Using Remote Desktop Software with the LAN-Cell 3

Technote LCTN3010

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

Minimum LAN-Cell Firmware Revision: 5.1.0

Note for LAN-Cell 2 Users:

A version of this TechNote for the LAN-Cell 2 is available on the Proxicast Technical Support website (http://support.proxicast.com). See TechNote *LCTN0010 Using Remote Desktop Software with the LAN-Cell 2*.

Document Revision History:

Date	Comments
May 9, 2012	First release

Introduction

One common use for the LAN-Cell is to provide access to a PC at a remote site. Users at a headquarters location (or on the road) want to be able to take control of a remote PC's screen and keyboard to operate the PC as if they were physically in front of the remote PC.

There are numerous "remote desktop" software packages available. Each one has unique and specific requirements for how it communicates between the Host (HQ) PC and the Remote (target) PC.

This TechNote includes examples configurations for:

1. Microsoft Windows Remote Desktop
2. VNC / RealVNC / TightVNC
3. pcAnywhere

For other packages, please consult with the software manufacturer to determine the necessary ports.

Example Network Topology

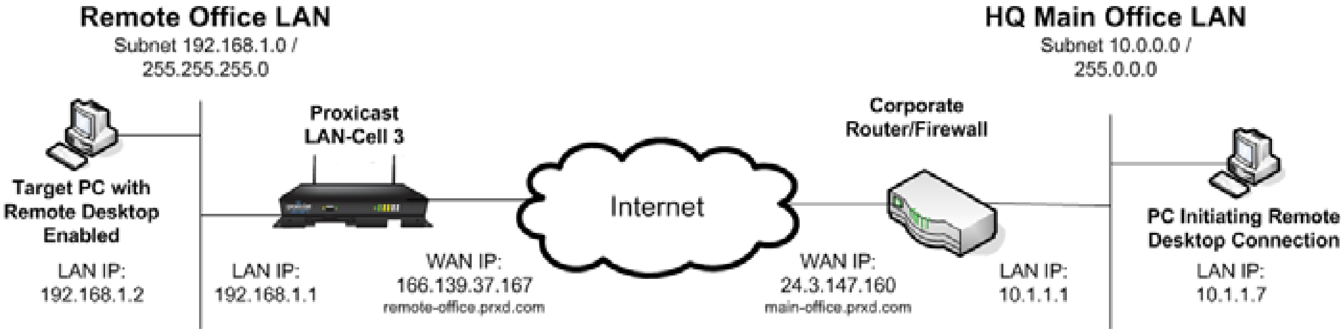


Figure 1: Example Network Topology

Usage Notes

- When configuring and testing remote desktop connections for the first time, it is helpful to have the LAN-Cell and the target PC physically near each other so that you can view the configuration and logs of each device while testing.

- In this example, the remote office LAN-Cell has a static WAN IP address (166.139.37.167). Some remote desktop software packages support fully qualified domain names (FQDN) in addition to IP addresses as the name of the target PC. If your LAN-Cell has a dynamic WAN IP address, you may be able to use the LAN-Cell 3's default DDNS name (*serial#.proxidns.com*) or your own DNS name (e.g. *remote-office.prxd.com*) by setting up a DynDNS account, hostname, and configuring the remote LAN-Cell to update a DDNS provider with its current WAN IP address. See the *LAN-Cell User's Guide* for additional information on DDNS.

- Some cellular network operators restrict "inbound" traffic from the Internet to remote devices based on IP ports, addresses or your account. Please check with your cellular carrier to ensure that the ports necessary for your remote desktop software are not being blocked by their network. If the carrier is unwilling to open the necessary ports, you must implement a VPN solution to access your remote PC.

- If your HQ PC is behind a firewall, you must ensure that it is configured to pass the necessary IP traffic on the remote desktop software ports in both directions.

