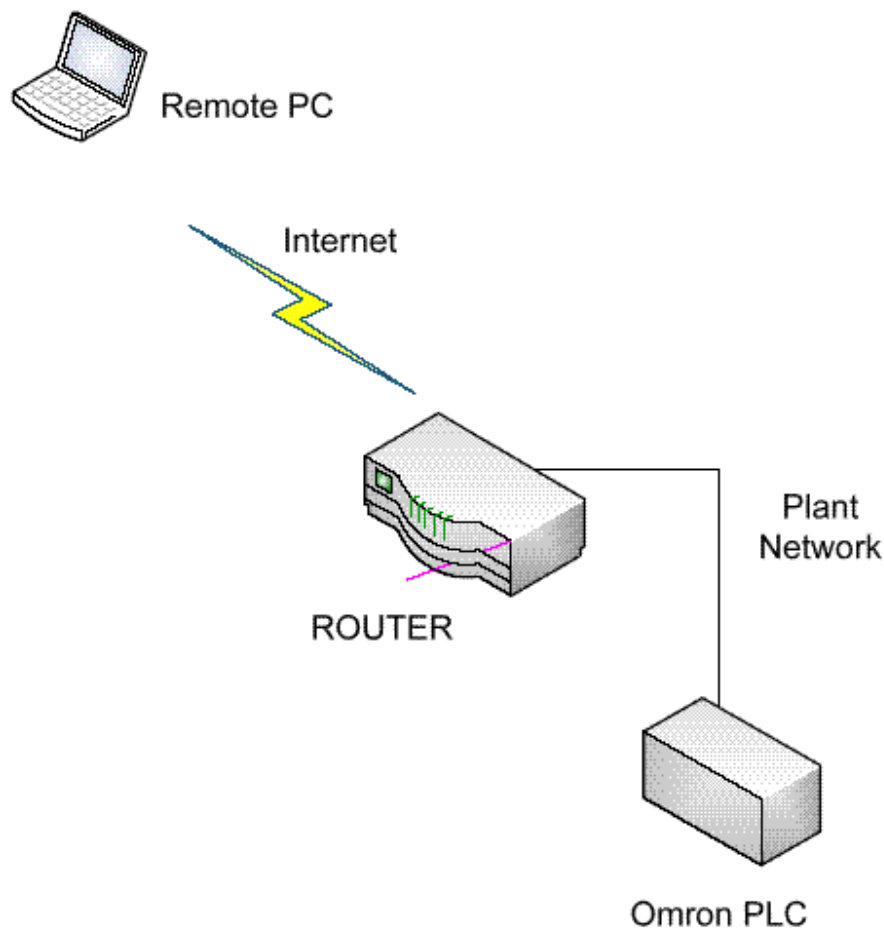


How Safe is Allowing Remote Access to Omron PLCs Via the Internet and How is it Accomplished?

Jay Hughes, Project Engineer, Omron Electronics LLC



Abstract

With the advent of the Internet, manufacturing firms and OEMs have gained access to a new method of monitoring, troubleshooting, and programming automation devices remotely. While this can provide great advantages to programmers and maintenance personnel, it also raises security concerns for IT departments. The purpose of this document is to explore how to open access to Omron PLCs on the Internet, and to discuss the security risks that this poses for IT departments.

With the advent of the Internet, manufacturing firms and OEMs have gained access to a new method of monitoring, troubleshooting, and programming automation devices remotely. While this can provide great advantages to programmers and maintenance personnel, it also raises security concerns for IT departments. The purpose of this document is to explore how to open access to Omron PLCs on the Internet, and to discuss the security risks that this poses for IT departments. This document will be limited in scope to PLCs, but is conceptually similar for other components, and the components that communicate to the PLCs (VFDs, temperature controllers, etc). Although there are other methods of providing remote access (remote desktop applications, VPN, etc), this document will focus on direct communications across the Internet.

