

Meerdere exemplaren van OSPF-netwerken met SNMP-contexten beheren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[SNMP-contextbewustzijn](#)

[Configuratie](#)

[Verifiëren](#)

[SNMPv2-verificatie](#)

[SNMPv3-verificatie](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document biedt voorbeeldconfiguraties voor SNMPv2 en SNMPv3 die beschrijven hoe u SNMP-contexten kunt gebruiken om meerdere instanties van Open kortste Pad First (OSPF) te beheren.

[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.


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.


[Conventies](#)

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\)](#) voor

[meer informatie over documentconventies.](#)

Achtergrondinformatie

De OSPF MIB die door IETF ([RFC 1850](#) ) wordt gedefinieerd, is ontworpen om met slechts één OSPF-proces/instantie op een bepaalde router te werken.

Bijvoorbeeld, er is slechts één enkel *ospfRouterID* object, niet een tabel van hen. Om meerdere instanties aan te kunnen, stelt [RFC 4750](#)  voor om SNMPv3-contexten te gebruiken om per-instantie-views te geven.

SNMP-contextbewustzijn

Alvorens de IOS SNMP codecontext bewust te maken zou het systeem een meer of minder willekeurige "standaard" instantie kiezen wanneer het de scalar objecten en sommige tabellen teruggaf. In deze gevallen was informatie uit de andere instanties niet beschikbaar via SNMP. Voor wat andere tabellen, zou SNMP de inzendingen uit alle gevallen samenvoegen zonder enige manier om te onderscheiden wat was. In veel gevallen kan dit leiden tot dubbele of dubbele items. Het was vooral geen goede praktijk in PE-CE configuraties waar IP adressen en buurrouter-IDs niet uniek zouden kunnen zijn. Dit maakte de controle en het oplossen van individuele CE instanties moeilijk of onmogelijk.

Met de huidige context-bewuste IOS code (wanneer geen context wordt gespecificeerd), bestaat het oude gedrag voor scalar voorwerpen nog. De enige verandering is dat het nu alle in plaats van slechts enkele van de tabellen aan de zelfde "standaard"OSPF instantie beperkt zoals de scalars. Wanneer contexten worden geleverd, kunnen de SNMP vragen aan een bepaalde OSPF instantie worden gericht, en alle informatie voor die instantie kan op een consistente en ondubbelzinnige manier worden opgehaald.

Als SNMPv3 gebruikt wordt, kan de context string direct bij de enquête geleverd worden. SNMPv2c biedt geen context. U kunt echter SNMP-community strings in kaart brengen naar contexten in de IOS-configuratie, en deze contexten kunnen worden gebruikt om SNMPv2-polls te sturen naar een specifieke OSPF-instantie.

Configuratie

Dit configuratievoorbeeld is gebaseerd op SNMPv2:

```
router 1
Router1#
router ospf 1
  router-id 1.1.1.111
  log-adjacency-changes
  snmp context context1
!
router ospf 2
  router-id 4.4.4.111
  log-adjacency-changes
  snmp context context2
```

```

!--- Associates the SNMP context with the instance. !
snmp-server user u2 g2 v2c !--- Configures the user u2
to the SNMP group g2 and !--- specifies the group is
using the SNMPv2c security model. snmp-server group g2
v2c !--- Configures the SNMP group g2 and specifies !---
the group is using the SNMPv2c security model. snmp-
server group g2 v2c context context1 snmp-server group
g2 v2c context context2 snmp-server community public RO
!--- Community access string to permit access !--- to
the SNMP. snmp-server community cx1 RO snmp-server
community cx2 RO snmp-server context context1 snmp-
server context context2 snmp mib community-map cx1
context context1 security-name u2 !--- Associates the
SNMP community cx1 with !--- the context context 1. snmp
mib community-map cx2 context context2 security-name u2

```

Dit configuratievoorbeeld is gebaseerd op SNMPv3:

router 1

```

Router1#
router ospf 1
  router-id 1.1.1.111
  log-adjacency-changes
  snmp context context1
!
router ospf 2
  router-id 4.4.4.111
  log-adjacency-changes
  snmp context context2
!
snmp-server user u1 g1 v3
snmp-server group g1 v3 noauth
snmp-server group g1 v3 noauth context context1
snmp-server group g1 v3 noauth context context2
snmp-server context context1
snmp-server context context2

```

N.B.: Gebruik het [Opdrachtupgereedschap](#) (alleen [geregistreeerde](#) klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Verifiëren

U kunt de opdracht **tussenstappen** op elke client gebruiken om de uitvoer te controleren.

Opmerking: [Uitvoer Tolk Tool](#) (alleen [geregistreeerde](#) klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

SNMPv2-verificatie

SNMPv2

```

linux>snmpwalk -c public -v2c irp-view14:7890 OSPF-
MIB::ospfRouterId.0
OSPF-MIB::ospfRouterId.0 = IPAddress: 4.4.4.111

```

```
linux>snmpwalk -c cx1 -v2c irp-view14:7890 OSPF-  
MIB::ospfRouterId.0  
OSPF-MIB::ospfRouterId.0 = IPAddress: 1.1.1.111  
  
linux>snmpwalk -c cx2 -v2c irp-view14:7890 OSPF-  
MIB::ospfRouterId.0  
OSPF-MIB::ospfRouterId.0 = IPAddress: 4.4.4.111
```

[SNMPv3-verificatie](#)

SNMPv3

```
linux>snmpwalk -u u1 -v3 irp-view14:7890 OSPF-  
MIB::ospfRouterId.0  
OSPF-MIB::ospfRouterId.0 = IPAddress: 4.4.4.111  
  
linux>snmpwalk -u u1 -v3 -n context1 irp-view14:7890  
OSPF-MIB::ospfRouterId.0  
OSPF-MIB::ospfRouterId.0 = IPAddress: 1.1.1.111  
  
linux>snmpwalk -u u1 -v3 -n context2 irp-view14:7890  
OSPF-MIB::ospfRouterId.0  
OSPF-MIB::ospfRouterId.0 = IPAddress: 4.4.4.111
```

[Gerelateerde informatie](#)

- [OSPF-configuratiebeheer met SNMP](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)