De PPP CHAP-verificatie configureren en begrijpen

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[Achtergrondinformatie](#)
[CHAP configureren](#)
[Eenvoudige en tweevoudige verificatie](#)
[Opdrachten en opties voor CHAP-configuratie](#)
[Transactioneel voorbeeld](#)
[Aanroepen](#)
[uitdaging](#)
[Reactie](#)
[Respons (vervolg)](#)
[Verifieer CHAP](#)
[Resultaat](#)
[CHAP voor probleemoplossing](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe het Challenge Handshake Authentication Protocol (CHAP) de identiteit van een peer verifieert door middel van een handdruk in drie richtingen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe te om PPP op de interface door toe te laten encapsulation ppp uit.
- Het **debug ppp negotiation** opdrachtoutput. Zie debug ppp-onderhandelingsoutput begrijpen voor meer informatie.
- Hoe u problemen kunt oplossen wanneer de fase Link Control Protocol (LCP) niet in de open staat is. Dit komt doordat de PPP-verificatiefase niet begint totdat de LCP-fase is voltooid en zich in de open staat bevindt. Indien de debug ppp negotiationhet bevel wijst er niet op dat LCP open is, moet u problemen oplossen deze kwestie alvorens u te werk gaat.

Opmerking: dit document is niet gericht op MS-CHAP (versie 1 of versie 2).

Gebruikte componenten

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

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

Achtergrondinformatie

Het Challenge Handshake Authentication Protocol (CHAP) (gedefinieerd in RFC 1994) verifieert de identiteit van de peer door middel van een drierichtings-handshake. Dit zijn de algemene stappen die in CHAP worden uitgevoerd:

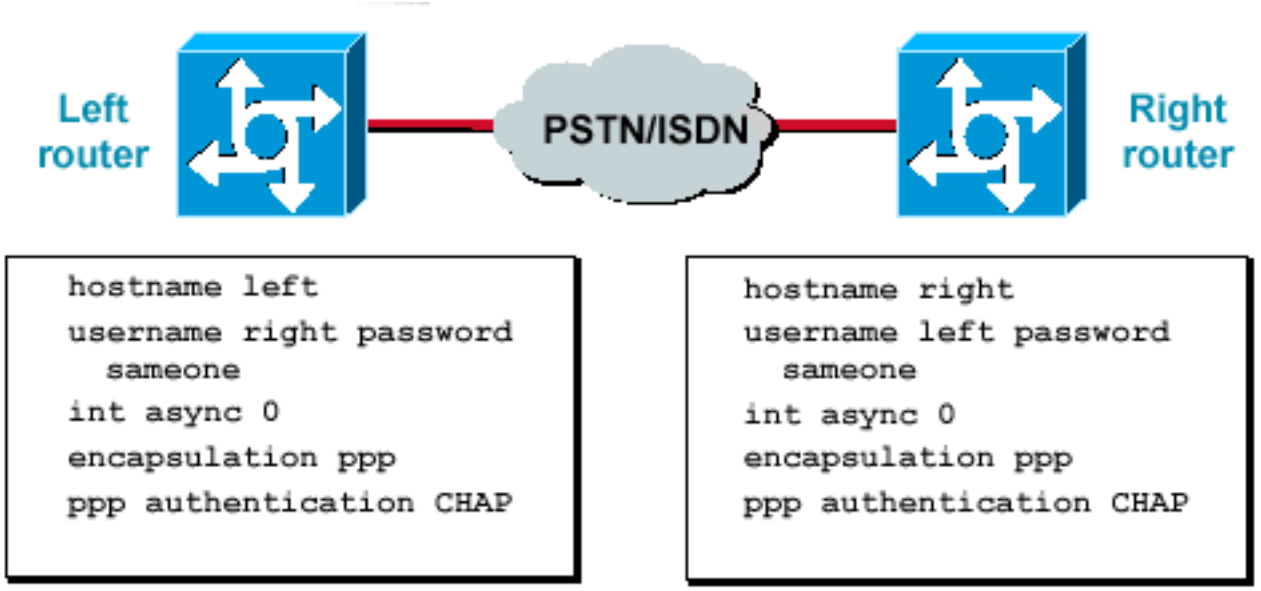
1. Nadat de fase LCP (Link Control Protocol) is voltooid en de CHAP tussen beide apparaten is overeengekomen, stuurt de verificator een challenge bericht naar de peer.
2. De peer reageert met een waarde die wordt berekend met een unidirectionele hashfunctie (Message Digest 5 (MD5)).
3. De authenticator controleert het antwoord aan de hand van zijn eigen berekening van de verwachte hashwaarde. Als de waarden overeenkomen, is de verificatie geslaagd. Anders wordt de verbinding beëindigd.

