启用安全模式的ONS15454 IP编址

目录

[简介：](#)
[先决条件:](#)
[要求:](#)
[背景信息:](#)
[安全模式行为：](#)
[安全节点锁定和解锁行为：](#)
[有用注释：](#)
[相关的思科支持社区讨论](#)

简介：

本文档介绍在思科传输控制器(CTC)中启用安全模式的ONS 15454节点分配的基本配置IP地址。

先决条件:

思科推荐网络中TCP/IP和数据通信网络(DCN)管理的基本知识。

要求:

ONS15454控制器卡，用于ONS设备

ONS平台特定系统软件

背景信息:

如果安装了TCC2P卡，则使用安全模式提供双IP编址。当安全模式关闭（有时称为中继器模式）时，在IP Address字段中输入的IP地址将应用于ONS 15454背板LAN端口和TCC2P TCP/IP(LAN)端口。当安全模式打开时，IP Address字段显示分配给TCC2P TCP/IP(LAN)端口的地址，超级用户可以启用或禁用背板IP地址的显示。

TCC2、TCC2P、TCC3、TNC、TNCE、TSC和TSCE卡默认为中继器模式。在此模式下，前端和后端以太网(LAN)端口共享一个MAC地址和IP地址。TCC2P、TCC3、TNC、TNCE、TSC和TSCE卡允许您将节点置于安全模式，这样可防止前接入工艺端口用户通过背板端口访问LAN。

安全模式行为：

将TCC2P、TCC3、TNC、TNCE、TNCE、TSC或TSCE节点从中继器模式更改为安全模式允许您为ONS 15454调配两个IP地址，并导致节点分配不同的MAC地址。在安全模式下，为ONS 15454背板LAN端口调配一个IP地址，为卡以太网端口调配另一个IP地址。两个地址都位于不同的子网中，为工艺接入端口和ONS 15454 LAN提供了额外的分层。如果启用安全模式，则为背板LAN端口和卡以太网端口调配的IP地址必须遵循一般IP编址准则，并且必须位于彼此不同的子网中。

在安全模式下，分配给背板LAN端口的IP地址变为私有地址，通过中心局LAN或私有企业网络将节点连接到操作支持系统(OSS)。超级用户可以配置节点以隐藏或显示CTC、路由表或TL1自治消息报告中背板的LAN IP地址。

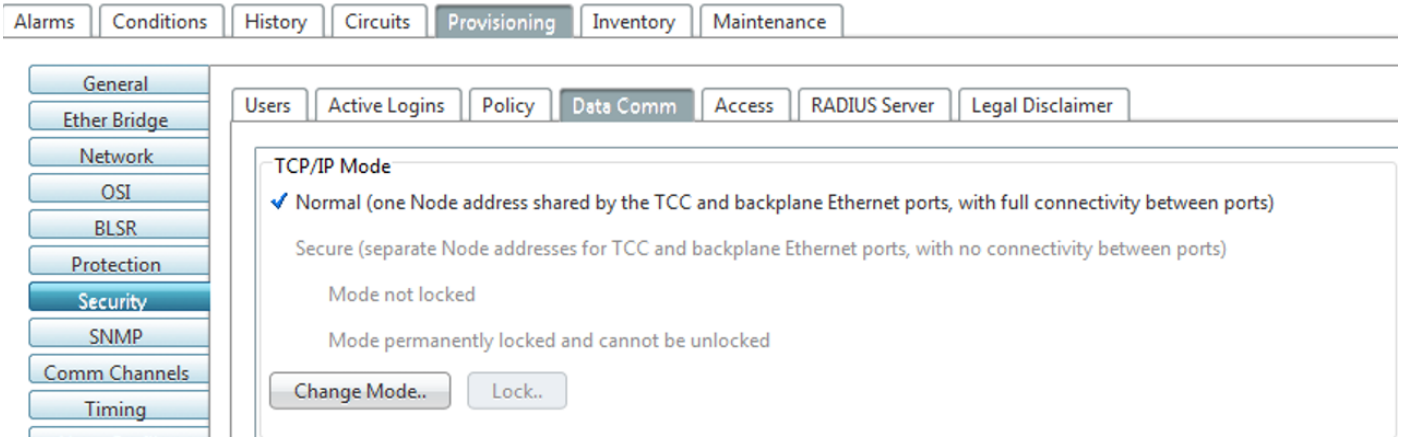
在中继器模式下，节点可以是GNE或ENE。将节点置于安全模式会自动打开SOCKS代理并将节点默认为GNE状态。但是，节点可以更改回ENE。在中继器模式下，可以禁用ENE的SOCKS代理（有效隔离LAN防火墙之外的节点），但在安全模式下不能禁用。The Net/Subnet Mask Length — 键入子网掩码长度（以位表示子网掩码长度的十进制数），或单击箭头调整子网掩码长度。同一子网中所有ONS 15454节点的子网掩码长度相同。MAC Address —（仅显示）显示ONS 15454 IEEE 802 MAC地址。

