Configuratie- en probleemoplossing van PPP Password-verificatie Protocol (PAP)

Inhoud

Inleiding

Point-to-Point Protocol (PPP) ondersteunt momenteel twee verificatieprotocollen: Wachtwoord-verificatieprotocol (PAP) en Challenge Handshake Authentication Protocol (CHAP). Beide worden gespecificeerd in RFC 1334 en worden ondersteund op synchrone en asynchrone interfaces.

- PAP biedt een eenvoudige methode voor een ver knooppunt om zijn identiteit vast te stellen met behulp van een tweevoudige handdruk. Nadat de fase van de PPP link-instelling is voltooid, wordt een gebruikersnaam en wachtwoordpaar herhaaldelijk door het externe knooppunt over de link verzonden (in duidelijke tekst) totdat de verificatie wordt erkend, of totdat de verbinding wordt beëindigd.
- PAP is geen beveiligd verificatieprotocol. De wachtwoorden worden in de duidelijke tekst over de link verzonden en er is geen bescherming tegen afspelen of proefaanvallen. De afstandsknooppunt heeft de frequentie en de timing van de inlogpogingen in handen.

Voor meer informatie over het oplossen van PPP-verificatie (met behulp van PAP of CHAP), raadpleeg de verificatie van probleemoplossing PPP (CHAP of PAP) voor een volledig, stap-voor-stap stroomschema voor het oplossen van de PPP-verificatiefase. Voor meer informatie over het oplossen van alle fasen in PPP (LCP, Verificatie, NCP), raadpleeg PPP-probleemoplossing in PPP-stroomschema voor een compleet stroomschema voor het stapsgewijze oplossen van alle gerelateerde fasen en onderhandelde parameters.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

CHAP wordt geacht veiliger te zijn omdat het gebruikerswachtwoord nooit over de verbinding wordt verzonden. Raadpleeg voor meer informatie over CHAP het begrip en het configureren van PPP CHAP-verificatie.

Ondanks zijn tekortkomingen kan PAP worden gebruikt in de volgende omgevingen:

- Een grote geïnstalleerde basis van clienttoepassingen die CHAP niet ondersteunen
- Onverenigbaarheden tussen verschillende verkoopimplementaties van CHAP
- OMSTANDIGHEDEN WAARIN ER EEN LICHTSTUURwachtwoord MOET ZIJN VOOR HET simuleren van de inloging op de afstandsbediening

Unidirectionele VS bidirectionele verificatie

Net als bij de meeste soorten authenticatie ondersteunt PAP bidirectionele (tweerichtingsverkeer) en unidirectionele (één manier) authenticatie. Met unidirectionele verificatie wordt alleen de zijde die de oproep ontvangt (NAS) geauthentificeerd als de externe zijde (client). De externe client authenticeert de server niet.

Met bidirectionele authenticatie stuurt elke kant onafhankelijk een Authenticate-request (AUTH-REQ) en ontvangt ofwel een Authenticate-ACK (AUTH-ACK) of Authenticate-Not Recognition (AUTH-NAK). Deze kunnen gezien worden met de **opdracht** debug ppp authenticatie. Een voorbeeld van dit debug bij de client wordt hieronder getoond:

```
*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.
```

In de bovenstaande debug uitvoer was de authenticatie tweerichtings. Maar als de unidirectionele authenticatie was ingesteld, zouden we alleen de eerste twee debug lijnen zien.

Configuratieopdrachten

Er zijn drie opdrachten vereist voor de normale PAP-verificatie die hieronder worden beschreven:

PPP-authenticatiepagina [bellen]

De router waarop de opdracht voor de PPP-verificatie **is ingesteld**, zal PAP gebruiken om de identiteit van de andere kant (peer) te controleren. Dit betekent dat de andere kant (peer) zijn gebruikersnaam/wachtwoord aan het lokale apparaat moet aanbieden ter verificatie.

