Proxicast

LAN-Cell 2

Firmware Release Notes

Release 4.02(AQP.1)

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

July 25, 2007

Proxicast LAN-Cell 2
Firmware 4.02(AQP.1)D0
Release Notes

Date: Jul., 25, 2007

Versions:

ProxiOS Version: V4.02(AQP.1) | 07/25/2007
Bootbase Version: V1.08 | 11/01/2006

Supported Platforms:

Proxicast LAN-Cell 2

Supported PC-Card Modems:

- Sierra Wireless Aircard 595 (EV-DO RevA, EV-DO Rev0, 1xRTT)
- Sierra Wireless Aircard 875 (HSUPA, HSDPA, UMTS, EDGE, GPRS)
- Sierra Wireless Aircard 860 (HSDPA, UMTS, EDGE, GPRS)
- Sierra Wireless Aircard 850 (HSDPA, UMTS, EDGE, GPRS)
- Huawei E612 (WCDMA, GPRS)
- Huawei E620 (HSDPA, WCDMA, EDGE, GPRS)

Notes:

1. Restore to Factory Defaults Setting Requirement: **Yes**.
2. The setting of ignore triangle route is on in default ROM FILE. Triangle route network topology has potential security issues. If you are not clear about it, please refer to Appendix for the triangle route issue.
3. IKE process in phase 2 will check ID information between system and the peer. If you find that the IPSec connection has failed, please check your settings.
4. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the LAN-Cell.
5. SUA/NAT address loopback feature was enabled on LAN-Cell by default, however, if users do not need it, a C/I command "ip nat loopback off" could turn it off.
6. In WLAN configuration, a switch for enable / disable WLAN is added. The default value is "disable" since WLAN without any security setting is vulnerable. Please configure MAC filter, WEP and 802.1X when you enable WLAN feature.
7. The default port roles for LAN/DMZ setting is: port 1 to port 4 are all LAN ports.
8. WAN and CELLULAR must be on different subnets.
9. 802.11h is not supported.
10. 5.25~5.7 GHz is not supported.
11. If you change country code, please reboot device to get the correct wireless RF channels.

Known Issues:

System Limitations

[Bandwidth Management]

1. Bandwidth Management doesn't work on wireless LAN.

[MISC]

1. At SMT24.1, the collisions for WAN, LAN and DMZ port are not really counted.
2. Symptom: LAN host can ping Internet while LAN host change cable from LAN port to DMZ port.
   Condition:
   (1) Host connects to LAN port and gets DHCP address from router.
   (2) Unplug LAN host cable and plug it into DMZ port.
   (3) The host can still ping Internet using LAN DHCP address
   (4) The scenario will continue about 30secs.
3. When device is writing flash, all the interrupt/service will be stopped. (Firmware upload will take tens of seconds)

Issues

[Bandwidth Management]

1. Bandwidth management H.323 service does not support Netmeeting H.323 application.
2. Using BWM in PPPoE/PPTP mode, there are two filters for FTP and H323 ALG
   (1) If we execute FTP first then H323 cannot pass through LAN-Cell.
   (2) If we execute H323 before FTP, all functions work properly.
3. In some cases, BWM (Fairness-Based mode) cannot manage bandwidth accurately.
   Ex. In WAN interface, there are two subclasses for FTP service, their speed are 100Kbps and 500Kbps, the traffic match the filter which speed is 500Kbps may only use half of it's bandwidth.

[Wireless]

1. Wireless traffic is blocked.
   Topology:
   PC--------wireless LAN-Cell 2's Wan-------Internet
   (1) PC using wireless connect to LAN-Cell 2.
   (2) Set a global IP as LAN-Cell 2's WAN IP.
   (3) Using TfGen and set the configuration as follows:
      i. Utilization: 1000000
      ii. Destination: 1.1.1.1
   (4) After a period of time, the PC can scan the wireless SSID but can't associate with LAN-Cell 2.

