Konfiguration und Fehlerbehebung für PPP Password Authentication Protocol (PAP)

Inhalt

Einführung

Point-to-Point Protocol (PPP) unterstützt derzeit zwei Authentifizierungsprotokolle: Password Authentication Protocol (PAP) und Challenge Handshake Authentication Protocol (CHAP). Beide sind in RFC 1334 angegeben und werden auf synchronen und asynchronen Schnittstellen unterstützt.

- PAP stellt eine einfache Methode für einen Remotecnoten bereit, um seine Identität mithilfe eines bidirektionalen Handshakes zu etablieren. Nach Abschluss der PPP-Verbindungsphase wird vom Remote-Knoten wiederholt (in Klartext) ein Benutzername- und Kennwortpaar über die Verbindung gesendet, bis die Authentifizierung bestätigt ist oder bis die Verbindung beendet ist.
- PAP ist kein sicheres Authentifizierungsprotokoll. Passwörter werden in Klartext über den Link gesendet, und es besteht kein Schutz vor Wiedergabe- oder Test-and-Error-Angriffen. Der

Remotecnoten steuert die Häufigkeit und das Timing der Anmeldeversuche.

Weitere Informationen zur Fehlerbehebung bei der PPP-Authentifizierung (entweder mit PAP oder CHAP) finden Sie unter Fehlerbehebung bei der PPP-Authentifizierung (CHAP oder PAP) für eine vollständige, schrittweise Ablaufübersicht zur Fehlerbehebung in der PPP-Authentifizierungsphase. Weitere Informationen zur Fehlerbehebung aller PPP-Phasen (LCP, Authentifizierung, NCP) finden Sie im Dokument PPP Troubleshooting Flowchart für ein vollständiges Flussdiagramm zur schrittweisen Fehlerbehebung aller zugehörigen PPP-Phasen und ausgehandelten Parameter.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

CHAP gilt als sicherer, da das Benutzerkennwort nie über die Verbindung übertragen wird. Weitere Informationen zu CHAP finden Sie unter Grundlagen und Konfigurieren der PPP CHAP-Authentifizierung.

Trotz seiner Mängel kann PAP in den folgenden Umgebungen verwendet werden:

- Eine große Anzahl von Client-Anwendungen, die CHAP nicht unterstützen
- Inkompatibilitäten zwischen verschiedenen CHAP-Implementierungen verschiedener Anbieter
- Situationen, in denen ein Klartext-Kennwort verfügbar sein muss, um eine Anmeldung am Remotehost zu simulieren

Unidirektionale und bidirektionale Authentifizierung

Wie bei den meisten Authentifizierungstypen unterstützt PAP die bidirektionale (bidirektionale) und unidirektionale (unidirektionale) Authentifizierung. Mit unidirektionaler Authentifizierung authentifiziert nur die Seite, die den Anruf empfängt (NAS) die Remote-Seite (Client). Der Remote-Client authentifiziert den Server nicht.