Overview

All remote desktop software works by employing a piece of “terminal server” software on the remote target PC and a “terminal emulator” piece of software on the initiating (HQ) PC. The terminal server software “listens” on a specific IP port for commands sent from the terminal emulator and then translates those commands into the equivalent keyboard and mouse inputs on the target PC. The terminal sever software also captures the screen (and sometimes audio) output of the target PC and sends that data back to the terminal emulator over an IP port (sometimes the same port as the commands, sometimes using different ports). The terminal emulator then paints the HQ PC’s screen with the updated image from the remote PC.

In order to configure the LAN-Cell 3 for remote desktop software, you will need the following information:

- Public WAN IP address of the LAN-Cell (or a DDNS hostname)
- Private static LAN IP address of the target PC
- The IP port number(s) and type (TCP/UDP) that your remote desktop software package uses for communications

In the examples below, it is assumed that you have already installed and configured both the terminal server and terminal emulator pieces of software on the respective PCs. Please consult your software application documentation for further information. The examples also assume that the LAN-Cell configuration is at “factory defaults” before starting the remote desktop configuration.

Configuring the LAN-Cell for remote desktop access is straight-forward and involves 2 basic steps:

1. <u>Static LAN IP</u>

You must assign the target PC a fixed IP address so that the LAN-Cell will know where to send remote desktop traffic on its private LAN subnet. You can either manually assign a static IP address to your PC using its operating system tools, or let the LAN-Cell’s DHCP server assign the same address to the PC every time (see Appendix A).

2. <u>Port-Forwarding</u>

By default, all WAN traffic is terminated in the LAN-Cell and must be forwarded to specific addresses on the LAN. This is because the LAN-Cell performs Network Address Translation, converting the single public WAN IP address into the private subnet addresses of your LAN. You will define specifically where WAN traffic received on a given port will be sent on the LAN subnet. The LAN-Cell 3 will automatically create the necessary firewall rules to permit traffic to flow to the LAN based on your port forwarding rules.

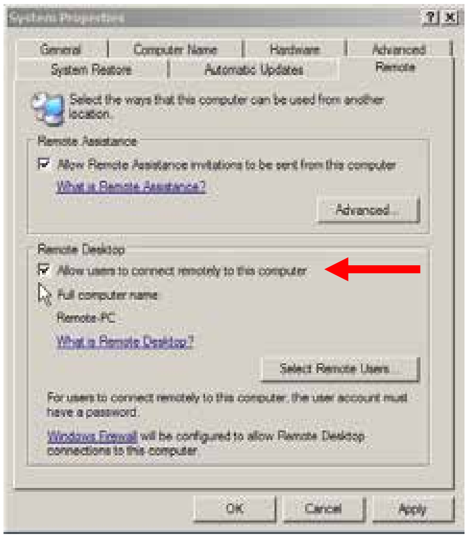
If the remote PC is on a DMZ subnet or defined as a Virtual Host, you can skip the port-forwarding configuration step, as all traffic is permitted to DMZ and Virtual Host devices.

Microsoft Windows Remote Desktop Example

The Remote Desktop software built into Windows XP, Vista, Windows 7, etc. uses TCP port 3389 (RDP) for both command and response data traffic. This is the only port which must be opened in the firewall and forwarded to the PC.

Step 1:

Ensure that your remote PC has Remote Desktop Connections enabled (Figure 2). This is configured in Control Panel->System->Remote



Select the ways that this computer can be used from another location.

