Addressing PCI DSS Compliance with BEC LTE Routers

Table of Contents

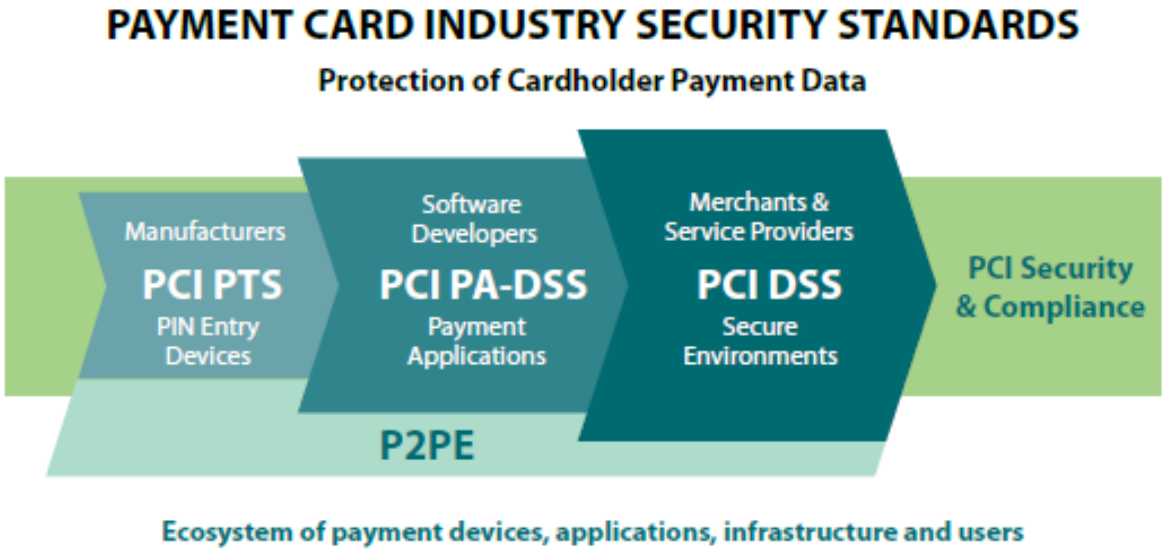
Background

According to PrivacyRights.org – more than 895+ million records with sensitive information have been breached between January 2005 and December 2015. As you are a key participant in payment card transactions, it is imperative that standard security procedures and technologies are implemented to thwart theft of cardholder data.

Merchant-based vulnerabilities may appear almost anywhere in the card-processing ecosystem Including point-of-sale devices; mobile devices, personal computers or servers; wireless hotspots; web shopping applications; paper-based storage systems; the transmission of cardholder data to service providers, and in remote access connections. Vulnerabilities may also extend to systems operated by service providers and acquirers, which are the financial institutions that initiate and maintain the relationships with merchants that accept payment cards
Compliance with the PCI DSS helps to alleviate these vulnerabilities and protect cardholder data.

Overview

PCI Security Standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with requirements for software developers and manufacturers of applications and devices used in those transactions. The Council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council, American Express, Discover Financial Services, JCB, MasterCard and Visa Inc.



PCI Security Standards

PCI Data Security Standard (PCI DSS)

The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you accept or process payment cards, PCI DSS applies to you.

PIN Transaction Security (PTS) Requirements

The PCI PTS is a set of security requirements focused on characteristics and management of devices used in the protection of cardholder PINs and other payment processing related activities. The requirements are for manufacturers to follow in the design, manufacture and transport of a device to the entity that implements it. Financial institutions, processors, merchants and service providers should only use devices or components that are tested and approved by the PCI SSC (www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php).

Payment Application Data Security Standard (PA-DSS)

The PA-DSS is for software vendors and others who develop payment applications that store, process or transmit cardholder data and/or sensitive authentication data, for example as part of authorization or settlement when these applications are sold, distributed or licensed to third parties. Most card brands encourage merchants to use payment applications that are tested and approved by the PCI SSC.
Validated applications are listed at:
www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

PCI Point-to-Point Encryption Standard (P2PE)

This Point-to-Point Encryption (P2PE) standard provides a comprehensive set of security requirements for P2PE solution providers to validate their P2PE solutions, and may help reduce the PCI DSS scope of merchants using such solutions. P2PE is a cross-functional program that results in validated solutions incorporating the PTS Standards, PA-DSS, PCI DSS, and the PCI PIN Security Standard.
Validated P2PE solutions are listed at:
https://www.pcisecuritystandards.org/approved_companies_providers/validated_p2pe_solutions.php

PCI DSS Security Requirements

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. “System components” include network devices, servers, computing devices, and applications. Examples of system components include but are not limited to the following:

- ✓ Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the CDE.
- ✓ Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- ✓ **Network components including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.**
- ✓ Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- ✓ Applications including all purchased and custom applications, including internal and external (for example, Internet) applications.
- ✓ Any other component or device located within or connected to the CDE.

