GE MDS Orbit MCR™
Applications Guideline
Via: VPN / IPsec / Port Forwarding / Static (1:1) NAT

APPLICATION NOTES

The goal of this document is to provide Orbit MCR users with the means to setup networks involving port forwarding or IPsec VPN Tunnels. The following examples are meant to assist in the setting up of these networks or provide insight into the available configurations that the Orbit MCR can provide. Each example will provide a pictorial representation and bulleted information that will highlight the necessary parameters that need to be set in order to achieve the setup.

These examples are designed for use via the Cell Interface. A properly provisioned SIM card will need to be purchased from a cellular provider and installed before Cell configurations can be attempted.

Many of these applications use a 2E1S (2 Ethernet, 1 Serial) hardware configuration.
Units with a 1E2S (1 Ethernet, 2 Serial) hardware configuration may require an additional external Ethernet Switch or the use of Wi-Fi.

For additional support or additional knowledge on these setups;

GEMDS Website: http://www.gedigitalenergy.com/Communications/	
Application Notes on the Orbit MCR Website: GEMDS Orbit Application Notes: Topics such as x.509 Certificate Generation, IPsec VPN with RSA Certificates	
Technical Manual on the Orbit MCR website; publication 05-6632A01.	
GEMDS Learning and Development YouTube Channel	

Contact GEMDS directly:

GE Learning and Development Email: training.multilin@ge.com **905-927-7070**	**Technical Support** GEMDS.techsupport@GE.com **1-800-474-0964 Option #3**

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).[1]

Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at Application layer. Hence, only IPsec protects any application traffics over an IP network. Applications can be automatically secured by its IPsec at the IP layer. Without IPsec, the protocols of TLS/SSL must be inserted under each of applications for protection.

Internet Key Exchange (IKE) Before secured data can be exchanged; a security agreement between two computers must be established. In this security agreement, called a security association (SA), both agree on how to exchange and protect information**.**

To build this agreement between the two computers, the Internet Engineering Task Force (IETF) has established a standard method of security association and key exchange resolution named Internet Key Exchange (IKE) which:

- Centralizes security association management, reducing connection time.
- Generates and manages shared, secret keys that are used to secure the information.

This process not only protects communication between computers, it also protects remote computers that request secure access to a corporate network. In addition, this process works whenever the negotiation for the final destination computer (endpoint) is performed by a security gateway.

Port forwarding is a name given to the combined technique of:

1. Translating the address or port number of a packet to a new destination
2. Possibly accepting such packet(s) in a packet filter (firewall)
3. Forwarding the packet according to the routing table.

The destination may be a predetermined network port (assuming protocols like TCP and UDP, though the process is not limited to these) on a host within a NAT-masqueraded, typically private network, based on the port number on which it was received at the gateway from the originating host.

The technique is used to permit communications by external hosts with services provided within a private local area network

Network address translation (**NAT**) is a methodology of modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another. **1:1 NAT** is a method so devices within the same Subnet (or overlapping Subnets) may establish a secure connection.

Virtual private network (**VPN**) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it is directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions.

Table of Contents

Contents

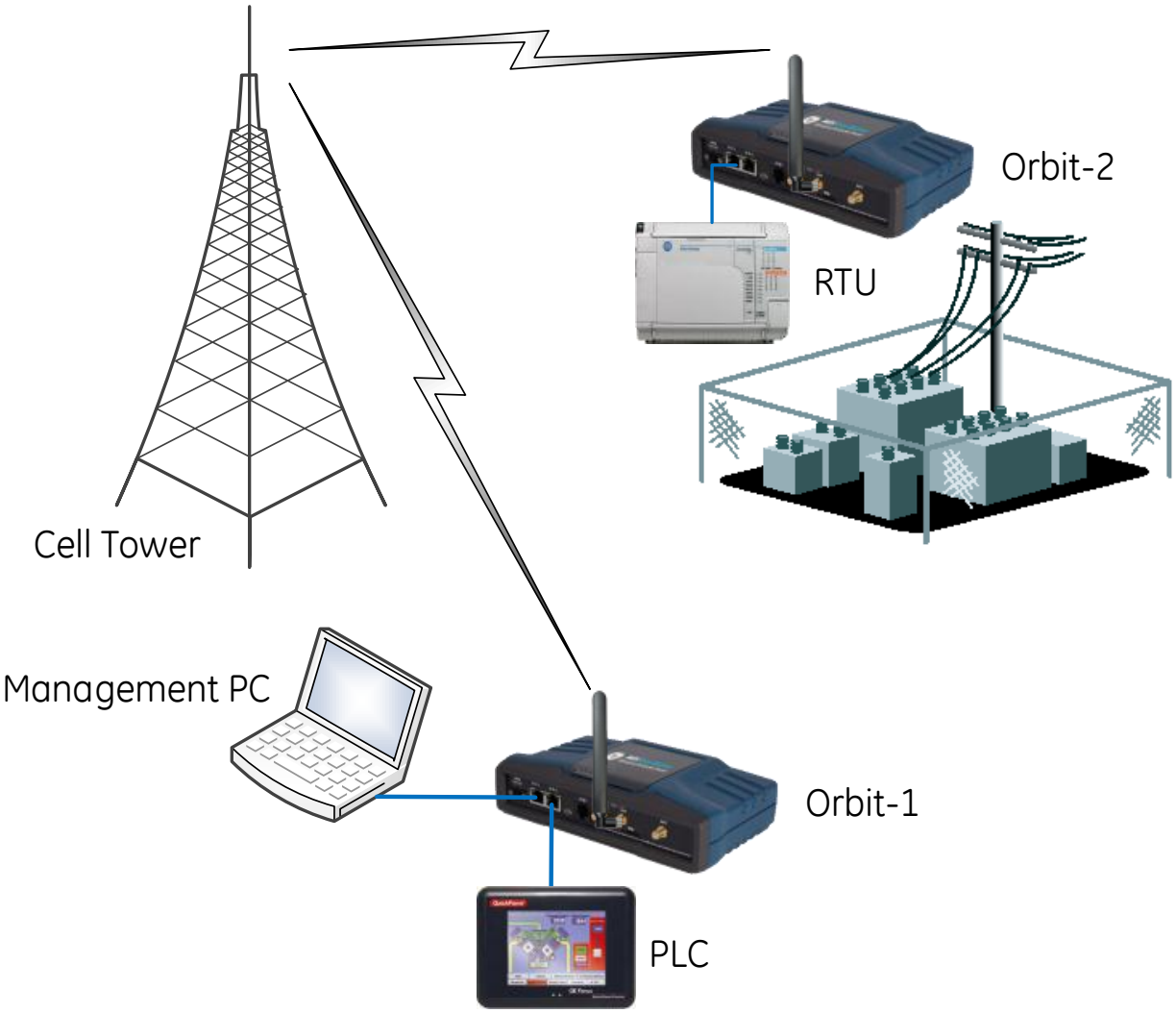
YouTube Channel Videos to reference

(w/mouse: Ctrl + Click to follow the link)