Remote Assistance

☑ Allow Remote Assistance invitations to be sent from this computer

Remote Desktop

☑ Allow users to connect remotely to this computer

Full computer name:
Remote-PC

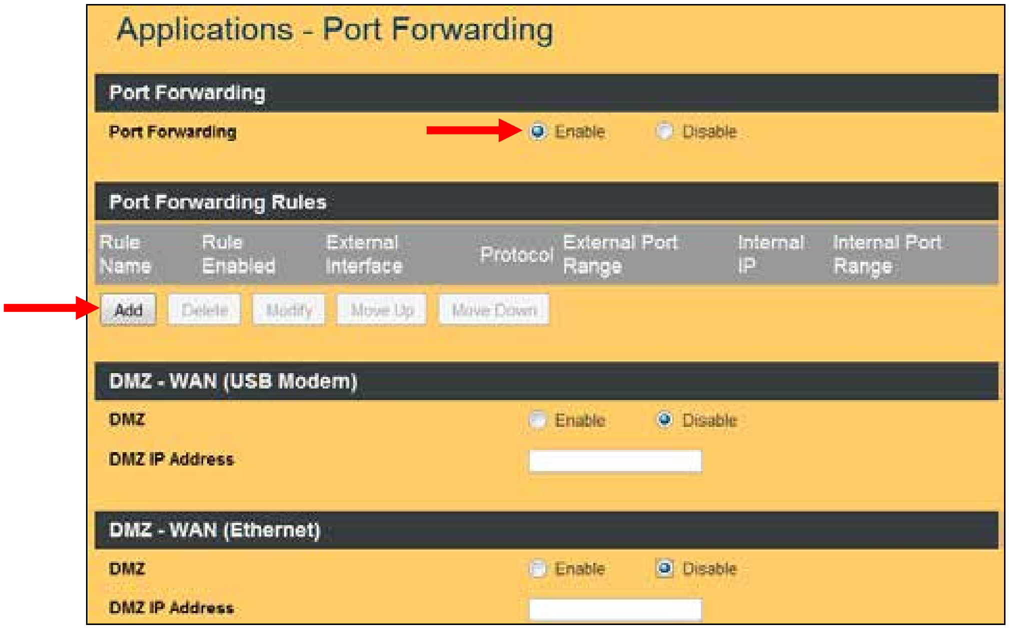
For users to connect remotely to this computer, the user account must have a password.

Windows Firewall will be configured to allow Remote Desktop connections to this computer.

Figure 2: Enabling Remote Desktop Connections in Windows XP

Step 2:

In the LAN-Cell 3, go to APPLICATIONS->PORT FORWARDING as shown in Figure 3.



Applications - Port Forwarding

Port Forwarding

Port Forwarding ● Enable ○ Disable

Port Forwarding Rules

Rule Name	Rule Enabled	External Interface	Protocol	External Port Range	Internal IP	Internal Port Range

DMZ - WAN (USB Modem)

DMZ ○ Enable ● Disable

DMZ IP Address

DMZ - WAN (Ethernet)

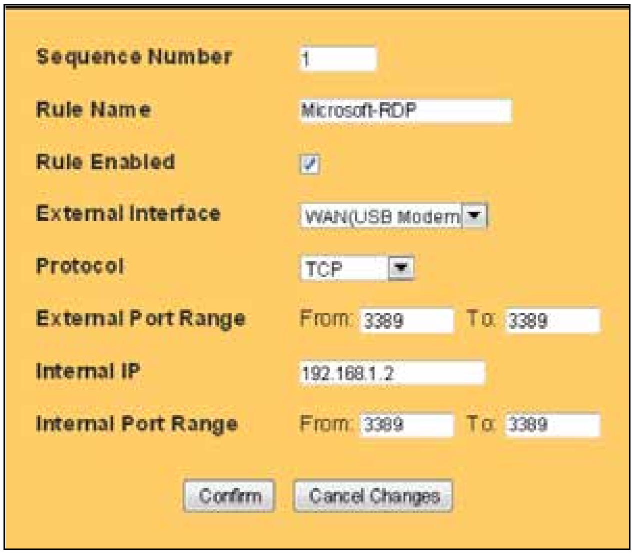
DMZ ○ Enable ● Disable

DMZ IP Address

Figure 3: Port Forwarding Summary Screen

Step 3:

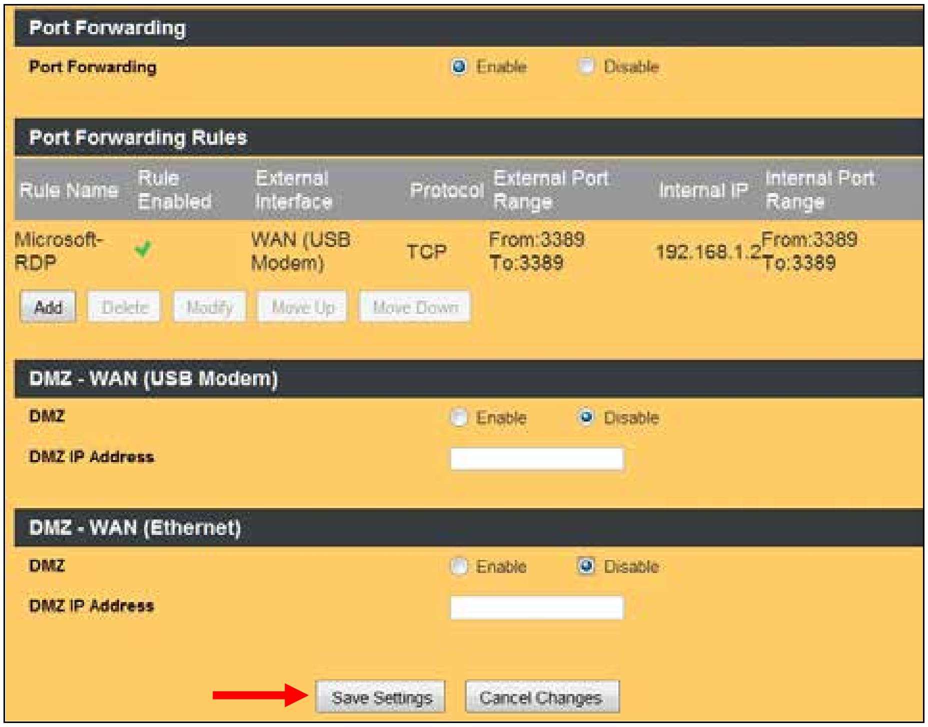
Click the ADD button to display the Port Forwarding Rule popup screen shown in Figure 4.



Sequence Number	1
Rule Name	Microsoft-RDP
Rule Enabled	☑
External Interface	WAN(USB Modem ▾
Protocol	TCP ▾
External Port Range	From: 3389 To: 3389
Internal IP	192.168.1.2
Internal Port Range	From: 3389 To: 3389

Figure 4: Port Forwarding Rule Screen

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 Microsoft Remote Desktop, you need to forward External Port TCP/3389 to the remote PC ("server") 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 Port 3389 as the Internal Port as well. Click Confirm to return to the summary screen (Figure 5). Click the Save Settings button to save the new rule.



Port Forwarding

Port Forwarding ● Enable ○ Disable

Port Forwarding Rules

Rule Name	Rule Enabled	External Interface	Protocol	External Port Range	Internal IP	Internal Port Range
Microsoft-RDP	✓	WAN (USB Modem)	TCP	From:3389 To:3389	192.168.1.2	From:3389 To:3389

DMZ - WAN (USB Modem)

DMZ ○ Enable ● Disable

DMZ IP Address

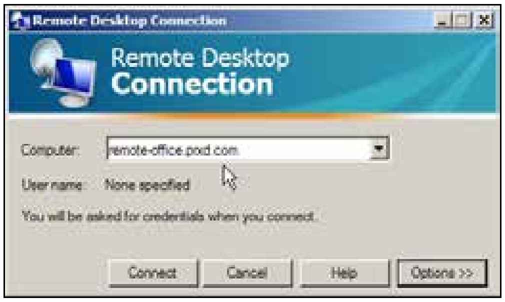
DMZ - WAN (Ethernet)

DMZ ○ Enable ● Disable

DMZ IP Address

Figure 5: Port Forwarding Rule Defined

Configuration of the LAN-Cell is now complete. Use the Microsoft Remote Desktop software on your HQ PC to initiate a connection to the remote PC using either its WAN IP address or FQDN (if defined). See Figure 6.



