Best Practices for Remote Sites

Tech Note LCTN0018

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 Tech Note applies to LAN-Cell models:

LAN-Cell 2:
LC2-411

Minimum LAN-Cell Firmware Revision: N/A

Document Revision History:

Date	Comments
Nov. 30, 2009	First release

Introduction

A common use for the Proxicast LAN-Cell 2 is to provide remote access to equipment located at sites which are typically unmanned (e.g. weather stations, oil & gas wells, security monitoring platforms, etc.). In these situations, maximizing the reliability of Internet connectivity for applications and remote management is critical due to the high cost of deploying technicians to these remote sites.

This Tech Note presents a series of recommended steps you can take when planning a remote site deployment and configuration examples that can help the LAN-Cell maintain reliable Internet connectivity for your application.

Summary

- Determine the Best Available Cellular Carrier
- Maximize Cellular Signal Strength
- Provide Clean, Reliable Power
- Use Card-Lock & Card-Guard
- Use NEMA Enclosures for Outdoor or Dusty Locations
- Change the Default Password
- Keep the LAN-Cell's Firewall ON
- Enable Wi-Fi Security
- Disable Unused LAN Ports
- Disable Unused System Features
- Use Static IP if Available
- Set Up Dynamic DNS (DDNS)
- Use the WAN Connectivity (Ping) Check Feature
- Enable the Check IPSec Tunnel Connectivity (Dead Peer Detection) Feature
- Use the LAN-Cell's System Restart Timer
- Keep the Time at GMT
- Enable Remote Management Ports
- Use Cell-Sentry
- E-Mail Logs to a Repository Address
- Setup a SYSLOG Server
- Use Proxicast's ProxiVIEW Central Management Dashboard

Site Planning

Successful remote site deployments begins with a careful assessment of the site's requirements.

- **Determine the Best Available Cellular Carrier**

  In many cases, more than one cellular carrier may provide coverage at your remote site. Consult with the carriers' coverage maps or your account representatives to determine which carrier offers the best service at your remote location. You should avoid "roaming" deployments where the remote site is serviced by a cellular partner rather than your primary cellular provider. If possible, determine the distance and direction to your carrier's nearest cellular tower.

- **Maximize Cellular Signal Strength**

  When planning remote site installations, you should evaluate the true signal strength available for the LAN-Cell, regardless of coverage commitments from your carrier. Signal strength can be affected by many difficult to predict and highly localized factors such as interference from other devices, multi-path distortion, antenna lead length, etc. It can even change throughout the day as carriers adjust for varying cell loads and power output. Even slight changes in antenna positioning can dramatically affect signal strength.

  It is best to use the LAN-Cell with the target 3G modem card and any external antenna systems when measuring and optimizing remote site signal strength. Every 3G modem card has a different RF sensitivity, but in general you should strive for RSSI values of -90 dBm or greater to ensure a stable 3G connection.

  Please refer to Proxicast Tech Note *LCTN0001 Cellular Antenna Issues* for more information on strategies for selecting and positioning antennas, amplifiers, and other signal enhancing equipment.

- **Provide Clean, Reliable Power**

  Reliable power is a prerequisite for the LAN-Cell 2 and all of your other remote site equipment. For sites powered by unregulated sources, consider installing Uninterruptible Power Supplies (UPS) and surge suppressors for AC equipment and/or DC power conditioning equipment.

  All externally mounted antennas should be equipped with properly grounded inline lightning suppressors to protect the equipment and site facilities.

Physical Security Considerations

The need for physical protection of your remote site assets is a given. The LAN-Cell 2 offers several ways of enhancing the security of your cellular communications link.

- **Use Card-Lock & Card-Guard**

  The Card-Lock system uses a nylon cable tie to secure the 3G card modem from accidental removal in mobile applications. It is also a deterrent for the casual removal of the modem by unauthorized users.