Deze verificatiemethode is afhankelijk van een "geheim" dat alleen bekend is bij de verificator en de peer. Het geheim wordt niet via de link verzonden. Hoewel de authenticatie slechts eenrichtingsverkeer is, kunt u over CHAP in beide richtingen onderhandelen, met behulp van dezelfde geheime set voor wederzijdse authenticatie.

Zie RFC 1994 voor meer informatie over de voor- en nadelen van CHAP.

CHAP configureren

De procedure om CHAP te configureren is vrij eenvoudig. Stel bijvoorbeeld dat u twee routers hebt, links en rechts, aangesloten over een netwerk, zoals in afbeelding 1.



Twee routers die over een netwerk zijn verbonden

Afbeelding 1 — Twee routers die over een netwerk zijn verbonden

Voltooi de volgende stappen om CHAP-verificatie te configureren:

1. Geef op de interface de opdracht **inkapseling ppp uit**.
2. Schakel het gebruik van CHAP-verificatie op beide routers in met de **ppp authentication chap** uit.
3. Configureer de gebruikersnaam en wachtwoorden. Hiervoor geeft u de **username username password password**commando, waarbij de gebruikersnaam de hostnaam van de peer is. Zorg ervoor dat:De wachtwoorden zijn aan beide uiteinden identiek.De routernaam en het wachtwoord zijn precies het zelfde, omdat zij hoofdlettergevoelig zijn.

   Opmerking: standaard gebruikt de router zijn hostnaam om zich te identificeren met de peer. Deze CHAP-gebruikersnaam kan echter worden gewijzigd via de ppp chap hostname uit. Zie PPP-verificatie met de ppp-chap hostname en ppp-verificatie chap en bel Opdrachten voor meer informatie.

Eenvoudige en tweevoudige verificatie

CHAP is gedefinieerd als een unidirectionele verificatiemethode. U gebruikt echter CHAP in beide richtingen om een tweerichtingsverificatie te maken. Daarom, met bidirectionele CHAP, wordt een afzonderlijke handdruk met drie richtingen geïnitieerd door elke kant.

In de implementatie van Cisco CHAP, moet de opgeroepen partij standaard de oproepende partij verifiëren (tenzij de verificatie volledig is uitgeschakeld). Daarom is een eenrichtingsauthenticatie die wordt geïnitieerd door de opgeroepen partij de minimum mogelijke authenticatie. De oproepende partij kan echter ook de identiteit van de opgeroepen partij verifiëren, wat resulteert in een tweerichtingsverificatie.

Eenvoudige verificatie is vaak vereist wanneer u verbinding maakt met apparaten die niet van Cisco zijn.

Voor eenrichtingsverificatie configureert u de **ppp authentication chap callin**bevel op de roepende router.

Tabel 1 toont wanneer de beloptie moet worden geconfigureerd.

Tabel 1: Wanneer moet u de beloptie configureren

Verificatietype	Klant (bellen)	NAS (genaamd)
Enkele weg (unidirectioneel)	**ppp-verificatie-chap-bellen**	**ppp-verificatiekaart**
Bidirectioneel (bidirectioneel)	**ppp-verificatiekaart**	**ppp-verificatiekaart**

Zie PPP-verificatie met de ppp-chap hostname en ppp-verificatie chap en bel Opdrachten voor meer informatie.

