6330-MX / 6335-MX

accelerated™

Connected is Everything™

Table of Contents

Accelerated Notices

User Manual

Configuration Examples

Supplemental Information

Antenna Notes and Solutions

Automated Failover with Static WAN IP

MX- and SR-series routers will not failover to their cellular interface automatically when a static IP is set on the primary WAN.

Available Workaround: Enable Active Recovery. Click here for step-by-step guidance.

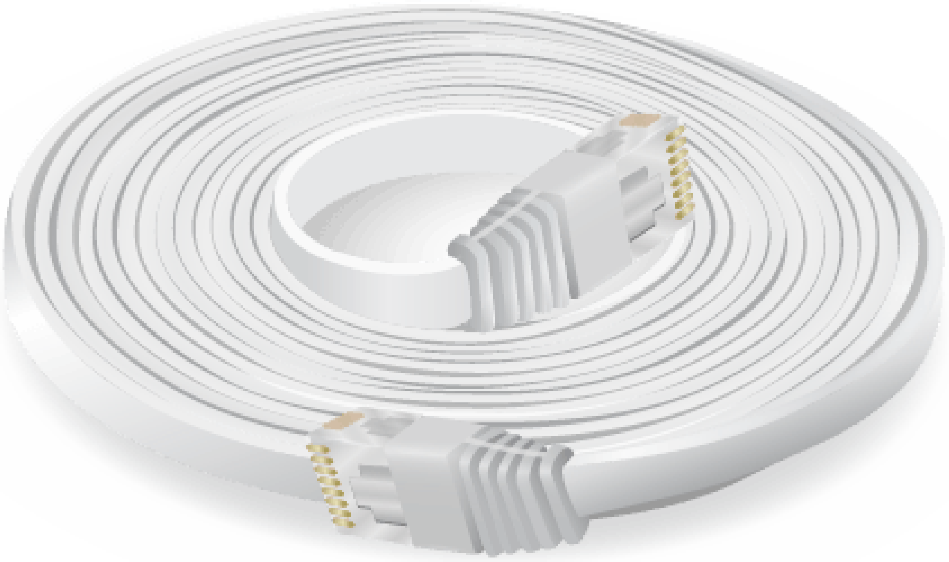
Firmware Fix: TBD

Package Contents

6330-MX Unit

Cellular Antennas (2x)