The PCI Data Security Goals

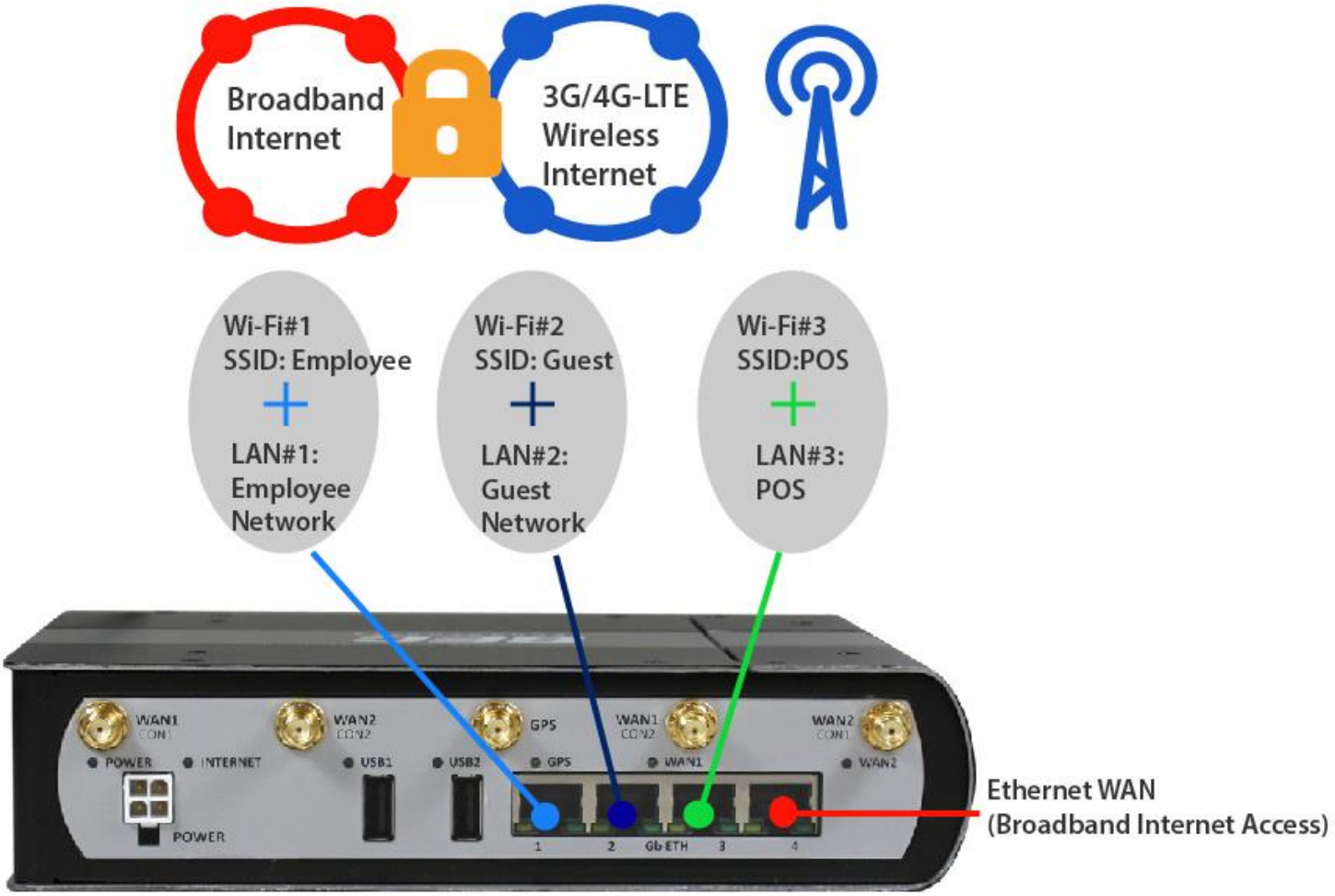
PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Device Configuration Diagram

The following device diagram represents a typical network configuration that Includes:

- Ethernet WAN Internet Access with 3G, 4G/LTE Failover
- Ethernet and Wi-Fi access for employees and networked devices
- Secured VPN Access
- Guess Wi-Fi access for customers



Device Configuration Recommendations

Key Features & Capabilities to PCI Compliance

- Multiple Network Segmentations
- (4) Gigabit Ethernet LAN Ports can be assigned to different and individual groups
- (4) Wireless SSIDs can be assigned to different and individual groups
- Wireless Security with WPA-PSK / WPA2-PSK
- Wireless MAC Filter
- VPN up to 32 secured tunnels
  - Secured IPSec VPN with powerful DES/ 3DES/ AES
  - Secured PPTP VPN with Pap/ Chap/ MPPE authentication
  - Secured L2TP VPN with Pap/Chap authentication
  - Secured GRE VPN tunnel
- Firewall Security
  - Stateful Packet Inspection (SPI)
  - DoS Preventing
  - IP/MAC/URL Filtering
  - DoS Attach Prevention
  - Password Protection
  - Application Level Gateway (ALG)
- Network Features
  - Virtual Server
  - De-Militarized Zone (DMZ)
  - Application Level Gateways (ALG)
- Access Control to block PING, FTP, Web, Telnet, etc access from WAN and/or LAN
- Remote System Log
- E-mail Alters
- Virtual LAN (VLAN)
- BECloud (BEC LCMS) Management

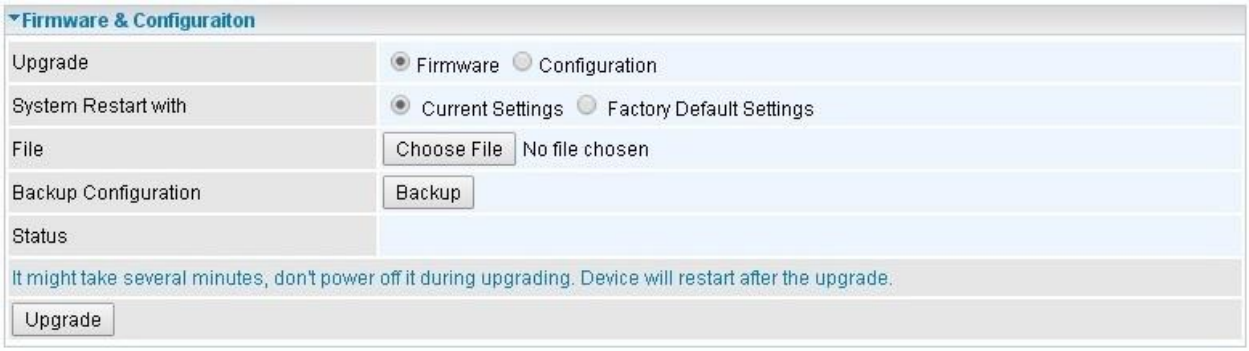
MXConnect 4G/LTE Router Configuration Steps

Step 1: Upgrade router to the latest firmware version

BEC provides an easy way to update the latest firmware to take advantage of feature enhancements and improvements to your MXConnect 4G/LTE router.