Computer: remote-office.pxd.com

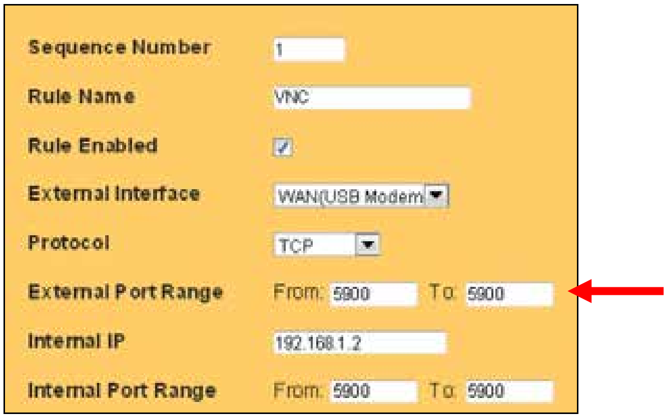
User name: None specified

You will be asked for credentials when you connect.

Figure 6: Initiating a Remote Desktop Connection

VNC Example

Configuring VNC / RealVNC / TightVNC is the same as configuring Microsoft Windows Remote Desktop, except that VNC uses TCP port 5900 instead of 3389. Follow the Microsoft RDP example but substitute the VNC port number in the Port Forwarding Rule screen (Figure 7).



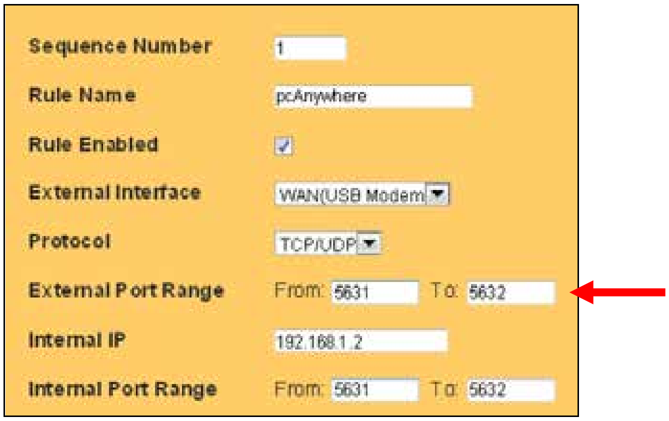
Sequence Number	1
Rule Name	VNC
Rule Enabled	☑
External Interface	WAN(USB Modem
Protocol	TCP
External Port Range	From: 5900 To: 5900
Internal IP	192.168.1.2
Internal Port Range	From: 5900 To: 5900

Figure 7: VNC Port Forwarding

pcAnywhere Example

pcAnywhere is similar to the other remote desktop applications, except that it uses 2 ports: a TCP port for data and a UDP port for status messaging. Recent versions of pcAnywhere use TCP/5631 and UDP/5632. Older versions use other ports (see Figure 9 below).

For the Port Forwarding Rule, include both incoming ports 5631 and 5632 as shown in Figure 8 (both TCP and UDP packets are forwarded).



Sequence Number	1
Rule Name	pcAnywhere
Rule Enabled	☑
External Interface	WAN(USB Modem ▾
Protocol	TCP/UDP ▾
External Port Range	From: 5631 To: 5632
Internal IP	192.168.1.2
Internal Port Range	From: 5631 To: 5632