Ethernet Cable



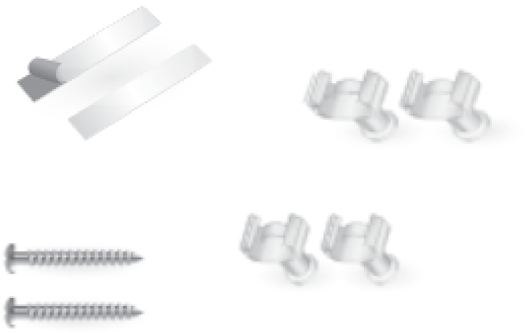
Power Supply Unit

Power-over-Ethernet (PoE) Injector

Temporary Battery Pack

Mounting Bracket

Mounting Accessories

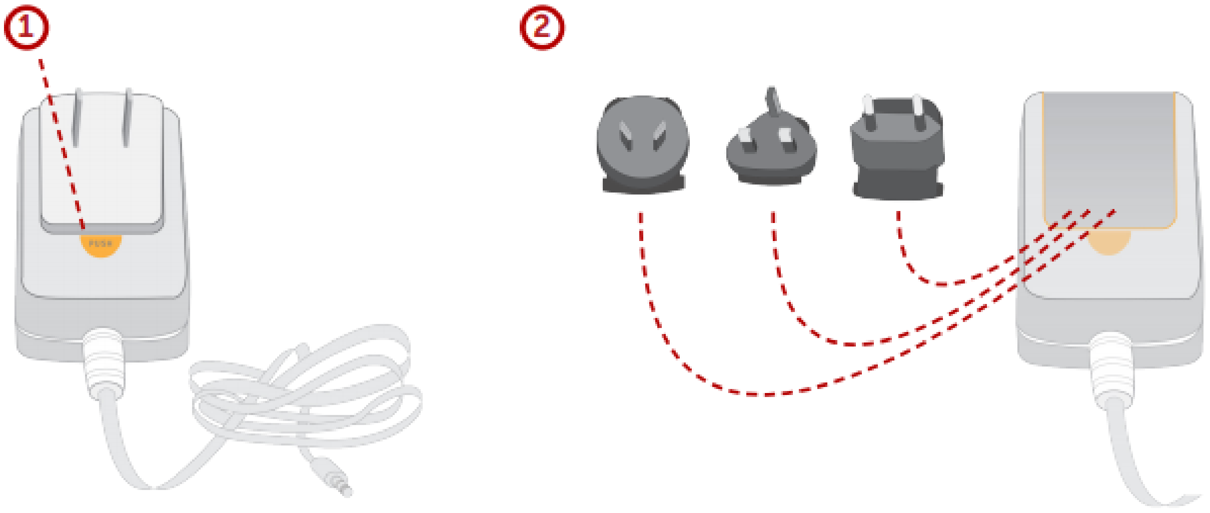


Exchanging Power Tips

The 6330-MX router may include four interchangeable plug tips that allows the Power Supply Unit (PSU) to operate in most countries. The PSU comes with the United States style plug installed.

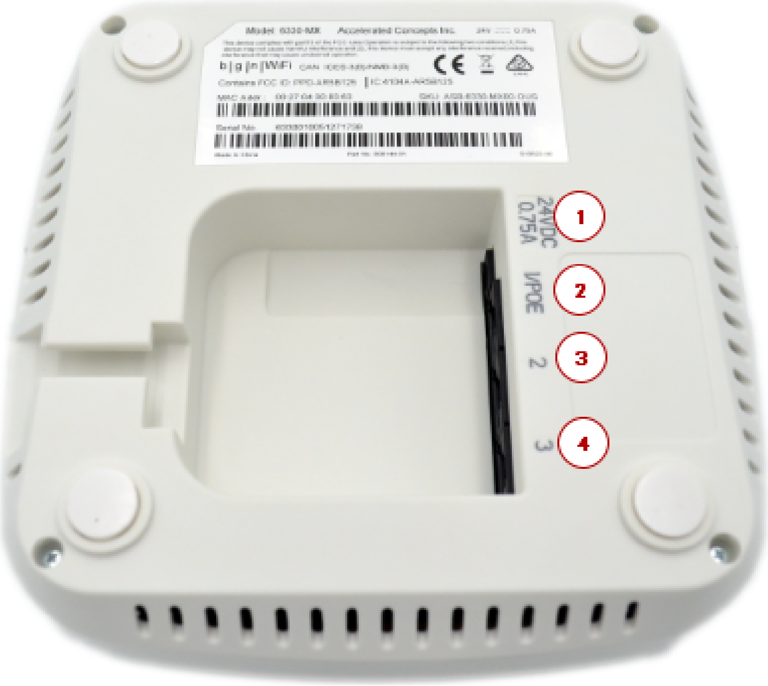
To change the plug tip:

- While holding down the "PUSH" button, slide the current plug tip forward.
- Pull off the attached plug tip.
- Slide the new tip down into place until it clicks.