To upgrade the firmware to your MXConnect 4G/LTE router, please download or copy the firmware to your local environment first. Click **"Choose File"** to specify the path of the firmware file. Then, click **"Upgrade"** to start upgrading process. After completing the firmware upgrade, the MXConnect 4G/LTE router will automatically restart and run the new firmware.

To upgrade the latest firmware, go to ***Configuration >> Maintenance >> Firmware & Configuration***

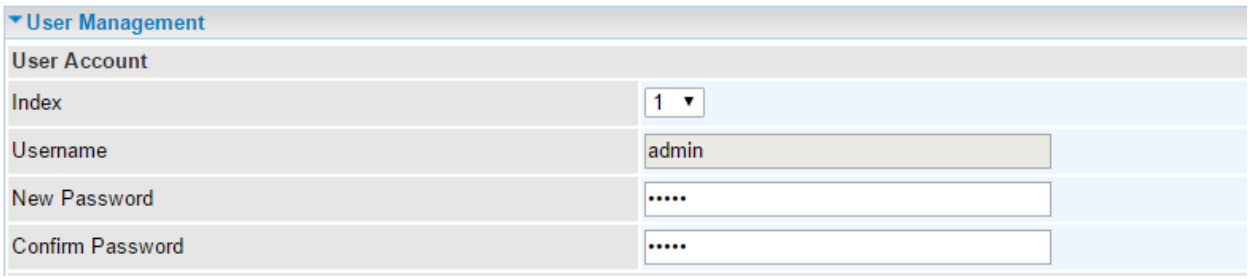


Step 2: Change the Default Admin Password

BEC MXConnect 4G/LTE routers all come with a generic username and password. PCI DSS requires for a change to router's username and password for security purpose. The User Management section, in the web GUI, grants the system administrator abilities to change GUI login credentials and also grant access control for other local users.

Please change your MXConnect 4G/LTE router with a strong and unique admin password.

To change default Administrator (Admin) password, go to ***Configuration >> Maintenance >> User Management***



Step 3: Secure WAN Connectivity

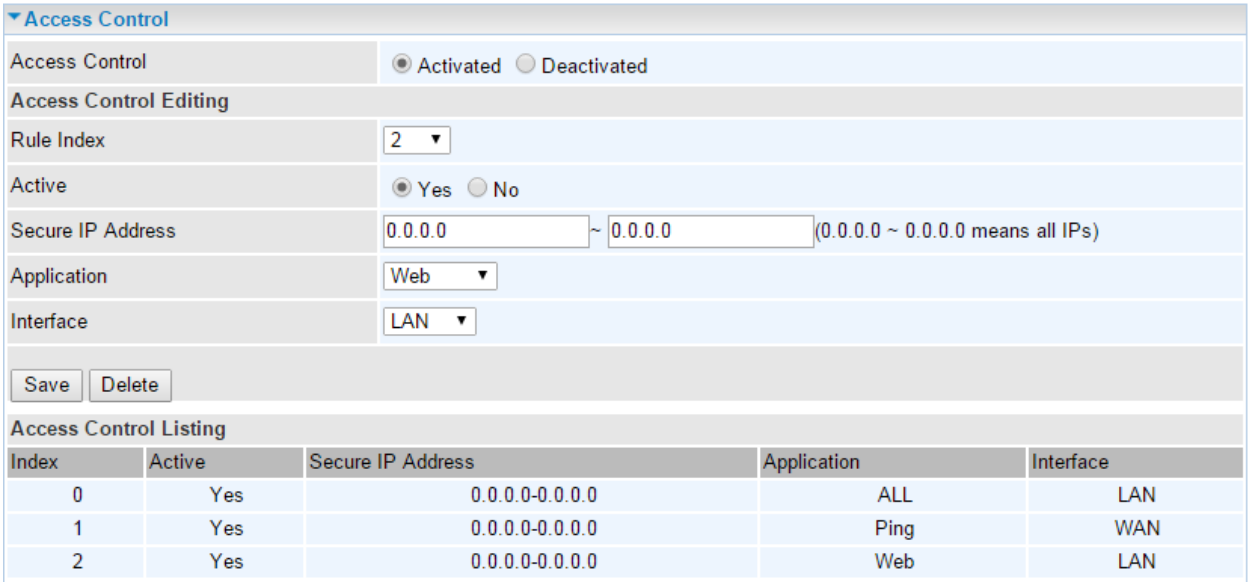
Block WAN Ping Responses: Block any PING from external to the MXConnect 4G/LTE router.

WAN Ping is **enabled/allowed** by default, please delete Index #1.

Disable Remote Web Administration Access: Prevent administrator to access to the MXConnect 4G/LTE router GUI (Web UI) remotely.

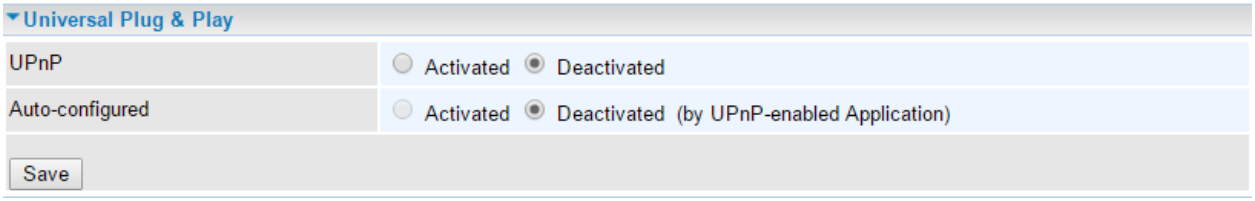
Create new rule, select application **Web** then choose **LAN** Interface to allow local (LAN) GUI access, See Index #2.

To configure WAN Ping and Remote GUI Access, go to ***Configuration >> Access Management >> Access Control***



Disable UPnP: Turn off the automatic peer-to-peer network connectivity for PCs and other network devices.

To configure the Universal Plug & Play (UPnP), go to ***Configuration >> Access Management >> Universal Plug & Play***



Setup VNP Connection: VPN is a private network that connects the MXConnect 4G/LTE router with remote networks through the Internet. It provides security through tunneling protocols and security procedures by encrypting all sending or receiving packets.

