Accessing Remote Devices via the LAN-Cell 3

Technote LCTN3017

Proxicast, LLC
312 Sunnyfield Drive
Suite 200
Glenshaw, PA 15116

1-877-77PROXI
1-877-777-7694
1-412-213-2477

Fax:
1-412-492-9386

E-Mail:
support@proxicast.com

Internet:
www.proxicast.com

This TechNote applies to LAN-Cell models:

LAN-Cell 3:
LC3-52U

Document Revision History:

Date	Comments
May 16, 2012	Initial Release

Introduction

One of the most common applications for the LAN-Cell 3 is to provide users anywhere on the Internet with access to one or more devices at a remote location. Devices such as IP Cameras, Networked Digital Video Recorders (NVR/DVR), Programmable Logic Controllers (PLC), Remote Telemetry Units (RTU), SCADA equipment, data loggers, and other IP-enabled devices can be easily accessed remotely via the LAN-Cell.

This TechNote provides an overview of how to configure the LAN-Cell and your equipment for direct remote access. An example using a DVR is presented for illustration purposes. The process is similar for all other types of equipment. An alternative approach is to create a Virtual Private Network (VPN) between a PC or a router at your main location and the remote LAN-Cell. The VPN approach is covered in the *LAN-Cell 3 Users Guide* and several VPN-related TechNotes.

Proxicast has also prepared a TechNote specifically for using PC remote-control software such as VNC, PC-Anywhere and Windows Remote Desktop with the LAN-Cell. Please see *LCTN3010: Using Remote Desktop Software with the LAN-Cell 3* for tips on configuring the LAN-Cell for these specific software packages.

Background

The procedure for establishing remote access to devices connected to the LAN-Cell is straightforward and can be broken down into four steps:

1. Attach the equipment to the LAN-Cell's LAN subnet
2. Locate the LAN-Cell on the Internet
3. Determine the IP ports required for communication
4. Forward incoming traffic from the Internet to the equipment

We will configure the LAN-Cell 3 to permit access to a Digital Video Recorder (Figure 1) throughout this TechNote as an illustration of the LAN-Cell parameters that must be set to enable remote access.

Before attempting to configure the LAN-Cell, ensure that you have gathered all of the necessary configuration information (see Table 1). It is easiest to test remote access if you configure the LAN-Cell and your equipment before installing them in a remote location.

Table 1: Remote Access Parameters

Item	TechNote Example Values	Your System
LAN-Cell LAN IP	IP: 192.168.1.1 Subnet Mask: 255.255.255.0	IP: Subnet Mask:
DVR IP Settings	IP: 192.168.1.2 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.1	IP: Subnet Mask: Default Gateway:
DVR Application Ports	TCP-3000 TCP-3001 TCP-8800	
ISP / APN	AT&T / "i2gold"	
LAN-Cell Public IP Dynamic DNS Name	166.139.37.167 (static) 001B39123456.proxidns.com	

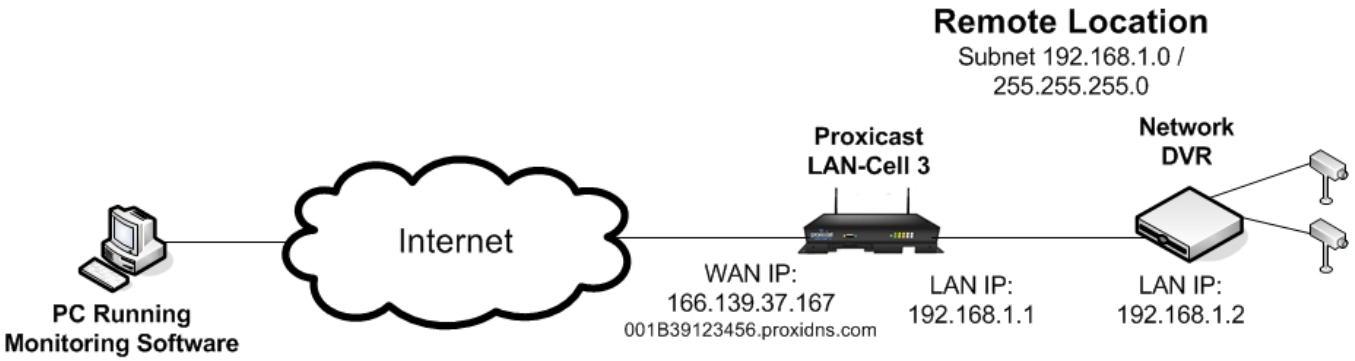

Figure 1: Remote Access to DVR Example

Prerequisites:

- The LAN-Cell is already configured for Internet access via its WAN and/or USB Cellular modem.
- Devices attached to the LAN segment of the LAN-Cell are able to access the Internet (e.g. open a web page on a PC, etc) via the LAN-Cell.
- If there are any intervening firewalls between the monitor PC and the LAN-Cell, ensure that these firewalls permit the necessary IP ports (see Step 3).

1. Attach the equipment to the LAN-Cell's LAN subnet

Use the DVR's management software to set its IP address information. The DVR should be assigned a "static" IP address that is part of the LAN-Cell's LAN subnet[1]. The LAN-Cell's LAN IP address must be the DVR's Default Gateway. If this value is not set in the DVR, it will not be able to properly reply to remote access requests. In our example, the DVR IP settings would be:

DVR IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1

After configuring the DVR's IP settings, attach the DVR to one of the 4 Ethernet LAN ports on the LAN-Cell.

2. Locate the LAN-Cell on the Internet

Static IP
If your LAN-Cell has been assigned a "static" IP address by your ISP (cellular carrier), note this value. You will use this IP address to access the remote LAN-Cell and attached equipment. In our example, the LAN-Cell has a static IP address of 166.139.37.167.

Dynamic IP / DDNS
If you do not have a "static" IP address (or prefer to access your device by name rather than number) you can use the "permanent" Dynamic DNS (DDNS) name assigned to each LAN-Cell (*serial#.proxidns.com*). Optionally, you can setup an account with a third-party DDNS provider such as DynDNS.com and configure the LAN-Cell to update your DDNS provider with its current WAN and/or CELL IP address every time the IP address changes.

[1] You can optionally use the DHCP reservation technique to assign a specific IP address to the DVR's MAC address via DHCP. See the LAN-Cell menu SECURITY > OUTBOUND MAC CONTROL

3. Determine the IP ports required for communication

Every IP-based application uses one or more numbered “ports” to communicate between devices. Each IP address has only a single instance of each port number. Many common network applications have “well-defined” port numbers assigned by convention and agreement via the Internet Assigned Numbers Authority (IANA).

Check with your equipment manufacturer and documentation for the list of port numbers required by your application software. Many applications require multiple ports or ranges of ports. The DVR and monitoring software in our example are using TCP ports 3000-3001 and 8800.

Note on TCP/UDP Port Usage:

The LAN-Cell 3 uses port TCP-8080 for its internal web management application and several other ports to listen for various requests from other devices. If your equipment must use port TCP-8080 or any of the ports listed in Table 2, you must change the LAN-Cell’s port or use port-translation to avoid conflicts.

Table 2: LAN-Cell 3 Default Port Usage

Default LAN-Cell Service Port #	Application
53	DNS (cannot be changed)
161	SNMP
500	IKE (VPN) (cannot be changed)
1720	H.323 (cannot be changed)
1723	PPTP (VPN) (cannot be changed)
4500	NAT-T (VPN) (cannot be changed)
8080	HTTP
8123	SSH (cannot be changed)
49152	UPnP

Note on Cellular Carriers & ISP’s:

Your ability to access specific port numbers depends on the service you have with your ISP (cellular carrier) and any network restrictions they have in place. Contact your ISP with the list of required application port numbers to ensure that you have the proper type of service that permits “inbound” access to these ports.

As of the time of this writing, the major U.S. cellular carriers have the following policies in effect:

Table 3: U.S. Cellular Carrier Port Restrictions

Carrier	Port Restrictions
Verizon Wireless	
3G (CDMA)	All ports open
4G (LTE)	Depends on APN used:
APN=vzwinternet (default)	All ports blocked via NAT
Static IP APN's (xxxx.vzwstatic)	All ports open
AT&T	Depends on APN used:
isp.cingular & broadband	All ports blocked via NAT
internet & I2GOLD	All ports open[2]
Sprint 3G (CDMA)	Most ports open. Port 80 blocked.
T-Mobile	All ports blocked. Contact third-party M2M service providers for alternate APNs

4. Forward incoming traffic from the Internet to the equipment

You must now tell the LAN-Cell which device(s) on the LAN are to receive the data on each port. The LAN-Cell 3 automatically opens the necessary ports in its firewall once you define the required Port Forwarding rules.