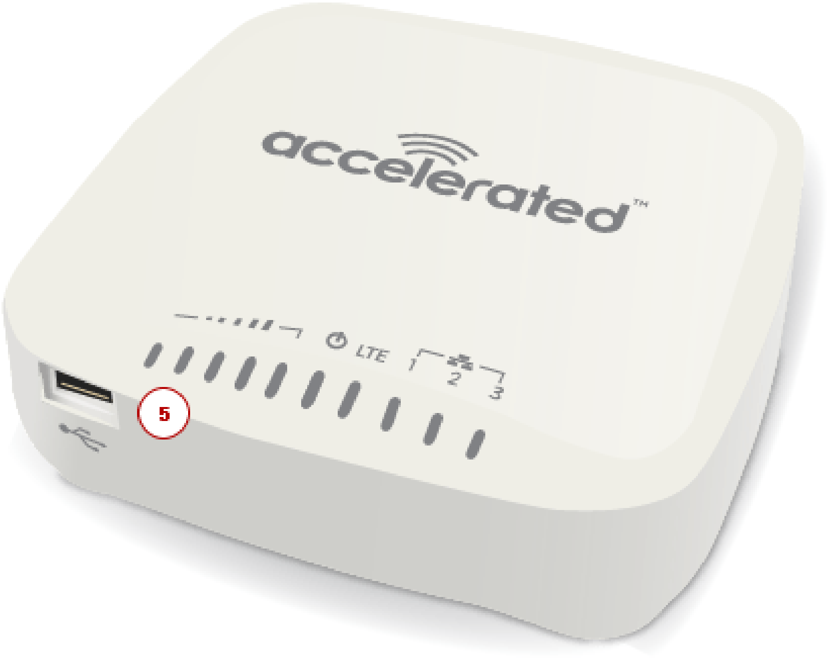
Hardware Features

Bottom of 6330-MX



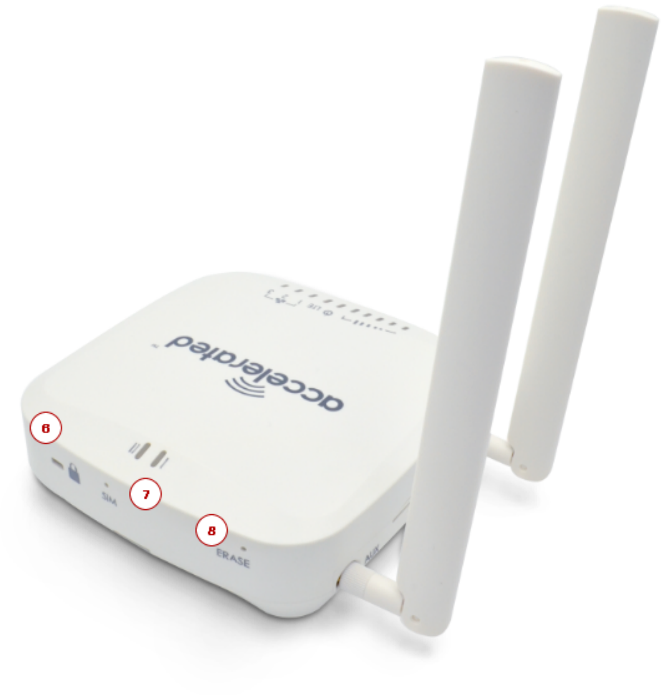
1. Power Socket
2. PoE Ethernet Port
3. LAN Ethernet Port
4. WAN Ethernet Port

Front of the 6330-MX



5. USB Port

Back of the 6330-MX



6. Lock Slot
7. Manual SIM Select Button
8. Erase Button

The **SIM button** is used to manually toggle between the two SIM slots included in the CM module. (For more information about the plug-in module, click here.)

The **ERASE button** will reset any changes made to the devices configuration (while preserving any firmware updates) if pressed *once*. Pressing the button twice in succession or holding it down for longer than a single press will clear the device's settings to factory defaults, including firmware.

Plug-In LTE Modem

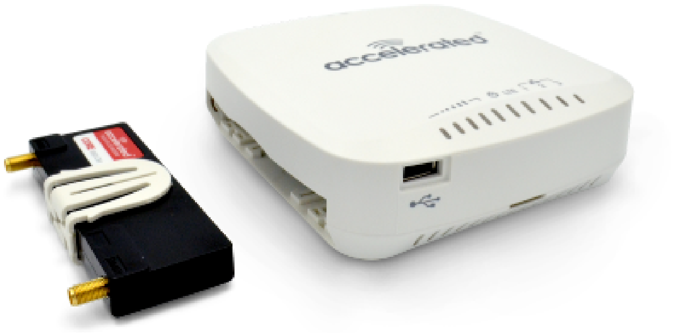
There is a label on the bottom of the MX-series router that indicates the plug-in modem's IMEI number.

(The modem is referred to as the 1002-CM.)

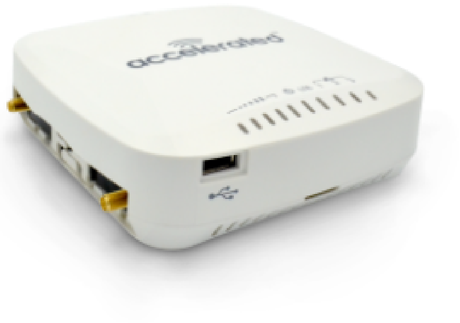
Verify this IMEI number is an exact match to that on the plug-in modem itself, as well as the label on the router's packaging.

