Minimizing Cellular Data Costs Using the LAN-Cell 2

Technote LCTN0005

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 2:
LC2-411

Minimum LAN-Cell Firmware Revision: 4.02(AQP1) 07/25/2007.

Document Revision History:

Date	Comments
March 28, 2008	First Release.

Introduction

Many cellular network operators impose limitations on the amount of data (or number of minutes) that can be used on a particular service plan. Even so-called “unlimited” plans often have maximum allowance caps that can trigger expensive “overage charges” from the carrier or even result in having your cellular data account suspended or cancelled.

In addition, most cellular network operators offer a variety of service plans at different price levels. Users who have applications with well-defined data transmission profiles can save significant amounts of money every month by purchasing a lower priced, lower capacity service plan (sometimes referred to as “telemetry plans”).

In each case, you may wish to minimize the chance of going over your plan’s monthly allotment. This TechNote highlights several features of the LAN-Cell 2 that help minimize and monitor your cellular data usage and costs. Please consult the *LAN-Cell 2 User’s Guide* for more detailed documentation on each feature.

LAN-Cell 2’s Data Usage Management Features

1. **Cell-Sentry** – Proxicast’s "watchdog" application on the LAN-Cell 2 that can proactively alert you via E-mail when user defined usage limits are approaching or even stop data transmissions to prevent costly plan allowance overages.

2. **Dial-On-Demand** – The LAN-Cell’s ability to make instantaneous 3G connections only when outbound packets need to be routed to the Internet over the cellular WAN interface and automatically drop the connections once the connection is idle.

3. **Bandwidth Management** – The LAN-Cell 2’s bandwidth management features allow you to restrict and prioritize the flow rate of packets destined for each interface. You can use bandwidth management to ensure that applications such as remote cameras do not send data at a rate that would consume your total plan’s allotment.

4. **Firewall Rules** – Using stateful packet inspection technology, the LAN-Cell allows you to define extremely granular firewall rules that can restrict the type of traffic flowing among all of the device’s interfaces. Rules can be implemented for specific IP addresses, protocols and ports, enabling administrators to block bandwidth hogging applications such as audio streaming or video conferencing.

5. **Keep-Alive Timers** – To maintain a cellular connection, the LAN-Cell has several interrelated timers which periodically send test packets to the cellular network. These timers can be manipulated to adjust the amount of data used for the keep-alive functions. The LAN-Cell can also be programmed to restart at specific times of the day and stay connected only for a fixed duration.

6. **Device & Protocol Filters** – Similar to Firewall Rules, device and protocol filters enable the LAN-Cell to restrict or allow specific types of traffic on an interface. Filtering is a powerful tool that gives you a high degree of flexibility in defining permissible types of traffic on each interface.

7. **Security Features** – You can use the LAN-Cell’s Wi-Fi security features and MAC filtering to prevent unauthorized users from accessing your Internet connection. You can also enable the LAN-Cell’s anti-probing features and turn-off unneeded management interfaces to reduce unsolicited traffic from hackers.

Understanding Your Application

The simplest way to reduce your cellular data usage is to avoid generating unnecessary traffic. The more you know about exactly what type of traffic your application is generating, the easier it will be for you to implement the recommendations in this TechNote and to minimize your total cellular data usage.

For example, if your application involves routine data collection or polling of remote equipment (e.g. retrieving data from data loggers, sending periodic data from weather stations, etc.), review your application requirements and software configuration to determine exactly how much data is being transferred and how often. These types of applications are prime candidates for low-cost "telemetry" plans once the data transmission profile is established.

Also review the protocols being used by your application software. Some systems generate lots of traffic because they assume that they are running on a high-bandwidth, zero-cost network like a LAN. If possible, eliminate or reduce excessive status messages, heartbeats, polling or other "chatty" traffic that can quickly drive up cellular usage. If you are unable to stop your software application from generating this type of traffic, consider implementing Firewall Rules or Protocol Filters to prevent the packets from being sent to the cellular interface (see below). If possible, implement data compression techniques at the source and destination points to reduce the amount of data transmitted.

Review how your cellular connection will be used for providing connectivity. For example, if your application involves security or traffic cameras, have the camera system send periodic frames to a central server where users can access them rather than allowing end-users to directly access the camera over the cellular network.

Once you have a good understanding of your anticipated cellular data usage patterns and application requirements, you can implement the appropriate strategies outlined below to minimize the traffic on the cellular interface and reduce the potential for expensive overage charges.

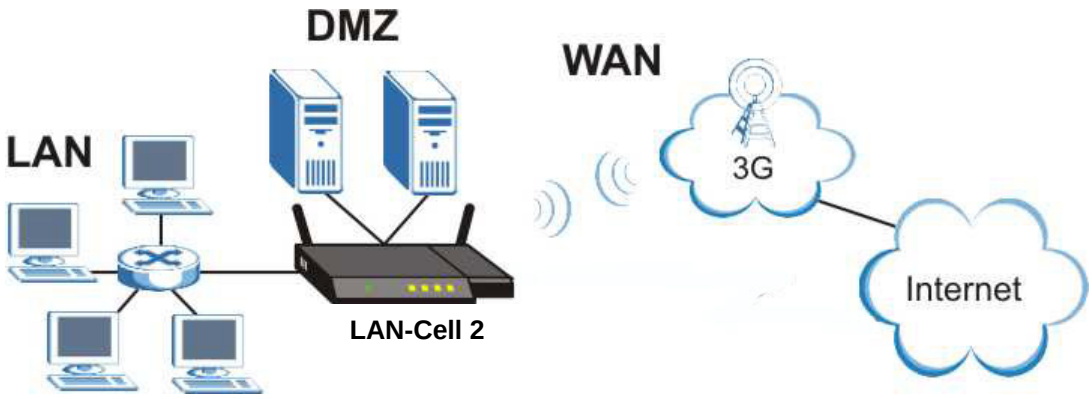

Figure 1: Typical LAN-Cell 3G Configuration

1. Cell-Sentry

The LAN-Cell 2's Cell-Sentry feature makes it easy to monitor your cumulative cellular data usage. You can get E-mail notification when certain thresholds are reached or stop the LAN-Cell from exceeding your monthly allocation of either minutes or megabytes of data.

Cell-Sentry parameters are defined on the bottom section of the WIRELESS>CELLULAR setup screen. The "budget" you define with Cell-Sentry stays with the serial number of the 3G modem (or SIM) in use, not the LAN-Cell. That way if you change 3G modem cards, you have the option of retaining your usage history should the card be reinserted in the LAN-Cell. Cell-Sentry usage counters are also preserved across system restarts and power-cycles. You can define when the counters are reset to match the Cell-Sentry budget period to your carrier's monthly billing cycle.

In the example shown in Figure 2, we have defined a total monthly data allowance of 5 GB, with a warning threshold of 80% (4 GB). When the 4 GB threshold is reached, the system will log the event in the LAN-Cell's event log and generate a system alert every 60 minutes. Once the total 5 GB budget is reached, we have configured Cell-Sentry to drop the active cellular connection and disallow any new connections until the budget is reset manually or automatically on the 7th of each month.

