Configuración y resolución de problemas del Protocolo de autenticación de contraseñas (PAP, por sus siglas en inglés) de PPP

Contenido

Introducción

El Point-to-Point Protocol (PPP) actualmente admite dos protocolos de autenticación: Protocolo de autenticación de contraseña (PAP) y Protocolo de confirmación de aceptación de la autenticación (CHAP). Ambos están especificados en RFC 1334 y están admitidos en interfaces sincrónicas y asincrónicas.

- PAP proporciona un método simple para que un nodo remoto establezca su identidad mediante una entrada en contacto bidireccional. Una vez que se completa la fase de establecimiento del link PPP, el nodo remoto envía de manera repetida un par de nombre de usuario y contraseña a través del link (en texto claro) hasta que se recibe el acuse de recibo

de la autenticación, o hasta que finaliza la conexión.
- PAP no es un protocolo de autenticación seguro. Las contraseñas se envían a través del enlace en texto sin formato y no hay protección contra la reproducción o los ataques de prueba y error. El nodo remoto controla la frecuencia y la sincronización de los intentos de registro.

Para más información sobre la localización de averías ppp autentificación (utilizando o el PAP o la CHAP), refiera a la autentificación de localización de averías PPP (CHAP o PAP) para un organigrama completo, paso a paso para localizar averías de la fase de la autentificación PPP. Para obtener más información sobre la solución de problemas de todas las fases PPP (LCP, Autenticación, NCP), consulte el documento Diagrama de flujo de solución de problemas PPP para obtener un diagrama de flujo completo para la resolución de problemas paso a paso de todas las fases PPP relacionadas y los parámetros negociados.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

CHAP se considera más seguro porque la contraseña de usuario nunca se envía a través de la conexión. Para obtener más información sobre CHAP, consulte Comprensión y Configuración de la Autenticación CHAP PPP.

A pesar de sus defectos, PAP puede usarse en los siguientes entornos:

- Una gran base de aplicaciones cliente instalada que no admite CHAP
- Incompatibilidad entre las distintas instrumentaciones de vendedores de CHAP
- Situaciones donde una contraseña de sólo texto deba estar disponible para simular un inicio de sesión en el host remoto.

Autenticación unidireccional versus bidireccional

Como con la mayoría de los tipos de autenticación, PAP admite autenticaciones unidireccionales (de una vía) y bidireccionales (de dos vías). Con la autenticación unidireccional, sólo el lado que recibe la llamada (NAS) autentica el lado remoto (cliente). El cliente remoto no autentica el

servidor.

Con la autenticación bidireccional, cada lado envía independientemente Authenticate-Request (AUTH-REQ) y recibe Authenticate-Acknowledge (AUTH-ACK) o Authenticate-Not Acknowledged (AUTH-NAK). Estos se pueden ver con el comando debug ppp authentication. A continuación, se muestra un ejemplo de esta depuración en el cliente:

```
*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.
```

En la salida de depuración antes mencionada, la autenticación era bidireccional. Sin embargo, si la autenticación unidireccional hubiese sido configurada, sólo se verían las dos primeras líneas de depuración.

Comandos de Configuración

Se requieren tres comandos para una autenticación PAP normal, descritos a continuación:

ppp autentificación pap [callin]

El router en que está configurado el comando ppp authentication pap utilizará PAP para verificar la identidad del otro lado (par). Esto significa que la otra parte (par) debe presentarle al dispositivo local su nombre de usuario/contraseña para verificarlos.

La opción **callin** dice que el router en el que está configurado el comando ppp authentication pap callin sólo autenticará al otro lado durante una llamada entrante. Para una llamada saliente, no autenticará el otro lado. Esto significa que el router que inicia la llamada no requiere de un pedido de autenticación (AUTH-REQ) de otro lado.

La siguiente tabla muestra cómo configurar la opción callin (Llamar):

Tipo de autenticación	Cliente (llamadas)	NAS (llamado)
Unidireccional	ppp authentication pap callin	ppp autentificación pap
Bidireccional	ppp autentificación pap	ppp autentificación pap

username <nombre de usuario> password <contraseña>

Este es el nombre de usuario y contraseña utilizados por el router local para autenticar el par PPP. Cuando el par manda su nombre de usuario y contraseña PAP, el router local revisará si el nombre de usuario y contraseña están configurados de forma local. Si hay una coincidencia exitosa, el par se autentica.

Nota: La función del comando username para PAP es diferente a su función para CHAP. Con CHAP, este nombre de usuario y contraseña se utilizan para generar la respuesta al desafío, pero PAP sólo lo usa para verificar si el nombre de usuario y la contraseña entrante son válidos.

Para una autenticación unidireccional, este comando sólo se requiere en el entrador llamado. Para la autentificación de dos sentidos este comando debe ser configurado en ambos lados.

PPP pap sent-username <nombre de usuario> password <contraseña>

Activa la autenticación PAP saliente. El router local utiliza el nombre de usuario y la contraseña especificados por el comando ppp pap sent-username para autenticarse en un dispositivo remoto. El otro router debe poseer este mismo nombre de usuario/contraseña configurados mediante el comando username descrito anteriormente.