1. Identify the SIM 1 and SIM 2 slots. If using only one SIM card, insert it into SIM 1. A second SIM may be inserted into slot SIM 2 for an alternate wireless carrier.
2. With the antennas' SMA connectors pointing outward, slide the 1002-CM modem into the SR-series router. A clicking sound will indicate it is properly inserted.

1



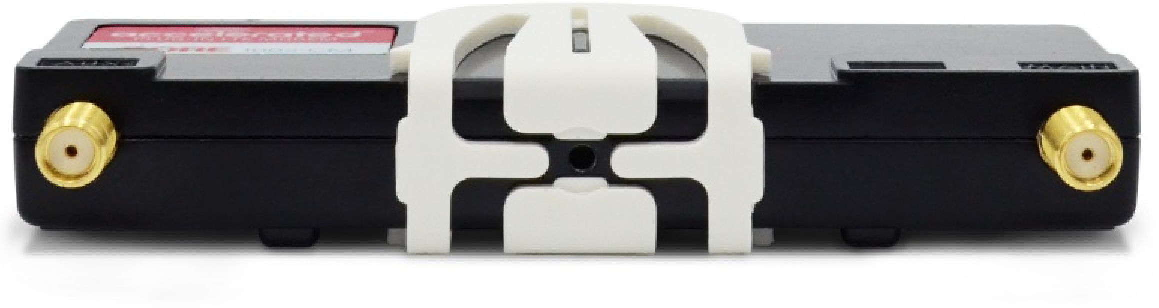
2



3. Slide the white plastic plate over the antenna connectors to cover the plug-in modem as shown; it will clip into place.
4. Affix the cellular antennas to the two connectors protruding from the device.

❗ Be sure to use the plate with the cut outs for the antenna connectors.

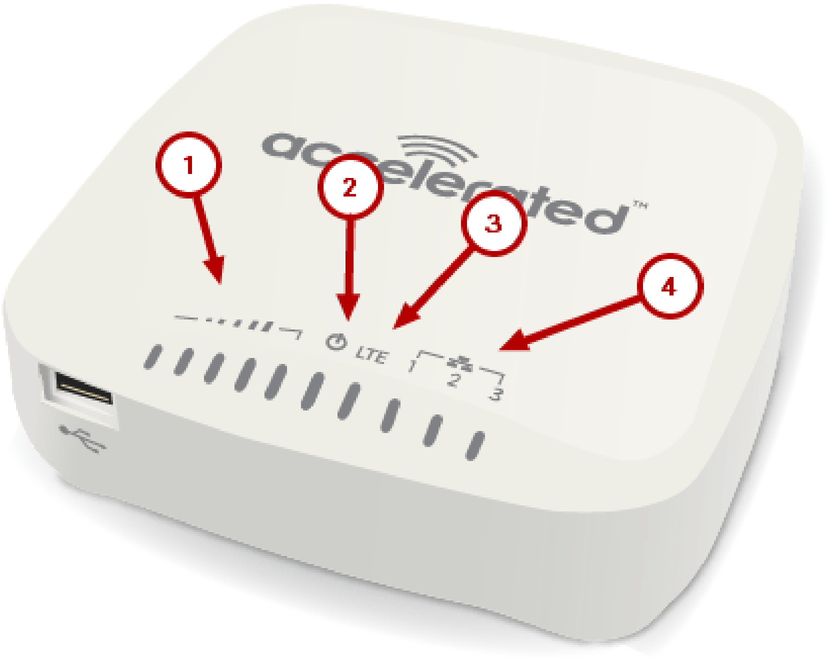
To remove the plug-in LTE modem, pinch the two vertical sides of the white clip (as shown below) and slide out the modem.



