeur récepteur et les tentatives de client de PPP de forcer le serveur pour authentifier à distance, la sortie du **debug ppp negotiation** (ou le **debug ppp authentication**) indiquerait`maui-soho-01(config)#interface BRI 0maui-soho-01(config-if)#ppp chap refuse`Ce message d'erreur est une indication d'une question de configuration et pas nécessairement d'une brèche dans

la sécurité.

3. 3. Vérifiez que le nom d'utilisateur et mot de passe, apparie celui configuré dans le **password password de** *nom d'utilisateur de* **ppp pap sent-username de** commande sur le pair.S'ils ne s'assortissent 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