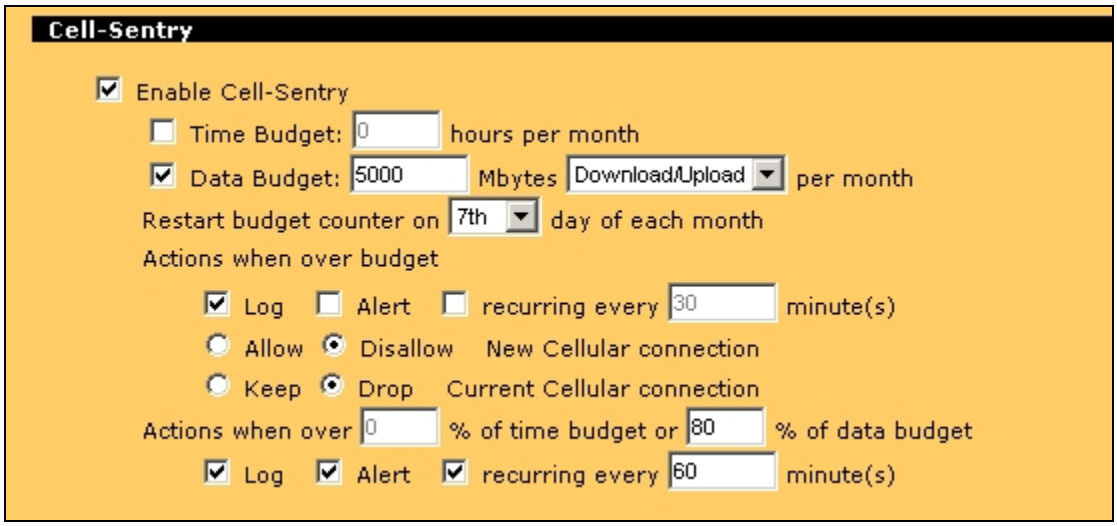

Figure 2: Cell-Sentry

To reset the Cell-Sentry budget manually, expand the Cellular Interface Status window on the HOME screen by clicking the Show Detail link and then clicking the Reset link (Figure 3).

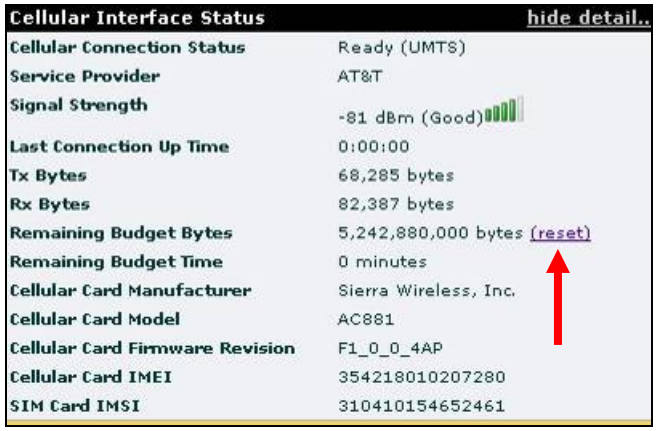

Figure 3: Cell-Sentry Status & Reset

In order to have the alerts sent via E-mail as well, the Mail Server parameters must be defined on the LOGS>SETTINGS screen (Figure 4). Be certain that the Cell-Sentry option is selected under Send Immediate Alerts on the bottom right of the Log Settings screen.

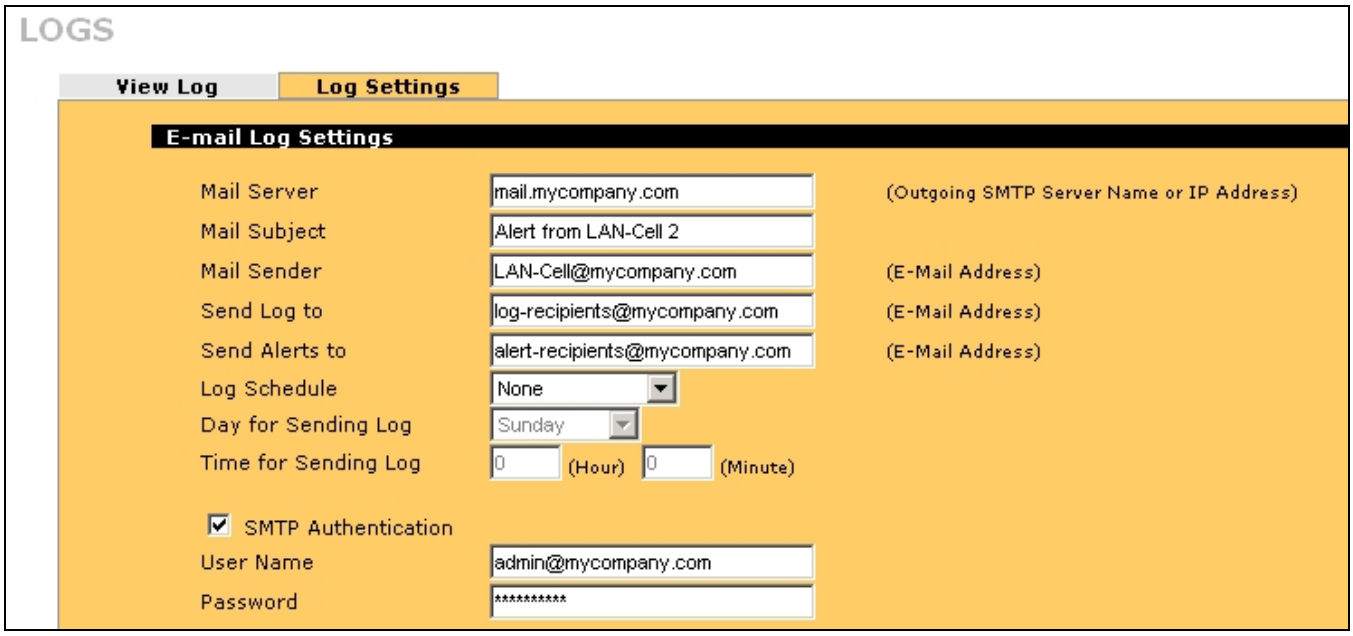

Figure 4: Log & Alert E-Mail Configuration

The content of the alert message sent is shown in Figure 5. If your cellular operator provides an E-mail to SMS service (for example phone#@vtext.com) then alerts can also be sent to your mobile phone as text messages.

```
No. Time                 Source IP             Destination IP        Note
  1|2008-03-29 05:05:57  |                     |                     |Cell-Sentry
    Warning: (IMSI: 310410154652461) Over 80% of data budget (839 Mbytes remain in 5000.00 Mbytes budget).

End of Alert
```

Figure 5: Alert E-Mail

Additionally, alerts can be sent to a central SYSLOG server or other central management console. Enter the destination SYSLOG server address or hostname on the LOGS>SETTINGS screen.

Figure 6: SYSLOG Server Settings

Even if you don't anticipate going over your monthly data allowance, Cell-Sentry can protect against "run-away" applications that mistakenly transmit when they should not or users who are consuming too much capacity.

