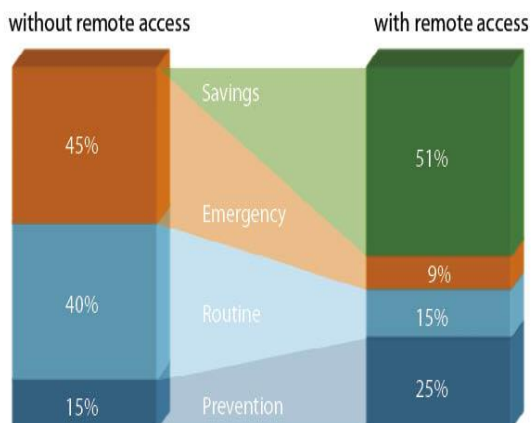


November 02, 2012

Remote Access for Troubleshooting and Maintenance

Field maintenance can be a costly and time consuming ordeal for OEMs, System Integrators and End-Users alike. The cost to travel and the ability to identify the root cause of a problem can be reduce if maintenance engineers have access to and/or ability to gather crucial data of the commissioned devices to troubleshoot the issues. In this Tech Corner, I will discuss a variety of ways to remotely access devices so that engineers can maintain and remedy issues to facilitate a cost effective troubleshooting process.

Remote Access for Remote Programming and Data Acquisition



Remotely accessing programmable devices such as PLCs, PACs, HMIs and Embedded Control Systems can reduce the frequency of travel significantly. Changes in a program to fix issues and being able to monitor in pseudo real-time (latency exists for any remote access) of prevalent issues can be done without costly travel. This also enables maintenance engineers to consequently be more knowledgeable of the issues and devise an organized and effective course of action before heading to the field site.

Recommended Considerations

- **Stable and Fast Internet Connection**
 - Landline based Internet connections such as DSL, Cable, and T1.
- **Timeout Settings of Software**
 - Timeout decisions of programming software and devices that will be interfacing with the remote machines typically needs to be considered in order to accommodate for the increased latency associated with remote connections.
 - Occasionally, Programming Softwares may have limitations on the maximum timeout network or communication settings.

Virtual Private Network (VPN)

- **What it is**
 - Standard method to remotely access Local Area Networks (LANs) predominantly in commercial applications; however, industrial sectors uses them as well.
 - It is secure with IPsec and can have additional security using software based encryption which is available in certain VPN routers.
 - When a VPN tunnel is established, the maintenance engineer will be able to access the LAN behind the tunnel using the Internet as the medium.
- **What you can do remotely**
 - Gain access to IP cameras to have a live view of the machine to troubleshoot.
 - Monitor the PLC as the machine runs to see any logical issues.
 - Re-load the PLC program with modifications.
 - Reprogram HMI screens.
 - Control the HMI.
 - Acquire data needed to analyze issues.
 - Remote Desktop to a configured computer.
- **The Issues**
 - Network Engineers that manage the Enterprise Network may have a difficult time providing a VPN tunnel to the Factory Network mainly because it is not controlled by them.
 - VPN access can be acquired by the End-User's Network Engineers but can be time consuming to gain credentials.
 - VPN tunnels given by the End-User's Network Engineers are usually temporary.
 - Not all VPN client software is the same.
 - Specific VPN client software given by the End-User must be used.
 - Sometimes you have to uninstall VPN client software by other End-Users in order to use the one you need.
 - Large Enterprise Networks have multiple routers and to have a VPN tunnel without compromising the Enterprise Network may require reconfiguration especially since the Automation Network is usually not managed by the Network Engineer.

VPN Suggested Solutions

Usually the Network Engineers suggests giving the Factory Floor its own dedicated Internet connection via DSL or Cable instead of having it go through the Enterprise Network (Office Network), but, this is not always the case.