  By also using the Card-Guard metal cover over the 3G modem, the removable modem card is hidden from view and tools are required to access the card. Some customers have even replaced the standard screws with "tamper-proof" screws (e.g. Torx, spanner, etc.) to make accessing the modem card even more difficult

  You can also make it more difficult to remove the LAN-Cell 2 from its permanent mounting by "reversing" the mounting feet so that the foot's wall-mount surface is beneath the LAN-Cell 2 and tamper-proof screws are used to mount the LAN-Cell to the wall-mounted feet.

- **Use NEMA Enclosures for Outdoor or Dusty Locations**

  The LAN-Cell 2's enclosure does not provide adequate ingress protection in wet or dusty environments. The LAN-Cell 2 (and any other sensitive equipment) should be mounted in a NEMA (National Electrical Manufacturers Association) cabinet rated for the type of conditions likely to be experienced at your remote site. Please refer to the NEMA website (http://www.nema.org) or this document for more information: http://www.nema.org/prod/be/enclosures/upload/NEMA_Enclosure_Types.pdf

Network Security Considerations

Because the LAN-Cell 2 will be connected to the public Internet via its 3G modem and or Ethernet WAN port, it is subject to all of the threats facing any other Internet connected system. Likewise, your LAN-Cell may be accessible on the "LAN" side by users who should not be authorized to access the system.

- **Change the Default Password**

  The LAN-Cell's default administrator password is pre-filled on the login screen and is well known. You should change the LAN-Cell's password before connecting it to the Internet. We recommend "strong" passwords of at least 8 characters including numbers and letters. Passwords are case-sensitive. The LAN-Cell also has a mechanism to help protect against "brute-force" password guessing attempts. See the SYS PWDERRTM command referenced in this knowledgebase article: http://www.proxicast.com/AbsoluteFM/?f=71

- **Keep the LAN-Cell's Firewall ON**

  We find that often users disable the LAN-Cell's internal firewall while troubleshooting their connectivity issues. We strongly recommend keeping the LAN-Cell's firewall enabled at all times. If you feel there is an issue with your firewall configuration that is affecting your remote access application, please contact Proxicast Technical Support for assistance.

  Also, be certain that you do not inadvertently create any "default" firewall rules which permit all inbound traffic from the Internet to flow to your private network(s). This effectively disables the firewall and eliminates your protection.

Even if your cellular carrier offers “firewall services”, keep the LAN-Cell’s firewall enabled to protect from “behind the firewall” attacks and other threats. For more details, please review Proxicast’s presentation: *Naked on the Internet: Securing Remote Cellular Data Communications*.

- **Enable Wi-Fi Security**

  If you are using the LAN-Cell 2’s built-in 802.11 a/b/g Wi-Fi Access Point (or additional external APs) be sure to enable security settings for Wi-Fi. The LAN-Cell’s default is no Wi-Fi security, but it supports WEP, WPA, WPA2 and 802.1x security options.

  MAC-level security is also available for Wi-Fi clients to limit the client devices which can connect to the AP to a known list of MAC addresses. Likewise, you can disable SSID broadcasting so that the LAN-Cell’s AP is not discoverable by client devices which do not know the SSID in advance. You should also adjust the AP’s power output to the minimum level necessary for your Wi-Fi clients to connect.

  Some customers choose to segregate Wi-Fi traffic onto its own subnet (WLAN) to enable finer-grained firewall rules. Define the WLAN subnet under the NETWORK > WLAN menu, then bind the Wi-Fi AP to the WLAN subnet on the WIRELESS > WI-FI screen.

- **Disable Unused LAN Ports**

  If you are concerned about remote site users connecting unauthorized devices to the LAN-Cell 2, you can effectively “disable” any unused LAN Ethernet ports:

  - Using the Port Roles screen, define all unused physical LAN ports as part of a virtual subnet other than the LAN, for example the DMZ or WLAN subnets.

  - Configure the DMZ or WLAN interfaces with private IP address subnets different than your LAN subnet and disable the DHCP server on those subnets by setting it to NONE.

  - Use the Firewall's Default Rules to drop packets flowing from the unused subnet (DMZ or WLAN) to the LAN, WAN and Cellular interfaces.