Orbit™ MCR | Device Management v1.0	
Orbit™ MCR | Static IP Configuration v1.2	
Orbit™ MCR 4G | Adding and Deleting Firewall Rules	
Orbit MCR I Network Address Translation NAT	

Orbit MCR™ I Cellular Interface Firewall and Nat Verification	
Orbit™ MCR | Port Forwarding	
Orbit MCR IPsec Windows IKEv2 Video	
Refer to IPsec Videos	
Static NAT	

Orbit to Orbit via Cell with Port Forwarding



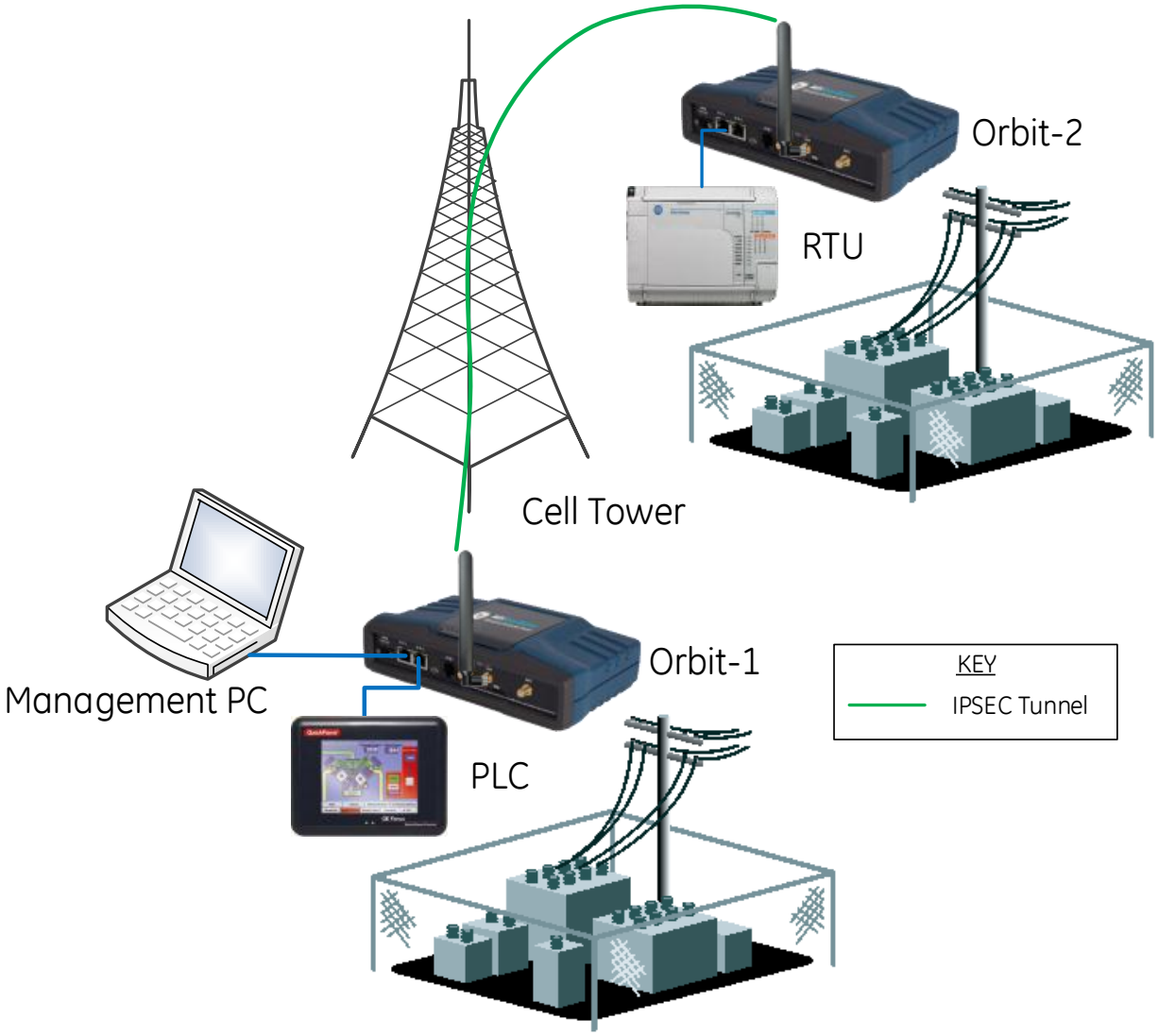
- This configuration allows a PLC connected to Orbit-1 to communicate with the RTU on the "LAN" side of Orbit-2.
- This also allows a Management PC to communicate with Orbit-1, Orbit-2, and the RTU through port forwarding rules.

The following must be configured to both Orbit-1 and Orbit-2;

Orbit to Orbit via Cell w/Port Forwarding

Configuration Steps	Manual Section	Single topic YouTube Channel Videos
Configure LAN side of Orbit to meet IP address requirements	**Bridging**	Orbit™ MCR | Static IP Configuration
Configure Firewall Service Rules:	**Packet Filtering (Firewall)**	Orbit™ MCR 4G | Adding and Deleting Firewall Rules
It is recommended to modify IN_UNTRUSTED and OUT_UNTRUSTED		
Configure LOCAL-NETS:		Orbit™ MCR 1 Cellular Interface Firewall and Nat Verification
LOCAL-NETS must match Local Subnet(s)		
Configure NAT to:	**Source Network Address Translation(NAT)**	Orbit MCR 1 Network Address Translation NAT
Change Source Address for outgoing Cell traffic		
Configure Port Forwarding Rules	**Destination NAT**	Orbit™ MCR | Port Forwarding
Configure Cell to use:	**Cell**	Orbit MCR™ I Cellular Interface Firewall and Nat Verification
Correct Firewall Service Rules for INPUT and OUTPUT Correct Firewall Service NAT Rules (Including Source Rule and Destination Rule)		

Orbit to Orbit via Cell with IPsec (1 Tunnel)

