

ONS 15454 IP-adressering met beveiligde modus

Inhoud

[Inleiding:](#)

[Voorwaarden:](#)

[Vereisten:](#)

[Achtergrondinformatie:](#)

[Beveiligd gedrag:](#)

[Secure Node vergrendeld en ontgrendeld gedrag:](#)

[Handige opmerkingen:](#)

[Gerelateerde Cisco Support Community-discussies](#)

Inleiding:

Het document beschrijft het IP-adres van de basisconfiguratie dat is toegewezen aan het ONS 15454-knooppunt met Secure Mode ingeschakeld in Cisco-transportcontroller (CTC).

Voorwaarden:

Cisco raadt de basiskennis van TCP/IP- en datacommunicatienetwerk (DCN)-beheer in een netwerk aan.

Vereisten:

ONS 15454 controllerkaarten voor ONS-apparaat

ONS Platform-specifieke systeemsoftware

Achtergrondinformatie:

Als TCC2P-kaarten zijn geïnstalleerd, is de dubbele IP-adressering beschikbaar in de beveiligde modus. Wanneer de veilige modus uit is (soms repeatermodus genoemd), is het IP-adres dat in het veld IP-adres is ingevoerd, van toepassing op de ONS 15454 backplane LAN-poort en de TCC2P TCP/IP (LAN)-poort. Wanneer de beveiligde modus is ingeschakeld, toont het IP-adresveld het adres dat is toegewezen aan de TCP/IP (LAN)-poort en kan de Superuser de weergave van het IP-backplane adres in- of uitschakelen.

De standaardinstelling van de kaarten TCC2, TCC2P, TCC3, TNC, TNCE, TSC, en TSCE om de herhalingsmodus te herhalen. In deze modus delen de front- en back-Ethernet (LAN)-poorten één MAC-adres en IP-adres. Met TCC2P-, TCC3-, TNC-, TNCE-, TSC- en TSEC-kaarten kunt u een knooppunt in een beveiligde modus plaatsen, waardoor een Ffront-access gebruiker niet via de backplane poort naar het LAN kan komen.

Beveiligd gedrag:

Door een knooppunt van TCC2P, TCC3, TNC, TNCE, TSC of TSCE van repeatermodus te wijzigen, kunt u twee IP-adressen voor ONS 15454 creëren en zorgt u voor het knooppunt om de

poorten verschillende MAC-adressen toe te wijzen. In veilige modus is één IP-adres voorzien voor de ONS 15454 backplane LAN-poort en is het andere IP-adres voorzien voor de Ethernet-poort van de kaart. Beide adressen wonen op verschillende subnetten, die een extra laag van scheiding tussen de haven van de ambachtstoegang en het LAN 15454 voorzien. Als de beveiligde modus is ingeschakeld, moeten de IP-adressen die voorzien zijn voor de backplane LAN-poort en kaart Ethernet-poort algemene IP-adresseringsrichtlijnen volgen en op verschillende subnetwerken van elkaar wonen.

In de beveiligde modus wordt het IP-adres dat aan de backplane LAN-poort is toegewezen, een privéadres dat het knooppunt verbindt met een besturingssysteem (OSS) via een netwerk van centrale kantoren of privé-ondernemingen. Een supergebruiker kan het knooppunt configureren om het LAN IP-adres van de backplane te verbergen of vrijgeven in CTC, de routingtabel of de autonome berichtgeving van TL1.

In de herhalingsmodus kan een knooppunt een BNE of ENE zijn. Wanneer u het knooppunt in de beveiligde modus plaatst, wordt automatisch de SOCKS-proxy ingeschakeld en wordt het knooppunt in de BNE-status omgezet. Het knooppunt kan echter worden gewijzigd in een ENE. In de herhalingsmodus kan de SOCKS-proxy van een ENE worden uitgeschakeld. U kunt het knooppunt effectief isoleren buiten de LAN-firewall, maar het kan niet worden uitgeschakeld in de beveiligde modus. De lengte van het Net/Subnet masker - Type de SUBNET masker (decimaal aantal dat de SUBNET maskerlengte in bits weergeeft) of klik de pijlen om de Subnet maskerlengte aan te passen. De SUBNET maskerlengte is het zelfde voor alle ONS 15454 knooppunten in zelfde subnet. Het MAC-adres - (alleen display) geeft het ONS 15454 IEEE 802 MAC-adres weer.

