Digital Energy
MDS

APPLICATION BULLETIN

NUMBER: AB11001
Jun 2011

GE MDS WiYZ

GE MDS, LLC., 175 Science Parkway, Rochester NY 14620 USA
Phone +1-585-241-5510, Fax +1-585-242-8369

GE MDS WiYZ Cellular Connectivity

WiYZ cellular connectivity use cases and recommended network setup

Table of Contents

Table of Figures

Revision History

Rev	Date	By	Revision Description
0.1	04/12/2011	Ajay Grewal	Initial draft
0.2	04/29/2011	Ajay Grewal	Revised after review

1 INTRODUCTION

1.1 Purpose

This document describes WiYZ cellular connectivity use cases and recommended network setup for supporting them in presence of different IP addressing modes and data connection characteristics of various cellular networks and providers.

1.2 Scope

This document does not describe how to configure WiYZ and its cellular interface to support the described use cases. Please refer to WiYZ system manual for details.

1.3 Abbreviations, Acronyms and Symbols

CDMA	Code Division Multiple Access
DRS	Data Reporting Service
EDGE	Enhanced Data Rates for GSM Evolution
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
IP	Internet Protocol
M2M	Machine-to-Machine
MVNO	Mobile Virtual Network Operator
SFTP	SSH File Transfer Protocol

1.4 Applicable Documents

The following documents form a part of this specification to the extent specified herein. Documents are listed in the order of precedence. Referenced documents are available from GE MDS or as an industry standard.

Ref	Title	Document Number	Location
WIYZ-SYS-MANUAL	WiYZ System Manual		

For more information, contact GE MDS Technical Services at techsupport@microwavedata.com, or by phone at +1-585-241-5510.

2 USE CASES

The WiYZ cellular connectivity feature enables customers to deploy WiYZ gateway at a remote hard-to-reach locations and access it from their SCADA and other management systems hosted in a central operations/data center (referred to as back-office hereafter). In particular, WiYZ cellular connectivity enables following use cases:

a. Management – Administration/Monitoring using Web-UI, SNMP, Telnet or SSH from a host/PC in the operations center.

b. IO Read/Write - WiYZ remote IO read/write using Modbus/TCP from the SCADA system.

c. DRS Service – Transferring IO data files from WiYZ gateway to a file server located in the data center using FTP or SFTP protocol.

d. Cellular Router - Routing IP traffic between devices connected to Ethernet/EntraNET/WiFi network and back-office network over cellular network.

3 SERVICE SETUP

This section describes various considerations that need to be taken into account when selecting service provider and a data plan for the WiYZ cellular connectivity.

3.1 Provider Selection

With WiYZ gateway, customer has following choices:

a. A CDMA2000 1xRTT based solution that works on Verizon Wireless network (a tier-1 provider) and with other M2M MVNOs (also known as tier-2 providers) that use Verizon Wireless network as their underlying network (e.g. KORE Telematics CDMA network).

b. A quad band 850/900/1800/1900MHz GPRS/EDGE based solution that works on any compatible tier-1 network (like AT&T) and with other M2M MVNOs (also known as tier-2 providers) that use such networks as their underlying network (e.g. KORE Telematics GSM US network) as along as proper SIM card is obtained and activated.

Following factors should be considered in choice of above solutions:

a. **Coverage**: The service provider network should provide adequate coverage for all sites where customer intends to deploy the gateway. The coverage maps are typically available on service provider websites.

b. **Costs:** The service costs can be classified into two categories:

   i. *One-Time Costs*: These costs typically include costs for SIM cards (for GPRS/EDGE solution), activation fees, site-to-site VPN setup fees etc.

   ii. *Recurring costs*: These costs typically include the monthly data plan fees for each of the activated units and any monthly maintenance fees (e.g. for VPN).

