

Probleemoplossing voor problemen bij het bladeren door internet met het gebruik van DSL-verbinding

Inhoud

[Inleiding](#)

[Vereisten](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Methodologie voor probleemoplossing](#)

Inleiding

Dit document beschrijft hoe u het probleem kunt oplossen dat zich voordoet wanneer de eindklant niet door het internet bladert via de dialerinterface met een IP van de ISP.

Vereisten

Voorwaarden

Cisco raadt u aan om kennis te hebben van een DSL-router die een IP van de ISP- en de end-of-customer-machine heeft.

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 de potentiële impact van elke opdracht begrijpen.

Methodologie voor probleemoplossing

Stap 1. Werken pings van PC naar 4.2.2.2? Als de pings op de PC niet doorlopen, volgt u dit:

a. Voer een traceroute uit van Windows met de opdracht **tracert 4.2.2.2**.

Als de router bereikbaar is, probeer dan b., als niet, controleer dan de connectiviteit van de router met de laptop.

b. Als het tracert bevel toont dat de router bereikbaar maar niet in staat is om verder te gaan dan het, de opdracht **debug ip nat** op de router uitvoeren. Controleer daarna de debugs in de NAT-

transaties niet en controleer of NAT: vertaling mislukt (A), pakje laten vallen.

Als u merkt dat deze berichten aanwezig zijn, controleer dan de NAT-configuratie en stel deze in om NATed voor de IP te laten zijn. Controleer de NAT-vertalingen met de hulp van de opdrachtgever en **toon ip-nat-vertaling**. Hieruit blijkt of het NAT correct werkt.

Stap 2. Als de pings op de pc succesvol zijn maar het bladeren niet werkt, volgt u dit:

a. Controleer de routerconfiguratie om te weten te komen of https/https expliciet wordt ontkend door een geconfigureerde toegangscontrolelijst (ACL).

b. Als er geen ACL is ingesteld, controleer dan de waarde van **mtu** die op het dialoogvenster is ingesteld.

c. Verander de waarde in 1492 met het gebruik van de commandeur **ip mtu 1492** op de dialerinterface. Controleer het bladeren.

d. Als browsen nog steeds mislukt, probeer dan de mss waarde aan te passen met de opdracht **ip tcp bijstellen-mss 1400**.

Opmerking: Met de TCP MSS-aanpassingsfunctie kunt u de configuratie van de maximale grootte van een segment (MSS) toestaan voor tijdelijke pakketten die een router oversteken, in het bijzonder TCP-segmenten in de SYN-bit-set, wanneer Point-to-Point Protocol over Ethernet (PPPoE) in het netwerk wordt gebruikt. PPPoE kapselt de Ethernet Maximum Transmission Unit (MTU) 1492, en als de effectieve MTU op de hosts (PCs) niet wordt gewijzigd, kan de router tussen de host en de server de TCP-sessies beëindigen. De opdracht **ip tcp adaptieve mss** specificeert de MSS-waarde op de intermediaire router van de SYN-pakketten om truncatie te voorkomen.