In de beveiligde modus worden de TCP/IP-poorten (LAN) aan voor- en achterkant toegewezen aan verschillende MAC-adressen en kan de backplane informatie worden verborgen of onthuld door een Superuser.

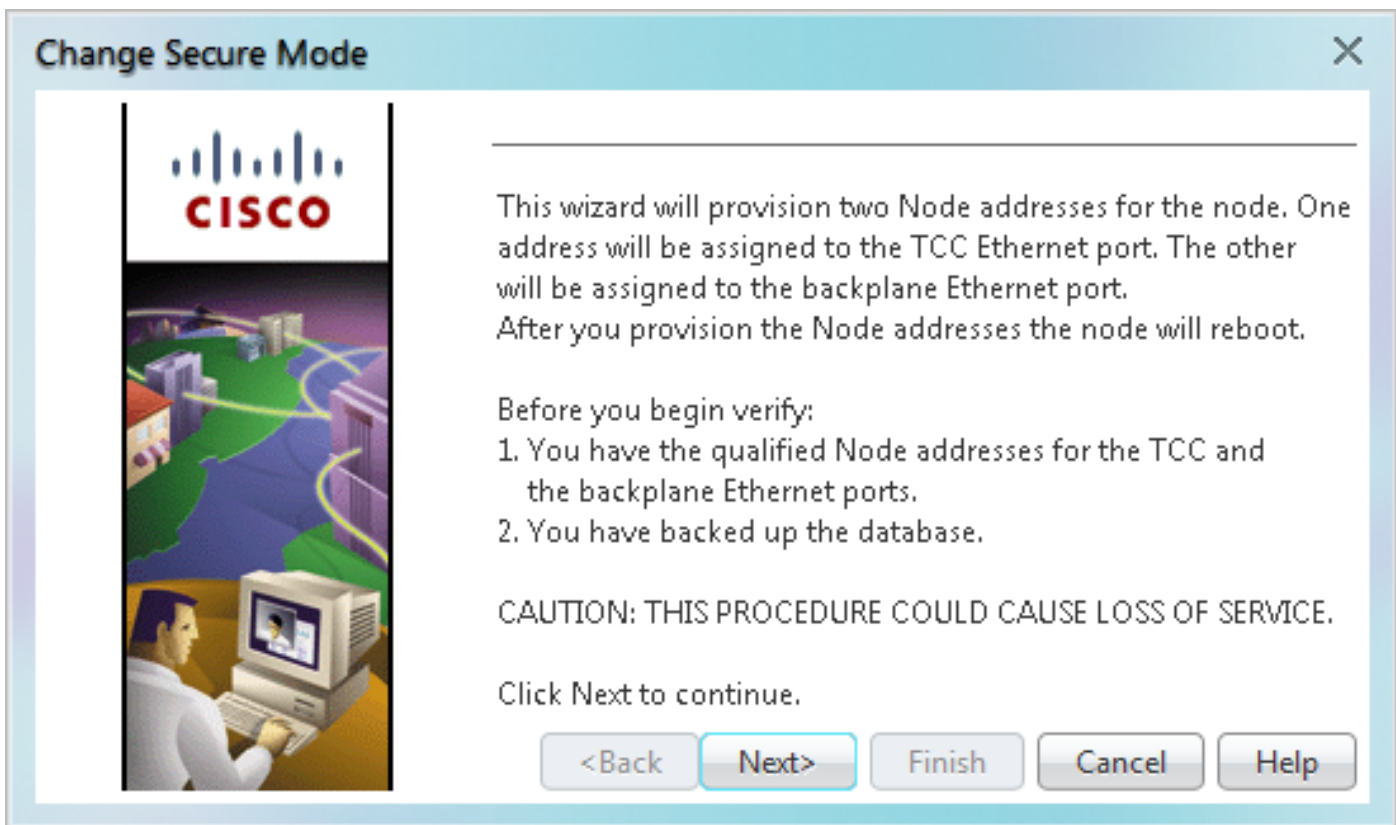
Het IP-adres dat aan de TCP/IP (LAN)-poort is toegewezen, moet op een ander doeleinde aanwezig zijn dan de backplane LAN-poort en de ONS 15454 standaardrouter. Controleer dat het nieuwe TCC2P IP-adres aan dit vereiste voldoet en is compatibel met ONS 15454 IP-adressen van het netwerk.