  This will prevent any devices from connecting to unused LAN ports unless they happen to know the IP subnet. Even if they do, the Firewall rules will prevent packets from flowing to the Internet or your LAN-based devices.

- **Disable Unused System Features**

  It is good practice to disable any of the LAN-Cell’s features which you are not specifically using. For example if you do not need to access the LAN-Cell itself via SSH, HTTPS or SNMP protocols, disable these options under ADVANCED > REMOTE MANAGEMENT. Likewise, in the FIREWALL section, you can enable anti-probing and denial of service measures by disabling responses to unsupported services requests and disabling Ping responses on the WAN and/or Cellular interfaces if you do not need this feature.

Remote Access

To access your LAN-Cell and other remote site equipment, you will need to know how to reach the site over the Internet. Your LAN-Cell will be assigned an IP address for its Ethernet WAN port (if connected to a DSL/Cable modem or other wired Internet Service Provider) and an IP address for its 3G modem (if used). In addition, your ISP must allow "inbound" initiated traffic from the Internet to your LAN-Cell; consult with your carrier to ensure that your 3G service has been properly provisioned.

You will be assigned either a "static" IP address which never changes or a "dynamic" IP address which may change upon every connection to the Internet. Please refer to Proxicast Tech Note *LCTN0017 Accessing Remote Devices* for more information on configuring remote access.

- **Use Static IP if Available**

  Some ISPs will assign a static IP address to your connection, usually for an additional up-front and/or monthly fee. A static IP is the most reliable means of identifying your LAN-Cell on the Internet. Note that for most 3G cellular carriers, "static IP" is really a form of DHCP Reservation – configure the LAN-Cell to accept a dynamic IP address from the carrier; you will receive the same address assignment every time.

- **Set Up Dynamic DNS (DDNS)**

  If a static IP address is not available or cost effective, the LAN-Cell 2 supports several Dynamic DNS providers (DynDNS, No-IP, RegFish) who provide near real-time mapping of dynamic IP addresses to fully qualified domain names. These services allow you to access the LAN-Cell and your remote equipment by logical name (e.g. router1.proxicast.com) rather than by IP address. See Proxicast Tech Note *LCTN0016 Configuring Dynamic DNS on the LAN-Cell 2*.

  Some customers with static IP addresses also use DDNS to make referencing their devices easier and more consistent across ISPs. Also, should the ISP change the "static" IP address for some reason, the remote site will still be accessible via the DDNS name.

Maximize Connectivity

Because sending technicians to remote sites is typically costly, we recommend the following to help maximize the "up-time" of the LAN-Cell's Internet connection.

- **Use the WAN Connectivity (Ping) Check Feature**

  The LAN-Cell 2 has a feature on the NETWORK > WAN screen that periodically sends an ICMP (ping) packet to a specific IP address (or DNS name) via the LAN-Cell's WAN interfaces. This is useful for generating traffic to keep the connection "alive". If the LAN-Cell does not receive the indicated number of responses in a timely manner, it will stop and restart the corresponding WAN interface to try to clear any connection problems.

  It is best to "ping" the ISP's default gateway if their gateway responds to ICMP requests. Some 3G cellular carriers to not permit their gateways to respond. In those instances, select another highly available Internet host such and the ISP's name servers, or a device over which you have direct control (e.g. your mail server, web server, corporate router, etc.). The table below lists the status of the major US cellular carrier's gateways at the time of publication.

Carrier	Default Gateway Responds to ICMP?	Alternate Host to Ping
AT&T	Yes	
Sprint	Yes	
T-Mobile (US)	Yes	
Verizon Wireless	No	ns1.myvzw.com ns2.myvzw.com

- **Enable the Check IPSec Tunnel Connectivity (Dead Peer Detection) Feature**

  If you are using a VPN as part of your remote access solution, you can enable the Check IPSec Tunnel Connectivity on the SECURITY > VPN CONFIG > NETWORK POLICY page to have the LAN-Cell 2 periodically send ICMP packets through the VPN tunnel to a device on the remote private network. This feature is similar in function to the WAN Connectivity Check, but monitors the status of the IPSec tunnel rather than the WAN connection itself.