在安全模式下，前TCP/IP(LAN)端口和后TCP/IP(LAN)端口分配了不同的MAC地址，并且背板信息可以隐藏或由超级用户显示。

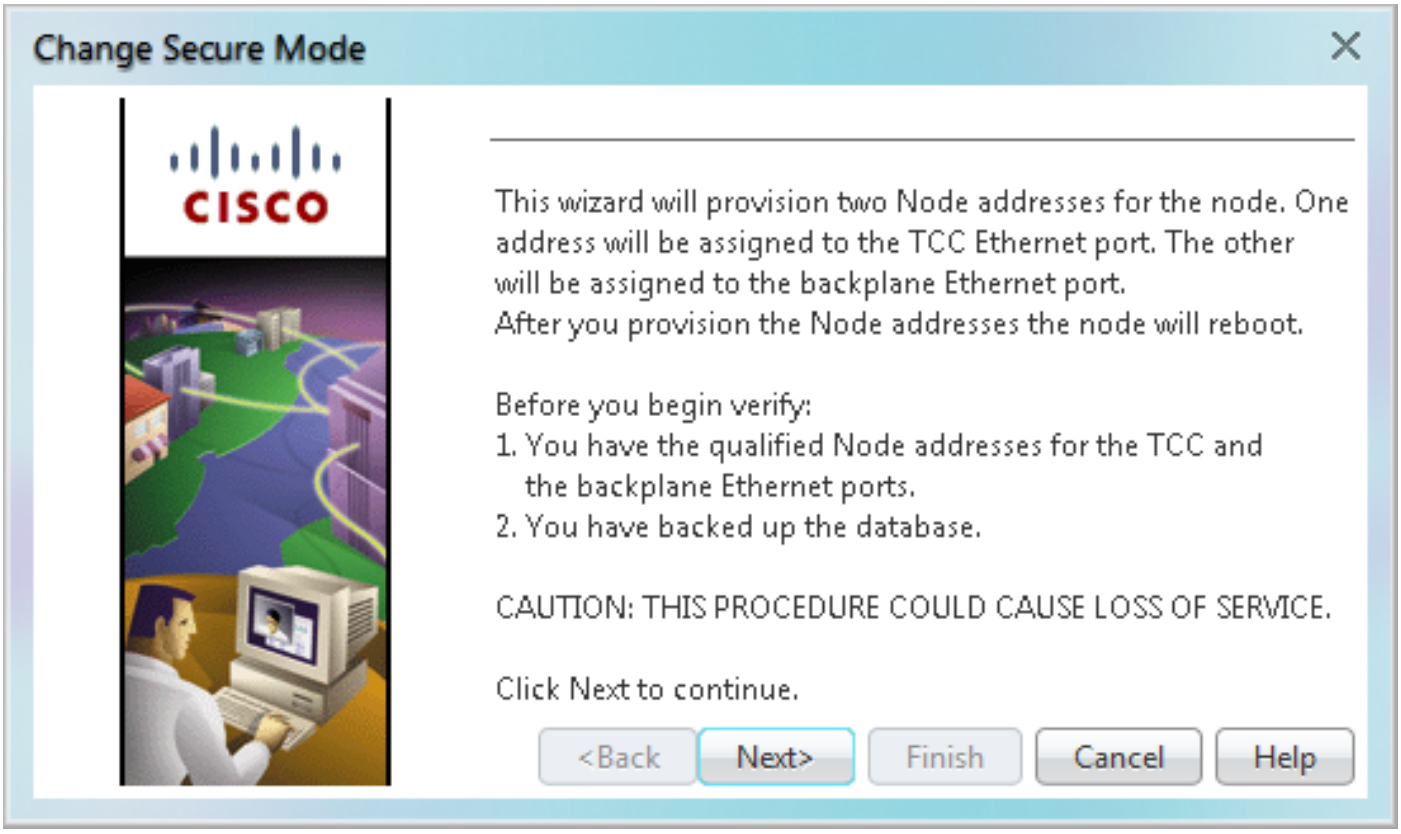
分配给TCC2P TCP/IP(LAN)端口的IP地址必须位于与背板LAN端口和ONS 15454默认路由器不同的子网中。验证新的TCC2P IP地址是否满足此要求并与ONS 15454网络IP地址兼容。

