Use PuTTY to Establish a Telnet Connection to ENE Through GNE

Document ID: 66069

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Background Information
Topology
Procedure
GNE Configuration
PuTTY
Establish a Telnet Session with the ENE
Establish a Telnet Session to an ML Series Card on the ENE
Related Information

Introduction

This document describes how you can establish a Telnet connection to the End−point Network Element (ENE) or the Multi−Layer (ML) Series cards on the ENE through a Gateway Network Element (GNE) from external networks. In order to do so, you can use PuTTY, which is an application that supports SOCKS version 5.

The GNE serves as an intermediary for connection with the ENEs. The GNE functions as a proxy firewall and an IP−address multiplexer, which allows connections to ENEs from areas outside internal networks.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ONS 15454
- Cisco ONS 15454 ML−Series Ethernet Cards
- SOCKS

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ONS 15454 version 4.6.x
- Cisco ONS 15454 version 5.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

SOCKS is an IETF (Internet Engineering Task Force) approved standard (RFC 1928) generic, proxy protocol for TCP/IP−based networking applications. The SOCKS protocol provides a flexible framework to develop secure communications through easy integration with other security technologies. The SOCKS protocol enables clients to connect to application servers to which the clients do not have direct access.

The default SOCKS port is 1080. SOCKS performs these four basic operations:

- Connection request
- Proxy circuit setup
- Application data relay
- Authentication

Only SOCKS version 5 supports authentication.

SOCKS includes two components:

1. The SOCKS server
2. The SOCKS client

You can implement the SOCKS server at the application layer, and the SOCKS client between the application and transport layers. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS Server, without direct IP−reachability.

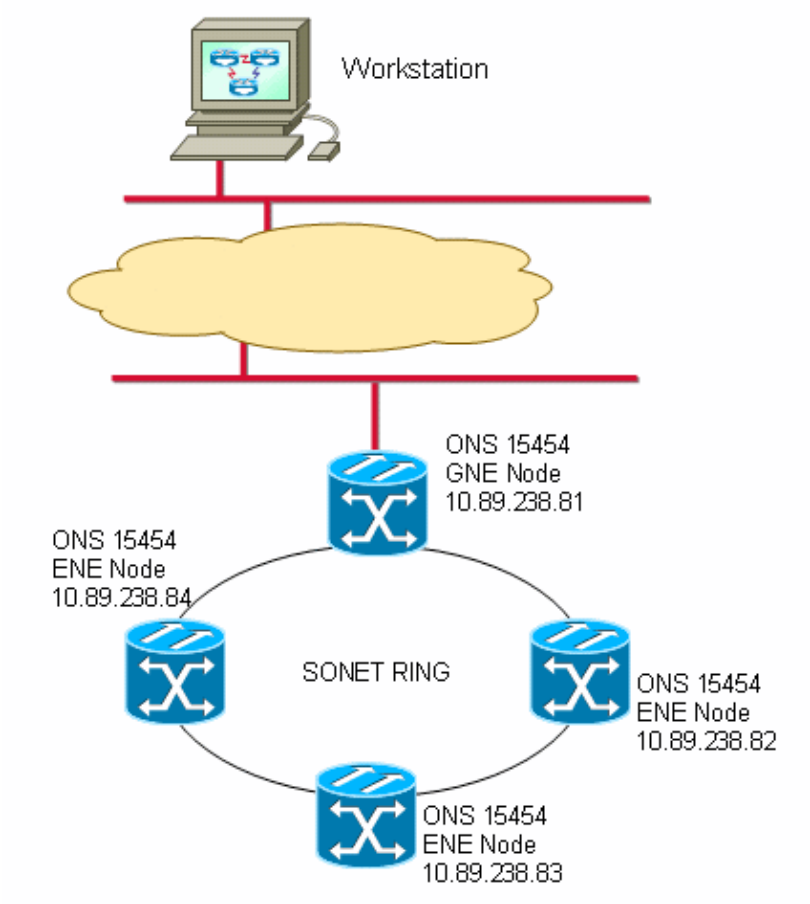
When an application client needs to connect to an application server, the client connects to a SOCKS proxy server. The proxy server connects to the application server on behalf of the client, and relays data between the client and the application server. For the application server, the proxy server is the client.