Moxa's Industrial Router

 <p>EDR-G902 Industrial firewall/VPN secure routers 1 WAN 10 VPN</p> <p>To learn more ▶</p> <p>Features</p> <ul style="list-style-type: none">• Firewall/NAT/VPN/Router all-in-one• High performance Gigabit copper/fiber combo port• 1 WAN• 10 VPN	 <p>EDR-G903 Industrial firewall/VPN secure routers 2 WAN 25 VPN</p> <p>To learn more ▶</p> <p>Features</p> <ul style="list-style-type: none">• Firewall/NAT/VPN/Router all-in-one• High performance Gigabit copper/fiber combo port• 2 WAN/1 DMZ• 25 VPN
---	---

○ What it is

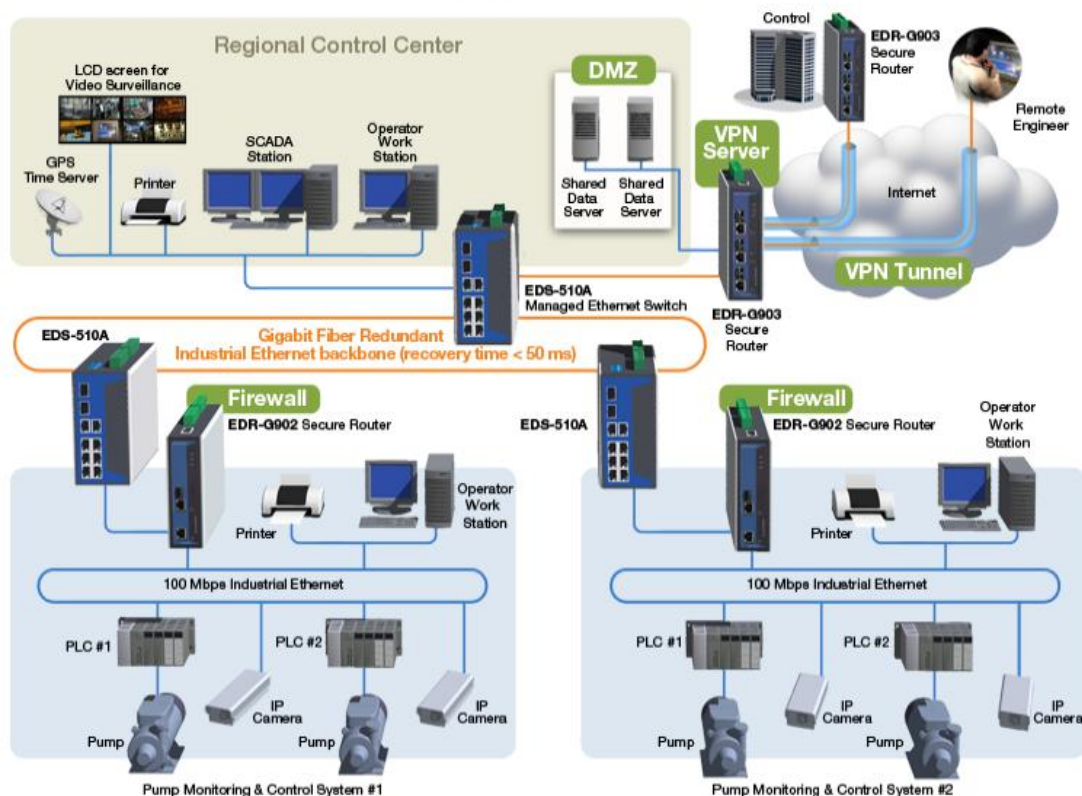
- Moxa's Industrial router is a router that provides Gigabit Copper or Fiber connectivity; ideal for large Factory Automation systems that requires full router/firewall capabilities.
- Has a built in VPN server that supports up to 25 VPN connections.
- Can Encrypt messages going through VPN tunnels for added security.
- Ideal for mission critical remote connectivity between sites.