[VPN]

1. Symptom: PC can't ping remote gateway through VPN tunnel under this special topology.
   Condition:
   PC------LAN LAN-Cell_A WAN----------LAN LAN-Cell_B WAN-------Internet
   (192.168.1.33） （192.168.100.33） (192.168.100.1) （172.202.77.145)

   (1) VPN configuration in LAN-Cell_A:
   WAN IP Address=192.168.100.33，WAN IP Subnet Mask=255.255.255.0， Gateway IP Address=192.168.100.1.
   Gateway policy，Name=IKE1，Remote Gateway Address=192.168.100.1，Pre-Shared Key=12345678.
   Network policy for IKE1，Active=enable，Name=IPSec1，Local Network/Starting IP Address=192.168.1.33，Remote Network/Starting IP Address=0.0.0.0
   (2) VPN configuration in LAN-Cell_B
   WAN IP Address=172.202.77.145，WAN IP Subnet Mask=255.255.0.0，Gateway IP Address=172.202.77.1.
   Gateway policy，Name=IKE1，Remote Gateway Address=192.168.100.33，Pre-Shared Key=12345678.

Network policy for IKE1，Active=enable，Name=IPSec1，Local Network/Starting IP Address=0.0.0.0，Remote Network/Starting IP Address=192.168.1.33.
(3) When we established the VPN tunnel between LAN-Cell_A and LAN-Cell_B, we can access LAN-Cell_B (192.168.100.1) with the remote management, such as Telnet, FTP…, this traffic will go through VPN tunnel. However, we can not ping LAN-Cell_B (192.168.100.1) successfully because this ICMP traffic did not go through VPN tunnel to LAN-Cell_B.

2. SNMP tools get LAN-Cell VPN MIB data, the index of received data are wrong if rules are larger than 1.
3. VPN rule swap does not support NAT Traversal.
4. When VPN tunnel is up with CELLULAR as “My Gateway”, VPN tunnel will not be dropped when CELLULAR WAN is disconnected.
5. Topology:
   PC1(1.33) --DUT---(VPN)----- LAN-Cell 2---PC5(2.33)
   PC2(11.33)--
   PC3(21.33)--
   PC4(31.33)--
   Configure as attached romfile.
   Steps:
   (1) DUT configures 2 IKE dynamic rules, and each attaches 2 IPSEC rules.
   (2) PC5 can ping PC3 and PC4 and the associated tunnels are built up.
   (3) When PC5 ping PC1, it will fail, and log shows ”[ID] : Remote IP [192.168.2.0] / [255.255.255.0] conflicts”.

[MISC]

4. The DMZ TxPkts counter increment at about 1 pkt/min even without any Ethernet cables ever connected.
5. Under PPTP encapsulation mode, we can not access some website like http://www.kimo.com.tw/
6. In eWC->Statistics, Tx data for Dial Backup is not correct.
7. Symptom: Dial Backup can’t work when Traffic Redirect is enabled.
   Condition:
   (1)Enable Traffic Redirect and Dial Backup
   (2)When disconnect WAN line, the traffic will go through Backup Gateway
   (3)At now, disconnect the Backup Gateway, the Dial Backup modem should be triggered. But it doesn’t.
8. Symptom : After system password hash, downgrade F/W, user can't use GUI
   Condition:
   (1) In patch 6 support password encrypted, CLI "sys pwdEncryption on". "sys md5 1234" will display a string "xxxxxxx"
   (2) Downgrade F/W to patch2 (not support password encrypted), SMT can use password "xxxxxxx" login but GUI can't
6. Triangle route issue（LAN side is responder）

Change History:

V4.02(AQP.1) | 07/25/2007

- Corrected minor cosmetic issues in the Web GUI.
- Expanded Cell-Sentry Data Budget field to maximum of 100,000 MB and alert recurring time field 46,000 minutes.
- Standardized cellular signal strength display between GSM and CDMA devices.

V4.02(AQP.1)b4 | 07/12/2007

Initial release to manufacturing.

Appendix 1 IPSec FQDN support

LAN-Cell A----------Router C (with NAT) ---------- LAN-Cell B
(WAN) (WAN) (LAN) (WAN)

If LAN-Cell A wants to build a VPN tunnel with LAN-Cell B by passing through Router C with NAT, A can not see B. It has to secure gateway as C. However, LAN-Cell B will send it packet with its own IP and its ID to LAN-Cell A. The IP will be NATed by Router C, but the ID will remain as LAN-Cell B sent.

In FQDN design, all three types, IP, DNS, E-Mail, can set ID content. For ID type is DNS or E-mail, the behavior is simple. LAN-Cell A and LAN-Cell B only checks the ID contents are consistent and they can connect.