通过CTC切换到安全模式的步骤：

第1步点击Provisioning > Security > Data Comm选项卡，如下所示：

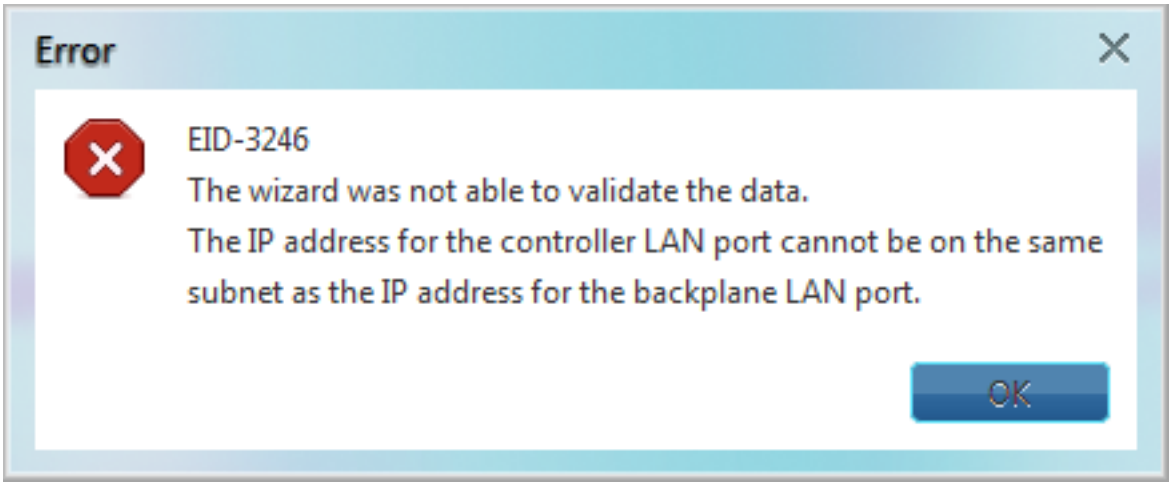


第2步点击Change Mode。



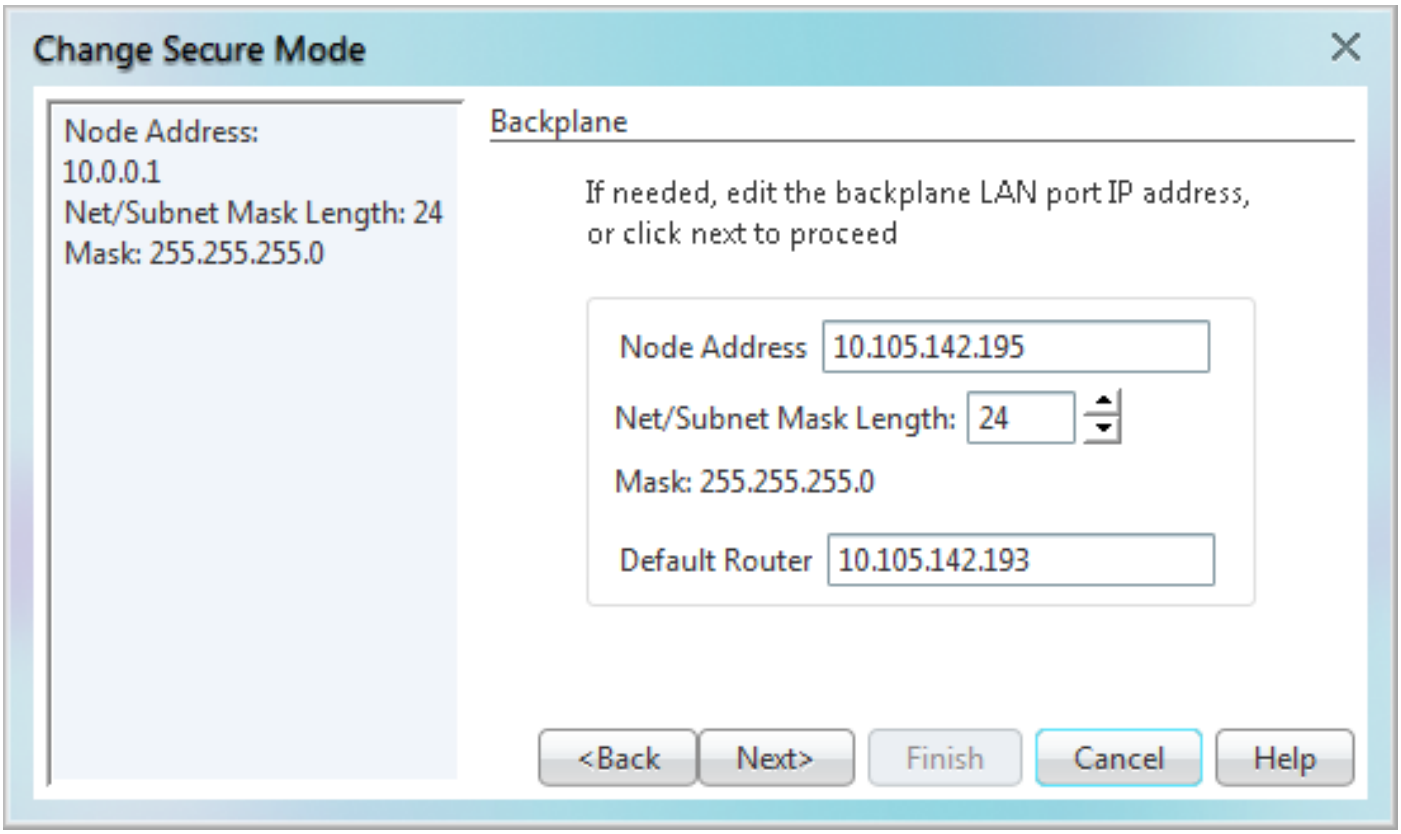
第3步查看Change Secure Mode页面上的信息，然后点击Next。

第4步在TCC以太网端口(TCC Ethernet Port)页面，输入TCC2P TCP/IP(LAN)端口的IP地址和子网掩码。IP地址不能与背板LAN端口或ONS 15454默认路由器位于同一子网中，如果不是，CTC中将出现以下错误。