Opdrachten en opties voor CHAP-configuratie

Tabel 2 geeft een overzicht van de opdrachten en opties voor CHAP:

Tabel 2: CHAP-opdrachten en -opties

Opdracht	Beschrijving
ppp-verificatie {chap | ms-chap | ms-chap-v2 | eap |pap} [bellen]	Deze opdracht maakt lokale verificatie van de externe PPP-peer met het gespecificeerde protocol mogelijk.
ppp chap hostname gebruikersnaam	Deze opdracht definieert een interfacespecifieke CHAP-hostnaam. Zie PPP-verificatie met de ppp-chap hostname en ppp-verificatie chap voor meer informatie.
PPPoE wachtwoord wachtwoord wachtwoord	Deze opdracht definieert een interfacespecifiek CHAP-wachtwoord.
ppp-richtingaanroep | bijschrift | toegewezen	Dit bevel dwingt een vraagrichting. Gebruik deze opdracht wanneer een router verward is over de vraag of de vraag inkomend of uitgaand is (bijvoorbeeld, wanneer verbonden back-to-back of verbonden door huurlijnen en de Channel Service Unit of Data Service Unit (CSU/DSU) of ISDN Terminal Adapter (TA) zijn geconfigureerd om te bellen).
ppp chap weigeren [callin]	Deze opdracht schakelt externe verificatie door een peer uit (standaard ingeschakeld). Met deze opdracht is de CHAP-verificatie uitgeschakeld voor alle oproepen, wat betekent dat alle pogingen van de peer om de gebruiker te dwingen om met behulp van CHAP te verifiëren worden geweigerd. De callin optie specificeert dat de router weigert om de verificatieuitdagingen van het KLOOFJE te beantwoorden die van de peer worden ontvangen, maar nog steeds vereist dat de peer alle uitdagingen van het KLOOFJE beantwoordt die de router verzendt.
ppp chap wait	Deze opdracht specificeert dat de beller eerst moet verifiëren (standaard ingeschakeld). Dit bevel specificeert dat de router niet aan een peer voor authentiek verklaart die om de authentificatie van het KLOOFJE verzoekt tot nadat de peer zich aan de router voor authentiek heeft verklaard.
ppp max-bad-auth	Deze opdracht specificeert het toegestane aantal verificatiepogingen (de standaardwaarde is 0). Met deze opdracht wordt een point-to-point interface geconfigureerd om zichzelf niet onmiddellijk na een verificatiefout te herstellen, maar om in plaats daarvan een bepaald aantal verificatiepogingen toe te staan.
ppp chap splitnamen	Deze verborgen opdracht staat verschillende hostnamen toe voor een CHAP-uitdaging en -respons (de standaardwaarde is uitgeschakeld).
ppp chap ignoreus	Deze verborgen opdracht negeert CHAP-uitdagingen met de lokale naam (de standaardwaarde is ingeschakeld).

Transactioneel voorbeeld

De diagrammen in deze sectie tonen de serie gebeurtenissen die tijdens een CHAP-verificatie tussen twee routers optreden. Dit zijn niet de werkelijke berichten die worden gezien in de debug ppp negotiationopdrachtoutput. Zie debug ppp-onderhandelingsoutput begrijpen voor meer informatie.