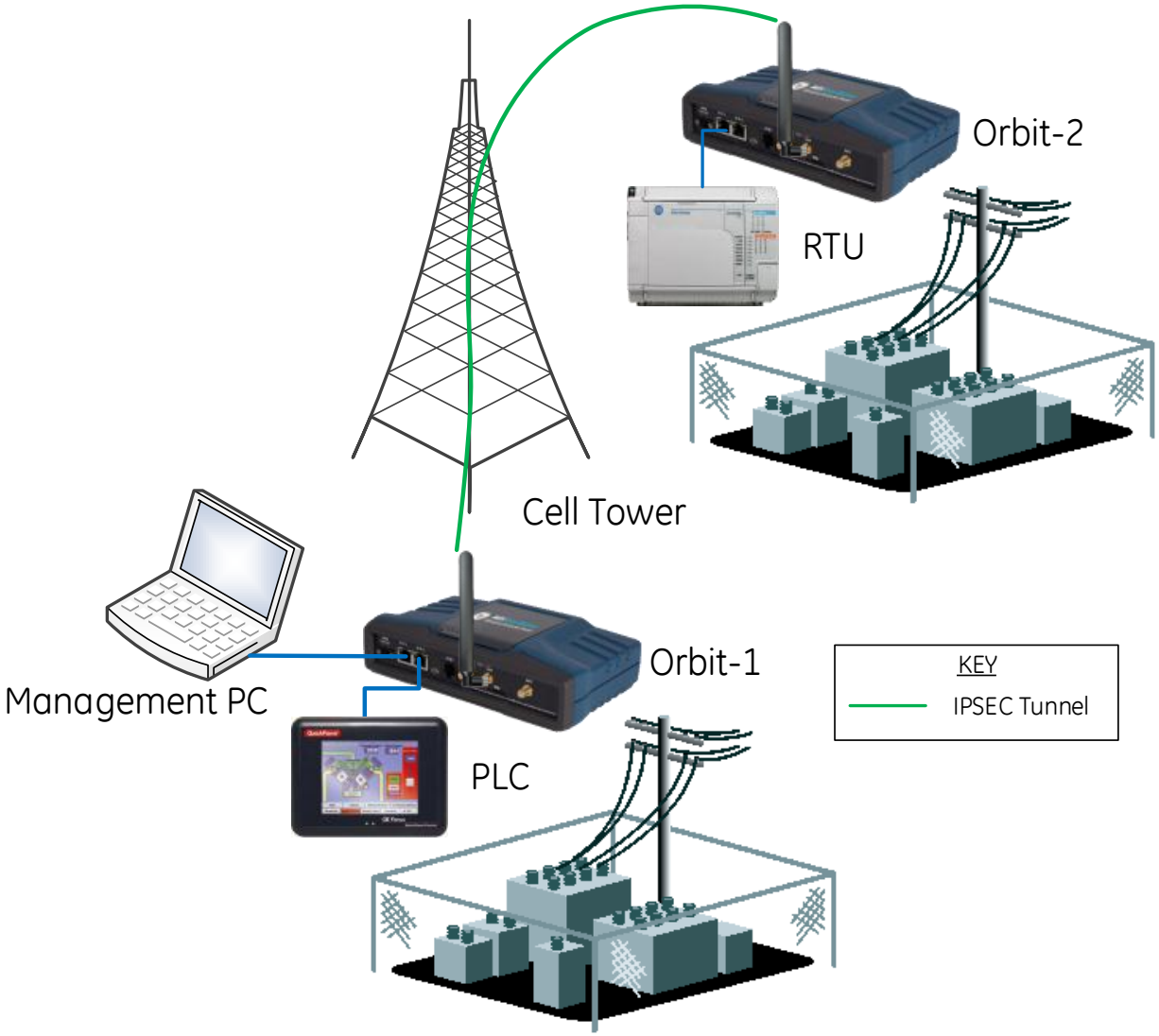


- This configuration allows a PLC connected to Orbit-1 to communicate with the RTU on the "LAN" side of Orbit-2 through a secure IPsec VPN Tunnel.
- This also allows a Management PC to communicate with Orbit-1, Orbit-2, and the RTU through a secure IPsec VPN Tunnel.

Orbit to Orbit via Cell w/IPsec (1 Tunnel)

Configuration Steps	Manual Section	Single topic YouTube Channel Videos
Configure LAN side of Orbit to meet IP address requirements	**Bridging**	Orbit™ MCR | Static IP Configuration
Configure Firewall Service Rules:	**Packet Filtering (Firewall)**	Orbit™ MCR 4G | Adding and Deleting Firewall Rules
It is recommended to modify IN_UNTRUSTED and OUT_UNTRUSTED		
Configure LOCAL-NETS:		Orbit™ MCR l Cellular Interface Firewall and Nat Verification
LOCAL-NETS must match Local Subnet(s) REMOTE-NETS must match Remote Subnet(s)		
Configure IKE:	**VPN**	**Refer to IPsec Videos**
Allow IKE Destination Traffic IN Allow IPsec Traffic IN Allow IPsec Traffic OUT		
Configure NAT to:	**Source Network Address Translation(NAT)**	Orbit MCR l Network Address Translation NAT
Change Source Address for outgoing Cell traffic Have no effect on IPsec Traffic ('not' rule within NAT)		
Configure Cell to use:	**Cell**	Orbit MCR™ l Cellular Interface Verification
Correct Firewall Service Rules for INPUT and OUTPUT Correct Firewall Service NAT Rule		
Configure IPsec Service:	**VPN & Certificate Management and 802.1X Authentication**	Orbit™ MCR | IPsec Command Line
Need to Configure: IKE Policy IKE Peer IPsec Policy IPsec Connection		