Basically the story is the same when ID type is IP. If user configures ID content, then LAN-Cell will use it as a check. So the ID content also has to match each other. For example, ID type and ID content of incoming packets must match “Peer ID Type” and “Peer ID content”. Or LAN-Cell will reject the connection.

However, user can leave “ID content” blank if the ID type is IP. LAN-Cell will put proper value in it during IKE negotiation. This appendix describes all combinations and behaviors of LAN-Cell.

We can put all combinations in to these two tables:

(Local ID Type is IP):

Configuration		**Run-time status	
My IP Addr	Local ID Content	My IP Addr	Local ID Content
0.0.0.0	*blank	My WAN IP	My WAN IP
0.0.0.0	a.b.c.d (it can be 0.0.0.0)	My WAN IP	a.b.c.d (0.0.0.0, if user specified it)
a.b.c.d (not 0.0.0.0)	*blank	a.b.c.d	a.b.c.d
a.b.c.d (not 0.0.0.0)	e.f.g.h (or 0.0.0.0)	a.b.c.d	e.f.g.h (or 0.0.0.0)

*Blank: User can leave this field as empty, doesn’t put anything here.
**Runtime status: During IKE negotiation, LAN-Cell will use “My IP Addr” field as source IP of IKE packets, and put “Local ID Content” in the ID payload.

(Peer ID Type is IP):

Configuration		*Run-time check
Secure Gateway Addr	Peer ID Content	
0.0.0.0	blank	Just check ID types of incoming packet and machine’s peer ID type. If the peer’s ID is IP, then we accept it.
0.0.0.0	a.b.c.d	System checks both type and content
a.b.c.d	Blank	1. System will check the ID type and the content.

		2. The contents will match only if the ID content of coming packet is a.b.c.d because system will put Secure Gateway Address as Peer ID content.
a.b.c.d	e.f.g.h	1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is e.f.g.h.

*Runtime Check: During IKE negotiation, we will check ID of incoming packet and see if it matches our setting of “Peer ID Type” and “Peer ID Content”.

Summary:

1. When Local ID Content is blank which means user doesn’t type anything here, during IKE negotiation, my ID content will be “My IP Addr” (if it’s not 0.0.0.0) or local’s WAN IP.
2. When “Peer ID Content” is not blank, ID of incoming packet has to match our setting. Or the connection request will be rejected.
3. When “Secure Gateway IP Addr” is 0.0.0.0 and “Peer ID Content” is blank, system can only check ID type. This is a kind of “dynamic rule” which means it accepts incoming request from any IP, and these requests’ ID type is IP. So if user put a such kind of rule in top of rule list, it may be matched first. To avoid this problem, we will enhance it in the future.

Appendix 2 Embedded HTTPS proxy server

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering.

The LAN-Cell's embedded HTTPS proxy server is basically an SSL server which performs SSL transactions, on behalf of the embedded HTTP server, with an SSL client such as MSIE or Netscape. As depicted by the figure below, when receiving a secure HTTPS request from an SSL-aware Web browser, the HTTPS proxy server converts it into a non-secure HTTP request and sends it to the HTTP server. On the other hand, when receiving a non-secure HTTP response from the HTTP server, the HTTPS proxy server converts it into a secure HTTPS response and sends it to the SSL-aware Web browser.

By default, the HTTPS proxy server listens on port 443 instead of the HTTP default port 80. If the LAN-Cell's HTTPS proxy server port is changed to a different number, say 8443, then the URL for accessing the LAN-Cell's Web user interface should be changed to https://hostname:8443/ accordingly.

Appendix 3 Wi-Fi Protected Access

Wi-Fi Protected Access(WPA) is a subset of the IEEE 802.11i. WPA improves data encryption by using TKIP, MIC and IEEE 802.1X. Because WPA applies 802.1X to authenticate WLAN users by using an external RADIUS server, so you can not use the Local User Database for WPA authentication.

For those users in home or small office, they have no RADIUS server, WPA provides the benefit of WPA through the simple "WPA-PSK". Pre-Shared Key(PSK) is manually entered in the client and LAN-Cell for authentication. LAN-Cell will check the client PSK and allow it join the network if it's PSK is matched. After the client pass the authentication, LAN-Cell will derived and distribute key to the client, and both of then will use TKIP process to encrypt exchanging data.