○ What you can do

- The EDR-G903 has a Physical DMZ (perimeter networking) WAN support to provide additional security for Enterprise Networks.
- The EDR-G903 supports WAN back-up to support multiple Internet Service Providers (ISPs).
- If the main WAN connection is lost, the router can switch to the other WAN port automatically.
- The EDR-G90X series has a firewall and encryption capabilities that will ensure security of data being pass through and being held within the LAN.
- The EDR-G90X series uses Gigabit ports allowing larger bandwidth support.
- The EDR-G90X can be configured as a VPN server or VPN client.

- The EDR-G90X can be configured for Peer to Peer VPN connection allowing two Routers to automatically establish a VPN connection with each other.
- Very useful for large Infrastructures that requires secure Peer to Peer connections.
- **The Issues**
 - There is a steep learning curve to fully utilize the capabilities of the EDR-G903 if you are not familiar with networking.
- **Example Application**
 - An area that requires network separation and security between each other would require such a system.
 - The following illustration below describes an example of how the EDR system can be used.
 - The EDR-G903 can be a front end device that can incorporate two forms of separation.
 - The DMZ WAN port is used to allow access of devices that can be Public to the Internet network.
 - The Regular WAN port is used as a WAN port that can allow VPN tunneling to devices and encrypt the messages for additional security.
 - The EDR-G902 can be used for additional network separation and firewall protection.

Secured Automation Network for Water Pumping Stations



 eWON VPN Router

- **What it is**
 - The eWON VPN Routers are preconfigured with the authentication credentials to establish a VPN tunnel using eWON's VPN service - Talk2M.
 - The VPN tunnel is based on the OpenVPN technology.
 - The device provides its own VPN tunnel thus reducing much of background work and resources the Network Engineers have to use.
- **What you can do**
 - With a consolidated VPN client there is no need to have multitudes of software installed in the computer.
 - It is a router that only the devices connected to the LAN ports of the eWON VPN Router are accessible, thus making it a feasible solution for Network Engineers.
 - Locally log tagged information plus users can gain access to the remote FTP server built-in.
 - Provide web interfaces to present pertinent data via a standard HTML web browser.
 - Programmed in BASIC to allow data calculations for faster analysis of tagged data.
 - Configured for Peer2Peer connectivity but recommended to connect up to two eWON routers.
 - Provide remote desktop if set-up accordingly along with a controlled security feature of a VPN tunnel.
- **The Issue**
 - Initial Set-ups may require some Technical Support due to the uniqueness of the product.
 - There will be some tweaks involved with the Programming software associated to the HMI and PLC to accommodate the increased Lag time by the VPN tunnel.
 - I recommend users to familiarize themselves with the product first before fielding a device. We have units available for 30-day evaluation and testing.