Orbit to Orbit via Cell with IPsec (1 Tunnel) 1 to 1 NAT

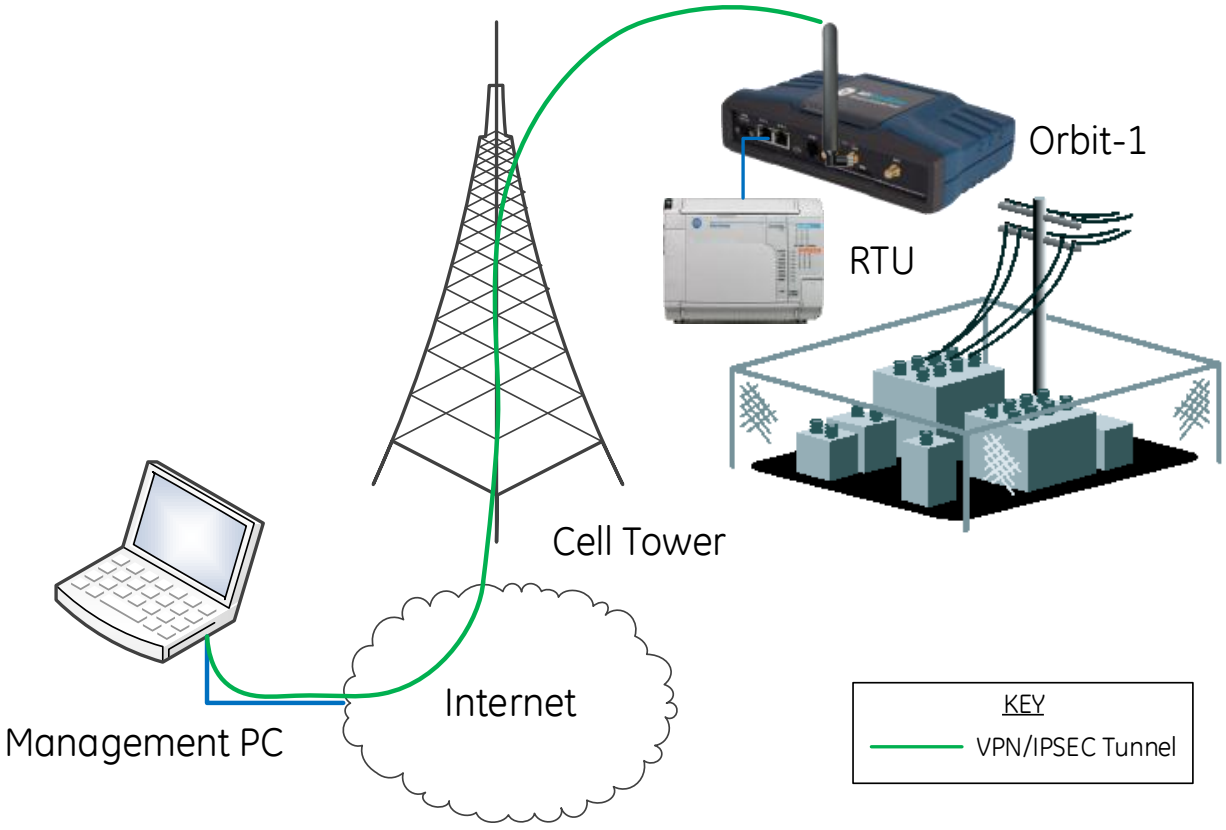


- This configuration allows a PLC connected to Orbit-1 to communicate with the RTU on the "LAN" side of Orbit-2 through a secure IPsec VPN Tunnel.
- This also allows a Management PC to communicate with Orbit-1, Orbit-2, and the RTU through a secure IPsec VPN Tunnel.
- This configuration also allows both sides of the tunnel to have overlapping subnets.

Orbit to Orbit via Cell w/IPsec (1 Tunnel) 1 to 1 NAT

Configuration Steps	Manual Section	Single topic YouTube Channel Videos
Configure LAN side of Orbit to meet IP address requirements	**Bridging**	Orbit™ MCR | Static IP Configuration
Configure Firewall Service Rules:	**Firewall and NAT**	Orbit™ MCR 4G | Adding and Deleting Firewall Rules
It is recommended to modify IN_UNTRUSTED and OUT_UNTRUSTED		
Configure LOCAL-NETS:		Orbit™ MCR l Cellular Interface Firewall and Nat Verification
LOCAL-NETS must match Local Subnet(s) REMOTE-NETS must match Remote Subnet(s)		
Configure IKE:	**VPN**	**Refer to IPsec Videos**
Allow IKE Destination Traffic IN Allow IPsec Traffic IN Allow IPsec Traffic OUT		
Configure NAT to:	**Source Network Address Translation(NAT)**	Orbit™ MCR I Network Address Translation NAT
Change Source Address for outgoing Cell traffic Have no effect on IPsec Traffic ('not' rule within NAT)		
Configure Cell to use:	**Cell**	Orbit™ MCR I Cellular Interface Verification
Correct Firewall Service Rules for INPUT and OUTPUT Correct Firewall Service NAT Rule		
Configure IPsec Service:	**VPN & Certificate Management and 802.1X Authentication**	Orbit™ MCR | IPsec Command Line
Need to Configure: IKE Policy IKE Peer IPsec Policy IPsec Connection		
Static NAT	**Static NAT**	**Orbit™ MCR | Static NAT over IPsec VPN**

