PPP-verificatie met behulp van de ppp chap hostname en ppp-verificatie ketting om opdrachten aan te roepen

Inhoud

Inleiding

PPP-onderhandeling omvat meerdere stappen, zoals LCP-onderhandeling (Link Control Protocol), verificatie en NCP-onderhandeling (Network Control Protocol). Als de twee partijen het niet eens kunnen worden over de juiste parameters, wordt de verbinding beëindigd. Zodra de link is gelegd, authentiseren de twee partijen elkaar met behulp van het authenticatieprotocol dat is overeengekomen tijdens LCP-onderhandeling. Verificatie moet succesvol zijn voordat de NCP-onderhandeling wordt gestart.

PPP steunt twee authenticatieprotocollen: Wachtwoord-verificatieprotocol (PAP) en Challenge Handshake Authentication Protocol (CHAP).

Voorwaarden

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de onderstaande software- en hardwareversies.

- Cisco IOS® softwarerelease 11.2 of hoger

Achtergrondinformatie

PAP-verificatie omvat een tweevoudige handdruk waarbij de gebruikersnaam en het wachtwoord via de link in duidelijke tekst worden verzonden; daarom biedt PAP-verificatie geen bescherming tegen afspelen en lijnbeugel.

De authenticatie van het KAP, aan de andere kant, verifieert de identiteit van het verre knooppunt periodiek met behulp van een handdruk van drie kanten. Nadat de PPP verbinding wordt gevestigd, stuurt de gastheer een "uitdaging" bericht naar het verre knooppunt. Het afstandsknooppunt reageert met een waarde die wordt berekend met behulp van een eenrichtingsknopfunctie. De gastheer controleert de reactie aan de hand van zijn eigen berekening van de verwachte hashwaarde. Indien de waarden overeenkomen, wordt de authenticatie erkend; anders wordt de verbinding beëindigd.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Als u aanvullende informatie wilt vinden over de opdrachten die in dit document worden gebruikt, gebruikt u het IOS-opnamegereedschap

Unidirectionele CHAP-verificatie configureren

Wanneer twee apparaten meestal gebruik maken van CHAP-authenticatie, stuurt elke kant een uitdaging uit waaraan de andere kant reageert en geauthentiseerd wordt door de uitdager. Elke partij authentificeert elkaar onafhankelijk. Als u met niet-Cisco routers wilt werken die geen authenticatie door de oproepende router of het oproepapparaat ondersteunen, moet u de **PPP authenticatieschap** gebruiken **die** opdracht **oproept**. Wanneer het gebruik van de opdracht **van** de **ppp authenticatie** met het **callin** sleutelwoord, zal de Server van de Toegang slechts het verre apparaat authentiseren als het afstandsapparaat de vraag (bijvoorbeeld, als het verre apparaat "binnen"aanbelde) in werking stelde. In dit geval wordt de authenticatie alleen gespecificeerd op inkomende (ontvangen) oproepen.

Een gebruikersnaam configureren die afwijkt van de naam van de router

Wanneer een externe Cisco-router zich verbindt met een Cisco-router of een niet-Cisco centrale router van een andere administratieve controle, een Internet Service Provider (ISP) of een draaischijf van centrale routers, is het nodig om een gebruikersnaam voor de verificatie te

configureren die niet overeenkomt met de hostnaam. In deze situatie wordt de hostname van de router niet of op verschillende tijdstippen (draaiend) weergegeven. Tevens kunnen de gebruikersnaam en het wachtwoord die door de ISP worden toegewezen niet de hostname van de externe router zijn. In zo'n situatie, wordt de **ppp chap hostname** opdracht gebruikt om een alternatieve gebruikersnaam te specificeren die gebruikt zal worden voor authenticatie.

Denk bijvoorbeeld aan een situatie waarin meerdere afstandsapparatuur een centrale locatie ingaat. Gebruik van normale CHAP-authenticatie, moet de gebruikersnaam (wat de hostname zou zijn) van elk extern apparaat en een gedeeld geheim op de centrale router worden geconfigureerd. In dit scenario kan de configuratie van de centrale router langdurig en omslachtig worden om te beheren; als de afstandsapparatuur echter een andere gebruikersnaam gebruikt dan hun hostname , kan dit worden vermeden . De centrale site kan worden geconfigureerd met één gebruikersnaam en één gedeeld geheim dat kan worden gebruikt om meerdere dialineklanten te authenticeren.

Netwerkdiagram

Als router 1 een vraag naar router 2 initieert, zou router 2 router 1 uitdagen, maar router 1 zou router 1 niet router 2 uitdagen. Dit komt voor omdat de **ppp authenticatie ketoestelling** opdracht op router 1 wordt gevormd. Dit is een voorbeeld van een unidirectionele authenticatie.

In deze instelling wordt de **ppp chap hostname alias-r1** opdracht ingesteld op Router 1. Router 1 gebruikt "alias-r1" als zijn hostname voor CHAP-verificatie in plaats van "r1." De naam van de router 2 dialer kaart zou moeten overeenkomen met de naam van de ppp-hostname van router 1; anders worden twee B-kanalen ingesteld , één voor elke richting .