Figure 8: pcAnywhere NAT Port Forwarding Rule

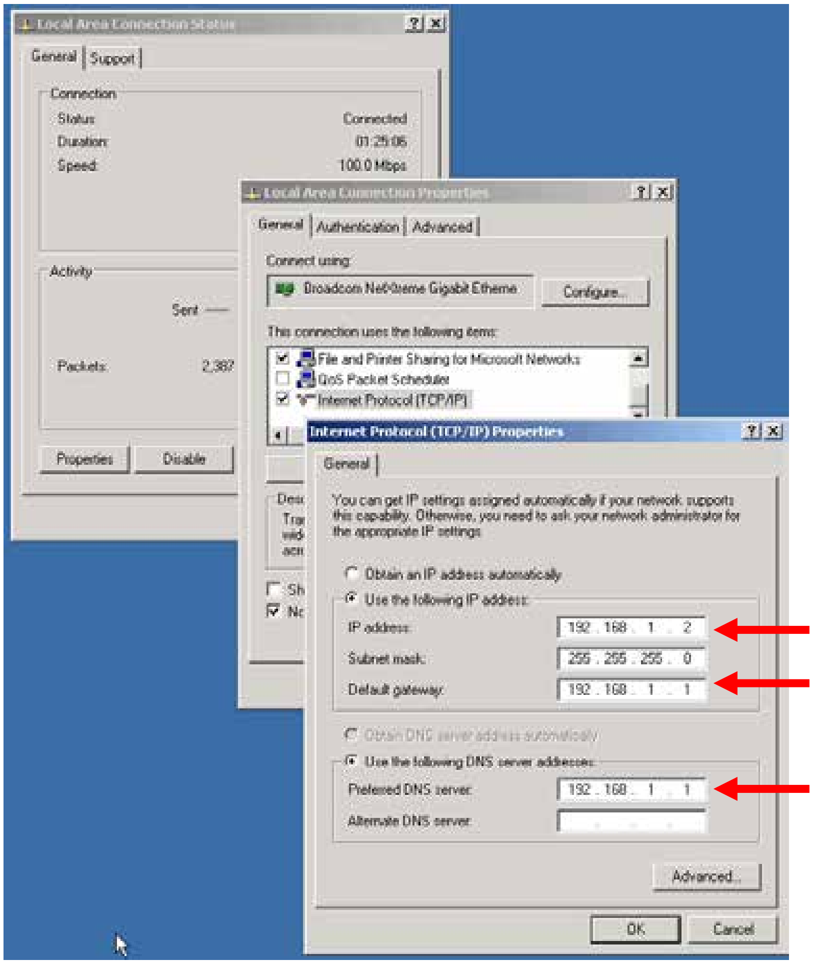
pcAnywhere version	TCP (data) port number	UDP (status) port number
2.0	65301	22
7.0	65301	22
7.50, 7.51	65301	22
CE	65301	22
7.52	5631	5632
8.x, 9.0	5631	5632
9.2	5631	5632
10.0, 10.5, 11.0, 11.5, 12.0	5631	5632

Figure 9: pcAnywhere Port Usage

Appendix A: Static IP Addressing For LAN Devices

Your remote PC must have a static (fixed) IP address so that the Port Forwarding rules can send data to the correct device. You can either configure your PC with a static IP address or let the LAN-Cell's DHCP server assign the same address to the PC every time it connects.

In Windows XP, you can assign a static IP address using Control Panel -> Network Connections -> Local Area Connection and setting the properties of the TCP/IP protocol to be a fixed IP address. Do not select a static IP address that falls within the LAN-Cell's DHCP server range (.33 to .161 by default). Set the Default Gateway and Primary DNS values to the LAN IP address of the LAN-Cell (Figure A-1).



Status: Connected
Duration: 01:25:06
Speed: 100.0 Mbps
Packets: 2,387

Connect using: Broadcom NetXtreme Gigabit Etherne

This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks
☐ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