PC to Orbit via Cell with IPsec (1 Tunnel) VPN

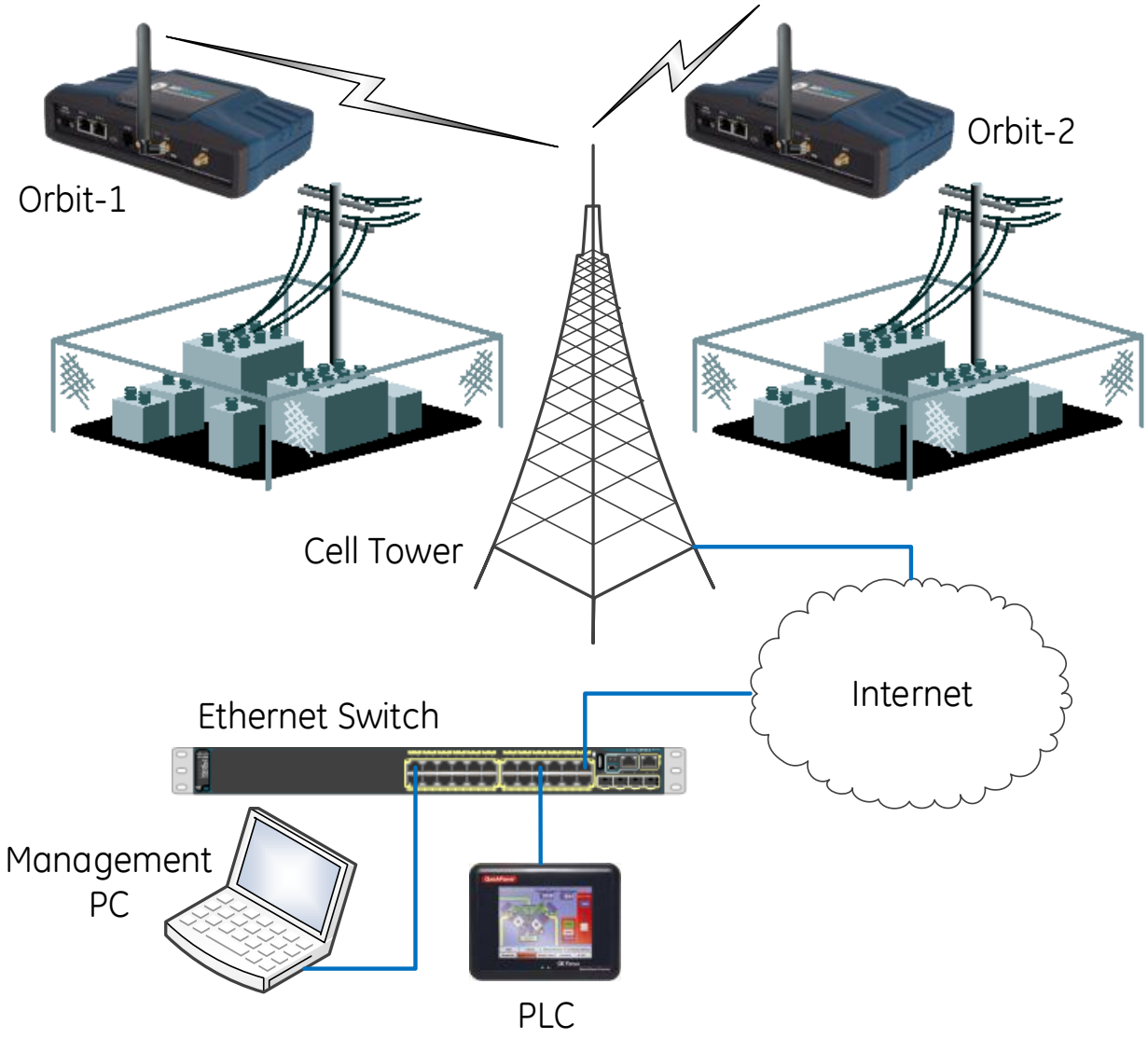


- This configuration allows a PC to connect to both the Orbit and any devices on the “LAN” side of the Orbit.
- This can be used in conjunction with other existing IPsec Tunnels.

PC to Orbit via Cell w/IPsec (1 Tunnel) VPN

Configuration Steps	Manual Section	Single topic YouTube Channel Videos
Configure LAN side of Orbit to meet IP address requirements	**Bridging**	Orbit™ MCR | Static IP Configuration
Configure Firewall Service Rules:	**Packet Filtering (Firewall)**	Orbit™ MCR 4G | Adding and Deleting Firewall Rules
It is recommended to modify IN_UNTRUSTED and OUT_UNTRUSTED		
Configure LOCAL-NETS:		Orbit™ MCR l Cellular Interface Firewall and Nat Verification
LOCAL-NETS must match Local Subnet(s) REMOTE-NETS must match Remote Subnet(s)		
Configure IKE:	**VPN**	**Refer to IPsec Videos**
Allow IKE Destination Traffic IN Allow IPsec Traffic IN Allow IPsec Traffic OUT		
Configure Cell to use:	**Cell**	Orbit™ MCR l Cellular Interface Verification
Correct Firewall Service Rules for INPUT and OUTPUT Correct Firewall Service NAT Rule		
Configure IPsec Service:	**VPN & Certificate Management and 802.1X Authentication**	Orbit™ MCR | IPsec Command Line
Need to Configure: IKE Policy IKE Peer IPsec Policy IPsec Connection		
Install Computer Certificates on PC		
Configure IKEv2 VPN Connection on PC (Win 7)		**Orbit™ MCR | IPsec Windows IKEv2 Video**

PLC to Orbit via Cell via Port Forwarding Rules

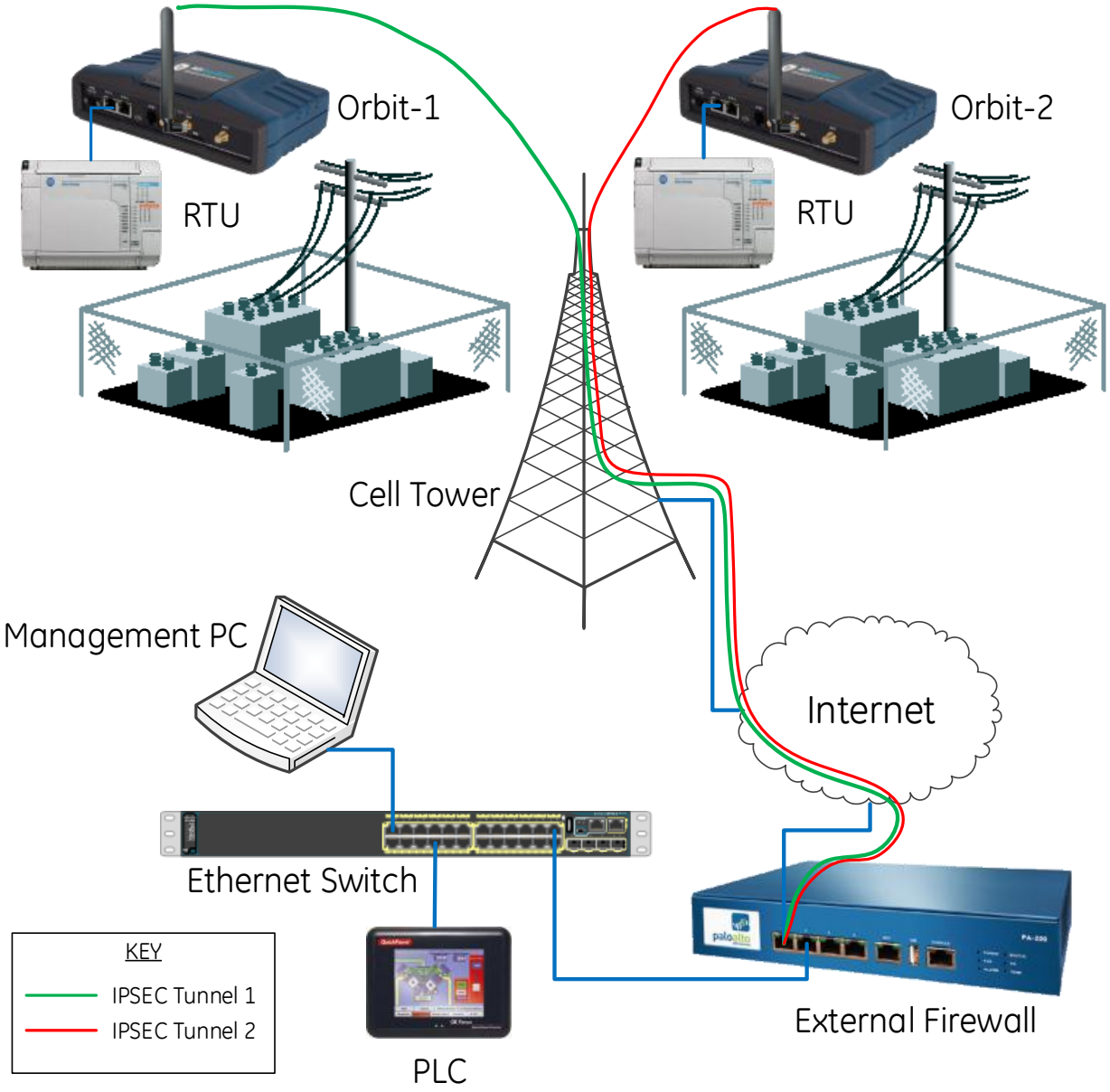


- This configuration allows a PLC connected to the internet to communicate with an RTU on the "LAN" side of the Orbit(s) through port forwarding rules.
- This also allows a Management PC to communicate with Orbit-1, Orbit-2, and the RTUs through port forwarding rules.