Note: Actual usage statistics on the carrier's network may differ from the LAN-Cell's counters. Set your budget limits lower than the maximum allowed on your plan.

2. Dial-On-Demand

Not all applications for the LAN-Cell require a constant Internet connection. For example, using the LAN-Cell to provide Internet access at a temporary location for a group of users, such as engineers at a construction site, requires an Internet connection only when the users make a request or send information. At other times, the connection can be shut down to minimize unwanted inbound traffic. This is especially helpful if Internet usage is metered on connection time rather than bytes transferred.

The digital nature of 3G connections enables virtually instantaneous connections to the Internet, so users will not notice that the cellular interface is going up and down between the times that they are actively using it.

To enable Dial-On-Demand, uncheck the Always On box on the WIRELESS>CELLULAR page and set a timeout period for when the connection will be dropped once no additional outbound traffic is detected (Figure 7).

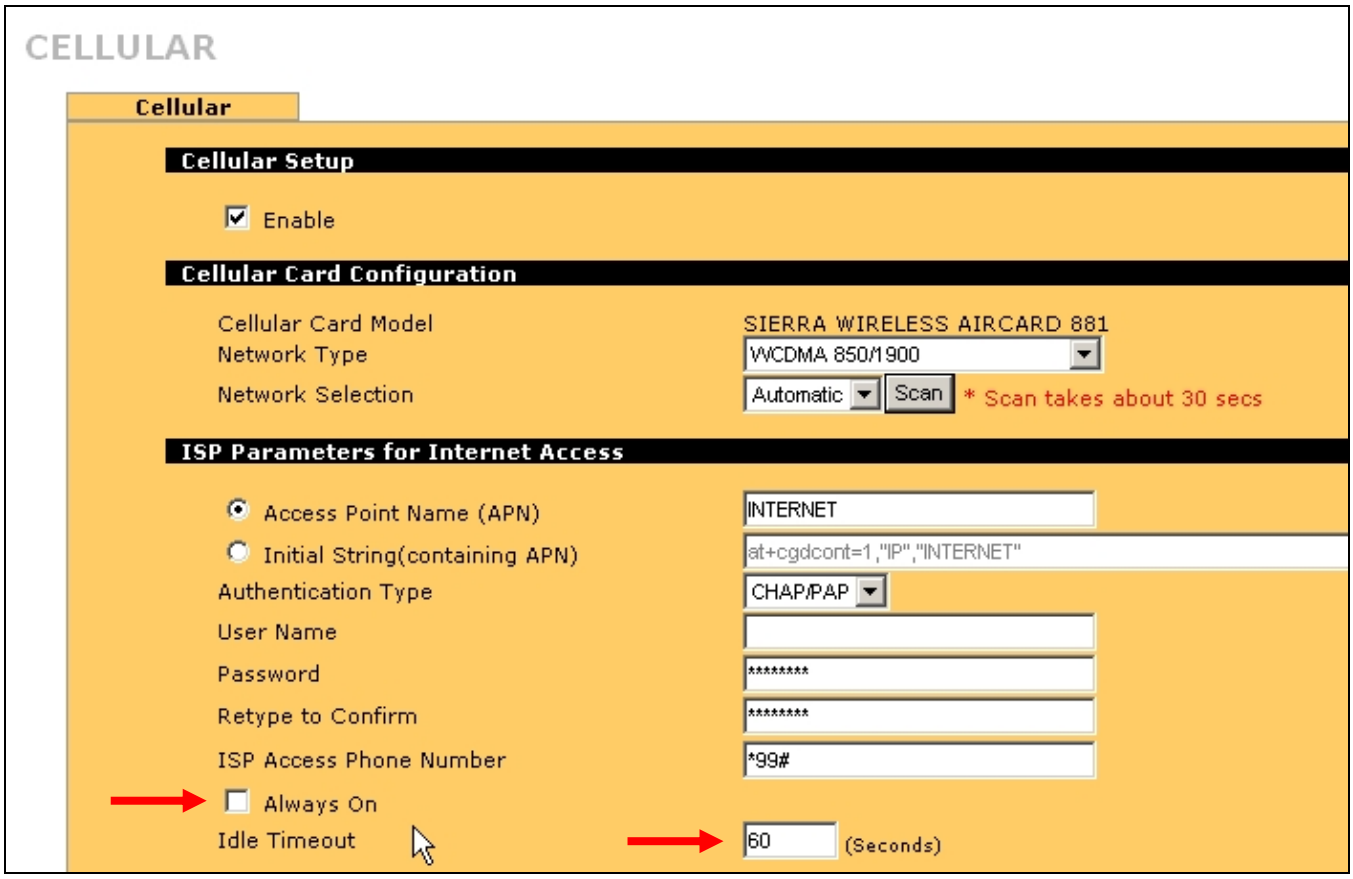

Figure 7: Dial-On-Demand Settings

The Dial-On-Demand feature can be combined with other strategies such as Firewall Rules and Filters to prevent certain types of traffic from triggering cellular connections. Dial-on-Demand can also be used with Keep-Alive timers to shut down the cellular interface after a keep-alive event has occurred (see Section 5).

3. Bandwidth Management

Bandwidth Management allows you to allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the LAN-Cell forwards certain types of traffic (especially real-time applications) with minimum delay for applications such as VoIP.

Bandwidth Management also allows you to configure the maximum allowed throughput rate for the cellular interface. This can be used to ensure that no applications from the LAN continuously saturate the cellular interface to the carrier's maximum capacity, thereby generating more traffic than is allowed by your service plan.

For example, assume that you have a monthly usage allotment of 5 GB of data. If your application were to continuously output data, the maximum rate you could sustain without exceeding 5 GB would be approximately 19 Kbps[1] (assuming no other traffic such as keep-alive packets, acknowledgements, etc). If you have a high-speed uplink connection such as HSUPA or EV-DO Rev A, you may have a maximum potential uplink speed of 500 Kbps or more. To prevent hitting the monthly cap, you can set the maximum allowable bandwidth on the cellular interface to 19 Kbps or lower.

Go to the BW MGMT option under the ADVANCED menu and enable bandwidth management on the cellular interface. Set the maximum speed to 19 Kbps (see Figure 8). Do not select Maximize Bandwidth Usage or the cellular interface will be allowed to burst up to its maximum capacity.