Topology

Consider the network diagram in Figure 1. The network has four NEs. One NE has LAN connectivity, and serves as the GNE. The other three NEs have only Data Communication Channel (DCC) connectivity. The NEs with only DCC connectivity need to use the NE with LAN connectivity to reach the data communications network (DCN), where the management stations reside.

In Figure 1, 10.89.238.81 is the GNE, and 10.89.238.82, 10.89.238.83 and 10.89.238.84 are the ENEs.

Figure 1 Topology



Procedure

In order to access an ENE, or a specific slot (for example, ML IOS), you need a Telnet application that is SOCKS−aware. The term "Socks−aware" implies that you must be able to configure an application like Telnet to access a SOCKS gateway.

GNE Configuration

In the sample topology, 10.89.238.81 serves as the GNE. Here is the required configuration (see Figure 2):

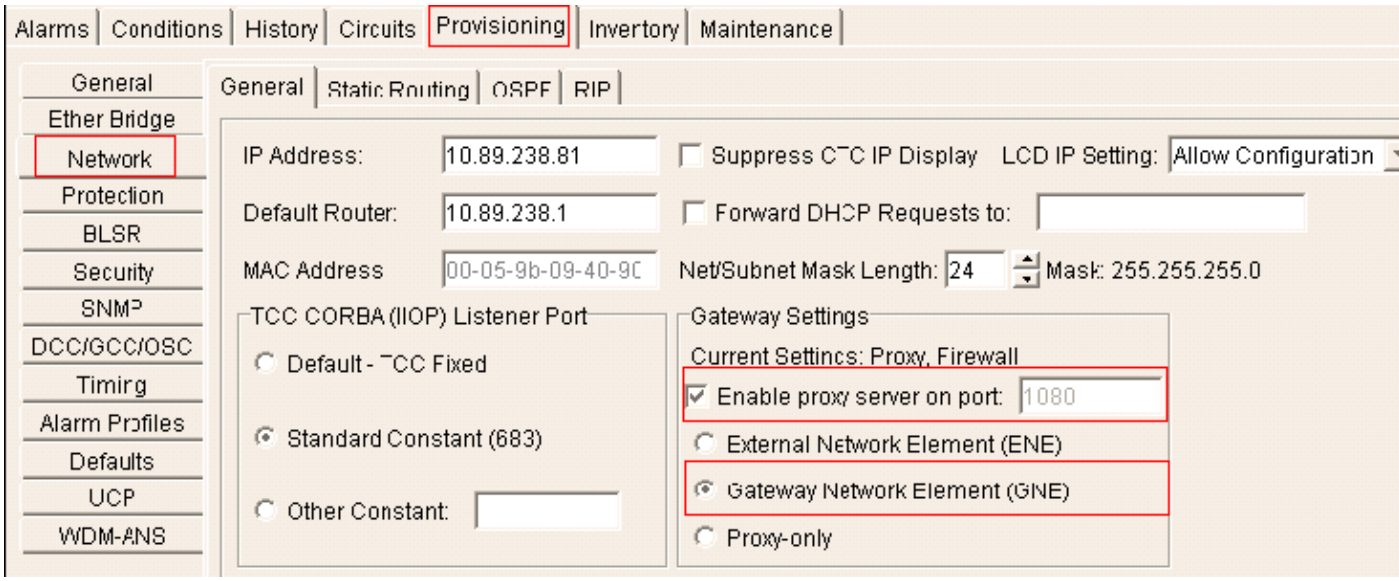
1. Click the **Provisioning > Network** tabs.
2. Check the **Enable proxy server on port** check box.
3. Select the **Gateway Network Element** (GNE) option.

This procedure turns on the firewall and the SOCKS proxy.