How does Omron provide access to PLCs across the Internet? Omron PLCs use fixed UDP and TCP ports for Ethernet communications. To allow access via the Internet, the IT department must implement Port Forwarding in the router that connects the plant network to the Internet. Typically, UDP Port 9600 is used for Omron PLCs. For example (using fictitious IP addresses) if a router has a WAN (Internet) IP address of 1.2.3.4, and a LAN (plant side) IP address of 192.168.1.100 with an Omron PLC connected with an IP address of 192.168.1.10, then the router would forward all UDP traffic arriving at IP address 1.2.3.4 on Port 9600 to the LAN IP address of 192.168.1.10. The PLC Ethernet module is programmed to send all Ethernet packets back to the router (192.168.1.100).

The question becomes: 'what security risk does this pose to the customer'? The answer is fairly simple: the security risk is very low. Hackers and other evildoers, when they are attempting to 'hack' into a network, usually go through a process of Port Snooping to determine what UDP and TCP ports on a router are open and connected to a PC (vulnerable). Standard Ethernet communication protocols are used in this process. When a router is forwarding a TCP or UDP port to an Omron PLC, the traffic is being delivered to a non Windows based operating system. This makes the PLC impenetrable to standard hacking methods. The PLC will only respond to Omron FINS (Factory Intelligent Network Services) commands, not standard Ethernet protocol commands. Thus to a hacker, it appears as though nothing is connected to the router on the port that was snooped (9600 for example), and they move on to other ports or IP addresses.

If remote access to the PLC is only required periodically (during an upgrade, maintenance, or down situation) then the Port Forwarding can be disabled unless remote access is necessary. Omron customers have successfully implemented Internet based communications for several years, without any known security breaches related to allowing access to the PLCs.

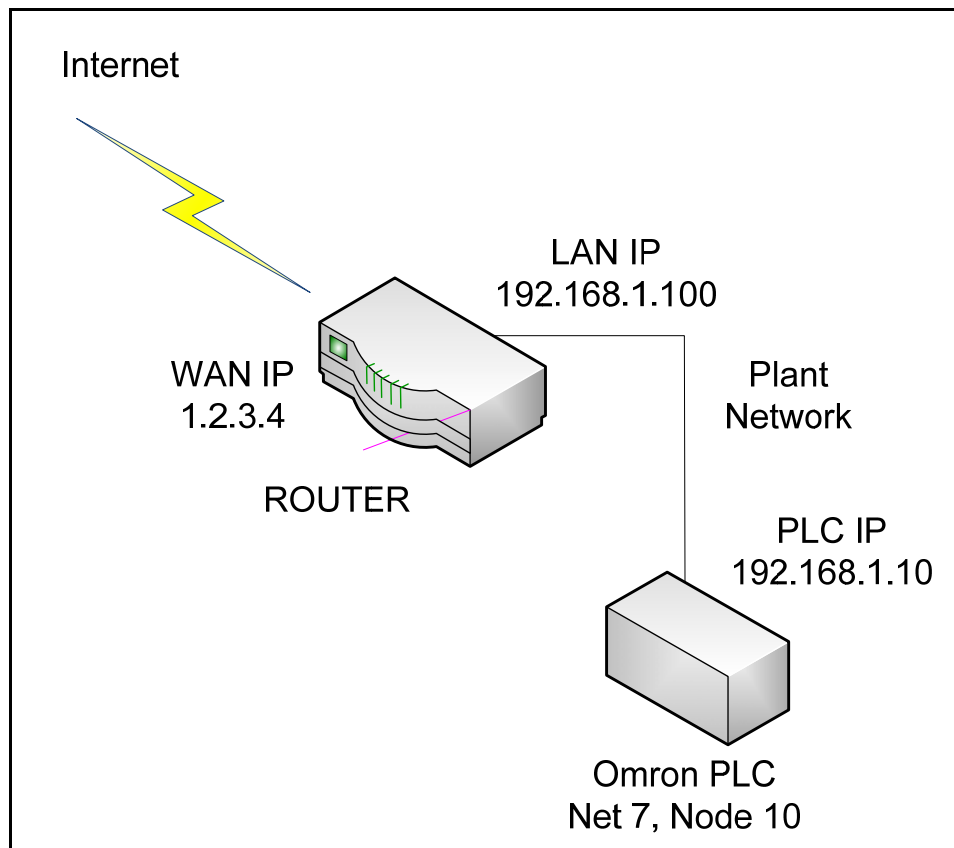
There are several factors that can prevent proper Internet communications with Omron PLCs, including Port Blocking at the site where the PC is located. Often a home network, which typically has fewer restrictions for Internet Access, is a good place to start testing Internet communications to Omron PLCs.