Appendix 4 IPSec IP Overlap Support

The LAN-Cell uses the network policy to decide if the traffic matches a VPN rule. But if the LAN-Cell finds that the traffic whose local address overlaps with the remote address range, it will be confused if it needs to trigger the VPN tunnel or just route this packet.

So we provide a CI command “ipsec swSkipOverlapIp” to trigger the VPN rule. For example, you configure a VPN rule on the LAN-Cell A as below:

Local IP Address Start= 1.1.1.1 End= 1.1.2.254
Remote IP Address Start= 1.1.2.240 End = 1.1.2.254

You can see that the Local IP Address and the remote IP address overlap in the range from 1.1.2.240 to 1.1.2.254.

(1) Enter “ipsec swSkipOverlapIp off”:
To trigger the tunnel for packets from 1.1.1.33 to 1.1.2.250. If there is traffic from LAN to IP Alias, the traffic still will be encrypted as VPN traffic and routed to WAN, you will find their traffic disappears on LAN.
(2) Enter “ipsec swSkipOverlapIp on”:
Not to trigger the tunnel for packets from 1.1.1.33 to 1.1.2.250. Even the tunnel has been built up, the traffic in this overlapped range still cannot be passed.

[Note]
If you configure a rule on the LAN-Cell A whose
Local IP Address Start= 0.0.0.0
Remote IP Address Start= 1.1.2.240 End = 1.1.2.254
No matter swSkipOverlapIp is on or off, any traffic from any interfaces on the LAN-Cell A will match the tunnel. Thus swSkipOverlapIp is not applicable in this case.

Appendix 5 VPN Local IP Address Limitation

There is a limitation when you configure the VPN network policy to use any Local IP address. When you set the Local address to 0.0.0.0 and the Remote address to include any interface IP of the LAN-Cell at the same time, it may cause the traffic related to remote management or DHCP between PCs and the LAN-Cell to work incorrectly. This is because the traffic will all be encrypted and sent to WAN.

For example, you configure a VPN rule on the LAN-Cell A as below:

Local IP Address Start= 1.1.1.1 End= 1.1.2.254
Remote IP Address Start= 1.1.2.240 End = 1.1.2.254

LAN-Cell LAN IP = 1.1.1.10

LAN-Cell LAN IP falls into the Local Address of this rule, when you want to manage the LAN-Cell A from $PC_{A,}$ you will find that you cannot get a DHCP Client IP from the LAN-Cell anymore. Even if you set your IP on PC_A as static one, you cannot access the LAN-Cell.

Appendix 6 VPN rule swap limitation with VPN Client on XAuth

Example 1:

LAN-Cell (WAN)---------- VPN Client

(IP:1.1.1.1) (IP:1.1.1.2)

LAN-Cell VPN Rule: Two IKE rule	
➢ Dynamic IKE rule: Security Gateway: 0.0.0.0 X-Auth: Server I. Policy one: - Name: “Rule_A” - Local: 192.168.2.0/24 - Remote: 0.0.0.0	➢ Static IKE rule: Security Gateway: 1.1.1.2 X-Auth: None I. Policy one: - Name: “Rule_B” - Local: 192.168.1.0/24 - Remote: 1.1.1.2/32

VPN Client
Security Gateway: 1.1.1.1 Phase one Authentication method: Preshare Key Remote: 192.168.1.0/24

In example 1, user may wonder why LAN-Cell swap to dynamic rule even VPN client only set authentication method as “Preshare Key” not “Preshare Key+XAuth”. The root cause is that some VPN Cients will send XAuth VID no matter what authentication mode that is set. Because of the XAuth VID, LAN-Cell will swap to dynamic rule.

This unexpected rule swap result is a limitation of our design. For LAN-Cell, when we got initiator’s XAuth VID in IKE Phase One period, we know initiator can support XAuth. To take account of security, we will judge that initiator want to do XAuth, and we will search one matched IKE Phase One rule with XAuth server mode as the top priority. To our rule swap scheme, we search static rule first then dynamic rule. In example 1, we will find the static rule, named “Rule_B”, to build phase one tunnel at first. After finished IKE phase one negotiation, we known initiator want to do XAuth. Since Rule_B has no XAuth server mode, we try to search another rule with correct IKE Phase One parameter and XAuth server mode. The search result will lead us to swap rule to dynamic rule, named “Rule_A”. Thus to build VPN tunnel will fail by Phase Two local ip mismatch.