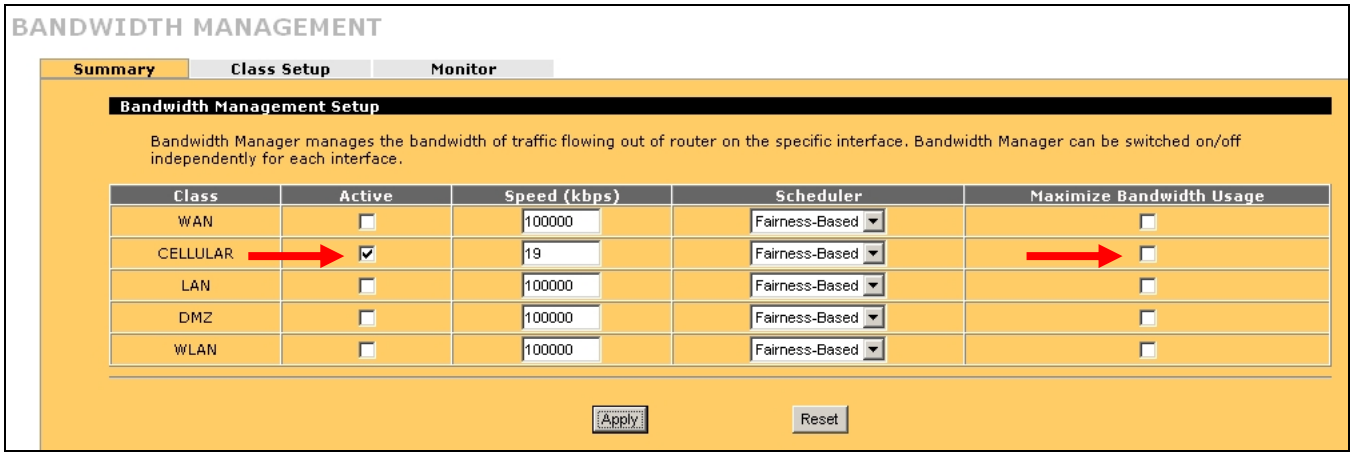

Figure 8: Bandwidth Limiting the Cellular Interface

[1] 5 GB/month = (5,000,000 KB * 10 bits/byte) / 30 days / 24 hours / 60 minutes / 60 seconds = 19.29 Kbps). Value is approximate due to variable length of TCP/UDP packets, packet header overhead, compression, etc.

4. Firewall Rules

The LAN-Cell's SPI firewall has the ability to permit or drop packets that match multiple criteria (rules) as the packets flow in each direction between each of the LAN-Cell's interfaces. This enables administrators to block certain packets from potentially high-bandwidth applications or users, or to limit the times when certain traffic is permitted to pass.

As an example, assume that you want to allow H.323 (voice & video-conferencing) traffic (TCP:1720) but only during normal weekday business hours (7 AM to 6 PM) and only from a specific LAN IP address (192.168.1.20). To accomplish this, you need to create only 1 firewall rule. In the Firewall section, select the Rule Summary Tab and the LAN to Cell packet direction. Insert a new rule as shown in Figure 9.

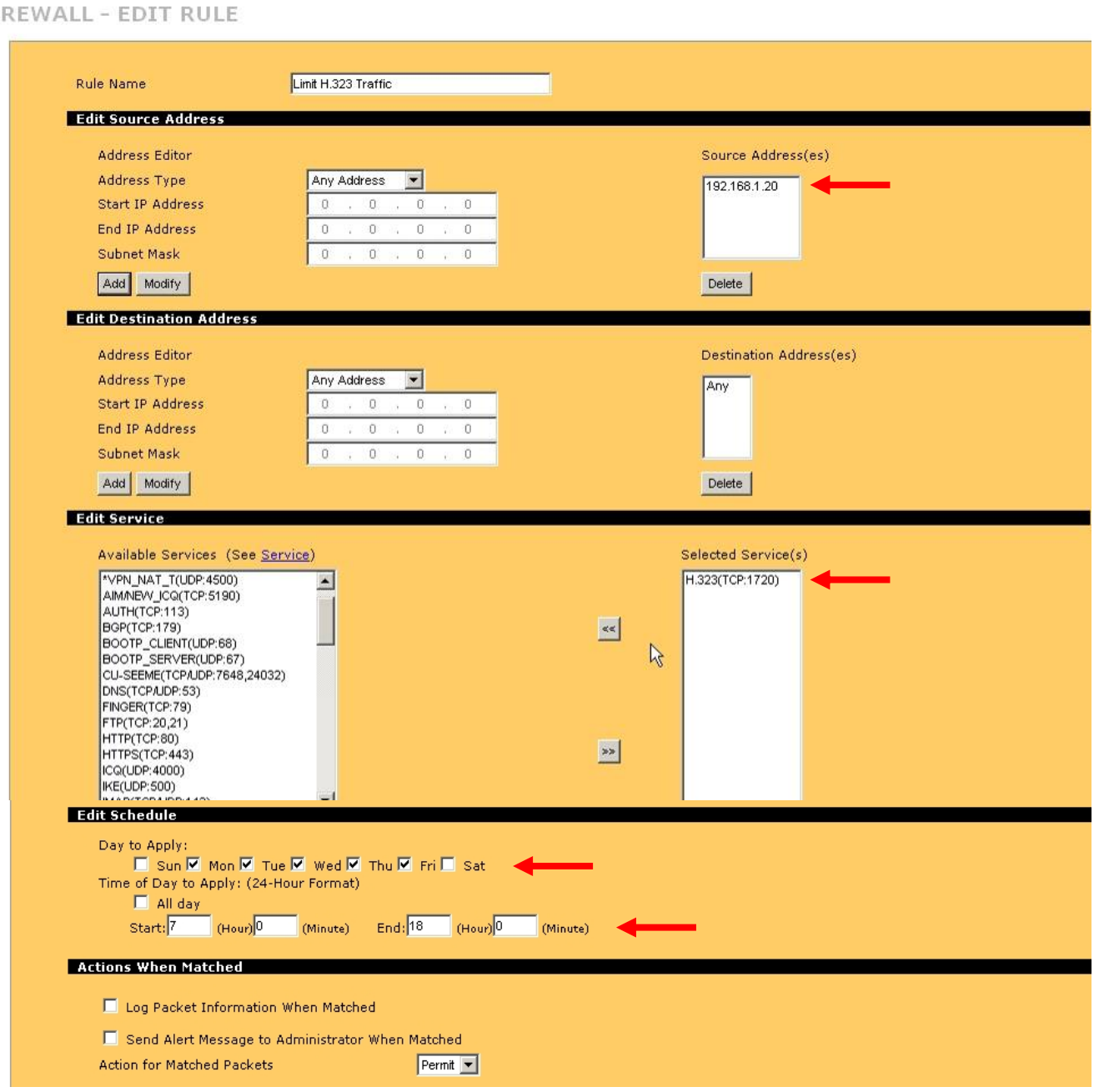

Figure 9: H.323 Firewall Rule

Once the rule is saved, the Rule Summary screen will appear as in Figure 10.