Aanroepen

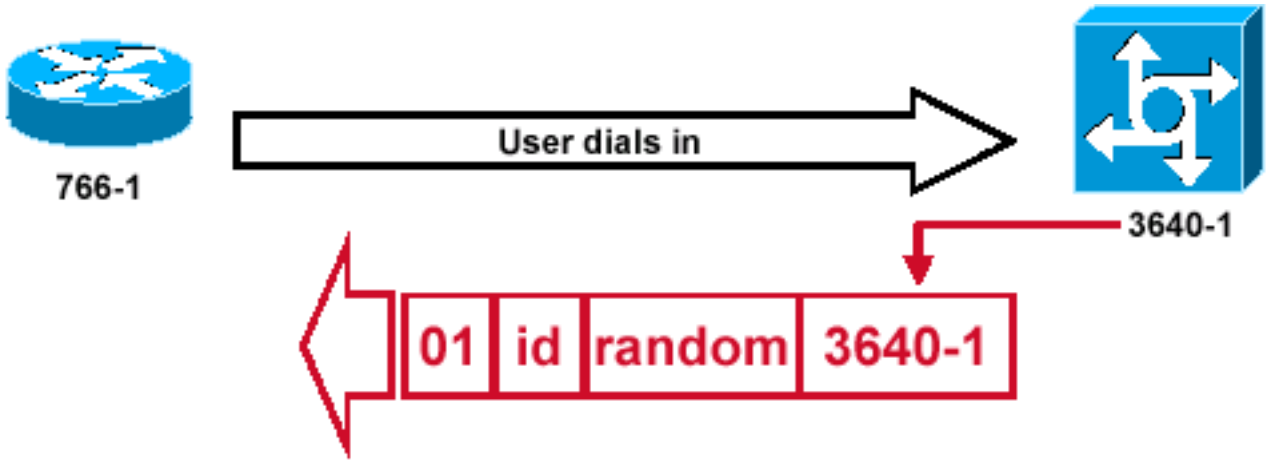
De oproep verschijnt

Afbeelding 2 — De oproep wordt ontvangen

Afbeelding 2 toont de volgende stappen:

1. De oproep komt binnen op 3640-1. De inkomende interface wordt geconfigureerd met de ppp authentication chap uit.
2. LCP onderhandelt over CHAP en MD5. Voor meer informatie over hoe dit te bepalen, zie debug ppp-onderhandelingsoutput begrijpen.
3. Een uitdaging van het KLOOFJE van 3640-1 aan de roepende router wordt vereist op deze vraag.

uitdaging



C HAP Challenge Packet is gebouwd

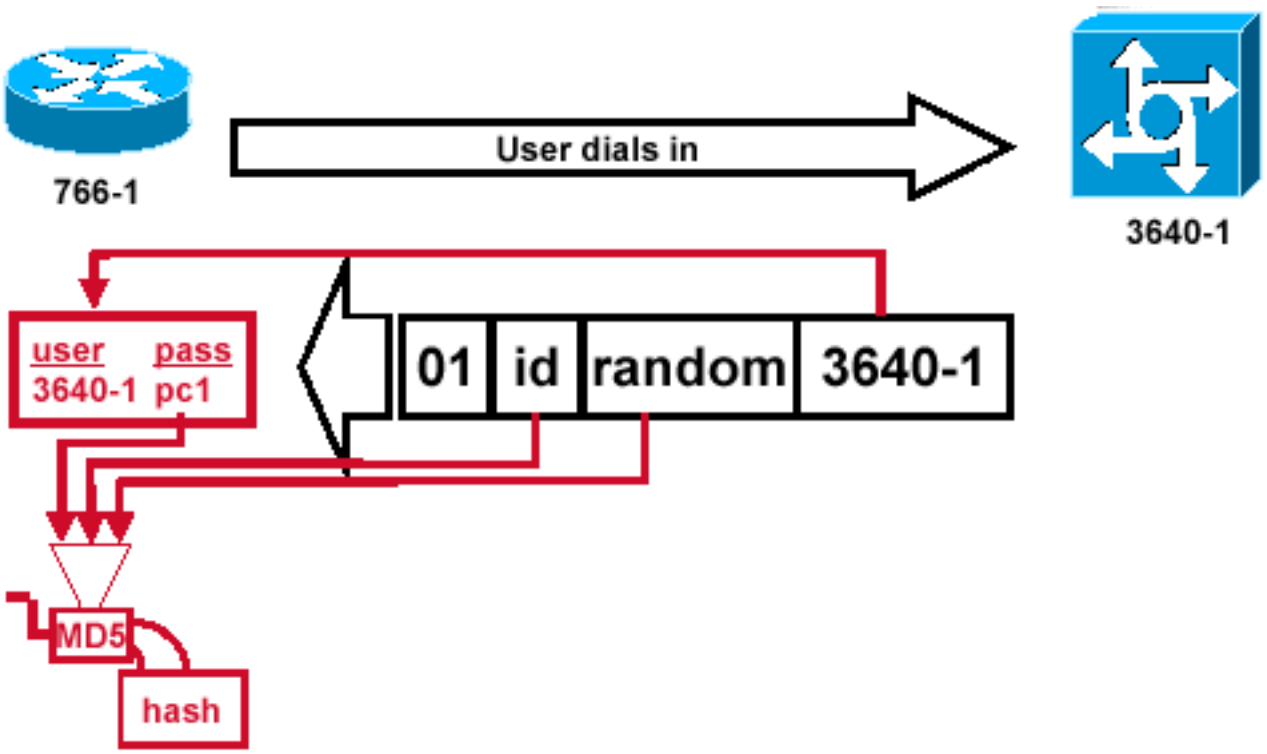
Afbeelding 3 — Er wordt een CHAP Challenge Packet gebouwd