BEC MXConnect series supports 4 VPN protocols – IPSec, PPTP, L2TP, and GRE.

IPSec-VPN is the most common protocol for cooperate VPN services; it is more complex and provides higher level of security.

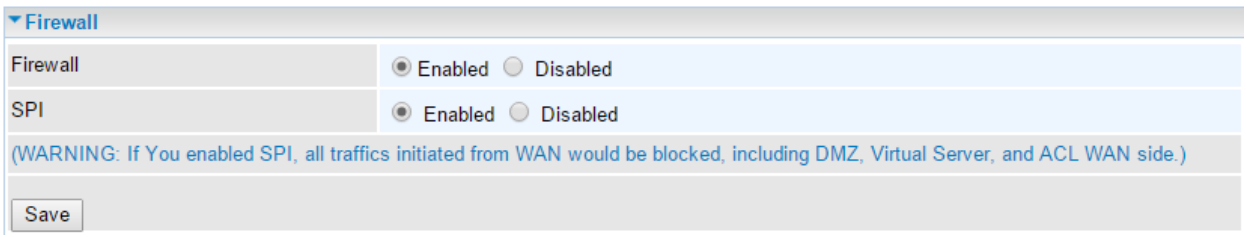
To configure the VPN, go to ***Configuration >> VPN***

Step 4: Configure the Firewall Security

Enable Firewall: Automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

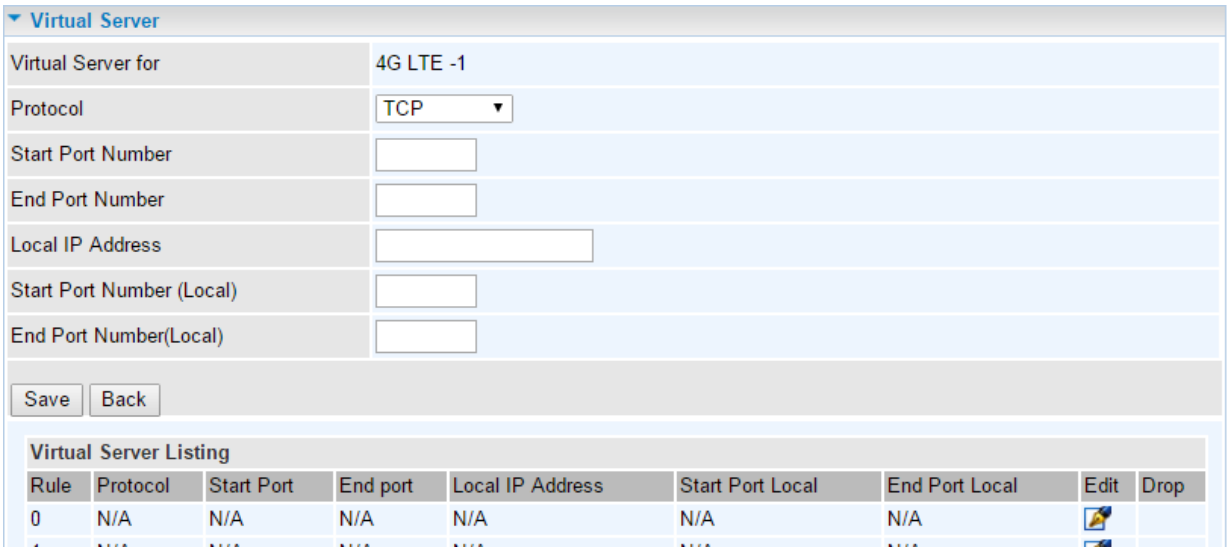
Enable SPI (Stateful Packet Inspection): That all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

To configure Network Time Server/Protocol, go to ***Configuration >> Advanced Setup >> Firewall***



Use Port Forwarding Rules: Port forwarding known as Virtual Server. After Firewall/SPI is enabled**,** external (inbound) traffic to local LAN network will get blocked. Create port forwarding rules to allow incoming traffic to reach to a specific server or device inside the LAN network.

To create Port Forwarding rule, go to ***Configuration >> Advanced Setup >> NAT***

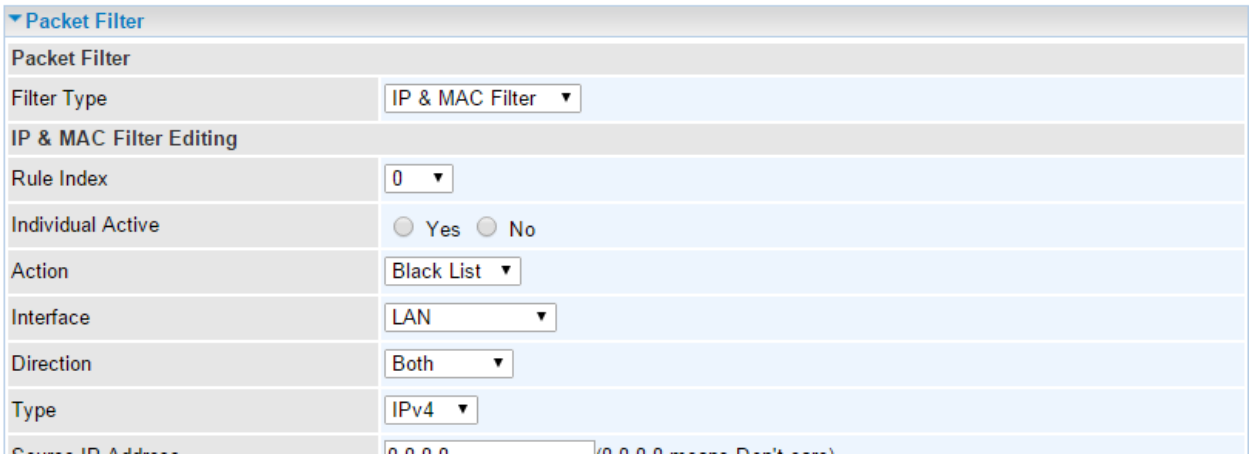


Use Wireless MAC Filtering: Use the filtering to create authorized (allow) or unauthorized (deny) accessing to a specific Wireless (SSID) LAN networks.