The firewall feature makes an NE behave as an IP packet filter between the LAN interface and DCC interfaces. The network drops packets from the LAN interface if the packets are not directed at the IP address of the NE. Exceptions to this rule include broadcasts, multicasts, and UDP packets addressed to port 391 for SNMP relay. The GNE does not forward traffic from DCC interfaces out to the LAN interface. As a result, ENEs are not IP−reachable from the DCN if you have enabled the firewall option on the GNE.

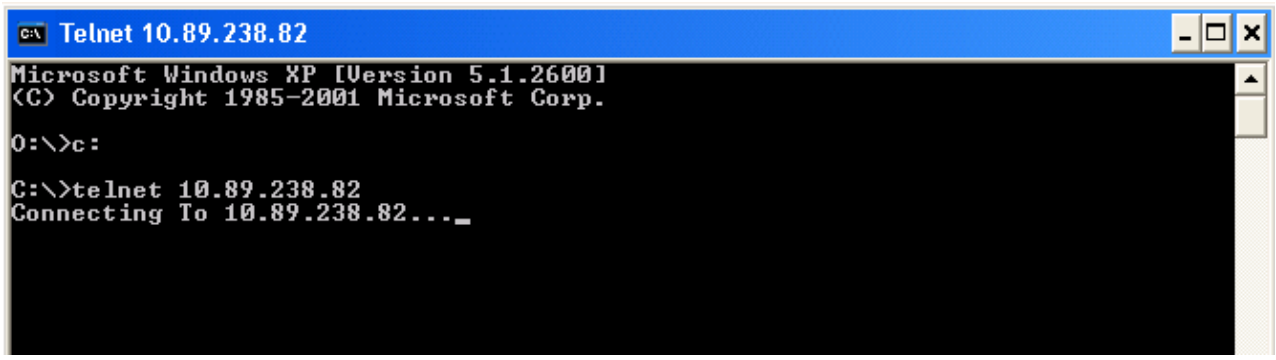
Enable GNE Proxy on the GNEs in order to allow CTC visibility to ENEs.

Figure 2 GNE Proxy Firewall Configuration



If the proxy firewall is on, a Telnet connection to the IP address of an ENE fails (see Figure 3).

Figure 3 Telnet Failure



PuTTY

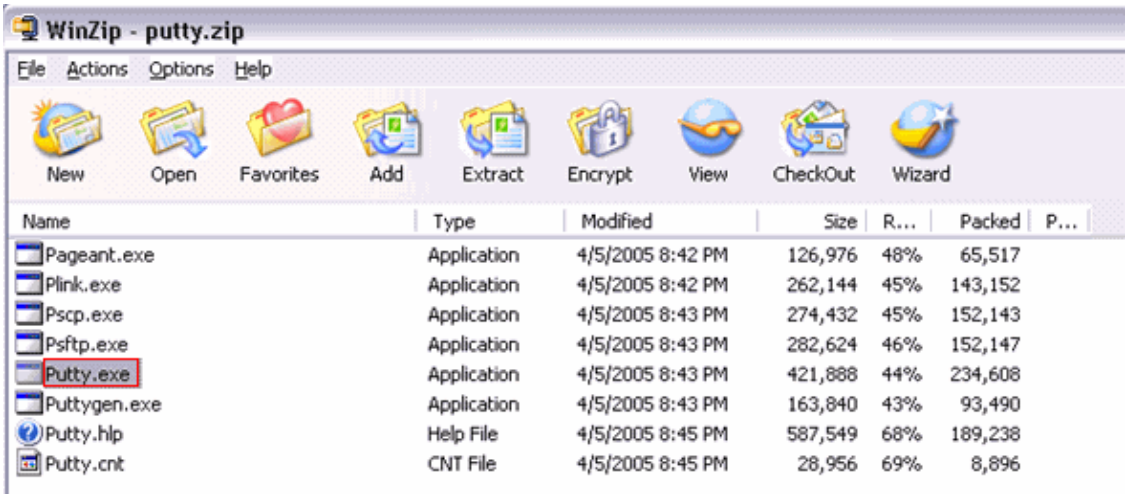
This procedure uses a SOCKS−aware Telnet freeware application called PuTTY. You can download PuTTY from the PuTTY Download Page .