Allowing Internet access: The setup

Allowing remote access to an Omron PLC is a fairly straightforward process. There are a few requirements that must be met to gain access:

1. The IP address of the router that attaches the factory network to the Internet must be a static IP address, or if it is Dynamic, the IP address must be known to the remote programmer.
2. The PLC Ethernet module must be a CS1W-ETN21 or CJ1W-ETN21 with firmware version 1.3 or higher, or the CPU must have a built in Ethernet module (CJ1M-CPU1x-ETN). CS1W-ENT11, CS1W-ENT01, CJ1W-ENT11 or previous Ethernet modules will not work for Internet based communications.

For simplicity of documentation, an example network will be setup as shown:



Ethernet Module Setup:

The Ethernet Module must be properly setup and operating locally on the network, including the proper setup of a local FINS Routing Table. In this example, a FINS Routing table has already been setup that identifies the Ethernet network as FINS Net 7. The PLC is FINS Node 10 on the network. These numbers are shown as an example, and may not match those of an actual network. The Ethernet module must be setup as shown, with the IP address and Sub-Net mask set, and the IP Router Table set to forward all responses from the Omron Ethernet module back to the router (192.1681.100).

The screenshot shows the 'CJ1W-ETN21(ETN21Mode) [Edit Parameters]' dialog box. The 'Setting' tab is selected, and the 'FINS/TCP' sub-tab is active. The dialog is divided into several sections:

- Broadcast:** Radio buttons for 'All 1 (4.3BSD)' (selected) and 'All 0 (4.2BSD)'.
FINS/UDP Port: Radio buttons for 'Default (9600)' (selected) and 'User defined' with a text box containing '0'.
FINS/TCP Port: Radio buttons for 'Default (9600)' (selected) and 'User defined' with a text box containing '0'.
TCP/IP keep-alive: A text box with '0' and the label 'min. [0: default (120)]'.
Destination IP address: A checked checkbox labeled 'Change to dynamic'.
- IP Address:** A text box containing '192.168.1.10'.
Sub-net Mask: A text box containing '255.255.255.0'.
Conversion: Radio buttons for 'Auto (dynamic)' (selected), 'Auto (Static)', 'Combined', and 'IP address table'.
Baud Rate: Radio buttons for 'Auto' (selected) and '10BASE-T'.
- FTP:** Text boxes for 'Login', 'Password', and 'Port No.' (containing '0', with '[0: Default(21)]' below it).
- IP Address Table:** An empty table with 'Ins' and 'Del' buttons below it.
- IP Router Table:** A table with one entry: '000.000.000.000 192.168.001.100'. It has 'Ins' and 'Del' buttons below it.

At the bottom of the dialog, there are buttons for 'Transfer[Unit to PC]', 'Transfer[PC to Unit]', 'Compare', 'SoftSW', 'Restart', 'Set Defaults', 'OK', and 'Cancel'.