To configure Wireless MAC Filtering, go to ***Configuration >> Interface Setup >> Wireless MAC Filter***

Use IP/MAC Filtering: Use the filtering to create authorized (white list) or unauthorized (black list) IP addresses accessing to LAN network.

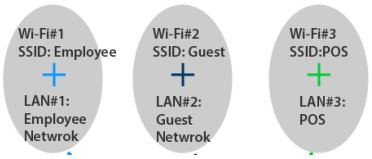
To configure IP/MAC Filtering, go to ***Configuration >> Access Management >> Packet Filter***

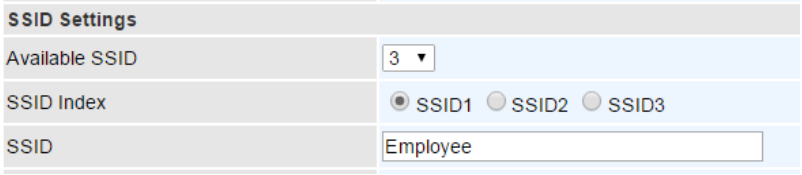


Step 5: Setup and Secure Wireless LAN

Setup multiple WI-FI SSIDs: Configure Wireless to change available SSID from default 1 to 3.

- Wi-Fi SSID 1 : “Employee”
- Wi-Fi SSID 2 : “Guest”
- Wi-Fi SSID 3 : “POS”





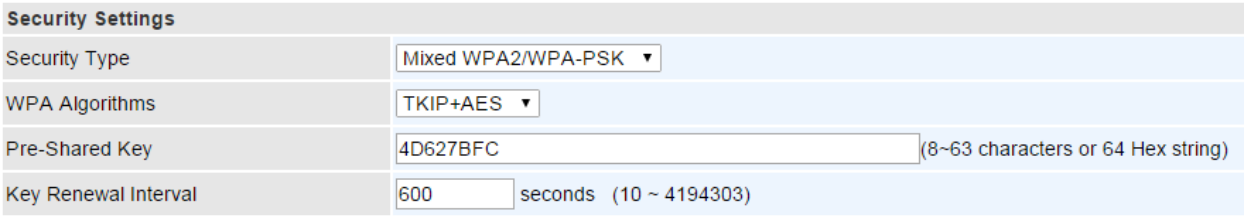
Enable / Disable Broadcast SSID:

- Wi-Fi SSID 1 (“Employee”): Broadcast SSID “NO”
- Wi-Fi SSID 2 (“Guest”): Broadcast SSID “YES”
- Wi-Fi SSID 3 (“POS”): Broadcast SSID “NO”

Disable WPS: Disable WPS in all three (3) Wi-Fi networks.

Setup Security Mode and Password:

- Wi-Fi SSID 1 (“Employee”): Security Type “Mixed WPA2/WPA-PSK”, WPA Algorithms “TKIP+AES”, and Pre-Shared Key (enter a strong password, 8-63 characters)
- Wi-Fi SSID 2 (“Guest”): Security Type (can be any of the encryption mode) and assign a password for the guest network.
- Wi-Fi SSID 3 (“POS”): Security Type “Mixed WPA2/WPA-PSK”, WPA Algorithms “TKIP+AES”, and Pre-Shared Key (enter a strong password, 8-63 characters)



To setup and configure Wireless, go to ***Configuration >> Interface Setup >> Wireless***

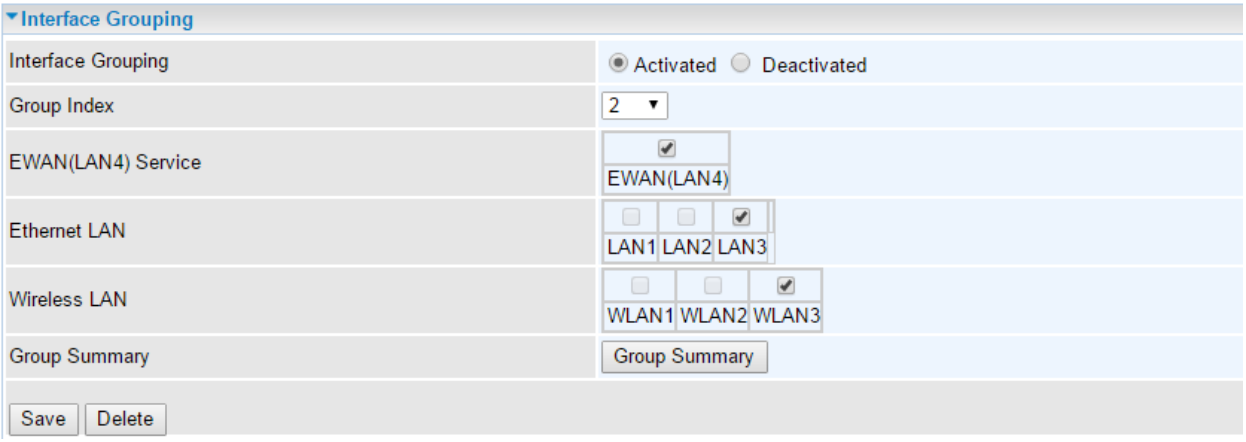
Step 6: Implement Network Segmentation

Enable VLAN for Each Network: Specify the VLAN ID (Virtual LAN ID) to identify which network to send the packet to.

To setup and configure VLAN ID, go to ***Configuration >> Interface Setup >> Internet***

Create Independent Network: Attach physical interfaces/ports (Internet, Ethernet, and Wireless), to be in the same network to allow them to communicate freely.