PLC to Orbit via Cell w/Port Forwarding Rules

Configuration Steps	Manual Section	Single topic YouTube Channel Videos
Configure LAN side of Orbit to meet IP address requirements	**Bridging**	Orbit™ MCR | Static IP Configuration
Configure Firewall Service Rules:	**Packet Filtering (Firewall)**	Orbit™ MCR 4G | Adding and Deleting Firewall Rules
It is recommended to modify IN_UNTRUSTED and OUT_UNTRUSTED		
Configure LOCAL-NETS:		Orbit™ MCR l Cellular Interface Firewall and Nat Verification
LOCAL-NETS must match Local Subnet(s)		
Configure NAT to:	**Source Network Address Translation(NAT)**	Orbit™ MCR l Network Address Translation NAT
Change Source Address for outgoing Cell traffic		
Configure Port Forwarding Rules	**Destination NAT**	Orbit™ MCR | Port Forwarding
Configure Cell to use:	**Cell**	Orbit™ MCR l Cellular Interface Verification
Correct Firewall Service Rules for INPUT and OUTPUT Correct Firewall Service NAT Rules (Including Source Rule and Destination Rule)		

External Firewall to Orbit via Cell w/IPsec (2 Tunnels)

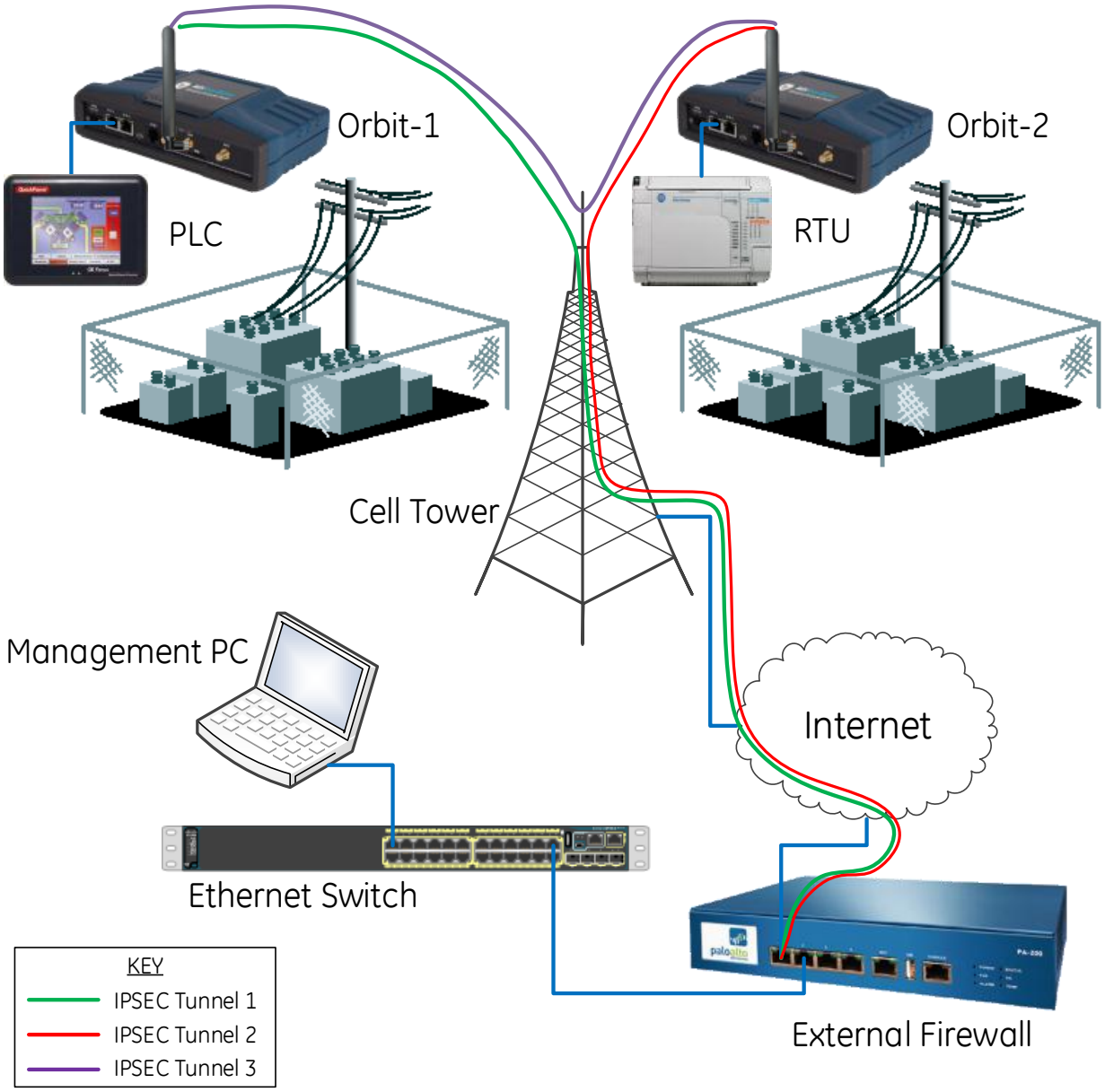


The following must be configured to both Orbit-1 and Orbit-2;

External Firewall to Orbit via Cell w/IPsec (2 Tunnels)

Configuration Steps	Manual Section	Single topic YouTube Channel Videos
Configure LAN side of Orbit to meet IP address requirements	**Bridging**	Orbit™ MCR | Static IP Configuration
Configure Firewall Service Rules:	**Packet Filtering (Firewall)**	Orbit™ MCR 4G | Adding and Deleting Firewall Rules
It is recommended to modify IN_UNTRUSTED and OUT_UNTRUSTED		
Configure LOCAL-NETS:		Orbit™ MCR I Cellular Interface Firewall and Nat Verification
LOCAL-NETS must match Local Subnet(s) REMOTE-NETS must match Remote Subnet(s)		
Configure IKE:	**VPN**	**Refer to IPsec Videos**
Allow IKE Destination Traffic IN Allow IPsec Traffic IN Allow IPsec Traffic OUT		
Configure NAT to:	**Source Network Address Translation(NAT)**	Orbit™ MCR I Network Address Translation NAT
Change Source Address for Public Traffic Have no effect on IPsec Traffic ('not' rule within NAT)		
Configure Cell to use:	**Cell**	Orbit™ MCR I Cellular Interface Verification
Correct Firewall Service Rules for INPUT and OUTPUT Correct Firewall Service NAT Rule		
Configure IPsec Service:	**VPN & Certificate Management and 802.1X Authentication**	Orbit™ MCR | IPsec Command Line
Need to Configure: IKE Policy IKE Peers (2 Peers MUST be configured 1/Tunnel) IPsec Policy IPsec Connections (2 Connections MUST be configured 1/Tunnel)		