Procedure om de beveiligingsmodus via CTC te wijzigen:

Stap 1 Klik op de tabbladen Provisioning > Beveiliging > Gegevenscompressie zoals hieronder weergegeven:

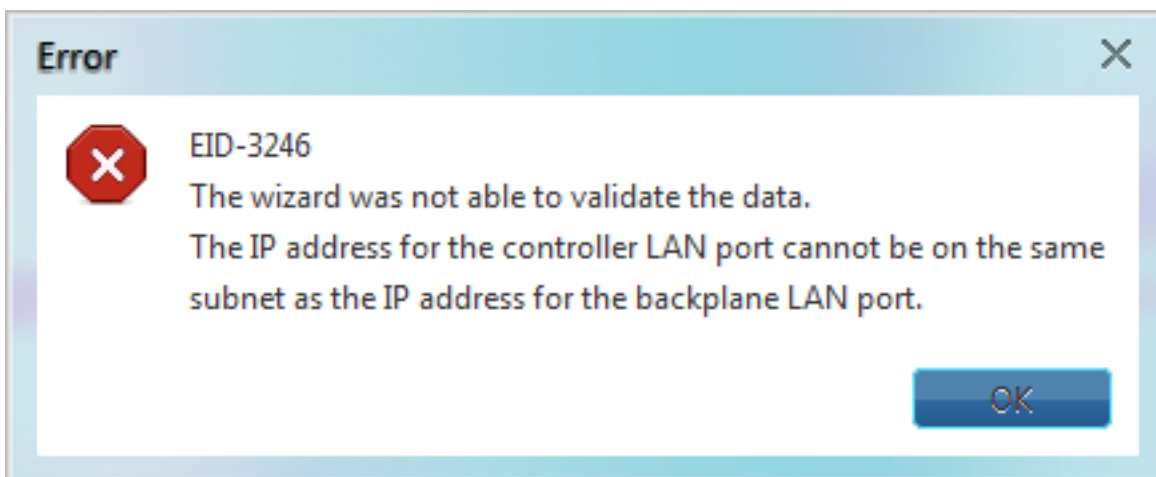
The screenshot shows the CTC web interface. At the top, there are tabs for Alarms, Conditions, History, Circuits, Provisioning, Inventory, and Maintenance. The 'Provisioning' tab is selected. Below this, there are sub-tabs for Users, Active Logins, Policy, Data Comm, Access, RADIUS Server, and Legal Disclaimer. The 'Data Comm' sub-tab is selected. On the left side, there is a vertical menu with options: General, Ether Bridge, Network, OSI, BLSR, Protection, Security (highlighted), SNMP, Comm Channels, and Timing. The main content area shows the 'TCP/IP Mode' configuration. It has two radio buttons: 'Normal (one Node address shared by the TCC and backplane Ethernet ports, with full connectivity between ports)' which is selected, and 'Secure (separate Node addresses for TCC and backplane Ethernet ports, with no connectivity between ports)'. Below these are two status indicators: 'Mode not locked' and 'Mode permanently locked and cannot be unlocked'. At the bottom of the configuration area are two buttons: 'Change Mode..' and 'Lock..'

Stap 2 Klik op Wijzigen.



Stap 3 Controleer de informatie op de pagina Beveiligingsmodus wijzigen en klik vervolgens op Volgende.