Configuraties

router 1

```
!
 isdn switch-type basic-5ess
 !
 hostname r1
 !
 username r2 password 0 cisco
 ! -- Hostname of other router and shared secret !
interface BRI0/0 ip address 20.1.1.1 255.255.255.0 no ip
directed-broadcast encapsulation ppp dialer map ip
20.1.1.2 name r2 broadcast 5772222
  dialer-group 1
  isdn switch-type basic-5ess
  ppp authentication chap callin
 ! -- Authentication on incoming calls only  ppp chap
hostname alias-r1
 ! -- Alternate CHAP hostname ! access-list 101 permit
ip any any dialer-list 1 protocol ip list 101 !
```

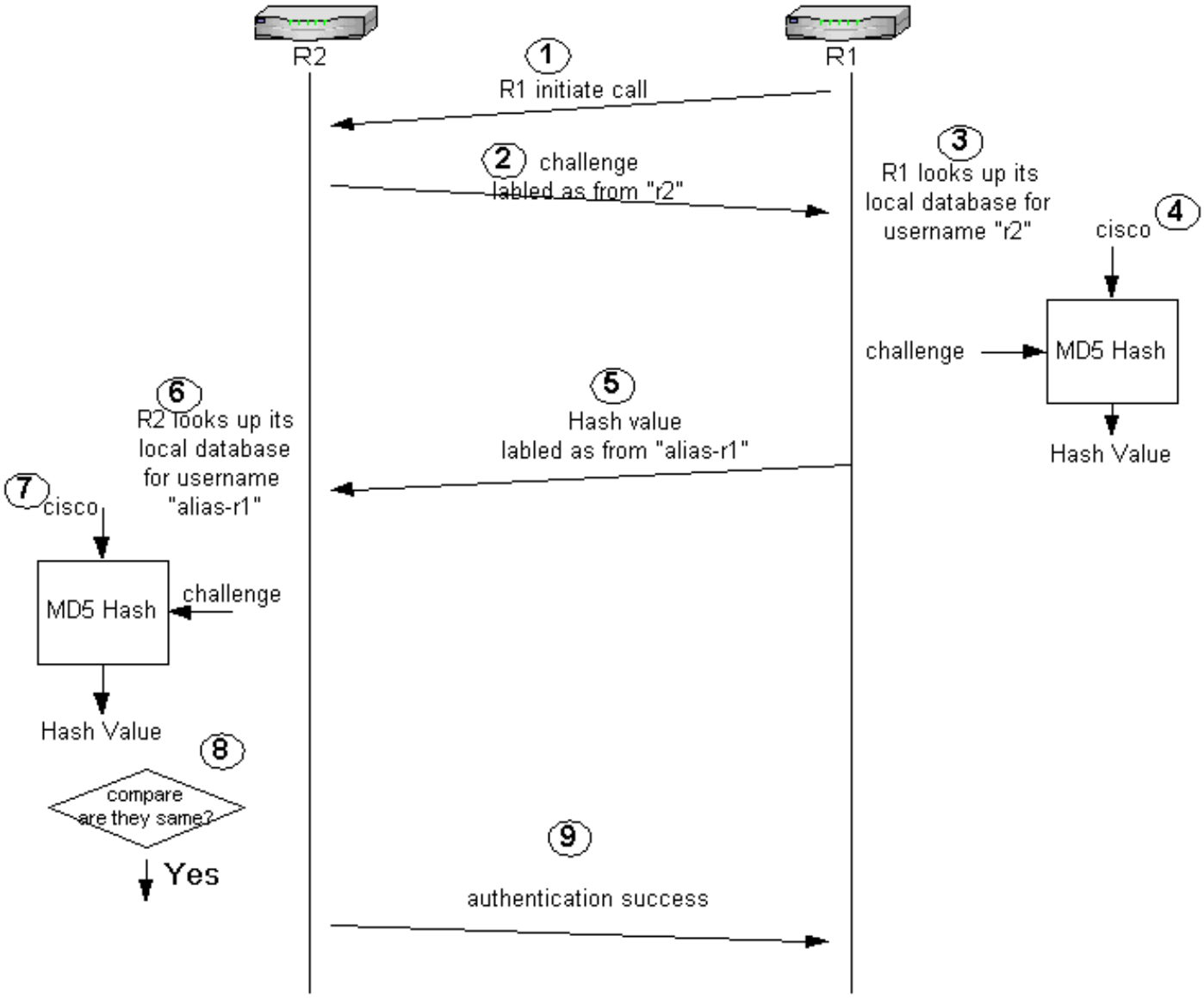
router 2

```
!
 isdn switch-type basic-5ess
 !
 hostname r2
 !
 username alias-r1 password 0 cisco
  ! -- Alternate CHAP hostname and shared secret. ! --
The username must match the one in the ppp chap hostname
! -- command on the remote router.

 !
 interface BRI0/0
  ip address 20.1.1.2 255.255.255.0
  no ip directed-broadcast
  encapsulation ppp
  dialer map ip 20.1.1.1 name
  alias-r1 broadcast 5771111
  ! -- Dialer map name matches alternate hostname
"alias-r1". dialer-group 1 isdn switch-type basic-5ess
ppp authentication chap ! access-list 101 permit ip any
any dialer-list 1 protocol ip list 101 !
```