Establish a Telnet Session with the ENE

Complete these steps in order to establish a Telnet session with the ENE:

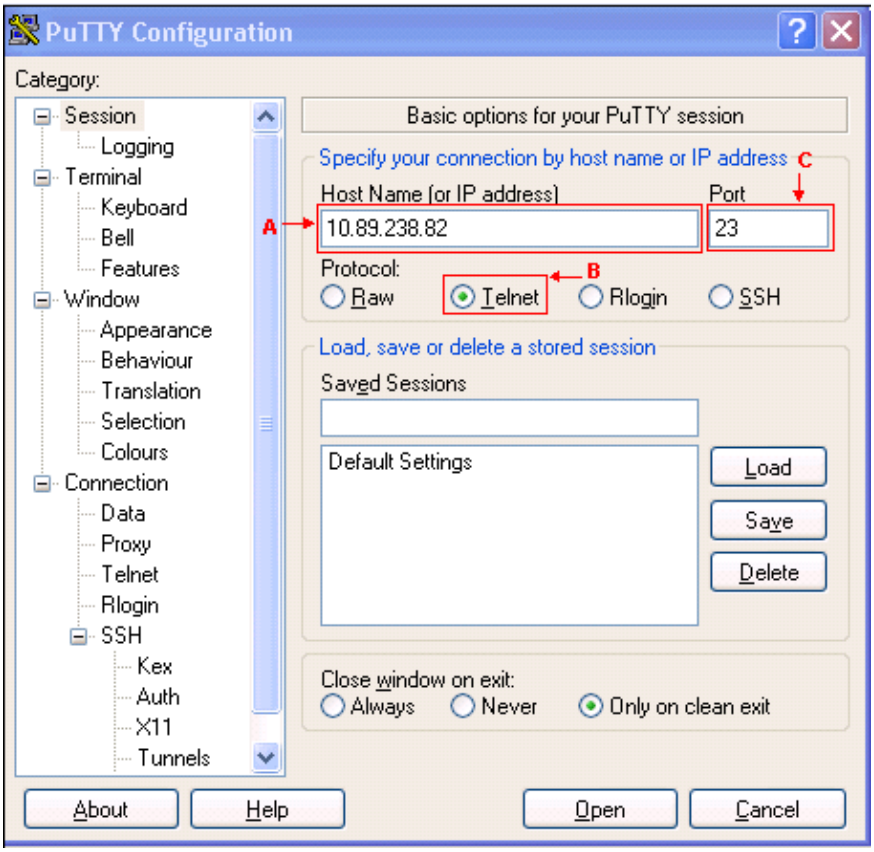
1. Execute **Putty.exe** to start the application (see Figure 4). Here is an example, when you download the application as a zipped file.