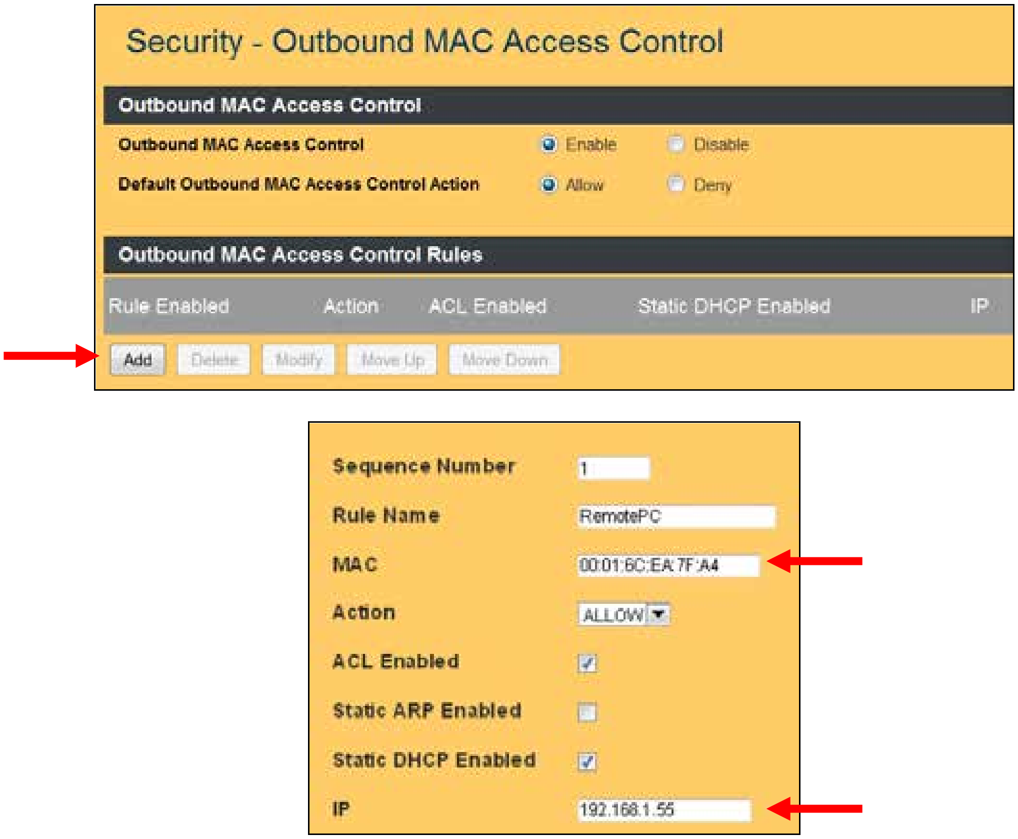
IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server: . . .

Figure A-1: Static IP Addressing in Windows XP

Alternatively, you can use the "static DHCP" feature (also known as DHCP reservation) in the LAN-Cell's DHCP server to assign the same IP addressing parameters to a given MAC address every time that MAC address must renew its DHCP lease. Go SECURITY->OUTBOUND MAC ACL (Figure A-2).



Security - Outbound MAC Access Control

Outbound MAC Access Control

Outbound MAC Access Control	● Enable	○ Disable
Default Outbound MAC Access Control Action	● Allow	○ Deny

Outbound MAC Access Control Rules

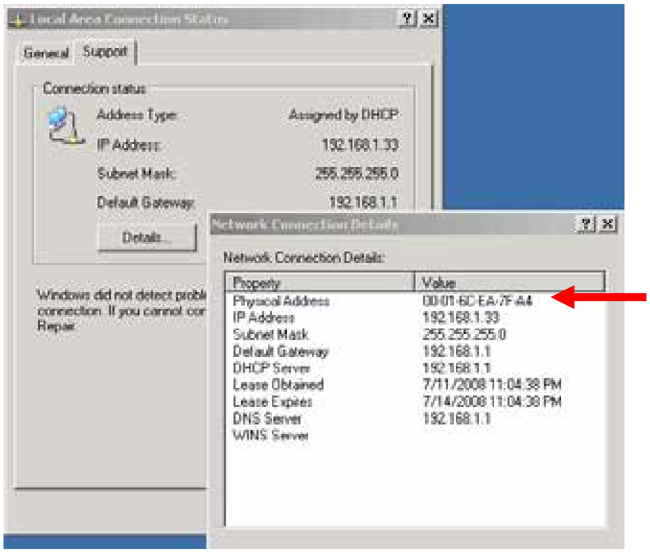
Rule Enabled	Action	ACL Enabled	Static DHCP Enabled	IP

Sequence Number	1
Rule Name	RemotePC
MAC	00:01:6C:EA:7F:A4
Action	ALLOW
ACL Enabled	☑
Static ARP Enabled	☐
Static DHCP Enabled	☑
IP	192.168.1.55

Figure A-2: Static DHCP Addressing in the LAN-Cell 3

Enter the remote PC's Ethernet MAC address in the format 11:22:33:44:55:66. Enter the desired "static" IP address for this PC. The selected IP address to be assigned must be within the defined DHCP pool range.