  Note that this is different than the “Nailed Up” parameter for the VPN tunnel. Nailed up simply means that the LAN-Cell will automatically initiate a tunnel whenever one is not defined. If the tunnel is defined, but not properly passing traffic, the Tunnel Connectivity feature will detect the failure and drop the tunnel. This feature is called “dead peer detection” on some other VPN systems. Only one side of a VPN tunnel should have the “Nailed up” parameter set to avoid “deadly embrace” situations where both sides attempt to establish tunnels simultaneously.

- **Use the LAN-Cell’s System Restart Timer**

  The LAN-Cell has a built-in timer that can be used to force the device to perform a “soft” restart on a scheduled basis. Many customers use this mechanism as a “fail-safe” for remotely located devices so that they are restarted at a known time every day. Others use the count-down timer feature to restart every X hours. See Proxicast Tech Note *LCTN00006 Using the System Restart Timer* for information on how to configure this feature.

  Some customers have also connected external device timers to force a power cycle on a regular basis.

Monitor Site Health

These strategies will help you conveniently monitor and troubleshoot the remote LAN-Cell and your equipment.

- **Keep the Time at GMT**

  By default, the LAN-Cell 2 will attempt to set its onboard real-time clock to an Internet-based time server as soon as a WAN connection is available. It defaults to the GMT (UTC) time-zone. We recommend keeping GMT as the time-zone and setting the clocks on any other remote site devices to GMT as well to help when comparing event logs during troubleshooting.

- **Enable Remote Management Ports**

  The LAN-Cell can be remotely managed via HTTP, HTTPS, Telnet and SSH protocols. These are enabled on all system interfaces by default. We recommend that you maintain at least one open remote management port for every LAN-Cell so that remote administration is possible over the Internet. If the LAN-Cell's remote management ports conflict with ones needed for your applications, please refer to Proxicast Tech Note *LCTN0015 Changing the LAN-Cell 2's Remote Management Ports*.

- **Use Cell-Sentry**

  The LAN-Cell 2 has a feature called Cell-Sentry which monitors the monthly 3G data usage for the PC-Card modem. You can use Cell-Sentry to ensure that your remote site does not exceed its monthly allocation of data traffic (e.g. 5 GB/month). Cell-Sentry can also send you routine E-Mails showing your cumulative data usage. Refer to Proxicast Tech Note *LCTN0005 Minimizing Cellular Data Costs*.

- **E-Mail Logs to a Repository Address**

  The LAN-Cell stores the 128 most recent event log entries in its dynamic memory. You can have the LAN-Cell periodically E-Mail the log data to an address to accumulate log history over an extended time-period. Some customers create a dedicated E-Mail repository account to store the logs. High priority "alerts" can be sent to a different E-Mail address so that action can be take as necessary. See the LOGS > LOG SETTING screen.

- **Setup a SYSLOG Server**

  If you have many remote sites to monitor, it may be easier to manage the large amount of LAN-Cell log data by setting up a standard SYSLOG server and configuring the LAN-Cell to forward all log entries to the SYSLOG server. See the LOGS > LOG SETTING screen.

  Depending on the features of your SYSLOG server, this may allow you to more easily sort the data, identify trends, and trigger other alerts or actions. There are many free or low-cost SYSLOG server packages available on the Internet.

- **Use Proxicast's ProxiVIEW Central Management Dashboard**

  Proxicast has developed a centralized management tool called ProxiVIEW Dashboard which allows you to easily manage hundreds of remote LAN-Cell's from a single web site. Device status is automatically polled and reported in an easy to use spreadsheet interface.

  ProxiVIEW includes a full SYSLOG server so that device log data can be kept indefinitely. It also includes graphing options to show trends such as cellular signal strength, data traffic usage, and VPN connectivity over time. Users can easily drill-down to the full HTTP, HTTPS, SSH, or Telnet interface of each LAN-Cell for detailed configuration. Contact Proxicast Sales for more information on ProxiVIEW.

# # #