   Figure 4 Putty.exe



2. Type the IP address of the ENE in the Host Name (or IP address) field (see arrow A in Figure 5).

Figure 5 ENE IP Address

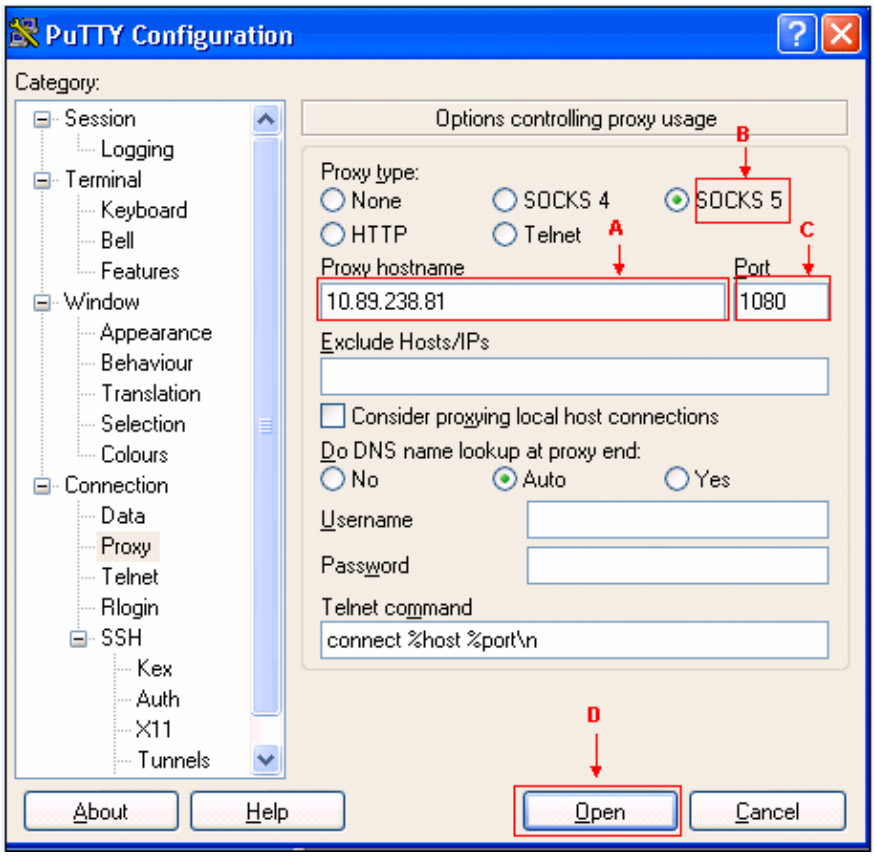


3. Select the **Telnet** option (see arrow B in Figure 5).

The default port for Telnet is 23. The value appears in the Port field (see arrow C in Figure 5).

4. Click **Open**.
5. Type the hostname in the Proxy hostname field (see arrow A in Figure 6).

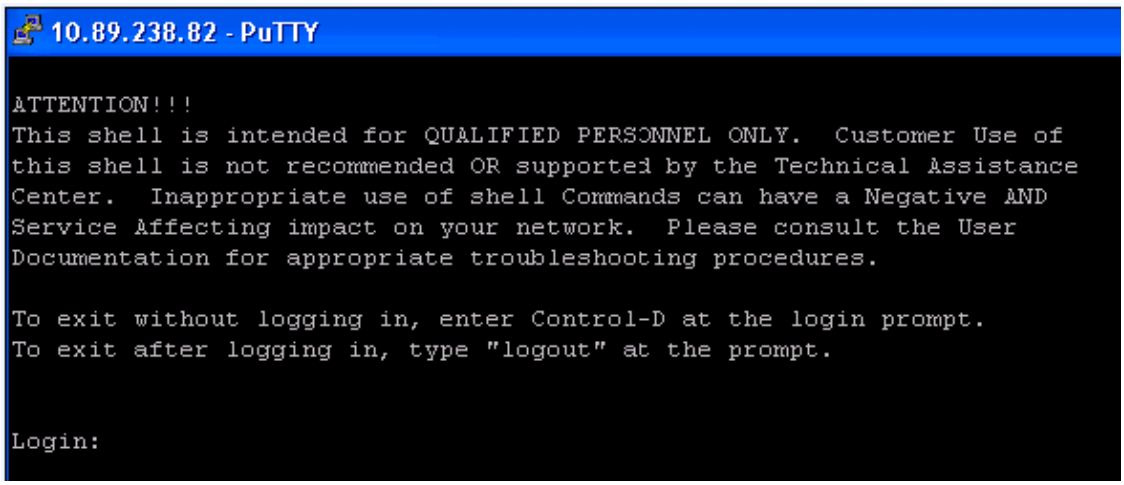
Figure 6 Proxy Hostname



6. Select the **SOCKS 5** option (see arrow B in Figure 6).

   The default port number is 1080, which appears in the Port field (see arrow C in Figure 6).
7. Click **Open** (see arrow D in Figure 6).
8. The Telnet session to the ENE starts (see Figure 7).