Bei bidirektionaler Authentifizierung sendet jede Seite unabhängig eine Authentifizierungs-Anfrage (AUTH-REQ) und erhält entweder eine Authentifizierungs-Bestätigung (AUTH-ACK) oder eine Authentifizierungs-Nicht bestätigt (AUTH-NAK). Diese sind mit dem **Befehl** debug ppp authentication **zu** sehen. Ein Beispiel für dieses Debuggen auf dem Client ist unten dargestellt:

```
*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 der obigen Debugausgabe war die Authentifizierung bidirektional. Wenn jedoch eine unidirektionale Authentifizierung konfiguriert worden wäre, würden wir nur die ersten beiden Debug-Zeilen sehen.

Konfigurationsbefehle

Für die normale PAP-Authentifizierung sind drei Befehle erforderlich (siehe unten):

ppp authentication pap [callin]

Der Router, auf dem der **Befehl** ppp authentication pap **konfiguriert ist,** verwendet PAP, um die Identität der anderen Seite (Peer) zu überprüfen. Dies bedeutet, dass die andere Seite (Peer) dem lokalen Gerät seinen Benutzernamen/sein Kennwort zur Überprüfung vorlegen muss.

Die **Anrufoption** besagt, dass der Router, auf dem der **Befehl** ppp authentication pap callin **konfiguriert ist, die andere Seite nur während eines eingehenden Anrufs authentifiziert.** Bei einem ausgehenden Anruf wird die andere Seite nicht authentifiziert. Das bedeutet, dass der Router, der den Anruf initiiert, keine Anforderung für die Authentifizierung (AUTH-REQ) von der anderen Seite benötigt.

Die folgende Tabelle zeigt, wann die **Anrufoption** konfiguriert wird:

Authentifizierungstyp	Client (anrufen)	NAS (genannt)
Unidirektional	ppp authentication pap callin	PPP-Authentifizierungspapier
Bidirektional	PPP-Authentifizierungspapier	PPP-Authentifizierungspapier

username <Benutzername> password <Kennwort>

Dabei handelt es sich um den Benutzernamen und das Kennwort, die der lokale Router zur Authentifizierung des PPP-Peers verwendet. Wenn der Peer seinen PAP-Benutzernamen und sein Kennwort sendet, überprüft der lokale Router, ob dieser Benutzername und das Kennwort lokal konfiguriert sind. Bei einer erfolgreichen Übereinstimmung wird der Peer authentifiziert.

Hinweis: Die Funktion des Befehls username für PAP unterscheidet sich von der Funktion für CHAP. Bei CHAP werden dieser Benutzername und das Kennwort verwendet, um die Antwort auf die Herausforderung zu generieren. PAP verwendet diese jedoch nur, um zu überprüfen, ob ein eingehender Benutzername und ein Passwort gültig sind.

Für die unidirektionale Authentifizierung ist dieser Befehl nur auf dem angerufenen Router erforderlich. Für die bidirektionale Authentifizierung ist dieser Befehl auf beiden Seiten erforderlich.

PPP-Seite hat einen Benutzernamen gesendet <Benutzername> Kennwort <Kennwort>

Aktiviert die ausgehende PAP-Authentifizierung. Der lokale Router verwendet den Benutzernamen und das Kennwort, die mit dem **Befehl** ppp pap sent-username angegeben sind, um sich bei einem Remote-Gerät zu authentifizieren. Auf dem anderen Router muss derselbe Benutzername/dasselbe Kennwort mit dem oben beschriebenen Befehl **username** konfiguriert sein.

Wenn Sie eine unidirektionale Authentifizierung verwenden, ist dieser Befehl nur auf dem Router erforderlich, der den Anruf initiiert. Für die bidirektionale Authentifizierung muss dieser Befehl auf beiden Seiten konfiguriert werden.

Konfigurationsbeispiel

In den folgenden Konfigurationsabschnitten werden die erforderlichen PAP-Befehle für ein unidirektionales Authentifizierungsszenario dargestellt.

Hinweis: Es werden nur die relevanten Abschnitte der Konfiguration angezeigt.

Konfiguration der Anruferseite (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.
```

Konfiguration der Empfangsseite (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.
```

Debugausgabe

Um ein PPP-PAP-Problem zu debuggen, verwenden Sie die **Befehle debug** ppp negotiation und **debug ppp authentication**. Es gibt zwei Hauptprobleme, auf die Sie achten müssen:

1. Stimmen beide Seiten darin überein, dass PAP die Authentifizierungsmethode ist?
2. Wenn ja, ist die PAP-Authentifizierung erfolgreich?

Informationen zur richtigen Beantwortung dieser Fragen finden Sie in den folgenden Debugging-Ressourcen. Bitte lesen Sie auch Verständnis der Debug-PPP-Aushandlung-Ausgabe für eine Erläuterung aller verschiedenen Debuglinien mit ihrer relativen Bedeutung während der verschiedenen PPP-Phasen, einschließlich PPP-Authentifizierung. Dieses Dokument ist hilfreich, um die Ursache für PPP-Verhandlungsfehler schnell zu ermitteln. Weitere Informationen zur Fehlerbehebung bei der PPP-Authentifizierung (entweder mit PAP oder CHAP) finden Sie unter Fehlerbehebung bei der PPP-Authentifizierung (CHAP oder PAP) für eine vollständige, schrittweise Ablaufübersicht zur Fehlerbehebung in der PPP-Authentifizierungsphase.

Debuggen der Anruferseite (Client) für eine erfolgreiche unidirektionale PAP-Authentifizierung

```
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.
```

Debugging mit der Bezeichnung Side (Server) für eine erfolgreiche unidirektionale PAP-Authentifizierung