Afbeelding 3 illustreert deze stappen in de CHAP-verificatie tussen de twee routers:

1. Een CHAP-provocatiepakket is gebouwd met deze kenmerken:01 = Identificatiecode van het type provocatiepakket.ID = volgnummer dat de uitdaging identificeert.willekeurig = een

redelijk willekeurig aantal dat door de router wordt geproduceerd.3640-1 = de authenticatienaam van de tegenstander.
2. De ID- en willekeurige waarden worden op de opgeroepen router bewaard.
3. Het provocatiepakket wordt naar de oproepende router verzonden. Er wordt een lijst van openstaande uitdagingen bijgehouden.

Reactie



Ontvang en MD5 verwerking van het Challenge Packet via de peer

Afbeelding 4 — Ontvang en MD5-verwerking van het Challenge-pakket via de peer

Afbeelding 4 illustreert hoe het provocatiepakket wordt ontvangen van de peer en verwerkt (MD5). De router verwerkt het inkomende CHAP-provocatiepakket op deze manier:

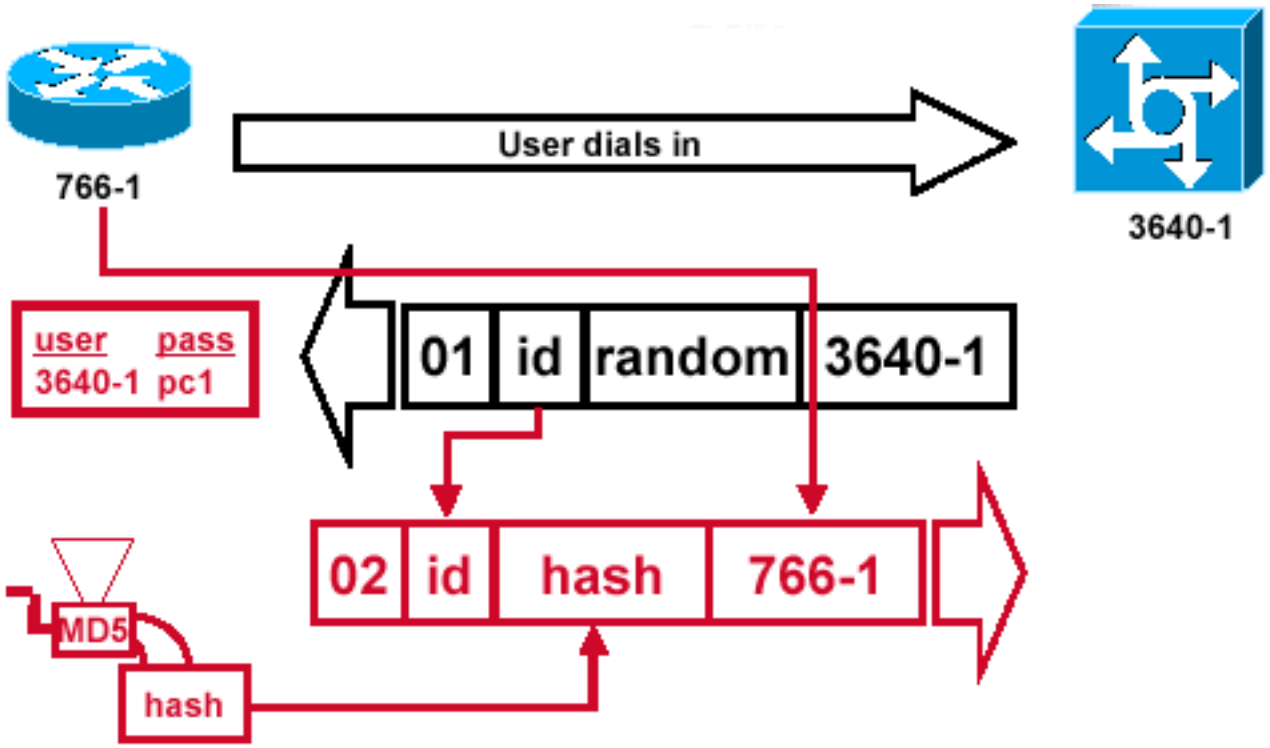
1. De ID-waarde wordt in de MD5-hashgenerator ingevoerd.
2. De willekeurige waarde wordt in de MD5-hashgenerator ingevoerd.
3. De naam 3640-1 wordt gebruikt om het wachtwoord op te zoeken. De router zoekt een ingang die de gebruikersbenaming in de uitdaging aanpast. In dit voorbeeld wordt gezocht naar:

```
username 3640-1 password pc1
```