Figure 7 Telnet Session to ENE

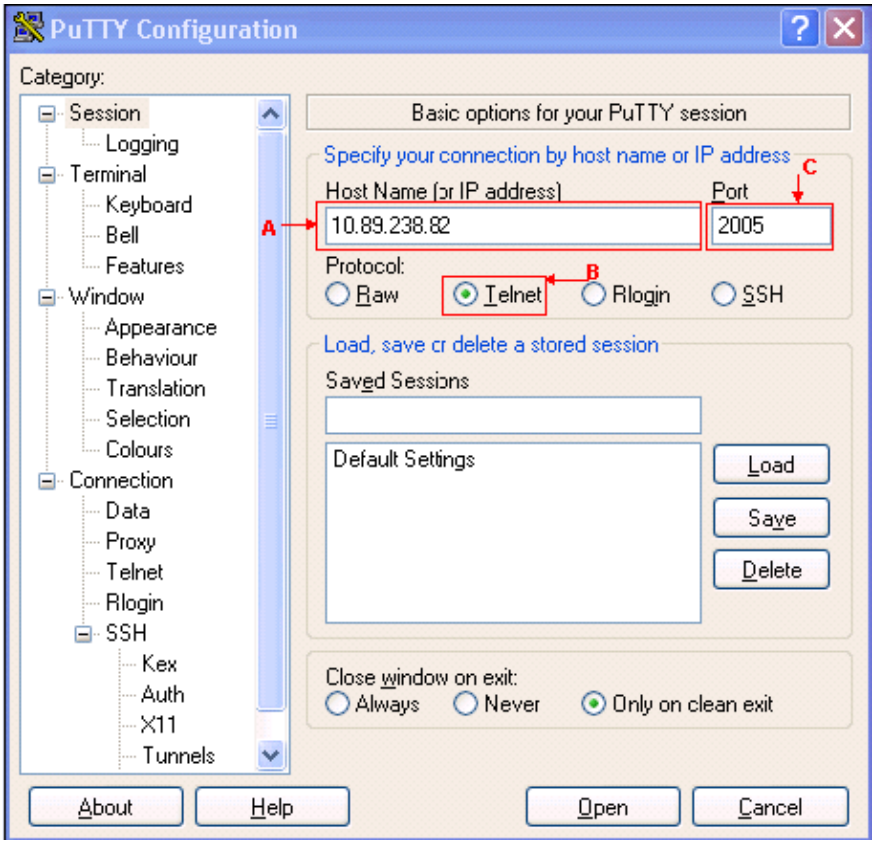


Establish a Telnet Session to an ML Series Card on the ENE

Complete these steps to establish a Telnet session to an ML Series card on the ENE:

1. Execute **Putty.exe** to start the application (see Figure 4).
2. Type the IP address of the ENE in the Host Name (or IP address) field (see arrow A in Figure 8).

Figure 8 ML Card IP Address

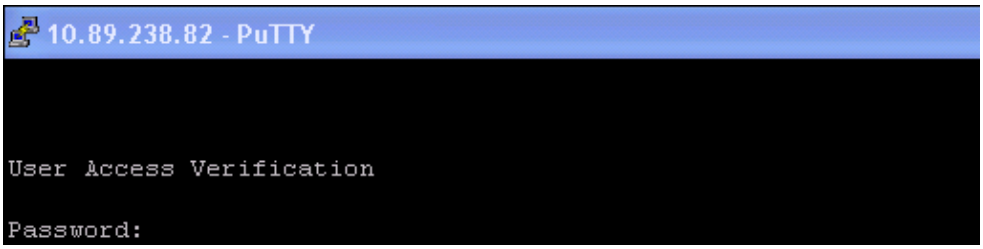


3. Click the **Telnet** radio button (see arrow B in Figure 8).

   The ML card is in slot 5. Therefore, the port number is 2005 (2000 plus slot number) (see arrow C in Figure 8).
4. Click **Open**.
5. Type the hostname in the Proxy Hostname field (see arrow A in Figure 6).
6. Click the **SOCKS 5** radio button (see arrow B in Figure 6).
7. Click **Open** (see arrow D in Figure 6).

   The Telnet session to the ML card starts (see Figure 9).

Figure 9 Telnet Session to ML Card



Related Information

- **PuTTY Download Page**
- **Technical Support & Documentation − Cisco Systems**

© 2013 − 2014 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Oct 05, 2005 Document ID: 66069