External Firewall to ORBIT via Cell w/IPsec (3 Tunnels)

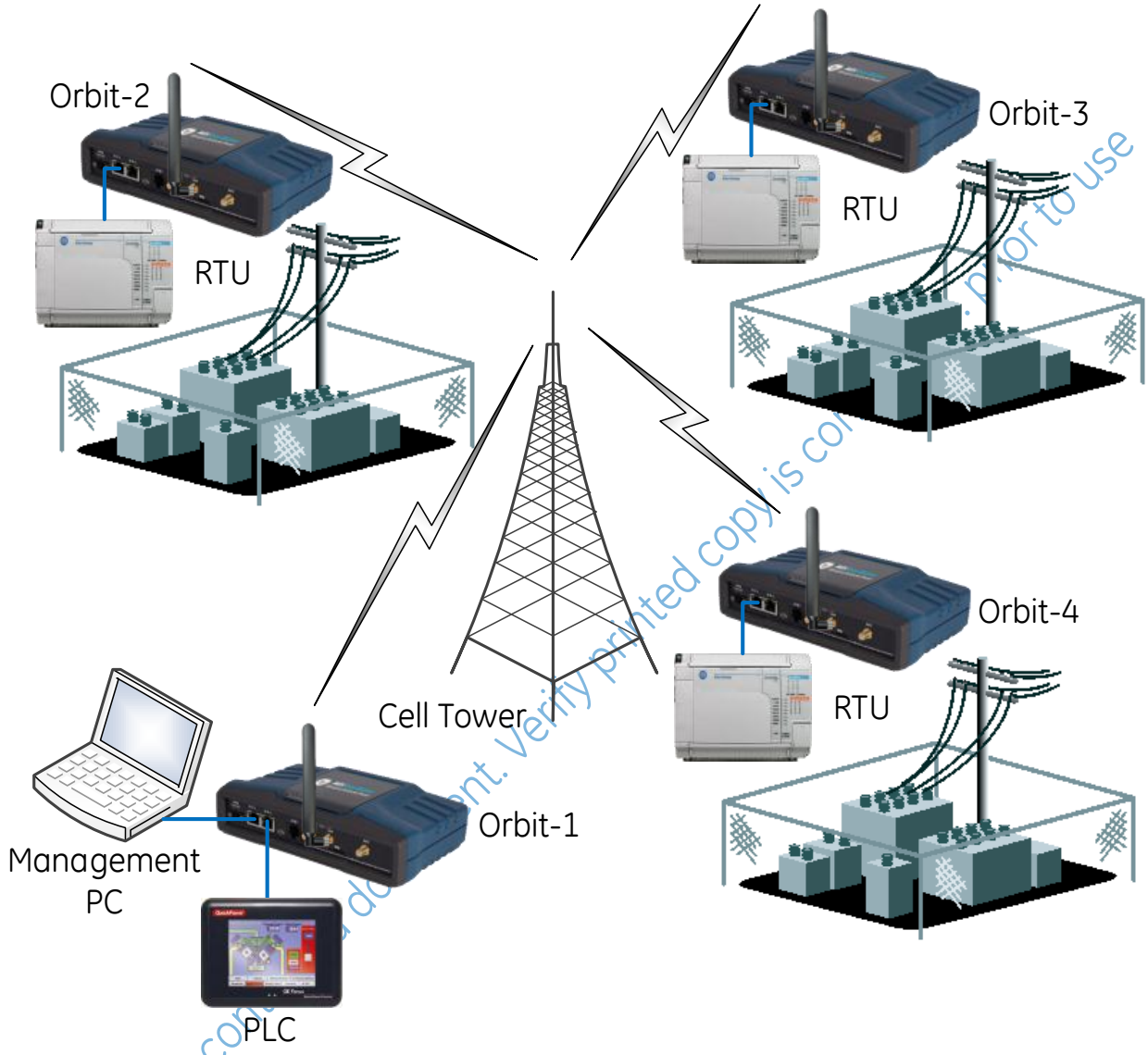


External Firewall to ORBIT via Cell w/IPsec (3 Tunnels)

Configuration Steps	Manual Section	Single topic YouTube Channel Videos
Configure LAN side of Orbit to meet IP address requirements	**Bridging**	Orbit™ MCR | Static IP Configuration
Configure Firewall Service Rules:	**Packet Filtering (Firewall)**	Orbit™ MCR 4G | Adding and Deleting Firewall Rules
It is recommended to modify IN_UNTRUSTED and OUT_UNTRUSTED		
Configure LOCAL-NETS:		Orbit™ MCR I Cellular Interface Firewall and Nat Verification
LOCAL-NETS must match Local Subnet(s) REMOTE-NETS must match Remote Subnet(s)		
Configure IKE:	**VPN**	**Refer to IPsec Videos**
Allow IKE Destination Traffic IN Allow IPsec Traffic IN Allow IPsec Traffic OUT		
Configure NAT to:	**Source Network Address Translation(NAT)**	Orbit™ MCR I Network Address Translation NAT
Change Source Address for Public Traffic Have no effect on IPsec Traffic ('not' rule within NAT)		
Configure Cell to use:	**Cell**	Orbit™ MCR I Cellular Interface Verification
Correct Firewall Service Rules for INPUT and OUTPUT Correct Firewall Service NAT Rule		
Configure IPsec Service:	**VPN & Certificate Management and 802.1X Authentication**	Orbit™ MCR | IPsec Command Line
Need to Configure: IKE Policy IKE Peers (3 Peers MUST be configured 1/Tunnel) IPsec Policy IPsec Connections (3 Connections MUST be configured 1/Tunnel)		