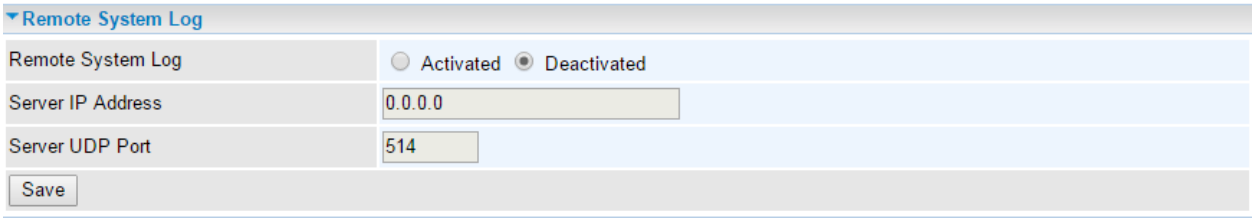
To create independent network, go to ***Configuration >> Advanced Setup >> Interface Grouping***



Step 7: Setup and Configure System Log Server

In System log section, the newer log event activities will automatically overwrite the older system log events in the MXConnect 4G/LTE series. Setup the System Log Server to store and synchronize all event logs in the MXConnect 4G/LTE router to an external Syslog Server.

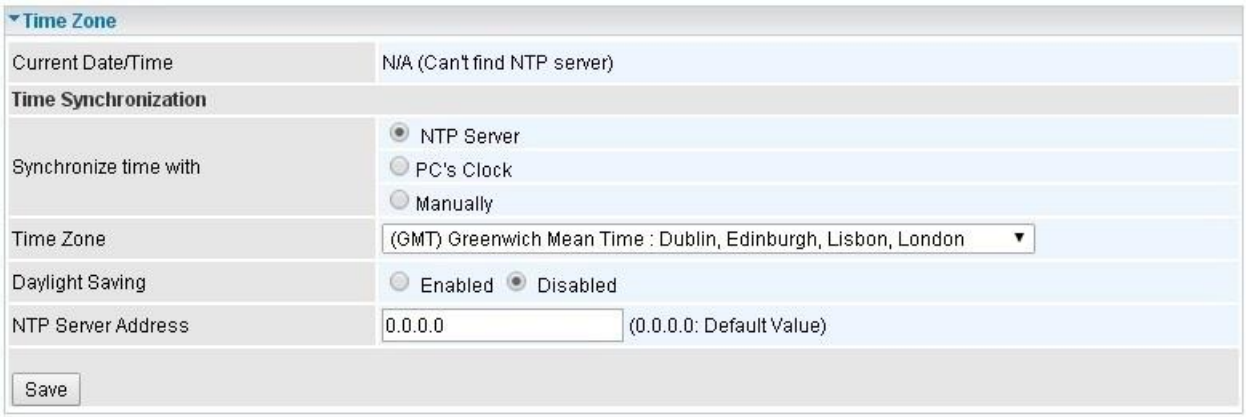
To setup a remote Syslog Server, go to ***Configuration >> Advanced Setup >> Remote System Log***



Step 8: Configure NTP Server / Internet Time

With default, the MXConnect 4G/LTE router does not have the correct local time and date, instead, here are several options to setup, maintain, and configure current local time/date in the device – synchronize time with **NTP Server**, **PC's Clock**, or **Manually**.

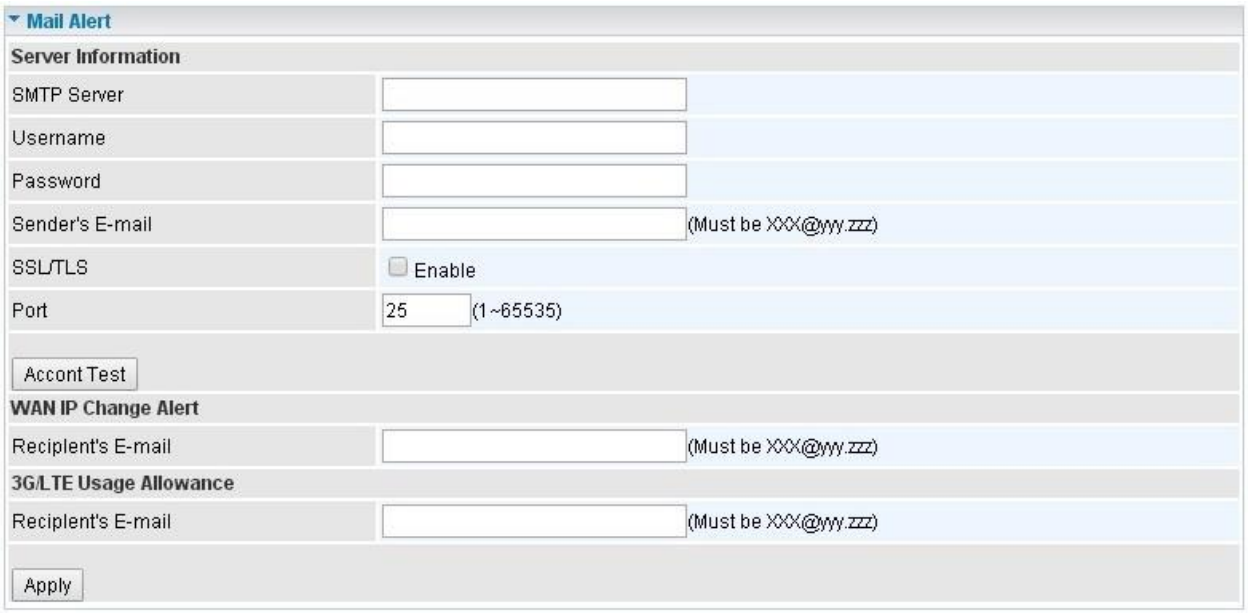
To configure Network Time Server/Protocol, go to ***Configuration >> Maintenance >> Time Zone***



Step 9: Setup Email Alerts

Mail alert is designed to keep system administrator or other relevant personnel alerted of any unexpected events that might have occurred to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.