   These service costs should be negotiated by the customer with the service provider. The provider may be willing to waive certain fees depending on specific situations.

c. Manageability: Some service providers provide customer portals that can be used for managing the customer account. These portals typically include following features:

   a. Information about customer service agreement (CDMA 1xRTT or GPRS service) and various data plans that are available to assign to each individual WiYZ gateway (e.g. CDMA 1xRTT 10MB plan, GPRS 250MB plan etc.)

b. Ability to request SIM cards for GPRS/EDGE based WiYZ gateway or ability to load ESN number in the system for CDMA based WiYZ gateway.

c. Ability to activate the WiYZ gateway cellular modem on a specific data plan and to de-activate later at any time.

d. Ability to monitor data usage from individual and group of gateways. Ability to set daily or monthly data thresholds for each gateway and receive alarms through emails when those thresholds are crossed.

e. Ability to view billing and invoice data for individual and group of gateways.

f. Ability to open problem tickets with the service provider.

Manageability is an important factor that customers should take into account as it can ease the process of obtaining, maintaining and monitoring the cellular service for fleet of WiYZ gateways.

3.2 Data Plan Selection

The various data plans offered vary from provider to provider but, typically, they fall in two categories:

a. **Pay-Per-Use**: Under these plans the data usage is aggregated and the customer is charged for total data used at end of the month.

b. **Pre-paid:** Under these plans data usage and price is fixed per gateway per month (e.g. $X for 10MB per gateway per month) and overages are charged at overage rates (e.g. $Y for each MB usage above fixed allowance).

Table 1 lists a sample data usage pattern that can help a customer estimate data usage for various WiYZ gateway use cases and select an appropriate plan to avoid overages. Please note that these are estimates only and data usage can vary widely depending on specific usage pattern.

Service	Data Usage per device per month	Comments
Web-UI Management	6MB	Estimated by visiting each web-page of WiYZ gateway three times and aggregating total data retrieved.
Data Reporting Service (DRS)	210MB	Estimated by configuring a system with 20 WiYZ remotes that publish all input channels on WiYZ remote every 1 sec.
Modbus/TCP IO Read/Write	32MB	Estimated by sending 50KB of request data and getting 1MB of response data per day.

Table 1 Sample Data Usage

For above sample data usage, a pre-paid plan of 250MB per device per month should suffice.

It is highly advised the customers activate the gateway with a conservative data plan and monitor data usage for a month (obtained from the service provider) and then switch the gateway to the appropriate data plan.

4 NETWORK SETUP

The WiYZ use cases described earlier fall into categories of Mobile Originated (MO) and Mobile Terminated (MT) data and hence require a network setup that is capable of supporting both traffic flows.

The typical data plans provided by the cellular operators assign dynamic IP address to the cellular modem. Also, cellular networks typically disconnect the data session after certain period of time, called PDP Idle Timeout, if there is no data sent/received to/from the modem. Following table shows the typical times for KORE networks.

Network	PDP Idle Timeout (mins)
KORE GSM US	240
KORE GSM CANADA	54
KORE CDMA	1435

Table 2 Typical PDP Idle Timeouts

Every time a new session is setup, the cellular network can assign a different IP address to the modem.

The mobile terminated use cases require that the IP address assigned to the modem be always known to the application (e.g. web browser, Modbus/TCP client etc.) in the back-office.

The WiYZ gateway features OpenVPN client solution that allows customer to pre-configure a static IP address for the gateway from a private IP address pool that is routable from within its network. The OpenVPN solution provides following benefits:

a. The OpenVPN client on WiYZ gateway ensures that the cellular data session is always kept active by periodically sending keep-alive packets if no data packets have been sent for certain period of time.

b. In the event that cellular data session gets disconnected, the OpenVPN client re-establishes the connection to the OpenVPN server ensuring that the customer applications in the back-office are always able to reach the gateway through a pre-configured static IP address hiding the dynamic IP address assigned to the modem.

c. The OpenVPN solution secures the end-to-end data flow between the WiYZ gateway and the OpenVPN server using industry standard TLS protocol, providing authentication, confidentially and integrity to the customer data flow.

The IP address assigned by the service provider could be either a public or private IP address.