Go to APPLICATIONS > PORT FORWARDING (Figure 2)

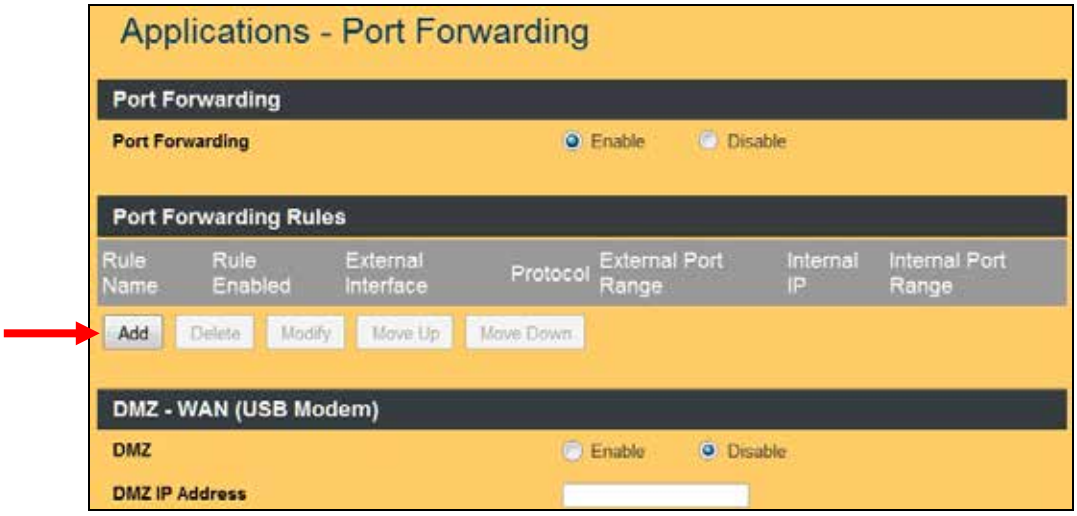

Figure 2: Port Forwarding Summary Screen

[2] Access to these APN's requires the *Mobile Terminated Data Service* feature on your AT&T account. Contact your AT&T representative about this service and access to "open" APN's.

Click the ADD button to create a new Port Forwarding Rule as shown in Figure 3.

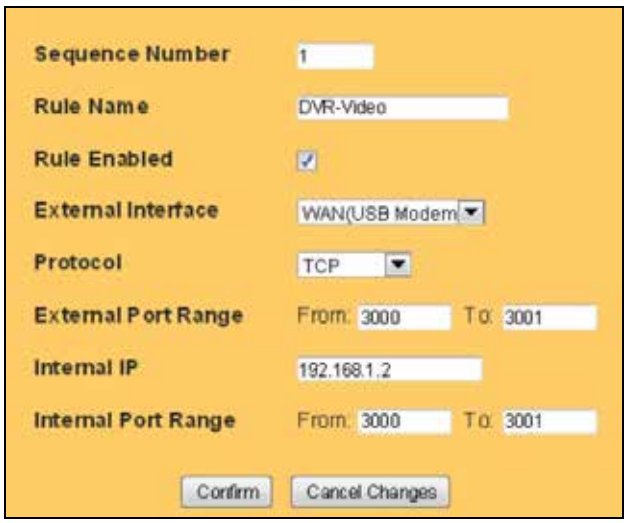

Figure 3: DVR-Video Port Forwarding Rule

Create a new Port Forwarding Rule by giving it a descriptive Rule Name (no spaces). Select the External Interface that this rule applies to (Ethernet or USB). Select the Protocol to forward (if you are unsure of the correct protocol, select TCP/UDP to forward both types). For our DVR example, you need to forward External Ports TCP-3300 to TCP-3001 to the DVR which has a static Internal IP address of 192.168.1.2. You do not need to do port-translation in this example, so use Ports 3300-3001 as the Internal Port as well. Click Confirm to return to the summary screen.