To setup an E-mail account to send out alters or notification e-mail, go to ***Configuration >> Advanced Setup >> Mail Alert***



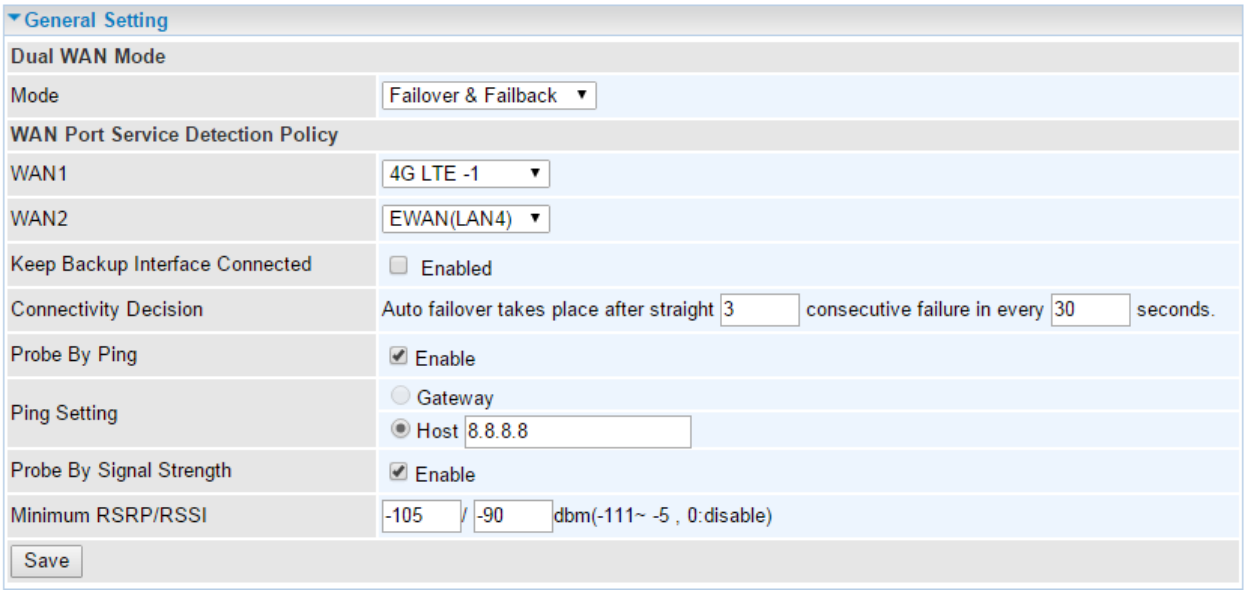
Step 10: Configure WAN Failover and Load Balance

With two independent Internet connection connected concurrently, MXConnect Series offers a reliable Internet connectivity and maximize bandwidth utilization for critical applications delivery.

WAN Failover and Failback: Auto failover/failback ensures always-online network connectivity. When primary WAN link (WAN1) fails, all traffic will switch over to the backup WAN (WAN2) seamlessly.

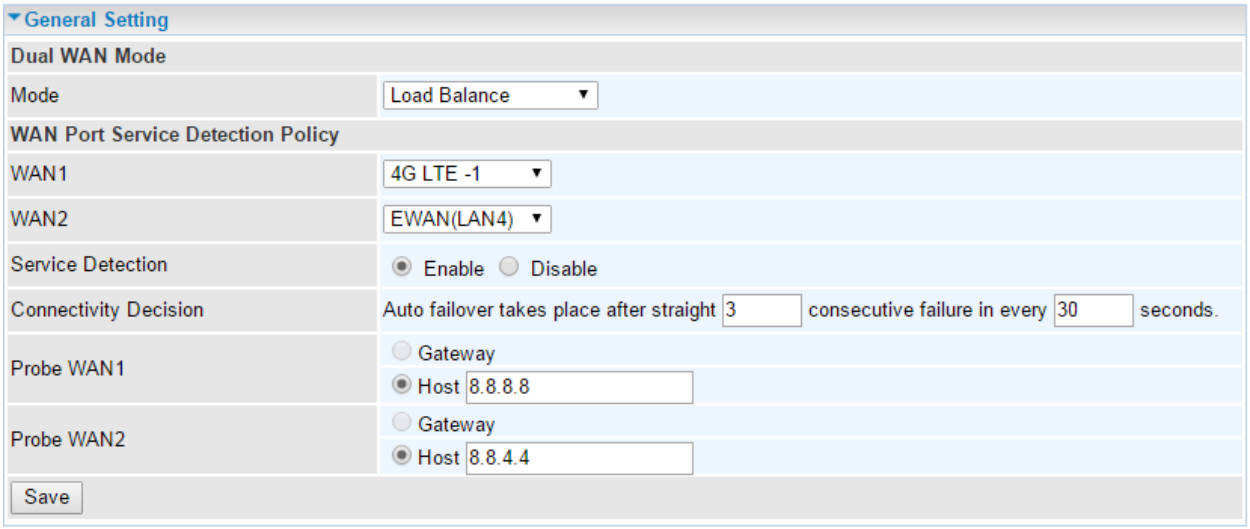
Again, when the primary link is restored, traffic will be handled over from WAN2 to WAN1.

To configure WAN Failover and Failback, go to ***Configuration >> Dual WAN >> General Setting >>*** *Select* ***Failover & Failback*** *mode*



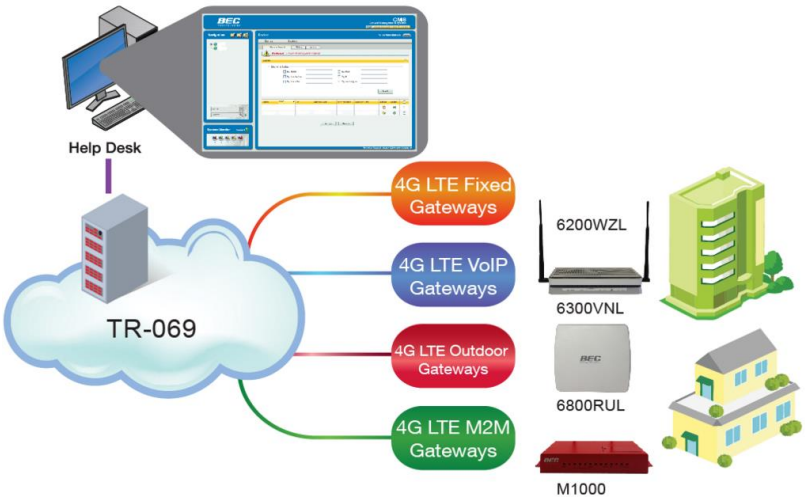
WAN Load Balance: Load Balance offers **Aggregate the bandwidth** of two links by forwarding packets to the low-traffic link for better performance. And **Traffic redirect** when one of the WANs becomes inactive, all traffic will be forwarded to the other path/WAN and Load Balance will get terminated until the other WAN comes back up.