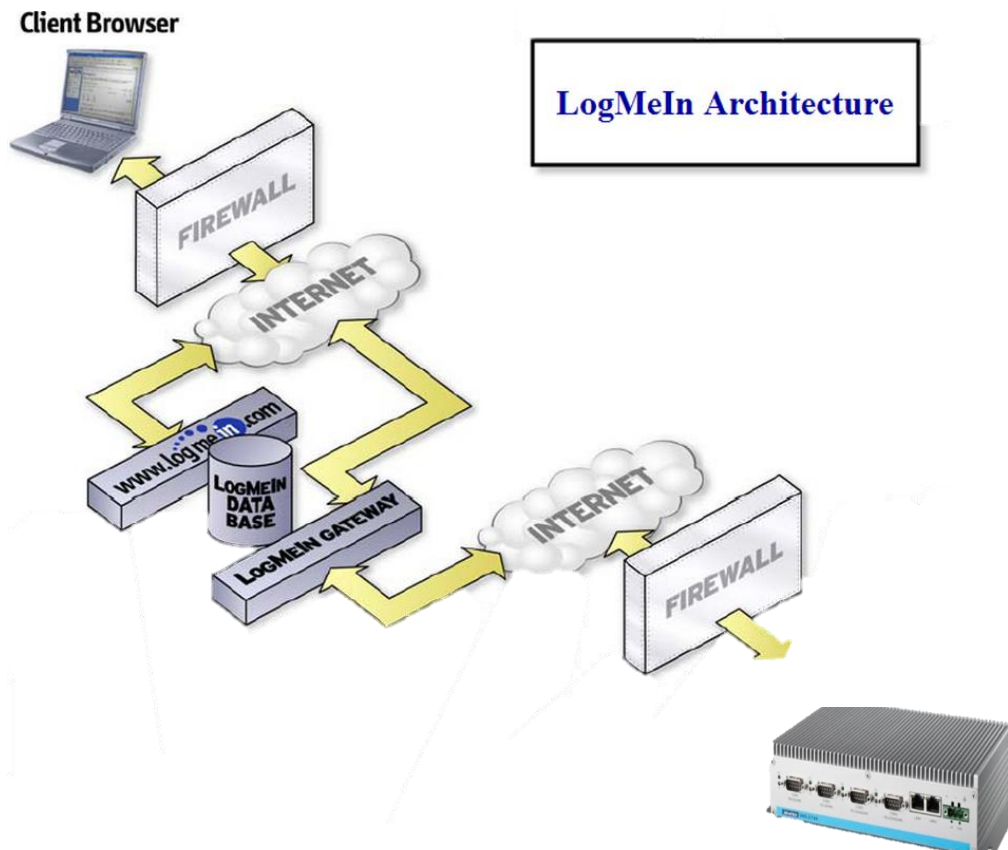
- **Example Applications**
 - The eWON router provides many benefits for OEMs and Systems Integrators that would like a canned VPN to access programs already implemented in the field.
 - A customer that has used the eWON solution to program PLCs and HMIs remotely has reduced the Project IT lead time by 40 to 50 percent.
 - Reduced hardware cost by 20 percent for remote connectivity.
 - Saved time to travel for minor to extensive program overhauls.



Canned Remote Desktop

- **What it is**
 - Gain remote access using software such as LogMeIn, TeamViewer, etc.
 - A canned version of remote desktop that can also be achieved through a VPN tunnel.
- **What you can do**
 - Provides access to a computer and interface with devices that are locally connected to the remote computer.
- **The Difference**
 - The programming software has to reside within the computer that the engineer is remotely connected to.
 - The commissioned computer has to support the requirements of the software being used.

- The engineer is essentially interfacing with the remote computer and interacts with whatever the computer is connected to.
- Essentially eliminates latency issues with programming software and devices since the interaction is done locally.



○ **The issues**

- Maintenance of the computers deployed to ensure that the OS, programming software, etc are up to date has to be done regularly.
- May require additional programming licenses be purchased to support this "local" computer.
- Back-ups of each computer have to be done regularly in case a computer crashes.
- Replacement of the computer can be an issue depending on the software and information that has to be re-installed.
- Repurchasing licenses.
- Matching firmware and software versions utilized in the system.

- Can pose issues as deployment increases due to dispersion of data that needs to be consolidated; like program changes, documentation changes, firmware upgrades, etc.
- Some end-users may not approve the usage of third party security features and prefers a controlled security environment like VPN.
- **Suggested Solutions**
 - Industrial Grade Computers
 - Using an Industrial Grade computer ensures that the computer commissioned complies with industrial standards allowing better longevity and reliability.
 - Canned desktop software like LogMeIn or TeamViewer can be used—where allowed.

Summary

In summary, there are a plethora of solutions for remote access to provide the Maintenance Engineers of System Integrators, OEMs and End-Users the tools and capabilities needed to service machines and systems while reducing frequency of unrequired travel. Essentially, pick a solution that accommodates the End-User's network policies and existing topology. Having interactions with the Network Engineers allows for a smoother commissioning of approved methods and a better relationship with the End-user.

References:

Product Information:

[QuantumAutomation: eWON Product Link](#)

[QuantumAutomation: Moxa Product Link](#)

[eWON: Customer Whitepaper Testimony](#)

[Moxa: Router Product Overview](#)

Additional and Reference Reading

[Wikipedia: VPN Concept](#)

[HowStuffWorks: VPN](#)