4. Het wachtwoord wordt ingevoerd in de MD5-hashgenerator.

Het resultaat is de one-way MD5-hashed CHAP-uitdaging die wordt teruggestuurd in de CHAP-respons.

Respons (vervolg)



CHAP-responspakket dat naar de verificator wordt verzonden, is gebouwd

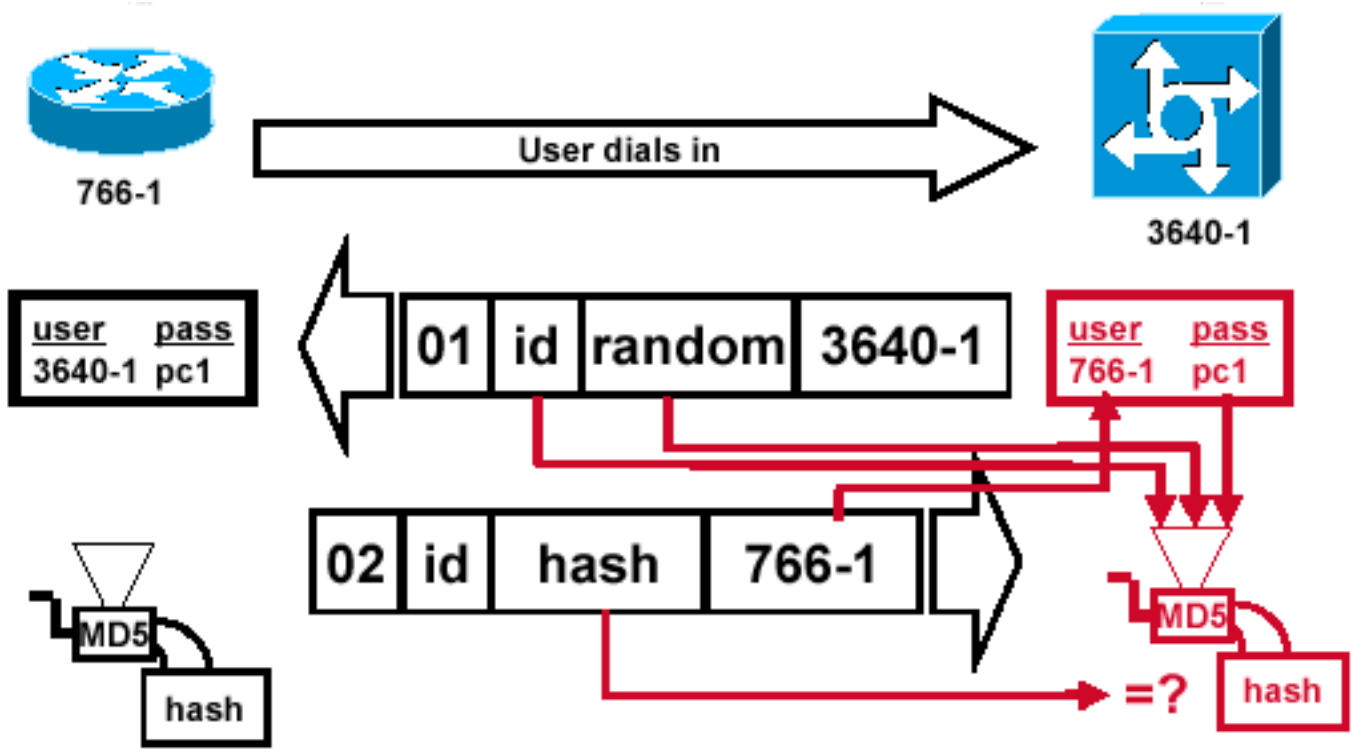
Afbeelding 5 — Het CHAP-responspakket dat naar de verificator wordt verzonden, is gebouwd