In the case where a public IP address is assigned to the modem, the WiYZ gateway can access any host that is accessible on the internet (i.e. has been assigned a public IP address) and vice versa.

In the case where a private IP address is assigned to the modem, the WiYZ gateway can access any host that is accessible on the internet (i.e. has been assigned a public IP address), however such an access is usually enabled via NAT firewall process on the service provider's network. The NAT process, typically, creates and maintains address/port translation entries for traffic exiting the cellular network towards the internet for finite duration of time. These entries need to be present for return traffic to be routed back to the gateway. This can cause issues for data initiated from the customer network towards the gateway. To solve this problem, it is advised that a site-to-site VPN be established between the customer network and the service provider network. This removes the NAT process from the data flow and allows seamless flow of bi-directional data between the customer network and the gateway.

Error! Reference source not found. shows a simplified network setup for either GPRS/EDGE or CDMA 1xRTT network for the case where a public IP address is assigned to the modem. In this case, the OpenVPN server needs to be made publicly addressable (e.g. by installing it in a DMZ network) and OpenVPN client enabled on the WiYZ gateway and configured to connect to the server.

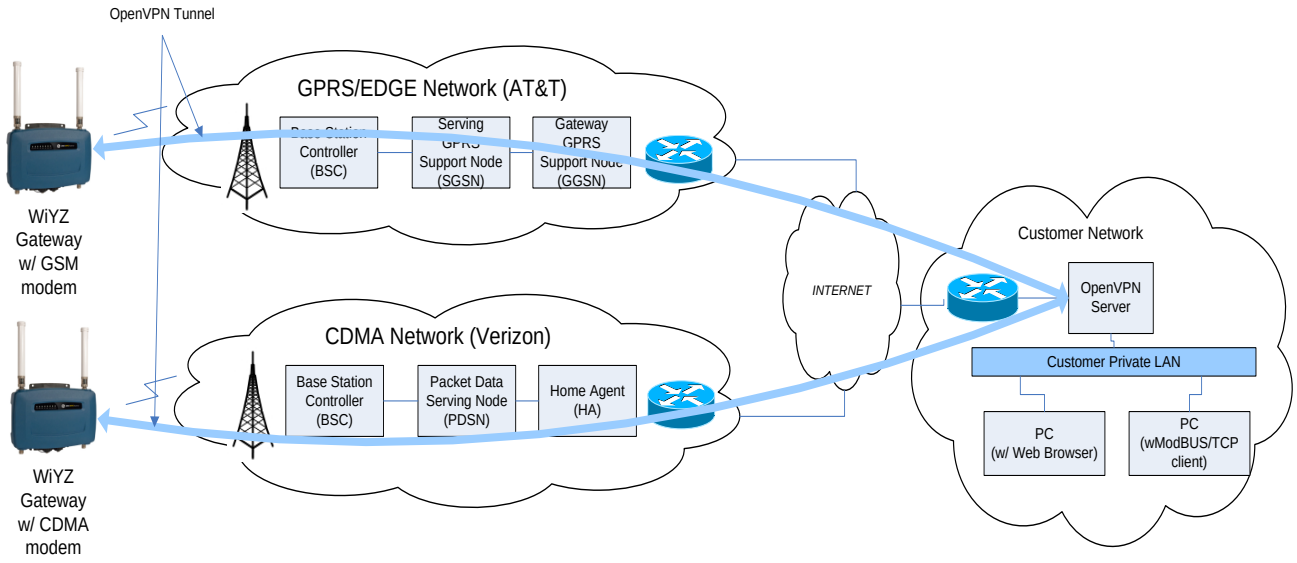

Figure 1 Network Setup with OpenVPN tunnel

Figure 2 shows a simplified network setup for either GPRS/EDGE or CDMA 1xRTT network for the case where a private IP address is assigned to the modem from the private IP address pool established through mutual agreement between the customer and service provider during site-to-site VPN setup. In this case, the OpenVPN server needs to be made addressable using an IP address from this pool and OpenVPN client enabled on the WiYZ gateway and configured to connect to the server.