You can obtain the Ethernet card's MAC address in Windows XP by examining the properties of your LAN connection (Figure A-3). The MAC address is also called the Physical Address.



Local Area Connection Status

Connection status

Address Type:	Assigned by DHCP
IP Address:	192.168.1.33
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1

Windows did not detect probl
connection. If you cannot cor
Repair.

Network Connection Details

Network Connection Details:

Property	Value
Physical Address	00-01-6C-EA-7F-A4
IP Address	192.168.1.33
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	192.168.1.1
Lease Obtained	7/11/2008 11:04:38 PM
Lease Expires	7/14/2008 11:04:38 PM
DNS Server	192.168.1.1
WINS Server	

Figure A-3: Obtaining the MAC Address in Windows XP

Appendix B: Troubleshooting

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

1. *Not being aware of all of the ports used by your remote desktop application*
   Please consult your documentation or contact the software manufacturer.

2. *Carrier blocking the necessary ports*
   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, “I2GOLD” APN or a custom APN for your company (the APNs “broadband” and “isp.cingular” block inbound connections and cannot be used to host remote servers). Sprint blocks some ports including port 80 but common remote desktop ports are open. On Verizon Wireless’ 4G/LTE network, all ports are blocked when using the default “vzwinternet” APN – a public, static IP address must be purchased.

   If you are unable to have the necessary ports opened and cannot move your application ports or use Port Translation, please refer to the Proxicast Support web site for more information on configuring the LAN-Cell for VPN access.

3. *Incorrect port forwarding*
   Double check the port range defined as well as the internal destination 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.

4. *Incorrect IP addressing on the remote PC*
   Ensure that the remote PC has the LAN-Cell’s LAN IP address as its default gateway and that the subnetting is correct.

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 the remote desktop software to communicate.

Appendix C: Frequently Asked Questions

Q: Can I access more than 1 remote PC attached to the LAN-Cell?

A: Yes. Configure the first PC as described in this TechNote. For other PC's either change the port(s) used by the remote desktop software or use Port Translation to map different "public" port(s) to the necessary private port(s). To access the secondary PC, you must append a colon and the port number to your remote desktop connection request, e.g. 166.139.37.167:3390

Q: What are my options if the cellular carrier is blocking the ports I need?

A: Check to see if they allow inbound traffic on any port. If so, change the remote desktop software to use this port, or use Port Translation to map the public port to the necessary private port. If no ports are available, then you must implement a VPN connection to the LAN-Cell. See the Proxicast Support web site for examples of configuring site-to-site and client-to-site VPNs.

Q: How is the configuration different if I'm using both the wired WAN and Cellular WAN interfaces (e.g. fail-over/backup)?

A: Follow the examples in this TechNote for the setting up access via the Cellular interface. Create the same set of Port Forwarding Rules for the Ethernet WAN interface.

Q: Do I need to configure Port-Forwarding if I'm using a VPN?

A: No. A properly configured VPN tunnel will make the LAN-Cell's LAN attached devices appear as if they are part of the HQ network. You can access the remote desktop PC just as if it were on the same network.

Q: What if my remote PC is connected to the LAN-Cell via Wi-Fi?

A: The configuration is the same as shown in these examples if the WLAN (Wi-Fi) access point is bridged to the LAN-Cell's LAN subnet.

Q: What if my remote PC is defined as being on the LAN-Cell's DMZ subnet?

A: The Port-Forwarding Rules are unnecessary in this case since the DMZ permits all inbound traffic by design.

Q: What if my remote desktop software uses ports TCP/8080, UDP/161 or UDP/500?

A: By default, these ports are used by the LAN-Cell 3's management features. You can either change your remote desktop software to use a different port, or change the LAN-Cell's management utilities to use a different port. See ADMIN->MANAGEMENT to change or disable the ports that the LAN-Cell uses. Remember to append the new port numbers to all future LAN-Cell device management requests.

# # #