Configurazione e risoluzione dei problemi del protocollo PAP (PPP Password Authentication Protocol)

Sommario

Introduzione

Il protocollo PPP (Point-to-Point Protocol) supporta attualmente due protocolli di autenticazione: Protocollo PAP (Password Authentication Protocol) e CHAP (Challenge Handshake Authentication Protocol). Entrambi sono specificati nella RFC 1334 e sono supportati sulle interfacce sincrone e asincrone.

- Il protocollo PAP fornisce un metodo semplice per consentire a un nodo remoto di stabilire la propria identità utilizzando un handshake bidirezionale. Al termine della fase di definizione del collegamento PPP, il nodo remoto invia ripetutamente una coppia nome utente/password attraverso il collegamento (in testo non crittografato) fino a quando non viene riconosciuta l'autenticazione o la connessione non viene terminata.
- PAP non è un protocollo di autenticazione sicuro. Le password vengono inviate attraverso il

link in formato testo non crittografato e non vi è alcuna protezione da attacchi di riproduzione o tentativi di commettere errori. Il nodo remoto controlla la frequenza e i tempi dei tentativi di accesso.

Per ulteriori informazioni sulla risoluzione dei problemi di autenticazione PPP (tramite PAP o CHAP), fare riferimento a Risoluzione dei problemi di autenticazione PPP (CHAP o PAP) per un diagramma di flusso completo e dettagliato che illustra la risoluzione dei problemi relativi alla fase di autenticazione PPP. Per ulteriori informazioni sulla risoluzione dei problemi relativi a tutte le fasi PPP (LCP, Autenticazione, NCP), consultare il diagramma di flusso per la risoluzione dei problemi PPP del documento per un diagramma di flusso completo che consenta di risolvere in modo dettagliato tutte le fasi PPP correlate e i parametri negoziati.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

La protezione CHAP è considerata maggiore in quanto la password utente non viene mai inviata attraverso la connessione. Per ulteriori informazioni sulla protezione CHAP, vedere Descrizione e configurazione dell'autenticazione CHAP PPP.

Nonostante le carenze, il PAP può essere utilizzato nei seguenti ambienti:

- Ampia base installata di applicazioni client che non supportano la protezione CHAP
- Incompatibilità tra le implementazioni di CHAP di diversi fornitori
- Situazioni in cui è necessario disporre di una password non crittografata per simulare un accesso all'host remoto

Autenticazione Unidirezionale E Bidirezionale

Come per la maggior parte dei tipi di autenticazione, PAP supporta l'autenticazione bidirezionale (bidirezionale) e unidirezionale (unidirezionale). Con l'autenticazione unidirezionale, solo il dispositivo che riceve la chiamata (NAS) autentica il dispositivo remoto (client). Il client remoto non autentica il server.

Con l'autenticazione bidirezionale, ciascun dispositivo invia in modo indipendente una richiesta di autenticazione (AUTH-REQ) e riceve una conferma di autenticazione (AUTH-ACK) o una richiesta

di autenticazione non riconosciuta (AUTH-NAK). Per visualizzarli, usare il comando debug ppp authentication. Di seguito è riportato un esempio di questo debug sul client:

```
*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.
```

Nell'output del comando debug sopra riportato, l'autenticazione è bidirezionale. Tuttavia, se è stata configurata l'autenticazione unidirezionale, verranno visualizzate solo le prime due righe di debug.

Comandi di configurazione

Di seguito sono descritti i tre comandi necessari per la normale autenticazione PAP:

ppp authentication pap [callin]

Il router su cui è configurato il comando ppp authentication pap utilizzerà il comando PAP per verificare l'identità dell'altro lato (peer). Ciò significa che l'altro lato (peer) deve presentare il proprio nome utente/password al dispositivo locale per la verifica.

L'opzione **callin** indica che il router su cui è configurato il comando ppp authentication pap callin eseguirà l'autenticazione solo sull'altro lato del router durante una chiamata in arrivo. Per una chiamata in uscita, non autenticherà l'altro lato. Ciò significa che il router che avvia la chiamata non richiede una richiesta di autenticazione (AUTH-REQ) dall'altro lato del collegamento

Nella tabella seguente viene illustrato quando configurare l'opzione di **chiamata**:

Tipo di autenticazione	Client (chiamata)	NAS (chiamato)
Unidirezionale	chiamata pap autenticazione ppp	app autenticazione ppp
Bidirezionale	app autenticazione ppp	app autenticazione ppp

username <nomeutente> password <password>

Nome utente e password utilizzati dal router locale per autenticare il peer PPP. Quando il peer invia il nome utente e la password PAP, il router locale controlla se il nome utente e la password sono configurati localmente. Se la corrispondenza ha esito positivo, il peer viene autenticato.

Nota: la funzione del comando username per PAP è diversa dalla funzione CHAP. Con la protezione CHAP, questo nome utente e questa password vengono utilizzati per generare la risposta alla richiesta di verifica, ma PAP la utilizza solo per verificare che un nome utente e una password in ingresso siano validi.

Per l'autenticazione unidirezionale, questo comando è richiesto solo sul router chiamato. Per l'autenticazione bidirezionale questo comando è necessario su entrambi i lati.

PPP pap nomeutente <nomeutente> password <password>

Abilita l'autenticazione PAP in uscita. Il router locale utilizza il nome utente e la password specificati dal comando ppp pap send-username per autenticarsi su un dispositivo remoto. Sull'altro router lo stesso nome utente/password deve essere configurato usando il comando **username** descritto sopra.

Se si utilizza l'autenticazione unidirezionale, questo comando è necessario solo sul router che avvia la chiamata. Per l'autenticazione bidirezionale questo comando deve essere configurato su entrambi i lati.