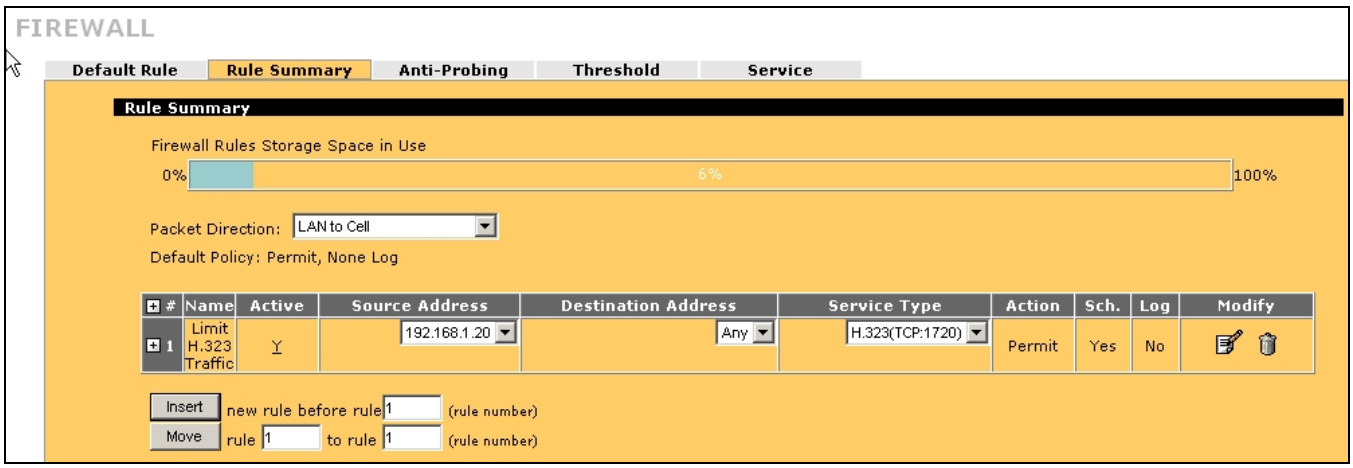

Figure 10: H.323 Firewall Rule Summary

You can add multiple rules for each packet direction to specify exactly which types of traffic are able to flow in each direction. If you change the LAN-Cell's default remote management ports or define port-forwarding rules, you will also need to create corresponding firewall rules to define the permitted traffic. You can use the Firewall's Default Rule screen to quickly define how packets that do not match any rule should be handled.

See the *LAN-Cell 2 User's Guide* for more information on defining Firewall Rules.

5. Keep-Alive Timers

The LAN-Cell 2 has several different mechanisms for monitoring cellular connections and keeping them up (alive).

LCP Echo Timers

At the Point-to-Point Protocol (PPP) layer, the LAN-Cell sends periodic Link Control Protocol (LCP) Echo Request packets to the cellular carrier's network to determine if the PPP connection is up and able to transfer data. If the carrier's side of the data connection does not respond to a certain number of LCP Echo Requests, the LAN-Cell assumes that the connection is down and will try to reestablish the link (if Always On is active).

The default LCP Echo parameters will consume approximately 6 MB/month of data capacity assuming an Always On connection. These parameters can be edited to decrease the amount of data used, albeit with a trade-off in how quickly the LAN-Cell is able to detect "dead" connections. Please see TechNote *LCTN0003 Adjusting the LAN-Cell PPP LCP Parameters* for more information on changing the default values.

WAN Connectivity Check

The LAN-Cell 2 also has a WAN Connectivity Check feature that can periodically send ICMP (ping) packets to a specific IP address or host name on the Internet (Figure 11). This "heartbeat" function can be used in situations where the ISP does not support LCP Echo or to ensure "end-to-end" connectivity to a remote host.

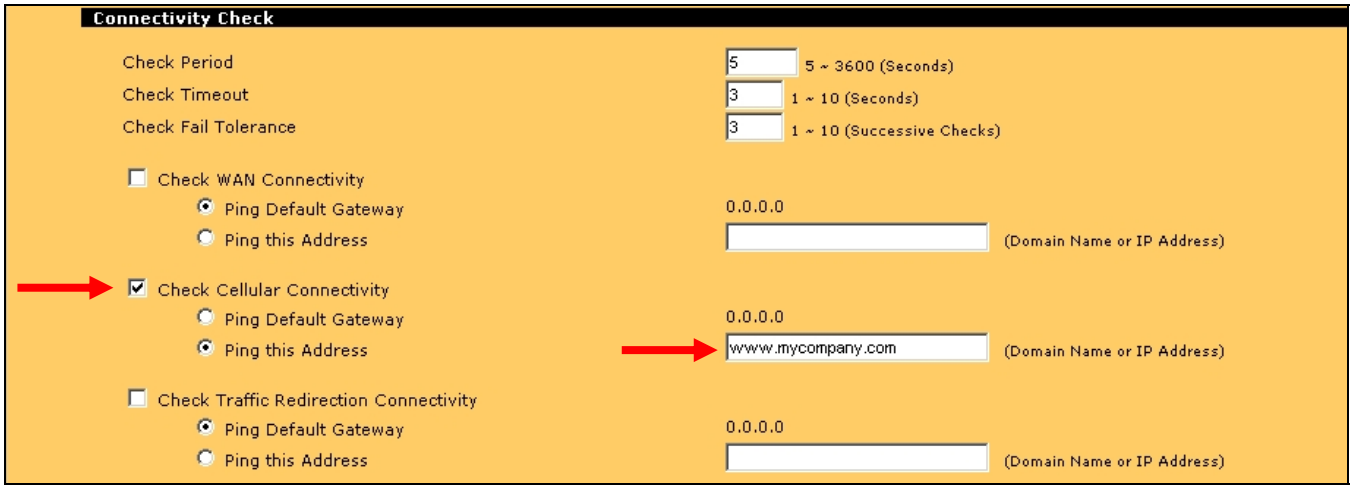

Figure 11: WAN Connectivity Check

If the WAN Connectivity Check fails, the LAN-Cell 2 will drop the cellular connection and periodically attempt to reestablish the connection. Note that most cellular ISPs do not respond to ping's on their routers, so select the IP address or fully qualified domain name of a high-availability Internet server as the destination. Also, WAN Continuity Check will not bring up a cellular connection unless the connection was previously shut down by the WAN Continuity Check process.

System Restart Timer

The LAN-Cell can also be programmed to restart at specific times or fixed intervals. While useful for resetting the device, the System Restart Timer can be combined with the Dial-On-Demand feature to bring up the cellular connection at specific times for specific lengths of time. For example, if you are retrieving data from a remote device, you could define a 15 minute (900 sec) window every 4 hours that the LAN-Cell would be connected to the Internet for you to retrieve the data. You will need to combine the System Restart and Dial-On-Demand features with a mechanism that will generate outbound traffic from the LAN-Cell to the Internet when the system restarts. One technique is to define a RADIUS server that the LAN-Cell will attempt to contact when the system starts up. Please see TechNote *LCTN0006 System Restart Timer* for information on programming the System Restart Timer.

6. Device & Protocol Filters

The LAN-Cell uses filters to decide whether to allow passage of a data packet. Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Filters can be used in conjunction with or in place of Firewall Rules.

Filters are an advanced topic and require a detailed understanding of exactly what types of traffic should be permitted on each interface. Filters are defined and applied using the LAN-Cell's System Management Terminal (SMT) interface which can be reached via Telnet, SSH or the serial Console port.

Filters are covered extensively in the *LAN-Cell 2 User's Guide* and are beyond the scope of this TechNote.