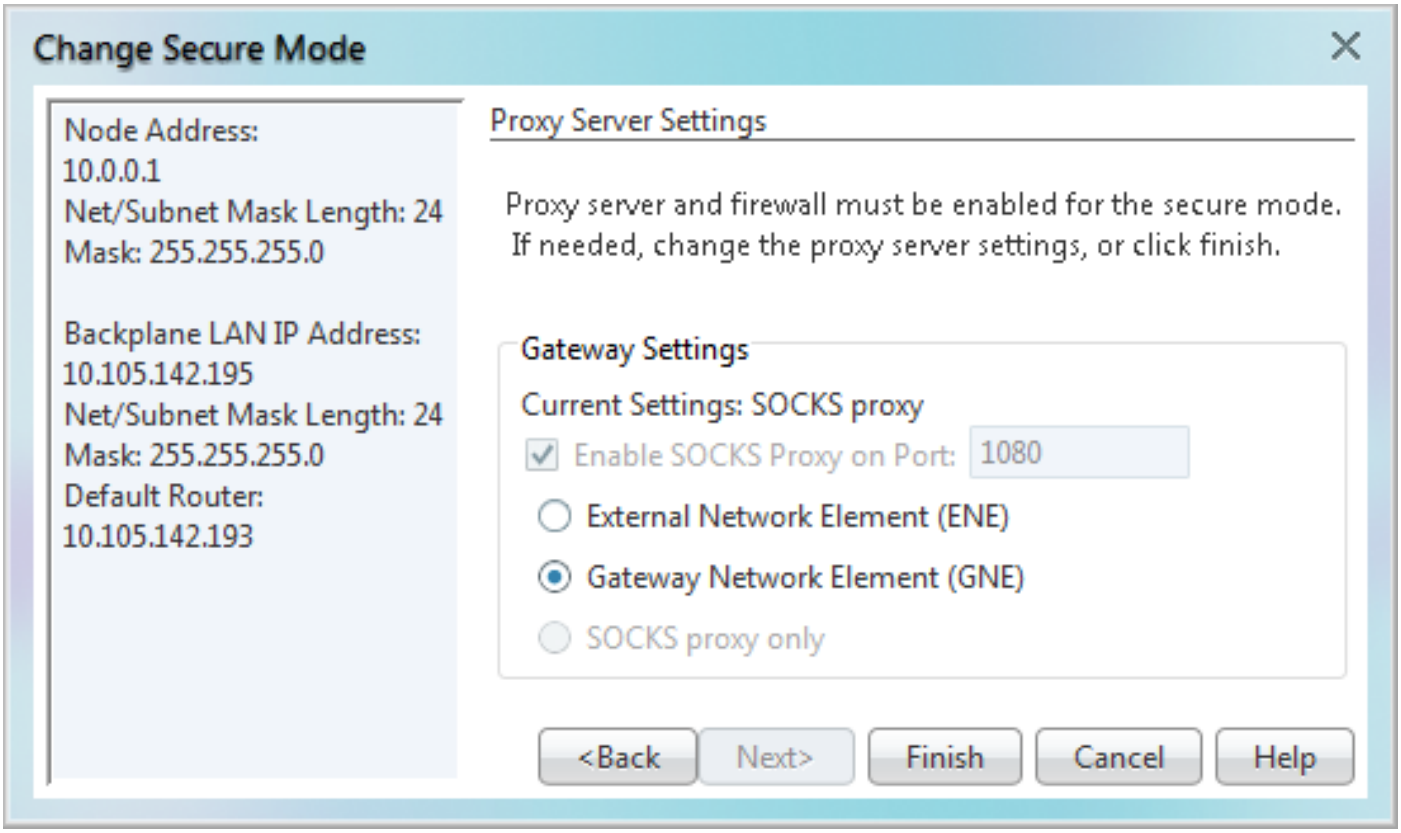
第5步确保第4步后，点击Next。

第6步如果需要，在Backplane Ethernet Port页面上，修改背板IP地址、子网掩码和默认路由器。(如果未发生ONS 15454网络更改，通常不修改这些字段。)



第7步点击Next。

第8步在SOCKS Proxy Server Settings页面上，选择以下选项之一：



- 外部网络元素(ENE) — 如果选中，则CTC计算机仅对CTC计算机所连接的ONS 15454可见。CTC计算机对连接到DCC的节点不可见。此外，防火墙已启用，这意味着节点会阻止IP流量在DCC和LAN端口之间路由。