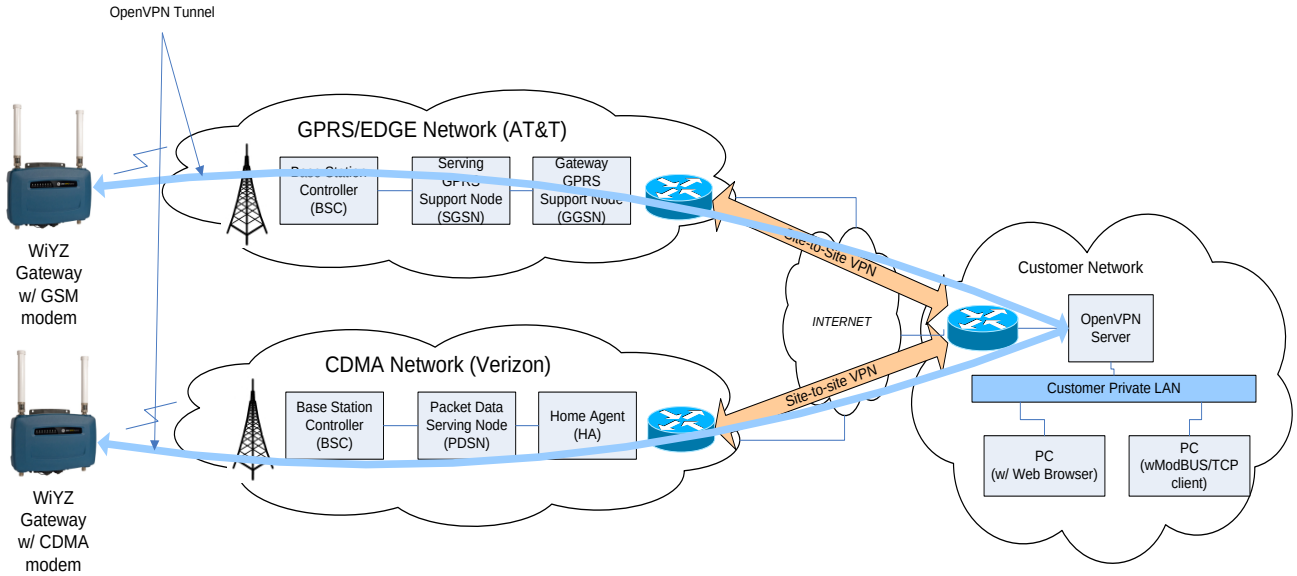

Figure 2 Network Setup with site-to-site VPN and OpenVPN tunnel

The customer should plan to execute following steps to achieve the above described network setup:

a. Choose a service provider, establish a service agreement (CDMA 1xRTT or GPRS/EDGE) and a set of data plans (pre-paid or pay-per-use) that cover the estimated usage for various use cases that customer may need to support on the WiYZ gateways.

b. If the service provider assigns private IP addresses, setup a site-to-site VPN between the customer network and cellular provider network to allow assignment of private IP addresses from an address pool that is routable to/from the customer network.

c. Install and Configure an OpenVPN server that is accessible from the cellular network. Establish an OpenVPN virtual private IP address pool from which the each gateway shall be assigned a static IP address. The back-office applications shall use this static IP address to access the gateway. Note that this address pool is different than the private IP address pool setup by the service provider for assigning dynamic IP addresses to the cellular modems.

d. For each deployed gateway, configure the OpenVPN server to assign a specific static IP address (from the virtual private IP address pool) based on the common name specified in the client certificate configured on the gateway.

e. For each deployed gateway, activate the cellular modem on a specific data plan based on its estimated usage pattern.

f. Authorize, Enable and Configure the OpenVPN client on the gateway to establish a secure IP tunnel to the OpenVPN server. Please refer to [WIYZ-SYS-MANUAL] for OpenVPN client configuration.

APPENDIX A - EXAMPLE NETWORK SETUP