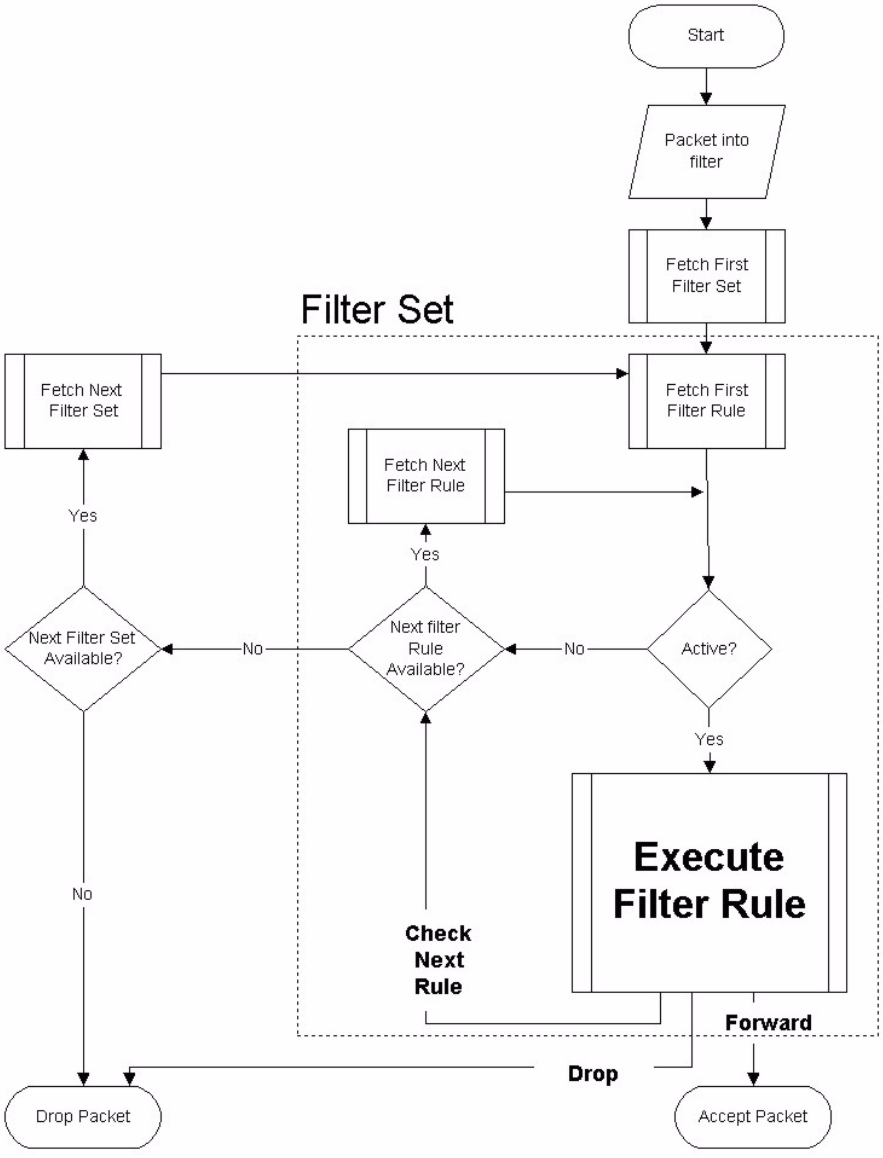

Figure 12: Filter Rule Flowchart

7. Security Features

Several of the LAN-Cell 2's built-in security functions can be employed to help reduce data usage on the cellular interface.

Unplanned cellular traffic can come from 2 sources:

1. Unsolicited in-bound traffic generated by probes from other Internet addresses (i.e. scans from hackers, misconfigured applications, etc.).
2. Unauthorized LAN-Cell users requesting Internet access.

Unsolicited traffic on the cellular interface is extremely common because your cellular network operator is acting as an ISP and providing you access to the "public" Internet. Therefore, the LAN-Cell is subject to the same types of probes and attacks that wired Internet routers face. Even cellular carriers who implement their own firewalls between their cellular network and the Internet cannot protect you from "peer" attacks launched by other cellular modem devices on their networks.

Unfortunately, this unsolicited traffic counts against your cellular data plan allowance and you can't stop it completely. However you can minimize its impact and discourage hackers from focusing on your LAN-Cell as an attack target as shown in Figures 13 - 20:

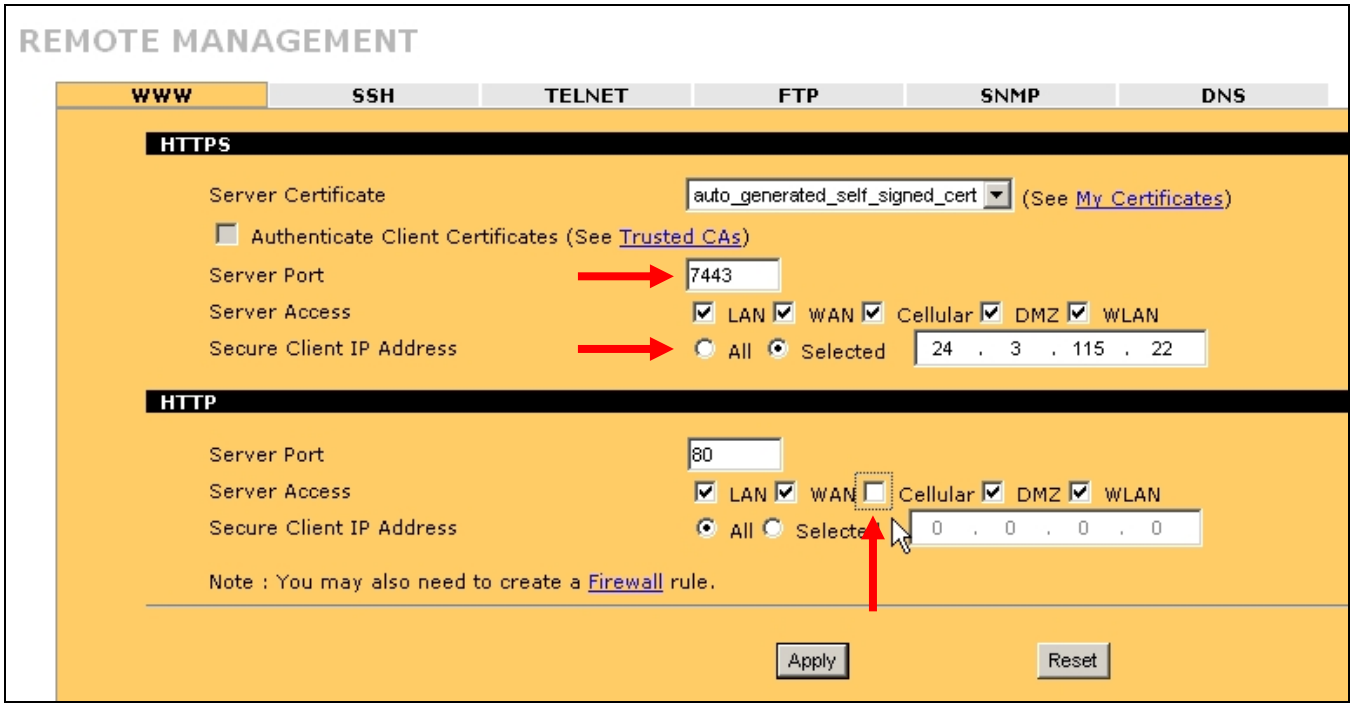

Figure 13: Restricting Remote Management Access

- Disable any unused Remote Management interfaces (Figure 13).
- Use the HTTPS and/or SSH ports for Remote Management instead of HTTP & Telnet.
- Allow access to the Remote Management interfaces only from trusted IP addresses.