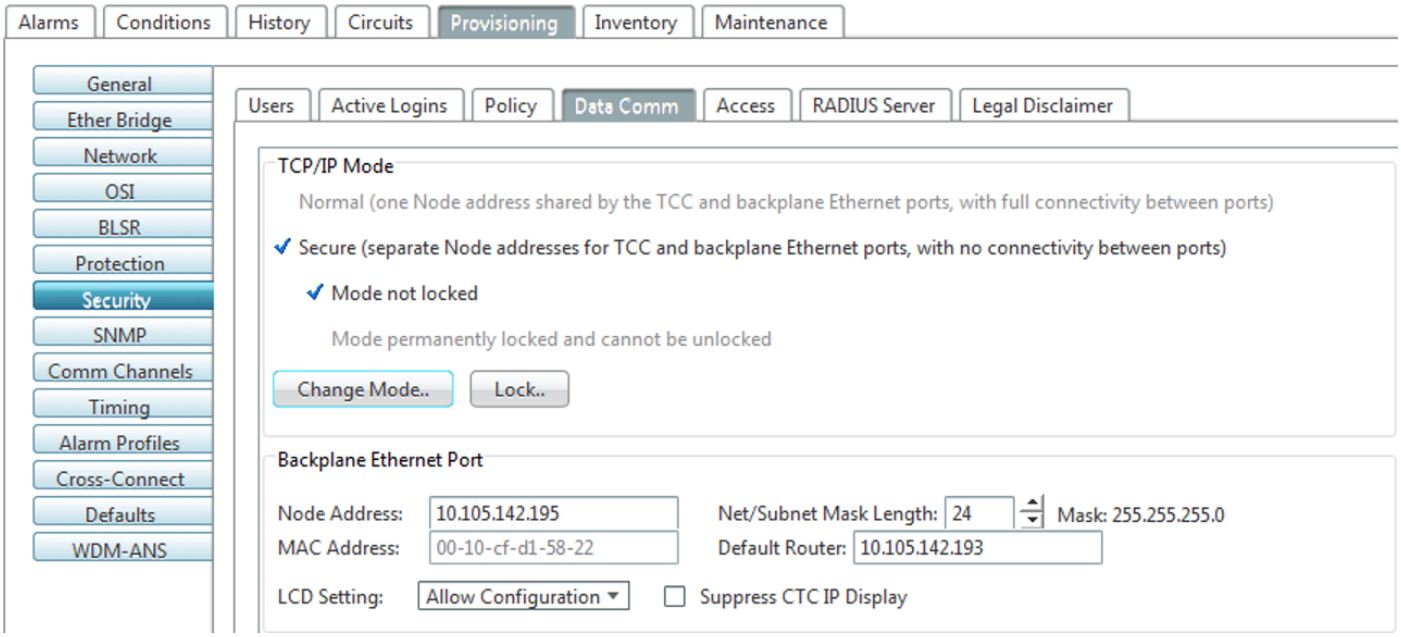
- 网关网络元素(GNE) — 如果选中，CTC计算机对其他DCC连接的节点可见。该节点防止IP流量在DCC和LAN端口之间路由。