```
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.
```

Fehlerbehebung PAP

Beantworten Sie bei der Fehlerbehebung für PAP die gleichen Fragen, die im Abschnitt Debugausgabe beschrieben sind:

1. Stimmen beide Seiten darin überein, dass PAP die Authentifizierungsmethode ist?
2. Wenn ja, ist die PAP-Authentifizierung erfolgreich?

Weitere Informationen zur Fehlerbehebung bei der PPP-Authentifizierung (entweder mit PAP oder CHAP) finden Sie unter Fehlerbehebung bei der PPP-Authentifizierung (CHAP oder PAP) für eine vollständige, schrittweise Ablaufübersicht zur Fehlerbehebung in der PPP-Authentifizierungsphase.

Die beiden Seiten sind sich nicht einig, dass PAP das Authentifizierungsprotokoll ist.

In einer bestimmten Konfiguration können Sie feststellen, dass die beiden Seiten PAP nicht als Authentifizierungsprotokoll akzeptieren oder stattdessen CHAP akzeptieren (wenn Sie PAP

wollten). Führen Sie die folgenden Schritte aus, um solche Probleme zu beheben:

1. Vergewissern Sie sich, dass der Router, der den Anruf empfängt, über einen der folgenden Authentifizierungsbefehle verfügt.

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

2. Stellen Sie sicher, dass für den Router, der den Anruf durchführt, der **PPP-Authentifizierungs-Pap-Anruf konfiguriert** ist.
3. Vergewissern Sie sich, dass auf der Anruferseite der Befehl **ppp pap sent-username *username* password *password*** korrekt konfiguriert ist, wobei Benutzername und Kennwort mit dem auf dem empfangenden Router konfigurierten Kennwort übereinstimmen.
4. Konfigurieren Sie den Befehl **ppp chap im Schnittstellenkonfigurationsmodus** des anrufenden Routers.Cisco Router akzeptieren standardmäßig CHAP als Authentifizierungsprotokoll. In einer Situation, in der der Client PAP ausführen möchte, der Zugriffsserver jedoch PAP oder CHAP (ppp authentication chap pap konfiguriert) ausführen kann, kann der Befehl **ppp chap ablehnen** verwendet werden, um den Client zu zwingen, PAP als Authentifizierungsprotokoll zu akzeptieren.

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

PAP-Authentifizierung ist nicht erfolgreich

Wenn beide Seiten PAP als Authentifizierungsprotokoll vereinbaren, die PAP-Verbindung jedoch ausfällt, handelt es sich höchstwahrscheinlich um ein Problem mit dem Benutzernamen/Kennwort.

1. Vergewissern Sie sich, dass auf der Anruferseite der Befehl **ppp pap sent-username *username* password *password*** korrekt konfiguriert ist, wobei Benutzername und Kennwort mit dem auf dem empfangenden Router konfigurierten Kennwort übereinstimmen.
2. Überprüfen Sie für die bidirektionale Authentifizierung, ob auf der Empfängerseite der Befehl **ppp pap sent-username *username* password *password*** korrekt konfiguriert ist, wobei Benutzername und Kennwort mit dem auf dem anrufenden Router konfigurierten Kennwort übereinstimmen.Wenn bei der bidirektionalen Authentifizierung der Befehl **ppp pap sent-username *username* password kennwort *password* nicht auf dem empfangenden Router vorhanden war und der PPP-Client versucht, die Remote-Authentifizierung des Servers zu erzwingen, gibt die Ausgabe der Debug-ppp-Aushandlung** (oder **Debug-PPP-Authentifizierung) Folgendes an:**

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

   Diese Fehlermeldung weist auf ein Konfigurationsproblem und nicht unbedingt auf eine Sicherheitslücke hin.
3. 3. Vergewissern Sie sich, dass der Benutzername und das Kennwort mit dem im Befehl **ppp pap sent-username *username* password *password* auf dem Peer** konfigurierten übereinstimmen.Wenn diese nicht übereinstimmen, wird folgende Meldung angezeigt:

   ```
   *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.
```

Zugehörige Informationen

- Konfigurieren der Authentifizierung
- PPP-Fehlerbehebung Flussdiagramm
- Fehlerbehebung Authentifizierung nach PPP (CHAP oder PAP)
- Debugging-PPP-Aushandlung
- PPP-Authentifizierung mit dem PPP-chap-Hostnamen und den ppp-Authentifizierungschap-Callin-Befehlen
- DFÜ-Technologie: Übersichten und Erklärungen
- Technischer Support und Dokumentation - Cisco Systems