De **callin** optie zegt dat de router dat de PPP **authenticatie-pagina die aanroep is ingesteld** alleen de andere kant tijdens een inkomend gesprek zal authentiseren. Voor een uitgaande telefoontje zal het de andere kant niet echt maken. Dit betekent dat de router die de oproep initieert geen verzoek om verificatie (AUTH-REQ) van de andere zijde vereist

De volgende tabel toont wanneer u de **bellenoptie** wilt configureren:

Verificatietype	Cliënt (bellen)	NAS (aangeroepen)
Unidirectioneel	PHP-authenticatiepagina oproepen	ppp-authenticatiepagina
gericht	ppp-authenticatiepagina	ppp-authenticatiepagina

Gebruikersnaam <gebruikersnaam> wachtwoord <wachtwoord>

Dit is de gebruikersnaam en het wachtwoord dat door de lokale router wordt gebruikt om de PPP-peer voor authentiek te verklaren. Wanneer de peer zijn PAP gebruikersnaam en wachtwoord verstuurt, zal de lokale router controleren of die gebruikersnaam en wachtwoord lokaal zijn ingesteld. Als er een succesvolle match is, is de peer authentiek.

Opmerking: de functie van de gebruikersnaam voor PAP is anders dan de functie voor CHAP. Met CHAP, worden deze gebruikersnaam en wachtwoord gebruikt om de reactie op de uitdaging te genereren, maar PAP gebruikt het alleen om te controleren of een inkomende gebruikersnaam en wachtwoord geldig zijn.

Voor eenrichtingsverificatie is deze opdracht alleen vereist op de opgeroepen router. Voor tweerichtingsverificatie is deze opdracht aan beide kanten nodig.

PPP pap verzonden gebruikersnaam <gebruikersnaam> <wachtwoord <wachtwoord>

Maakt uitgaande PAP-verificatie mogelijk. De lokale router gebruikt de gebruikersnaam en het wachtwoord die door de Pp-PHP verzonden-gebruikersnaam zijn opgegeven **om zichzelf** voor een extern apparaat te authentiseren. De andere router moet deze zelfde gebruikersnaam/wachtwoord hebben gevormd met gebruik van de hierboven beschreven **gebruikersnaam** opdracht.

Als u eenrichtingsverificatie gebruikt, is deze opdracht alleen nodig op de router die de oproep initieert. Voor tweerichtingsverificatie moet deze opdracht aan beide kanten zijn geconfigureerd.

Configuratievoorbeeld

De volgende configuratiesecties tonen de noodzakelijke PAP opdrachten voor een eenrichtingsauthenticatiescenario.

Opmerking: Alleen de relevante delen van de configuratie worden weergegeven.

Configuratie aan één zijde (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.
```

Configuratie ontvangerzijde (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.
```

Debug Outputs

Om een PPP PAP-kwestie te zuiveren gebruikt de debug PPP-onderhandeling en debug van ppp-verificatie opdrachten. Er zijn twee belangrijke kwesties waar u aandacht aan moet besteden:

1. Zijn beide partijen het erover eens dat PAP de methode van authenticatie is?
2. Zo ja, slaagt de PAP-verificatie dan in?

Raadpleeg de onderstaande specificaties voor informatie over hoe u deze vragen op de juiste manier kunt beantwoorden. Raadpleeg ook het gedeelte Begrip debug ppp onderhandeling voor een verklaring van alle verschillende zuiverende lijnen met hun relatieve betekenis tijdens de verschillende PPP-fasen, inclusief PPP-verificatie. Dit document is handig bij het snel bepalen van de oorzaak van fouten in PPP-onderhandeling. Voor meer informatie over het oplossen van PPP-verificatie (met behulp van PAP of CHAP), raadpleeg de verificatie van probleemoplossing PPP (CHAP of PAP) voor een volledig, stap-voor-stap stroomschema voor het oplossen van de PPP-verificatiefase.

Calling Side (client) debug voor een succesvolle eenmalige PAP-verificatie

```
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.
```

Geruchte Side (server) debug voor een succesvolle one-way PAP-verificatie

```
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.
```

PAP voor probleemoplossing

Wanneer u PAP-problemen oplossen, beantwoordt u dezelfde vragen die in de sectie Uitvoer van Debug worden getoond:

1. Zijn beide partijen het erover eens dat PAP de methode van authenticatie is?
2. Zo ja, slaagt de PAP-verificatie dan in?