Si utiliza la autenticación unidireccional, este comando sólo es necesario en el router que inicia la llamada. Para la autentificación de dos sentidos este comando debe ser configurado en ambos lados.

Ejemplo de configuración

Las siguientes secciones de configuración muestran los comandos PAP necesarios para un escenario de autenticación unidireccional.

Nota: Sólo se muestran las secciones pertinentes de la configuración.

Configuración de la parte que llama (cliente)

```
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.
```

Configuración del lado receptor (servidor)

```
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.
```

'Resultados de la depuración'

Para depurar un problema PPP PAP, utilice los comandos debug ppp negotiation y debug ppp authentication. Hay dos temas que tiene que observar:

1. ¿Están de acuerdo ambos lados en que el método de autenticación es PAP?
2. De ser así, ¿la autenticación PAP se realiza correctamente?

Consulte los debugs siguientes para obtener información sobre cómo responder correctamente a estas preguntas. Además, consulte Introducción a la Salida de debug ppp negotiation para obtener una explicación de todas las diferentes líneas de debugging con su significado relativo durante las diferentes fases PPP, incluida la autenticación PPP. Este documento es útil para determinar rápidamente la causa de los errores de negociación PPP. Para más información sobre la localización de averías ppp autentificación (utilizando o el PAP o la CHAP), refiera a la autentificación de localización de averías PPP (CHAP o PAP) para un organigrama completo, paso a paso para localizar averías de la fase de la autentificación PPP.

Depuración de la parte que llama (cliente) para realizar una autenticación PAP unidireccional correcta

```
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.
```

Depuración de la parte llamada (servidor) para realizar una autentificación PAP unidireccional correcta

```
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.
```

Solución de problemas de PAP

Mientras resuelve problemas de PAP, conteste las mismas preguntas que se muestran en la Sección de resultados de depuración:

1. ¿Están de acuerdo ambos lados en que el método de autenticación es PAP?
2. De ser así, ¿la autenticación PAP se realiza correctamente?

Para más información sobre la localización de averías ppp autentificación (utilizando o el PAP o la CHAP), refiera a la autentificación de localización de averías PPP (CHAP o PAP) para un organigrama completo, paso a paso para localizar averías de la fase de la autentificación PPP.

Ambas partes no coinciden sobre PAP como el protocolo de autenticación

En ciertas configuraciones, puede observarse que los dos lados no concuerdan en PAP como protocolo de autenticación o bien concuerdan en CHAP (mientras que se deseaba que fuera PAP). Utilice los siguientes pasos para solucionar los problemas:

1. Verifique que el router que recibe la llamada tenga uno de los siguientes comandos de autenticación

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

2. Compruebe que el router que realiza la llamada posee configurado el comando ppp authentication pap callin.
3. Verifique que el lado de llamada posea el comando ppp pap sent-username username password password correctamente configurado, donde el nombre de usuario y la contraseña coincidan con los configurados en el router de recepción.
4. Configure el comando ppp chap reject en el modo de configuración de la interfaz en el router de llamada.Los routers Cisco aceptarán CHAP como protocolo de autenticación de forma predeterminada. En una situación en la que el cliente desea hacer PAP pero el servidor de acceso puede hacer PAP o CHAP (ppp authentication chap pap configurado), el **comando ppp chap reject** se puede utilizar para obligar al cliente a aceptar PAP como protocolo de autenticación.

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

La autenticación PAP no tiene éxito

Si los dos lados están de acuerdo en PAP como protocolo de autenticación, pero la conexión PAP falla, es muy probable que se trate de un problema de nombre de usuario/contraseña.

1. Verifique que el lado de llamada posea el comando ppp pap sent-username username password password correctamente configurado, donde el nombre de usuario y la contraseña coincidan con los configurados en el router de recepción.
2. Para la autentificación en dos sentidos, verifique que el lado receptor tenga correctamente configurado el comando ppp pap sent-username username password password, donde el nombre del usuario y la contraseña coinciden con los configurados en el router de llamada.Al realizar la autenticación de doble sentido, si el comando ppp pap sent-username nombre de usuario password contraseña no estuviera presente en el router de recepción y el cliente PPP intenta forzar el servidor para autenticar en forma remota, el resultado de debug ppp negotiation (debug ppp autentication) indicaría

```
*Jan  3 16:47:20.259: Se0:1 PAP: Failed request for PAP credentials.  Username maui-nas-06
```

   Este mensaje de error indica un problema de configuración y no necesariamente una falla de seguridad.
3. 3. Verifique que el nombre de usuario y la contraseña coincidan con el configurado en el comando **ppp pap sent-username *username* password *password en el peer*.**Si no coinciden, verá este mensaje:

```
*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.
```

Información Relacionada

- Configuración de la Autenticación
- Diagrama de Flujo de Solución de Problemas de PPP
- Resolución de problemas de autenticación de PPP (CHAP o PAP)
- Introducción al resultado de debug ppp negotiation
- Autenticación de PPP utilizando los comandos ppp chap hostname y ppp authentication chap callin
- Tecnología de marcación manual: Descripciones y explicaciones
- Soporte Técnico y Documentación - Cisco Systems