Esempio di configurazione

Nelle sezioni di configurazione seguenti vengono illustrati i comandi PAP necessari per uno scenario di autenticazione unidirezionale.

Nota: vengono visualizzate solo le sezioni pertinenti della configurazione.

Configurazione lato chiamata (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.
```

Configurazione lato ricezione (server)

```
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.
```

Output di debug

Per eseguire il debug di un problema PPP PAP, utilizzare i comandi debug ppp negotiation ed debug ppp authentication. Ci sono due questioni principali a cui prestare attenzione:

1. Entrambe le parti concordano sul fatto che il PAP sia il metodo di autenticazione?
2. In caso affermativo, l'autenticazione PAP ha esito positivo?

Per informazioni su come rispondere correttamente a queste domande, consultare i seguenti debug. Inoltre, fare riferimento a Descrizione dell'output della negoziazione PPP di debug per una spiegazione di tutte le righe di debug con il relativo significato durante le diverse fasi PPP, compresa l'autenticazione PPP. Questo documento è utile per determinare rapidamente la causa degli errori di negoziazione PPP. Per ulteriori informazioni sulla risoluzione dei problemi di autenticazione PPP (tramite PAP o CHAP), fare riferimento a Risoluzione dei problemi di autenticazione PPP (CHAP o PAP) per un diagramma di flusso completo e dettagliato che illustra la risoluzione dei problemi relativi alla fase di autenticazione PPP.

Debug (client) lato chiamata per una corretta autenticazione PAP unidirezionale

```
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.
```

Debug lato (server) chiamato per un'autenticazione PAP unidirezionale riuscita

```
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.
```

Risoluzione dei problemi relativi a PAP

Per risolvere il problema relativo a PAP, rispondere alle stesse domande riportate nella sezione Output di debug:

1. Entrambe le parti concordano sul fatto che il PAP sia il metodo di autenticazione?
2. In caso affermativo, l'autenticazione PAP ha esito positivo?

Per ulteriori informazioni sulla risoluzione dei problemi di autenticazione PPP (tramite PAP o CHAP), fare riferimento a Risoluzione dei problemi di autenticazione PPP (CHAP o PAP) per un diagramma di flusso completo e dettagliato che illustra la risoluzione dei problemi relativi alla fase di autenticazione PPP.

Le due parti non sono d'accordo sul protocollo PAP come protocollo di autenticazione

In alcune configurazioni, è possibile notare che i due dispositivi non concordano sul protocollo PAP come protocollo di autenticazione oppure sul protocollo CHAP (quando si desiderava il protocollo PAP). Per risolvere questi problemi, procedere come segue:

1. Verificare che il router che riceve la chiamata disponga di uno dei seguenti comandi di

autenticazione

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

2. Verificare che per il router che effettua la chiamata sia configurata la chiamata del pap di autenticazione ppp.
3. Verificare che sul lato chiamante il comando ppp pap nomeutente inviato *nomeutente* password sia configurato correttamente, dove il nome utente e la password corrispondano a quelli configurati sul router ricevente.
4. Configurare il comando ppp chap rifiuta in modalità di configurazione interfaccia sul router chiamante.Per impostazione predefinita, i router Cisco accettano la protezione CHAP come protocollo di autenticazione. In una situazione in cui il client desidera eseguire il protocollo PAP ma il server di accesso può eseguire il comando PAP o CHAP (autenticazione ppp chap pap configurata), il comando **ppp chap rifiuta** può essere utilizzato per forzare il client ad accettare il protocollo PAP come protocollo di autenticazione.
```
maui-soho-01(config)#interface BRI 0
maui-soho-01(config-if)#ppp chap refuse
```

Autenticazione PAP non riuscita

Se le due parti concordano che il protocollo PAP sia il protocollo di autenticazione, ma la connessione PAP non riesce, è molto probabile che si sia verificato un problema di nome utente/password.

1. Verificare che sul lato chiamante il comando **ppp pap send-username password** sia **configurato correttamente, dove il nome utente e la password corrispondono a quelli configurati sul router ricevente.**
2. Per l'autenticazione bidirezionale, verificare che il lato ricevente abbia il comando **ppp pap nomeutente** *nomeutente* **password** *configurato* correttamente, dove il nome utente e la password corrispondono a quelli configurati sul router chiamante.Quando si esegue l'autenticazione a due vie, se il comando **ppp pap nomeutente inviato** *nomeutente* **password** ***password non è presente sul router ricevente e il client PPP tenta di forzare il server a eseguire l'autenticazione in remoto, l'output della*** **negoziazione ppp di debug** (o **autenticazione ppp di debug**) indica
```
*Jan  3 16:47:20.259: Se0:1 PAP: Failed request for PAP credentials.  Username maui-nas-06
```
Questo messaggio di errore indica un problema di configurazione e non necessariamente una violazione della sicurezza.
3. 3. Verificare che il nome utente e la password corrispondano a quelli configurati nel comando **ppp pap nomeutente** *nomeutente* **password** password del peer.Se non corrispondono, viene visualizzato questo messaggio:
```
*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.
```

Informazioni correlate

- Configurazione dell'autenticazione
- Diagramma di flusso per la risoluzione dei problemi PPP
- Risoluzione dei problemi di autenticazione PPP (CHAP o PAP)
- Informazioni sull'output del comando debug ppp negotiation
- Autenticazione PPP utilizzando i comandi ppp chap hostname e ppp authentication chap callin
- Tecnologia Dialup: Panoramiche e spiegazioni
- Documentazione e supporto tecnico – Cisco Systems