Afbeelding 5 illustreert hoe het CHAP-responspakket dat naar de verificator is verzonden, wordt gebouwd. In dit diagram worden de volgende stappen getoond:

1. Het antwoordpakket is samengesteld uit deze componenten:02 = Identificatiecode van het pakkettype van de CHAP-respons.ID = gekopieerd van het challenge pakket.hash = de uitvoer van de MD5 hashgenerator (de gehakte informatie van het challenge pakket).766-1 = de verificatienaam van dit apparaat. Dit is nodig voor de peer om de gebruikersnaam en wachtwoordinvoer op te zoeken die nodig is om de identiteit te verifiëren (dit wordt meer in detail uitgelegd in de sectie Controleer de CHAP).
2. Het reactiepakket wordt vervolgens naar de uitdager gestuurd.

Verifieer CHAP

Dit gedeelte bevat tips voor het verifiëren van uw configuratie.



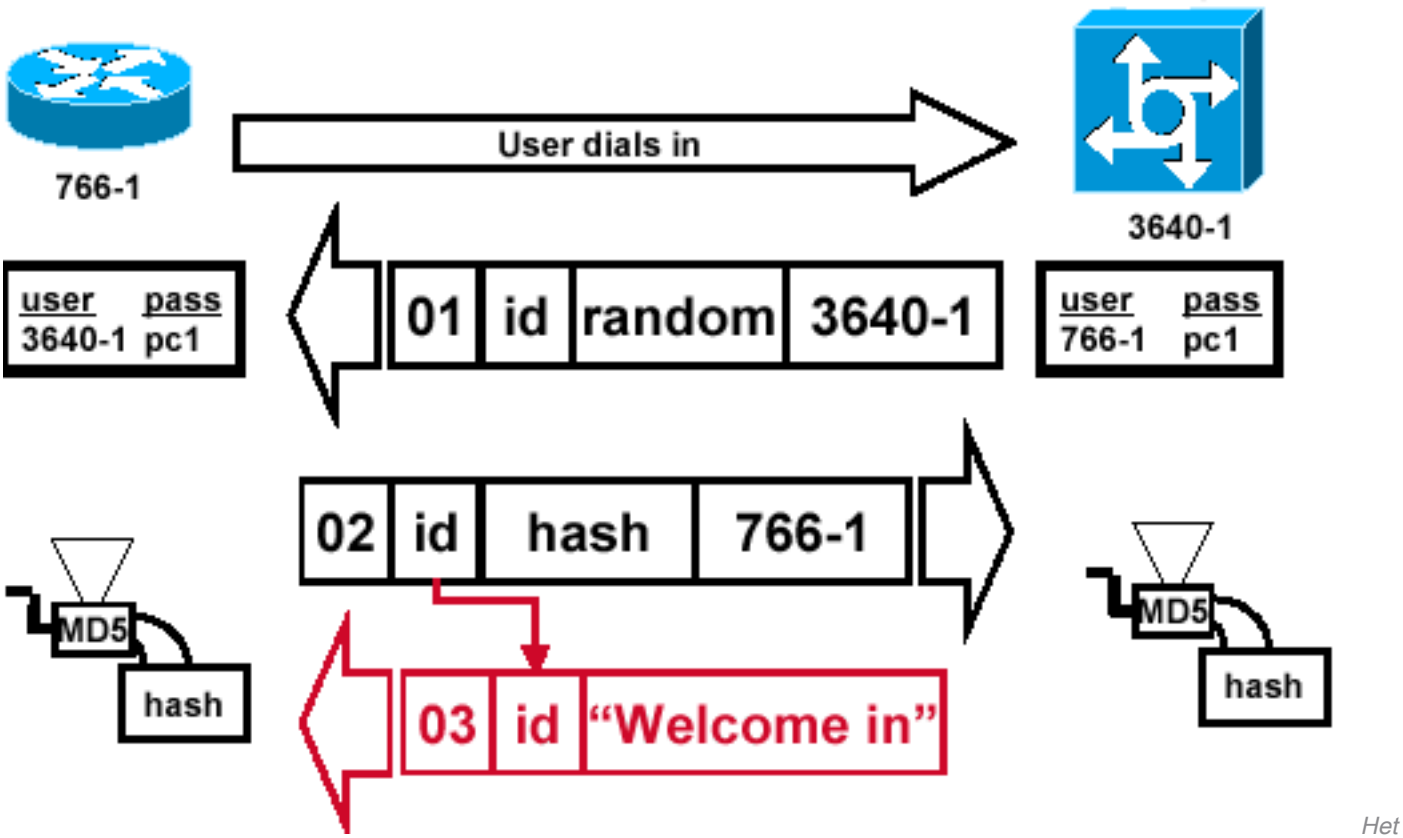
Challenger verwerkt het Response Packet

Afbeelding 6 — De uitdager verwerkt het responspakket

Figuur 6 toont hoe de uitdager het reactiepakket verwerkt. Hier zijn de stappen in kwestie wanneer het CHAP-responspakket wordt verwerkt (op de verificator):

1. De ID wordt gebruikt om het oorspronkelijke provocatiepakket te vinden.
2. De ID wordt ingevoerd in de MD5-hashgenerator.
3. De originele challenge random value wordt in de MD5 hash generator ingevoerd.
4. De naam 766-1 wordt gebruikt om het wachtwoord op te zoeken via een van deze bronnen:Lokale gebruikersnaam en wachtwoorddatabase.RADIUS- of TACACS+-server.
5. Het wachtwoord wordt ingevoerd in de MD5-hashgenerator.