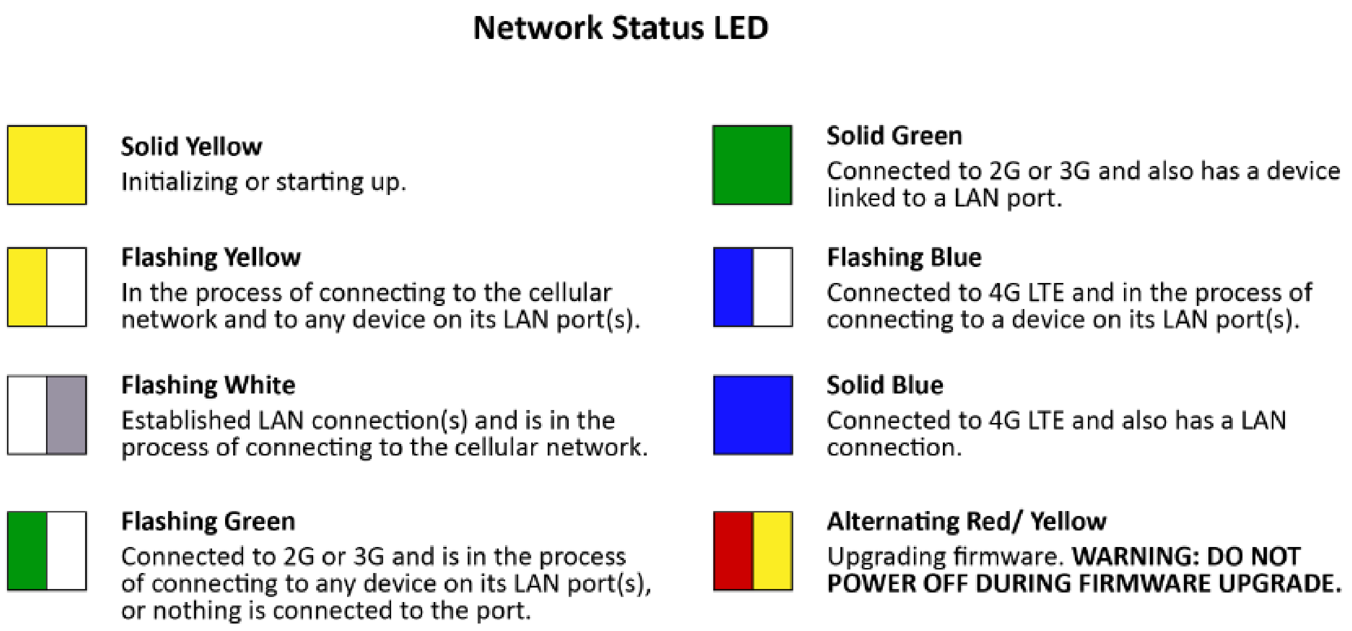
Device Status LEDs

Once power has been established, your device will initialize and attempt to connect to the network. Device initialization may take 30-60 seconds. By default your Accelerated 6330-MX will attempt to use DHCP to establish an Internet connection either through its cellular modem or Ethernet port 3.

1. Indicator lights on the Wireless Strength Indicator show you the cellular network signal strength.
2. The power LED confirms the unit is receiving electricity.
3. Cellular connectivity status is indicated by the color-coded LTE light.
4. Ethernet connections are confirmed via the light corresponding to the MX's port number.



LTE Status Indicators



Network Status LED

🟨 **Solid Yellow**
Initializing or starting up.

🟨⬜ **Flashing Yellow**
In the process of connecting to the cellular network and to any device on its LAN port(s).

⬜▨ **Flashing White**
Established LAN connection(s) and is in the process of connecting to the cellular network.

🟩⬜ **Flashing Green**
Connected to 2G or 3G and is in the process of connecting to any device on its LAN port(s), or nothing is connected to the port.