To avoid this scenario, the short-term solution is that we recommend is for the user to set two IKE rules with different Phase One parameter. The long-term solution is that VPN Client needs to modify the XAuth VID behavior. VPN Client should not send XAuth VID when authentication method is “Preshare key”, but send XAuth VID when authentication method is “Preshare key+XAuth”.

Appendix 7 The mechanism of Gratuitous ARP in the LAN-Cell

In the past, if the LAN-Cell gets a gratuitous ARP it will not update the sender's MAC mapping into its ARP table. In current design, if you turn on 'ip arp ackGratuitous active yes', the LAN-Cell will response such packet depends on two case: 'ip arp ackGratuitous forceUpdate on' or 'ip arp ackGratuitous forceUpdate off'. if you turn on forceUpdate, then the LAN-Cell gets gratuitous ARP, it will force to update MAC mapping into the ARP table, otherwise if turn off forceUpdate, then the LAN-Cell gets gratuitous ARP, it will update MAC mapping into the ARP table only when there is no such MAC mapping in the ARP table.

As an example for its purpose, assume there is a backup gateway on the network.. One day, the primary gateway shuts down and the backup gateway is up, the backup gateway is set as static IP as original gateway's IP, it will broadcast a gratuitous ARP to ask who is using this IP. If ackGratuitous is on, the LAN-Cell receive the gratuitous ARP from the backup gateway, it will also send an ARP request to ask who is using this IP. Once the LAN-Cell gets a reply from backup gateway, it will update its ARP table so that the LAN-Cell can keep a correct gateway ARP entry to forward packets. If ackGratuitous is off, the LAN-Cell will not keep a correct gateway ARP entry to forward packets.

There is one thing need to be noticed: update the ARP entry might still have dangers more or less if there is a spoofing attack. So we suggest if you have no opportunity to meet the problem, you can turn off ackGratuitous. forceUpdate on will be more dangerous than forceUpdate off because it update ARP table even when ARP entry is existing.

Appendix 8 The mechanism when the LAN-Cell receives a IKE packets with IC

[RFC 2407]The INITIAL-CONTACT(IC) status message may be used when one side wishes to inform the other that this is the first SA being established with the remote system. The receiver of this Notification Message might then elect to delete any existing SA's it has for the sending system under the assumption that the sending system has rebooted and no longer has access to the original SA's and their associated keying material.

The LAN-Cell has two ways to delete SA when it receives IC, it is switched by a global option 'ipsec initContactMode gateway/tunnel':

(1)ipsec initContactMode gateway

When the LAN-Cell receives a IKE packets with IC, it deletes all tunnels with the same secure gateway IP. It is default option because the LAN-Cell is site to site VPN device. Take the picture 1 as example, there are three VPN tunnels are created between LAN-Cell A and LAN-Cell B, but LAN-Cell A reboots for some reasons, and after rebooting, the LAN-Cell A will send a IKE with IC to the LAN-Cell B, then the LAN-Cell B will delete all existing tunnels whose security gateway IP is the same as this IKE's one and build a new VPN tunnel for the sender.

(2)ipsec initContactMode tunnel

When the LAN-Cell receives a IKE packets with IC, it deletes only one existing tunnel, whose security gateway IP is not only the same as this IKE's one and also its phase 2 ID(network policy) should match. It is suitable when your tunnel is created from a VPN peer to LAN-Cell and there are more than two this kind of VPN peers build tunnels behind the same NAT router. Take the picture 2 as example, PC 1, PC2 and PC3 has it's own VPN software to create tunnels with LAN-Cell. Suppose that the PC1, PC2 and PC3 separately create different tunnels with LAN-Cell for the traffic to PC4, PC5 and PC6, once the PC1 reboots for some reasons, and after rebooting, the PC1 sends a IKE with IC to the LAN-Cell B, then the LAN-Cell B will only delete the tunnel which is used by PC1 and PC4 and build a new VPN tunnel for it. So other tunnels will not be disconnected.