Configuratieverklaring

Raadpleeg de onderstaande cijfers voor een toelichting bij de cijfers:



1. In dit voorbeeld, initieert router 1 de vraag. Omdat router 1 met de **oproep van PPP** van de **authenticatiekaart** wordt gevormd, daagt deze de oproepende partij niet uit, die router 2 is.
2. Wanneer router 2 de vraag ontvangt, daagt het router 1 voor authenticatie uit. Standaard voor deze verificatie wordt de hostname van de router gebruikt om zichzelf te identificeren. Als het **ppp chap hostname *opdracht* is ingesteld**, gebruikt een router de naam in plaats van de hostname om zichzelf te identificeren. In dit voorbeeld wordt het probleem gelabeld zoals het uit "r2." komt.
3. router 1 ontvangt de uitdaging van de router 2 en kijkt in zijn lokale gegevensbestand voor gebruikersnaam "r2."
4. Router 1 vindt het "r2" wachtwoord, dat "cisco" is. router 1 gebruikt dit wachtwoord en de uitdaging van router 2 als invoerparameters van de MD5 hash-functie. De waswaarde wordt gegenereerd.
5. Router 1 verstuurt de waarde van de hash output naar router 2. Hier, aangezien de **ppp chap hostname** opdracht is ingesteld als "alias-r1", wordt het antwoord geëtiketteerd als afkomstig van "alias-r1."
6. Router 2 ontvangt het antwoord en zoekt de gebruikersnaam "alias-r1" in zijn lokale database voor het wachtwoord.
7. Router 2 vindt dat het wachtwoord voor "alias-r1" "cisco." router 2 gebruikt het wachtwoord en de uitdaging die eerder naar router 1 wordt verzonden als invoerparameters voor de MD5 hash-functie. De wasfunctie genereert een waswaarde.

8. Router 2 vergelijkt de hashwaarde die het genereerde en die welke het van router 1 ontvangt.
9. Aangezien de invoerparameters (uitdaging en wachtwoord) identiek zijn, is de hoofdwaarde gelijk aan de resulterende waarde in een succesvolle verificatie.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Voordat u een van de debug-opdrachten probeert, raadpleegt u Belangrijke informatie over debug Commands

Voorbeeld van output van foutopsporing

Hierna volgt een steekproefuitvoer van de opdracht **debug ppp-verificatie**:

router 1

```
r1#ping 20.1.1.2

 Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 20.1.1.2, timeout is 2 seconds:

  *Mar 1 20:06:27.179: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
  *Mar 1 20:06:27.183: %ISDN-6-CONNECT:
  Interface BRI0/0:1 is now connected to 5772222
  *Mar 1 20:06:27.187: BR0/0:1 PPP: Treating connection as a callout
  *Mar 1 20:06:27.223: BR0/0:1 CHAP: I CHALLENGE id 57 len 23 from "r2"
   ! -- Received a CHAP challenge from other router (r2) *Mar 1 20:06:27.223: BR0/0:1 CHAP:
Using alternate hostname alias-r1
  ! -- Using alternate hostname configured with ! -- ppp chap hostname command *Mar 1
20:06:27.223: BR0/0:1 CHAP: O RESPONSE id 57 Len 29 from "alias-r1" ! -- Sending response from
"alias-r1" ! -- which is the alternate hostname for r1 *Mar 1 20:06:27.243: BR0/0:1 CHAP: I
SUCCESS id 57 Len 4 ! -- Received CHAP authentication is successful ! -- Note that r1 is not
challenging r2 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 36/38/40 ms r1#
*Mar 1 20:06:28.243: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to
up r1# *Mar 1 20:06:33.187: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5772222 r2
```

router 2

```
r2#

  20:05:20: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
  20:05:20: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5771111
  20:05:20: BR0/0:1 PPP: Treating connection as a callin
  20:05:21: BR0/0:1 CHAP: O CHALLENGE id 57 Len 23 from "r2"
  ! -- r2 is sending out a challenge 20:05:21: BR0/0:1 CHAP: I RESPONSE id 57 Len 29 from
"alias-r1"
 ! -- Received a response from alias-r1, ! -- which is the alternate hostname on r1 20:05:21:
```

```
BR0/0:1 CHAP: O SUCCESS id 57 Len 4 ! -- Sending out CHAP authentication is successful 20:05:22:
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to up 20:05:26: %ISDN-6-
CONNECT: Interface BRI0/0:1 is now connected to 5771111 alias-r1
```

Gerelateerde informatie

- PPP-opdrachten voor Wide Area Network
- De betekenis van PPP en PPP-verificatie
- ISDN-debug-informatie