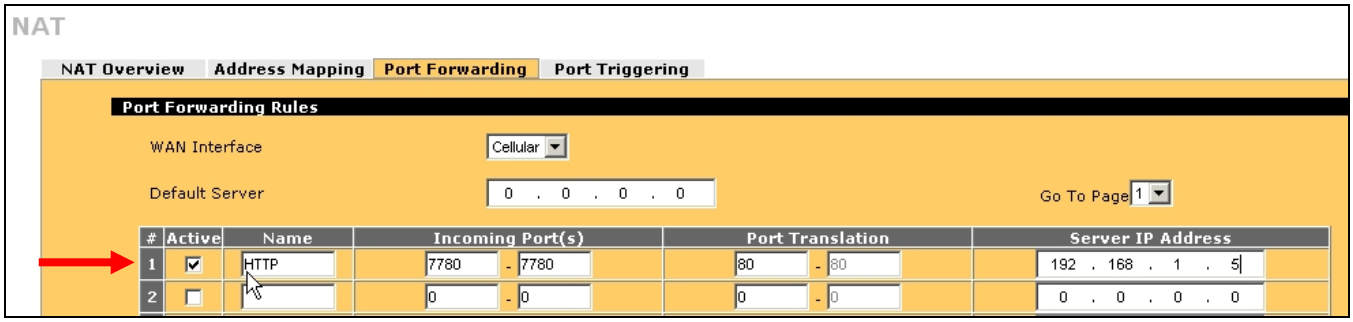

Figure 14: Port Forwarding & Translation

- Use NAT Port Forwarding only for ports that are necessary for your application.
- Use Port Translation to avoid commonly attacked ports such as 21, 23, 80, etc. (Figure 14). Remember to create Firewall Rules for incoming ports.

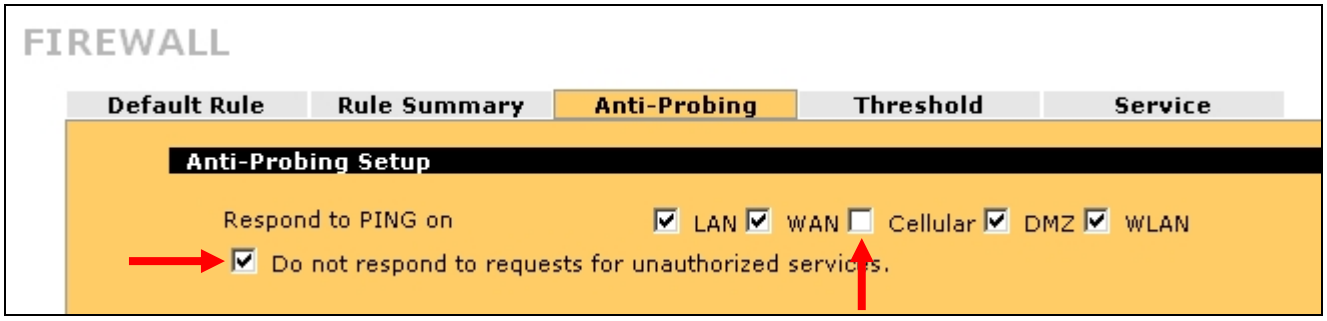

Figure 15: Anti-Probing

- Use the Anti-Probing features of the Firewall to disable Ping responses on the cellular interface and do not allow the LAN-Cell to respond to unauthorized service requests (Figure 15).
- Adjust the Firewall Threshold settings to enable Denial of Service (DoS) protection on the cellular interface and tune the DoS values as necessary.

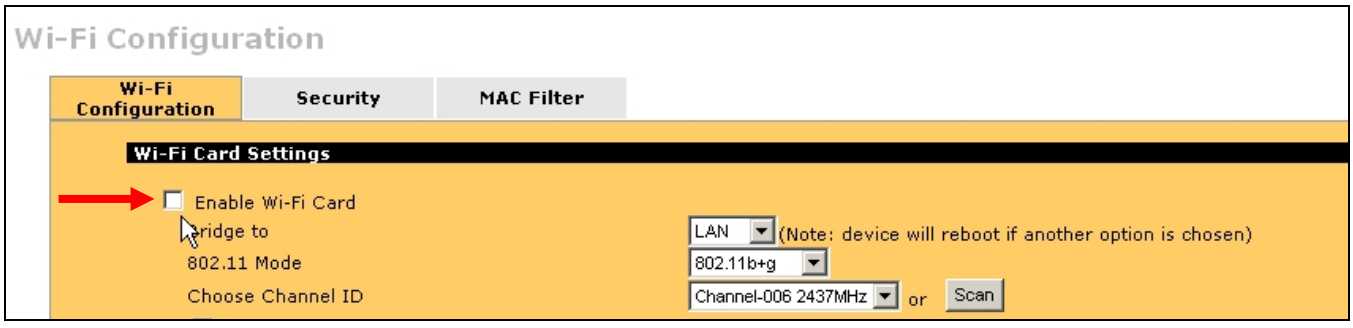

Figure 16: Disable Wi-Fi Access Point

- Turn off the Wi-Fi Access Point if it is not being used (it is off by default - Figure 16).

To prevent unauthorized users from accessing the Internet via the LAN-Cell 2:

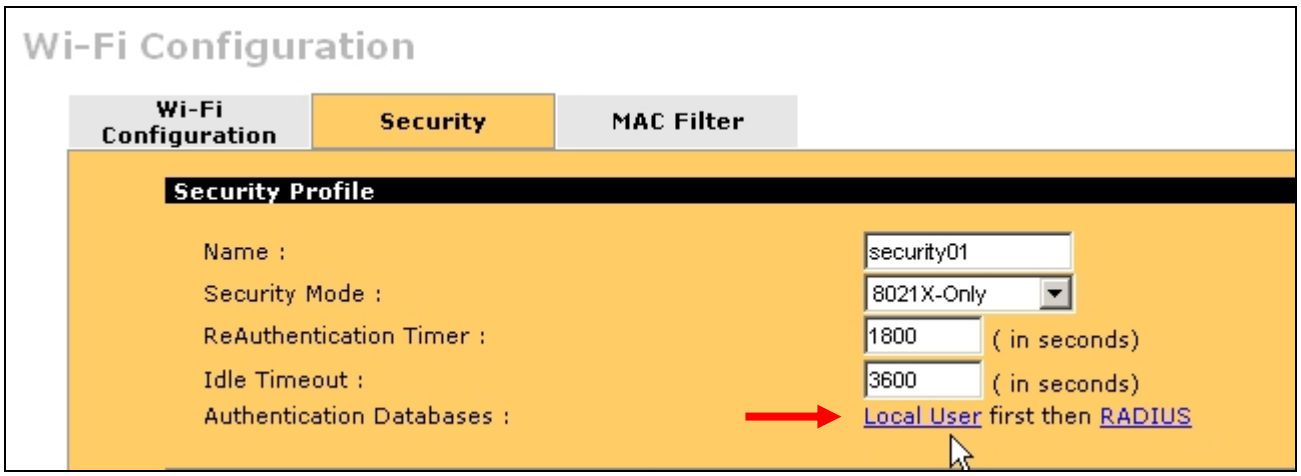

Figure 17: User Authentication for Wi-Fi

- If the Wi-Fi Access Point is enabled, define a Security Profile using one of the encrypted communication protocols that includes User Authentication (such as 8021X) and define the permitted users in the LAN-Cell's local user database or a remote RADIUS server (Figure 17).