Electronically controlled document. Verify latest revision before use

Orbit to Multiple Orbits via Cell w/Port Forwarding



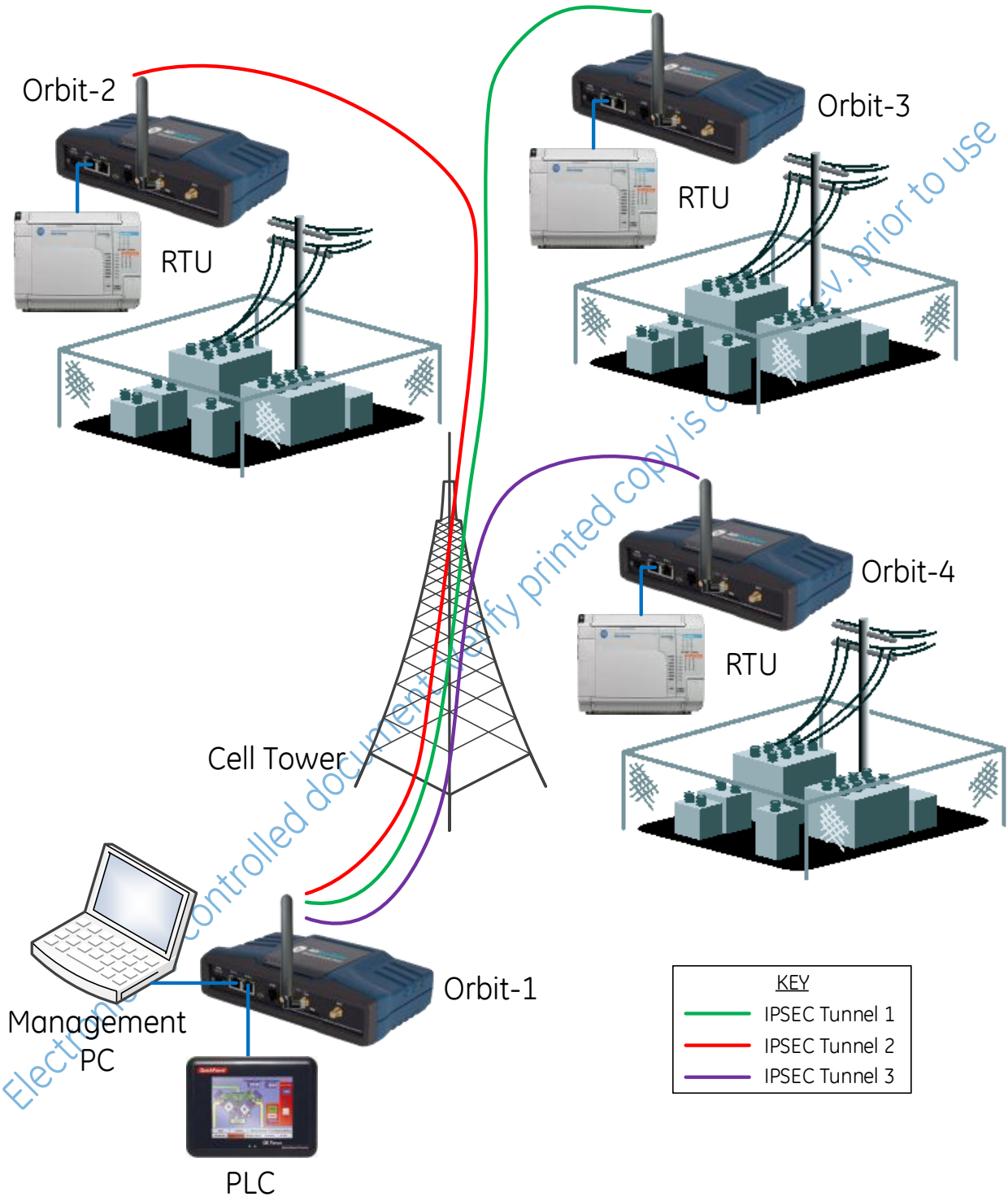
Electronically controlled document. Verify printed copy is current prior to use

Orbit to Multiple Orbits via Cell w/Port Forwarding

Configuration Steps	Manual Section	Single topic YouTube Channel Videos
Configure LAN side of Orbit to meet IP address requirements	**Bridging**	Orbit™ MCR | Static IP Configuration
Configure Firewall Service Rules:	**Packet Filtering (Firewall)**	Orbit™ MCR 4G | Adding and Deleting Firewall Rules
It is recommended to modify IN_UNTRUSTED and OUT_UNTRUSTED		
Configure LOCAL-NETS:		Orbit™ MCR I Cellular Interface Firewall and Nat Verification
LOCAL-NETS must match Local Subnet(s)		
Configure NAT to:	**Source Network Address Translation(NAT)**	Orbit™ MCR I Network Address Translation NAT
Change Source Address for outgoing Cell traffic		
Configure Port Forwarding Rules	**Destination NAT**	Orbit™ MCR | Port Forwarding
Configure Cell to use:	**Cell**	Orbit™ MCR I Cellular Interface Verification
Need to verify the correct Firewall Service Rules for: INPUT and OUTPUT Correct Firewall Service NAT Rules (Including Source Rule and Destination Rule)		

Electronically controlled document - Verify prior to use

Orbit to Multiple Orbits via Cell w/IPsec Tunnel(s)



Electronic controlled document. Verify printed copy is current rev. prior to use

Orbit to Multiple Orbits via Cell w/IPsec Tunnel(s)

Configuration Steps	Manual Section	Single topic YouTube Channel Videos
Configure LAN side of Orbit to meet IP address requirements **Configure Firewall Service Rules:**	**Packet Filtering (Firewall)**	Orbit™ MCR | Static IP Configuration Orbit™ MCR | Adding and Deleting Firewall Rules
It is recommended to modify IN_UNTRUSTED and OUT_UNTRUSTED		
Configure LOCAL-NETS:		Orbit™ MCR I Cellular Interface Firewall and Nat Verification
LOCAL-NETS must match Local Subnet(s) REMOTE-NETS must match Remote Subnet(s)		
Configure IKE:	**VPN**	**Refer to IPsec Videos**
Allow IKE Destination Traffic IN Allow IPsec Traffic IN Allow IPsec Traffic OUT		
Configure Cell to use:	**Cell**	Orbit™ MCR I Cellular Interface Verification
Correct Firewall Service Rules for INPUT and OUTPUT Correct Firewall Service NAT Rule		
Configure IPsec Service:	**VPN & Certificate Management and 802.1X Authentication**	Orbit™ MCR | IPsec Command Line
Need to Configure: IKE Policy IKE Peers (1 Peer MUST be configured for each Tunnel) IPsec Policy IPsec Connections (1 Connection MUST be configured for each Tunnel)		

Electronically controlled document

References:

1. Kent, S.; Atkinson, R. (November 1998). *IP Encapsulating Security Payload (ESP)*. IETF. RFC 2406.

Electronically controlled document. Verify printed copy is correct rev. prior to use

Digital Energy
MDS

GE MDS, LLC
175 Science Parkway
Rochester NY, 14610
Telephone: +1 585 242-9600
FAX: +1 585 242-9620
www.gemds.com