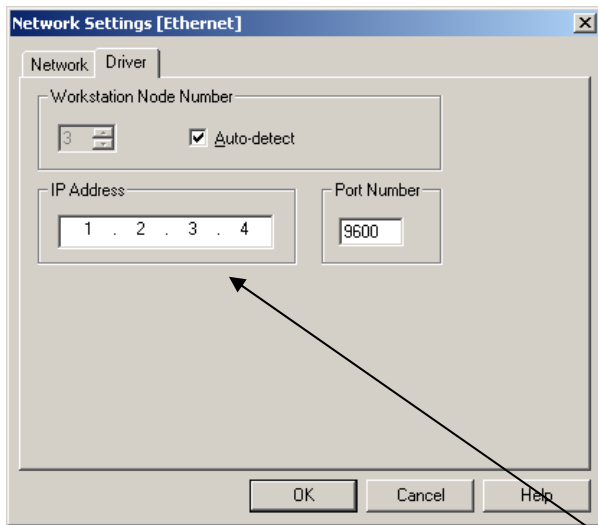
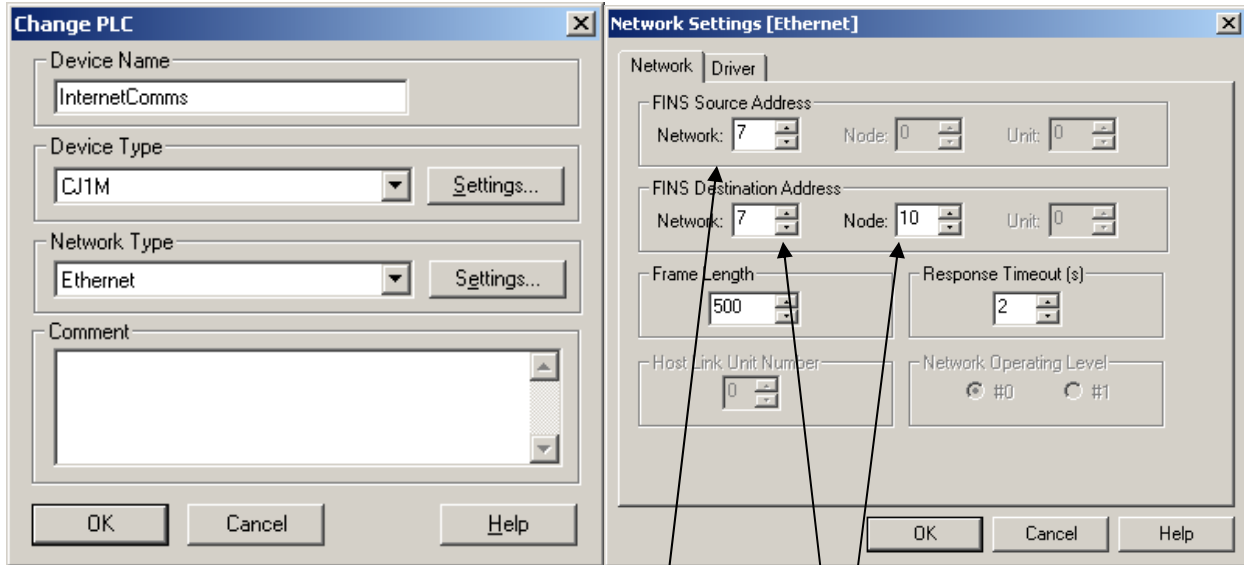
Router Setup

In the Router, Port Forwarding must be enabled, and UDP port 9600 (or TCP port 9600 if FIN Ethernet TCP is used) must be forwarded to the PLCs IP address of 192.168.1.10. The following is shown as an example, although different routers will have different setup screens.

Port Range					
Application	Start to	End	Protocol	IP Address	Enable
PLC	9600	to 9600	UDP	192.168.1.10	<input checked="" type="checkbox"/>

Testing the connection:

CX Programmer Connection:



The FINS Source Address Network and FINS Destination Address Network must match the number as setup in the FINS Routing Table in the PLC. 7 is used in this example. The Fins Destination Address Node must match the Node number of the PLC. 10 is used in this example.

The Internet (WAN) IP address of the router is used as the IP address. This is why a fixed IP address is necessary (or at least a known IP address).

Note: A reduced frame length of 500 bytes (from the default of 2000 bytes) will often increase communication stability by helping to combat Ethernet packet fragmentation on the Internet.

NS Runtime Connection:

Note: NS Runtime is only recommended for monitoring across the Internet, **not performing Control**.

The Network address must match the FINS Network address of the PLC. Network 7 is used in this example.

The last octet of the IP address of the PC that is running NS Runtime is used as the node address. If the PC is node 192.168.1.6, then 6 is used.

A FINS to IP conversion table entry is necessary to identify Node 10 (the PLC) as IP Address 1.2.3.4 (the WAN IP address of the router).

Node	IP Address
10	1.2.3.4

The Network address must match the FINS Network address of the PLC. 7 is used in this example.

The Node address of the PLC is used for the Host. This is 10 in this example.