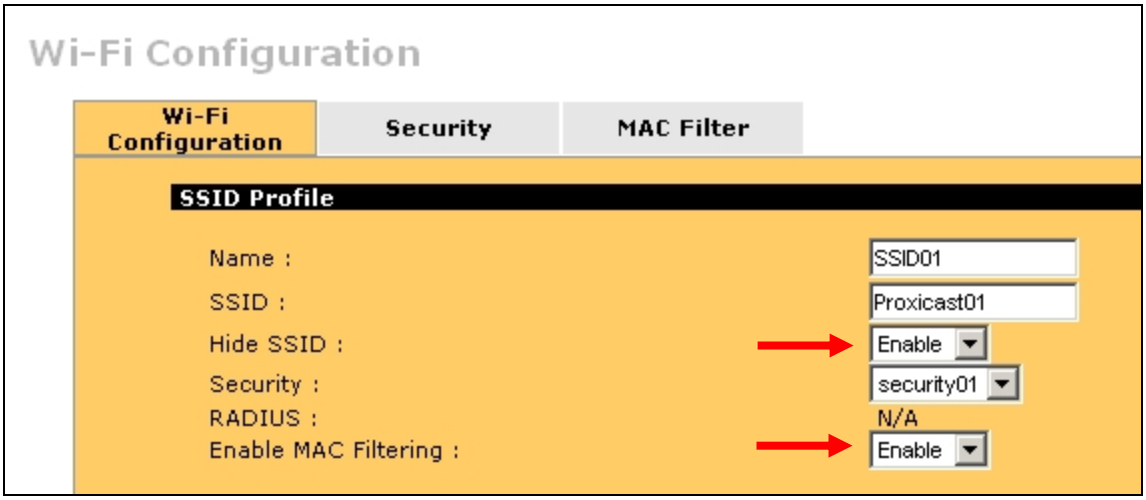

Figure 18: Disable SSID Broadcast & Enable MAC Filtering

- Disable the LAN-Cell's SSID broadcasting by enabling Hide SSID and enable MAC filtering in the SSID Profile (Figure 18).
- Define the MAC addresses of permitted Wi-Fi devices using the MAC Filter table.

To prevent unauthorized wired Ethernet users from “plugging in”, disable the DHCP server on the LAN and redefine all unused Ethernet ports as either DMZ or WLAN (Figure 19) and change the default Firewall rule for DMZ/WLAN to CELLULAR to be Drop (Figure 20).

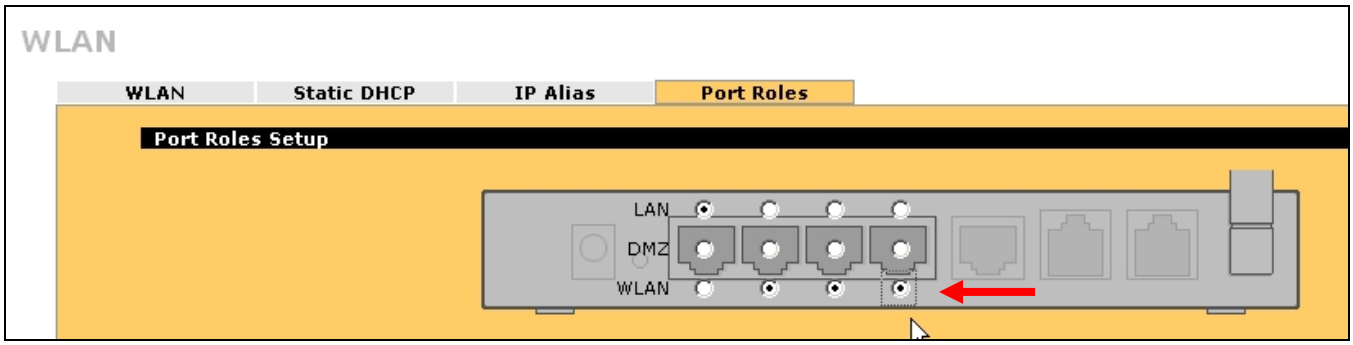

Figure 19: Port Roles

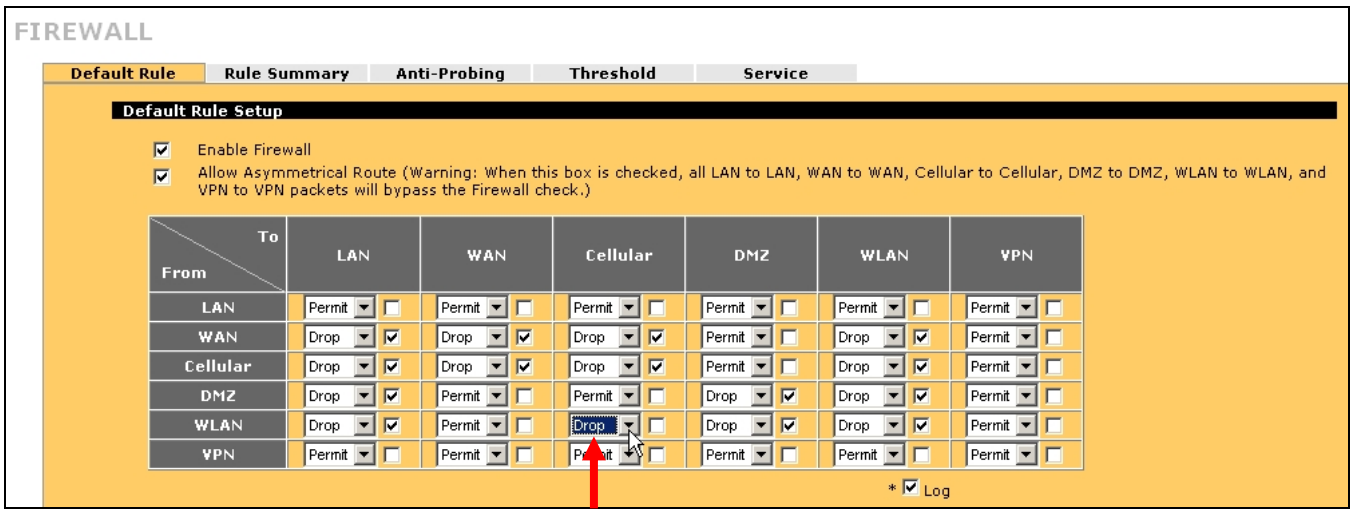

Figure 20: Drop Packets from Unused Ports to Cellular

# # #