注意：启用安全模式时，SOCKS代理服务器会自动启用。

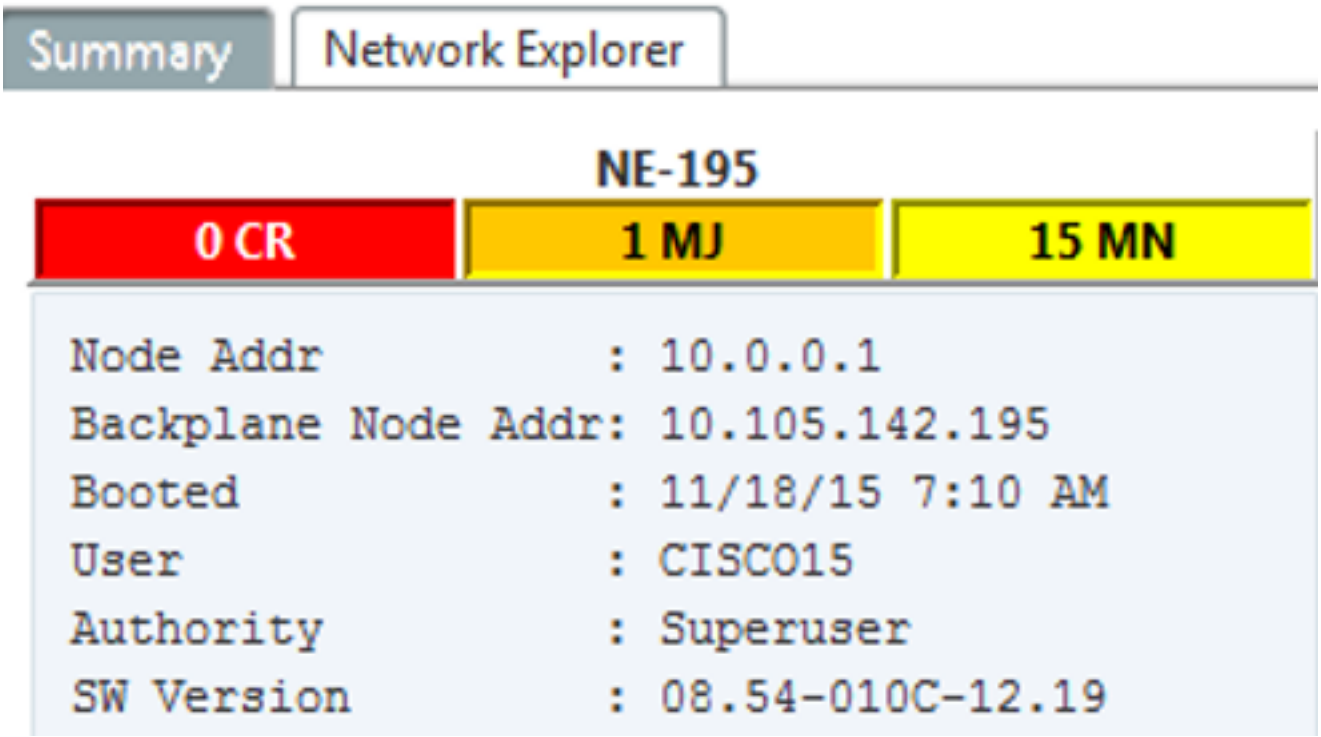
第9步点击Finish。

在接下来的30到40秒内，TCC2P卡将重新启动。CTC切换到网络视图，并出现CTC Alerts对话框。在网络视图中，节点变为灰色，“警报”选项卡中显示DISCONNECTED条件。

在CTC中启用安全模式后，请验证它们是否已正确定义节点，如下所示为一个测试节点。



另外，如下所示，在CTC节点视图中检验两个IP地址。



安全节点锁定和解锁行为：

在以安全模式运行的节点上可以锁定或解锁安全模式。默认状态为解锁状态，只有超级用户才能发出锁定。当安全模式被锁定时，任何网络用户都无法更改节点的配置（包括以太网端口状态）和锁定状态。要移除安全节点的锁，请联系思科技术支持为机架组件安排退货授权(RMA)。启用锁会永久更改机架的EEPROM。

如果重新加载活动TCC2P卡的数据库，则维护节点的配置锁。例如，如果尝试将未锁定节点数据库加载到锁定节点的备用TCC2P卡上，以便传输到活动TCC2P卡（不建议执行此操作），则未锁定节点的状态（通过上传的数据库）不会覆盖节点的锁定状态。如果尝试将锁定的数据库加载到未锁定安全节点的备用TCC2P卡上，活动TCC2P卡将上传该数据库。如果上传的默认值指示锁定状态，这将导致节点被锁定。如果在启用锁之前自定义了软件加载，则所有可锁定的调配功能将永久设置为加载中提供的自定义NE默认值，任何用户都无法更改。

有用注释：

- 如果在ENE中禁用了前接入端口和背板接入端口，并且节点与DCC通信隔离（由于用户调配或网络故障），则会自动重新启用前接和背板端口。
- 可以锁定安全模式，防止模式被更改。
- 启用安全模式会导致TCC2P、TCC3、TNC、TNCE、TSC和TSCE卡重新启动；卡重启会影响流量。
- 如果安装了TCC2卡或TCC2和TCC2P卡的混合，CTC中不提供安全模式选项。
- 启用安全模式会导致TCC2P卡重新启动；TCC2P卡重新启动会影响流量。
- 当TCC2卡作为备用卡添加到包含在安全模式下配置的活动TCC2P卡的节点时，该卡无法启动。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。