Repeat this process to create the second Port Forwarding Rule for the DVR-Control port TCP-8800 (Figure 4).

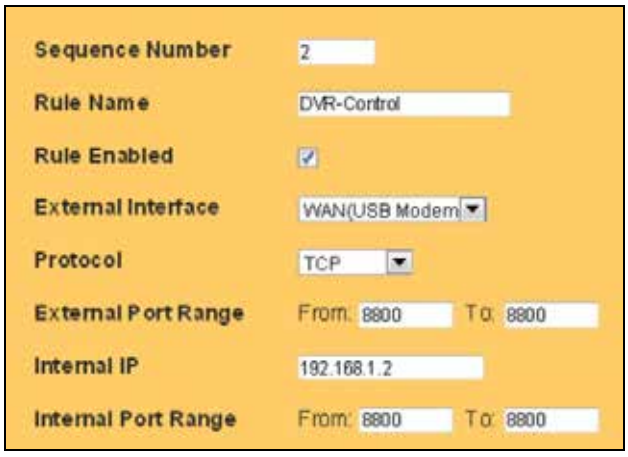

Figure 4: DVR-Control Port Forwarding Rule

After returning to the Port Forwarding Summary Screen (Figure 5), click the Save Settings to save your new rules.

Figure 5: Completed Port Forwarding Rules

In some instances, you may need to "translate" externally visible TCP/UDP port numbers to other port numbers used on your private LAN if you cannot modify a port number that your equipment is using and it conflicts with other devices or the LAN-Cell. You may also need to use port translation if you have more than 1 LAN device that must use the same port number. For example, you could translate incoming port 8002 to port 80 on 192.168.1.2 and incoming port 8003 to port 80 on 192.168.1.3. Port translation is not used in our example.

You are now ready to access your remote equipment over the Internet via the LAN-Cell.

Usage Notes

- You may repeat this process to define the parameters for any other remote LAN devices to which you need access.
- If you have both an Ethernet WAN and USB WAN connection (e.g. fail-over mode), you must define a set of Port Forwarding rules for each interface if both are to be used for remote access.
- Backup your LAN-Cell's configuration before and after configuring remote device access.
- You cannot directly "ping" the devices on the LAN-Cell's LAN since ICMP cannot not flow through the Network Address Translation (NAT) feature of the firewall. If you ping the LAN-Cell's WAN IP address or DDNS name, the LAN-Cell itself will respond to the ping (if this feature is not disabled and your ISP does not block ICMP traffic). Use your application software to test the connection to your remote equipment.

Troubleshooting

The most common difficulties encountered when setting up remote access via the LAN-Cell involve:

1. *Incorrect IP addressing on the remote equipment*
   Ensure that the remote equipment has the LAN-Cell's LAN IP address as its Default Gateway and that the subnetting is correct.

2. *Not being aware of all of the ports used by your application*
   Please consult your documentation or contact the software/equipment manufacturer.

3. *Carrier blocking the ports necessary*
   Consult with your cellular operator on what features are necessary on your account to allow inbound access to the necessary ports. For example, AT&T requires a feature called "mobile terminated data service" on your account and the use of either the "internet" APN or a custom APN for your company (the APN "broadband" blocks inbound connections and cannot be used to host remote servers). Sprint blocks some ports including port 80. Verizon Wireless has no inbound restrictions on its 3G network but requires a static IP APN for inbound access on its 4G/LTE network.

   If you are unable to have the necessary ports opened and cannot change your remote equipment configuration, use the Port Translation feature to map an open port to the required port for your application (e.g. public port 7780 translates to private port 80). You may also be able to set up a VPN to get around carrier-imposed port restrictions.

4. *Incorrect port forwarding*
   Double check the port range defined as well as the destination internal IP address. Do not map the same ports to more than one internal IP address unless you are using Port Translation with different incoming (public) ports.

5. *Corporate or PC-level firewalls blocking the necessary ports*
   Disable any software firewalls on the remote or HQ PCs. Ask your firewall administrator to open the necessary ports in your corporate firewall to allow your management software to communicate.

# # #