Stap 4 Op de TCP Ethernet-poortpagina voert u het IP-adres en het subnetmasker in voor de TCP2P TCP/IP (LAN)-poort. Het IP-adres kan niet op hetzelfde subtype aanwezig zijn als de backplane LAN-poort of de ONS 15454 standaardrouter en als dit niet het geval is zal de onderstaande fout in CTC voorkomen.



Stap 5 Klik op Volgende na het garanderen van stap 4.

Stap 6 Indien nodig, op de backplane Ethernet-poortpagina, wijzig het IP-adres, het subnetmasker en de standaardrouter. (U verandert deze velden normaal niet als er geen ONS 15454 netwerkwijzigingen zijn opgetreden.)

Change Secure Mode

Node Address:
10.0.0.1
Net/Subnet Mask Length: 24
Mask: 255.255.255.0

Backplane

If needed, edit the backplane LAN port IP address,
or click next to proceed

Node Address 10.105.142.195
Net/Subnet Mask Length: 24
Mask: 255.255.255.0
Default Router 10.105.142.193

<Back Next> Finish Cancel Help

Stap 7 Klik op Volgende.

Stap 8 Kies een van de volgende opties op de pagina Instellingen van de SOCKS Proxy-server:

Change Secure Mode

Node Address:
10.0.0.1
Net/Subnet Mask Length: 24
Mask: 255.255.255.0

Backplane LAN IP Address:
10.105.142.195
Net/Subnet Mask Length: 24
Mask: 255.255.255.0
Default Router:
10.105.142.193

Proxy Server Settings

Proxy server and firewall must be enabled for the secure mode.
If needed, change the proxy server settings, or click finish.

Gateway Settings
Current Settings: SOCKS proxy

Enable SOCKS Proxy on Port: 1080
 External Network Element (ENE)
 Gateway Network Element (GNE)
 SOCKS proxy only

<Back Next> Finish Cancel Help

- Extern netwerkelement (ENE) - Indien geselecteerd, is de CTC-computer alleen zichtbaar op ONS 15454 waar de CTC-computer is aangesloten. De CTC-computer is niet zichtbaar op de knooppunten die zijn aangesloten op de DCC. Bovendien is de firewall ingeschakeld, wat betekent dat het knooppunt voorkomt dat IP-verkeer tussen de DCC en de LAN poort wordt

verzonden.

- Gateway Network Element (GNE) - Indien geselecteerd, is de CTC-computer zichtbaar op andere met DCC verbonden knooppunten. Het knooppunt voorkomt IP-verkeer tussen de DCC en de LAN poort.

Opmerking: De SOCKS-proxy-server is automatisch ingeschakeld wanneer u de beveiligde modus activeert.

Stap 9 Klik op Voltooien.

Binnen 30 tot 40 seconden herstart de TCC2P-kaarten. CTC verandert in netwerkweergave, en het dialoogvenster CTC-meldingen verschijnt. In de netwerkweergave verandert het knooppunt in grijs en wordt een niet-verbonden toestand weergegeven in het tabblad Alarm.

Nadat u de beveiligde modus in CTC hebt ingeschakeld, controleert u of deze correct zijn gedefinieerd voor knooppunt zoals hieronder voor één testknooppunt wordt weergegeven.

The screenshot shows the CTC configuration interface. The top navigation bar includes tabs for Alarms, Conditions, History, Circuits, Provisioning (selected), Inventory, and Maintenance. The left sidebar lists various configuration categories: General, Ether Bridge, Network, OSI, BLSR, Protection, Security (selected), SNMP, Comm Channels, Timing, Alarm Profiles, Cross-Connect, Defaults, and WDM-ANS. The main content area is divided into sub-sections: Users, Active Logins, Policy, Data Comm (selected), Access, RADIUS Server, and Legal Disclaimer. The 'Data Comm' section is expanded to show 'TCP/IP Mode' and 'Backplane Ethernet Port' settings.