6. De hashwaarde die in het responspakket wordt ontvangen, wordt vervolgens vergeleken met de berekende MD5-hashwaarde. De authentificatie van het KLOOFJE slaagt als de berekende en ontvangen knoeiboelwaarden gelijk zijn.

Resultaat



Het succesbericht wordt naar de belrouter verzonden

Afbeelding 7 — Success Message wordt naar de belrouter verzonden

Figuur 7 illustreert het succesbericht dat naar de roepende router wordt verzonden. Dit omvat de volgende stappen:

1. Als de authentificatie succesvol is, wordt een het succespakket van het KLOOFJE gebouwd van deze componenten:03 = Type CHAP-succesbericht.ID = gekopieerd van het responspakket."Welkom in" is gewoon een tekstbericht dat een door de gebruiker leesbare uitleg geeft.
2. Als de verificatie mislukt, wordt er een CHAP-storingspakket gemaakt van deze componenten:04 = Type CHAP-foutbericht.ID = gekopieerd van het responspakket."Verificatiefout" of ander tekstbericht dat een door de gebruiker leesbare verklaring bevat.
3. Het succes of mislukkingspakket wordt dan verzonden naar de roepende router.

Opmerking: in dit voorbeeld wordt eenrichtingsverificatie weergegeven. Bij een tweerichtingsverificatie wordt dit gehele proces herhaald. De oproepende router stelt echter de eerste uitdaging in werking.

CHAP voor probleemoplossing

Raadpleeg Probleemoplossing voor PPP (CHAP of PAP)-verificatie voor informatie over het oplossen van problemen.

Gerelateerde informatie

- Begrijp debug ppp onderhandelingsoutput
- PPP-verificatie met de opdrachten ppp-chap hostname en ppp-verificatiechap
- Cisco technische ondersteuning en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.