To configure WAN Load Balancing, go to ***Configuration >> Dual WAN >> General Setting >>*** *Select* ***Load Balance*** *mode*



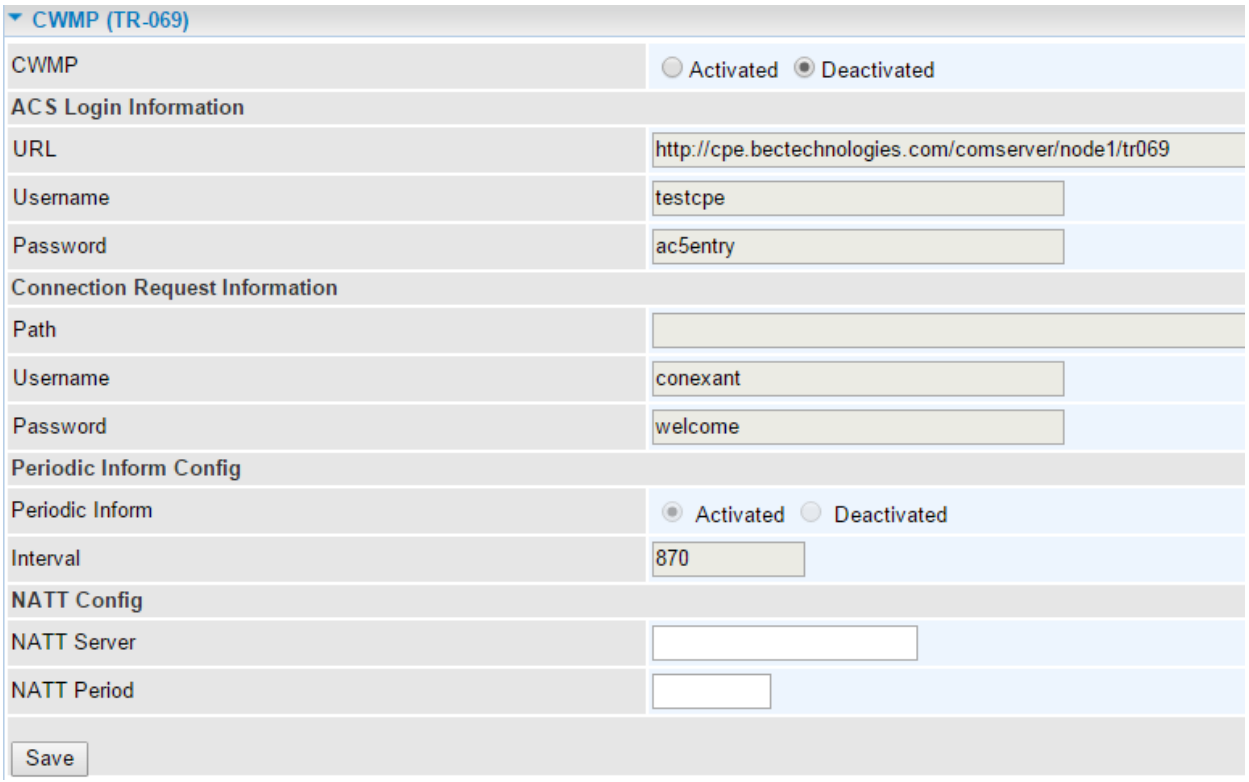
Step 11: Setup CWMP (TR-069) for BEC LCMS Management

BEC's LTE Remote Management System (LCMS) is a centralized management platform designed to offer Service Providers remote access and management of BEC LTE Fixed routers, VoIP gateways, Outdoor LTE routers and M2M modem multi-service gateways. With its comprehensive management tools, the BEC LCMS can minimize deployment, lower support expenses and maximize the operational efficiency and profitability for a service provider.



Setup the CWMP, short for CPE WAN Management Protocol also known as TR069, in the BEC MXConnect 4G/LTE router to establish a connection with BEC LCMS for automatic configuration and management over the air.

To enable CWMP (TR-069) to establish a connection with BEC Cloud, go to ***Configuration >> Access Management >> CWMP (TR-069)***



Conclusion

Since the inception of the Payment Card Industry Data Security Standard (PCI DSS) merchants and service providers that are involved in processing credit card payments have been laboring to understand, implement, and comply with its guidelines, now at Version 3.1.
By following the recommendations in this white paper, BEC Technologies customers can enhance the security of their networks and protect against inherent threats while making them more compliant with a PCI DSS Specifications.

For more information on PCI DSS Standard and Requirements, visit
https://www.pcisecuritystandards.org

About BEC Technologies, Inc.

BEC Technologies is a leading developer and manufacturer of 3G, 4G/LTE wireless broadband networking solutions for mobile operators, residential, enterprise and Industrial markets. BEC's comprehensive product portfolio of solutions incorporate Fixed Data Routers, VoIP/VoLTE Gateways, Rugged Outdoor, Industrial/M2M Connectivity, Public Safety, Fleet/Telematics and Cloud based remote device management. Our solutions are designed for high availability, reliability and secure connectivity all backed up with class-leading technical service and support.

Managing Millions of Connected Devices Worldwide, BEC is driving the global transformation to a connected world! For more information, please visit www.bectechnologies.net or follow us on Twitter @BECTechnologies.