TCP/IP Mode
Normal (one Node address shared by the TCC and backplane Ethernet ports, with full connectivity between ports)
 Secure (separate Node addresses for TCC and backplane Ethernet ports, with no connectivity between ports)
 Mode not locked
Mode permanently locked and cannot be unlocked
Change Mode.. Lock..

Backplane Ethernet Port
Node Address: 10.105.142.195 Net/Subnet Mask Length: 24 Mask: 255.255.255.0
MAC Address: 00-10-cf-d1-58-22 Default Router: 10.105.142.193
LCD Setting: Allow Configuration Suppress CTC IP Display

Verifieer ook beide IP-adres in de CTC-knoopweergave zoals hieronder wordt getoond.

NE-195

0 CR

1 MJ

15 MN

```

Node Addr           : 10.0.0.1
Backplane Node Addr: 10.105.142.195
Booted              : 11/18/15 7:10 AM
User                 : CISCO15
Authority            : Superuser
SW Version           : 08.54-010C-12.19

```

Secure Node vergrendeld en ontgrendeld gedrag:

De beveiligde modus kan worden vergrendeld of ontgrendeld voor een knooppunt dat in de beveiligde modus werkt. De standaardstatus wordt ontgrendeld en alleen een supergebruiker kan een slot uitgeven. Wanneer de beveiligde modus is vergrendeld, kan de configuratie van het knooppunt (inclusief Ethernet-poortstatus) en de status van het slot niet door een netwerkgebruiker worden gewijzigd. Om het slot van een veilig knooppunt te hebben verwijderd, neemt u contact op met Cisco Technical Support om een RMA (Return Material Authorization) te regelen voor de elf verzameling. Een slot mogelijk maken betekent een permanente verandering in het EEPROM van de plank.

Het configuratieslot van een knooppunt wordt gehandhaafd als de database van de actieve TCC2P-kaart opnieuw wordt geladen. Als u bijvoorbeeld probeert een niet-vergrendeld knooppuntgegevensbestand op de stand-by TCC2P-kaart van een vergrendeld knooppunt te laden voor overdracht naar de actieve TCC2P-kaart (een actie die niet wordt aanbevolen), heeft de status van het ontgrendelde knooppunt (via de geüploade database) geen voorrang op de status van het slot. Als u probeert een vergrendeld gegevensbestand op de standby TCC2P-kaart van een ontgrendeld beveiligd knooppunt te laden, wordt de database geüpload met de actieve TCC2P-kaart. Als de geüploade standaardinstellingen een vergrendelde status aangeven, veroorzaakt dit dat het knooppunt vergrendeld wordt. Als een software-lading is aangepast voordat een slot is ingeschakeld, worden alle vergrendelbare provisioningfuncties permanent ingesteld op de aangepaste standaardinstellingen van de software die in de lading zijn meegeleverd, en kunnen ze niet door een gebruiker worden gewijzigd.

Handige opmerkingen:

- Als zowel de voor- als de backplane toegangspoorten uitgeschakeld zijn in een ENE en het knooppunt geïsoleerd is van DCC-communicatie (vanwege gebruikersvoorzieningen of netwerkfouten), worden de voor- en backplane poorten automatisch opnieuw ingeschakeld.
- De beveiligde modus kan worden vergrendeld zodat de modus niet wordt gewijzigd.
- Het inschakelen van veilige modus veroorzaakt de herstart van de TCC2P-, TCC3-, TNC-, TNCE-, TSC- en TSCE-kaarten. de herstart van de kaart beïnvloedt het verkeer .

- De opties voor de beveiligingsmodus zijn niet beschikbaar in CTC als er TCC2-kaarten of een combinatie van TCC2- en TCC2P-kaarten zijn geïnstalleerd.
- Door de beveiligde modus in te schakelen wordt de TCC2P-kaart opnieuw opgestart. een TCC2P-kaart opnieuw start beïnvloedt het verkeer.
- De TCC2-kaart kan niet worden opgestart wanneer deze als standby-kaart wordt toegevoegd aan een knooppunt met een actieve TCC2P-kaart die in de beveiligde modus is geconfigureerd.