Voor meer informatie over het oplossen van PPP-verificatie (met behulp van PAP of CHAP), raadpleeg de verificatie van probleemoplossing PPP (CHAP of PAP) voor een volledig, stap-voor-stap stroomschema voor het oplossen van de PPP-verificatiefase.

Beide partijen zijn het niet eens over de PAP als het verificatieprotocol

In bepaalde configuratie kunt u opmerken dat beide partijen het niet eens zijn over PAP als het verificatieprotocol of dat ze het in plaats daarvan eens zijn over CHAP (wanneer u PAP wilt). Gebruik de volgende stappen om dergelijke problemen op te lossen:

1. Controleer dat de router die de oproep ontvangt één van de volgende authenticatie opdrachten heeft

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

2. Controleer dat de router die de oproep doet de IP-verificatiepagina heeft ingeschakeld.
3. Controleer dat de roeping kant het opnamewachtwoord van de opdrachtupp heeft dat door de *gebruikersnaam* voor de *gebruikersnaam* is ingesteld op de juiste manier ingesteld, waarbij de gebruikersnaam en het wachtwoord overeenkomen met die welke op de ontvangende router zijn ingesteld.
4. Configureer de opdrachtregel dat de toepassing van ppp in de interfaceconfiguratiemodus op de oproepende router geweigerd wordt.Cisco-routers zullen standaard CHAP als verificatieprotocol accepteren. In een situatie waarin de client PAP wilt uitvoeren maar de toegangsserver PAP of CHAP kan uitvoeren (**Pp-authenticatie kettingpagina ingesteld**), kan de **Pp** chap opdracht worden gebruikt om de client te dwingen PAP als verificatieprotocol te accepteren.

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

PAP-verificatie heeft geen succes

Als de twee partijen het eens zijn over PAP als het authenticatieprotocol, maar de PAP-verbinding mislukt, is het zeer waarschijnlijk een gebruikersnaam/wachtwoord probleem.

1. Controleer dat de keerzijde de opdracht **PPP-pagina voor verzonden *gebruikersnaam*** voor het **wachtwoord** van de *gebruikersnaam* ***correct*** heeft **ingesteld**, waarbij de gebruikersnaam en het wachtwoord overeenkomen met die welke op de ontvangende router zijn ingesteld.
2. Voor tweevoudige authenticatie, controleer of de ontvangende kant de opdracht **ppp** ingestuurd**-gebruikersnaam wachtwoord** correct heeft **ingesteld**, waarbij de gebruikersnaam en het wachtwoord overeenkomen met die welke zijn ingesteld op de oproepende router.Bij het doen van bidirectionele authenticatie, als de opdracht **PPP-pagina verzonden-gebruikersnaam wachtwoord voor *gebruikersnaam*** niet aanwezig was op de ontvangende router en de PPP client pogingen om de server tot authenticatie te dwingen, zou de uitvoer van **debug ppp onderhandeling** (of **debug ppp authenticatie) betekenen**

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

   Deze foutmelding is een indicatie van een configuratie probleem en niet noodzakelijkerwijs een inbreuk op de beveiliging.
3. 3. Controleer dat de gebruikersnaam en het wachtwoord overeenkomen met het wachtwoord dat in het **opdrachtupp** ingesteld is**, en dat de *gebruikersnaam*** voor de **gebruikersnaam op de peer is ingesteld.**Als deze niet overeenkomen, ziet u dit bericht:

   ```
   *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.
   ```

Gerelateerde informatie

- Verificatie configureren
- Stroomdiagram voor PPP-probleemoplossing

- Problemen oplossen PPP (CHAP of PAP)-verificatie
- De betekenis van debug ppp-onderhandeling
- PPP-verificatie met behulp van de ppp chap hostname en ppp-verificatie ketting om opdrachten aan te roepen
- Kiezertechnologie: Overzichten en toelichtingen
- Technische ondersteuning en documentatie – Cisco Systems