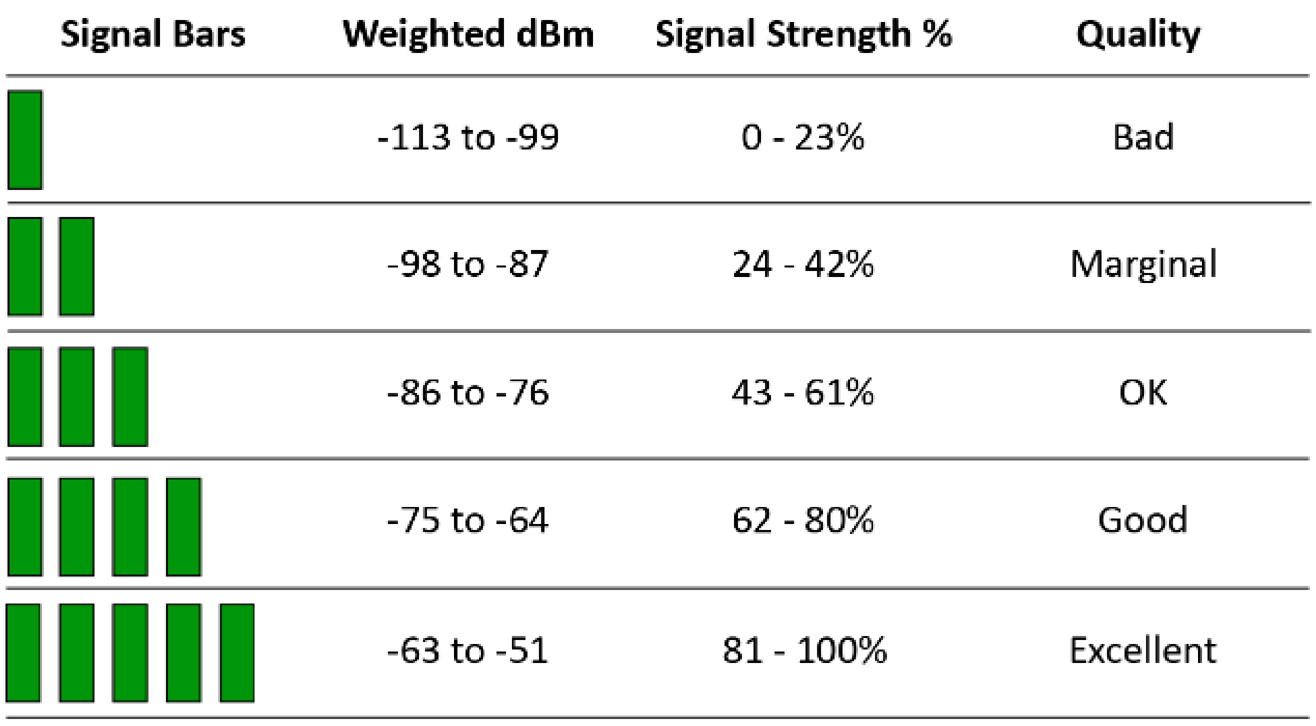
🟩 **Solid Green**
Connected to 2G or 3G and also has a device linked to a LAN port.

🟦⬜ **Flashing Blue**
Connected to 4G LTE and in the process of connecting to a device on its LAN port(s).

🟦 **Solid Blue**
Connected to 4G LTE and also has a LAN connection.

🟥🟨 **Alternating Red/ Yellow**
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Signal Strength Indicators



Signal Bars	Weighted dBm	Signal Strength %	Quality
🟩	-113 to -99	0 - 23%	Bad
🟩🟩	-98 to -87	24 - 42%	Marginal
🟩🟩🟩	-86 to -76	43 - 61%	OK
🟩🟩🟩🟩	-75 to -64	62 - 80%	Good
🟩🟩🟩🟩🟩	-63 to -51	81 - 100%	Excellent

The *weighted dBm* measurements are negative numbers, meaning the smaller negative values denote a larger number. So, for example, a -85 is a better signal than -90.

❗ NOTE: For more information regarding how signal strength is calculated and subsequently displayed via the LED indicators, refer to this explanation.

Site Survey

A cellular site survey is not necessary if your anticipated installation location is known to have strong cellular signal strength. If you are unsure of available cellular signal strength or are choosing between several installation locations, follow the below instructions to perform a site survey to determine your best possible installation location. After the optimal location has been determined, setup the 6330-MX with either the power supply unit or the PoE injector cable.

1. Follow the steps in the “Initial Setup” section above. During a site survey it is useful to use the included battery pack instead of the power supply unit to power the Accelerated 6330-MX. The battery pack will power your device for approximately two hours while you perform your site survey. The battery pack is not rechargeable and should be properly disposed of after use.
2. Move the Accelerated 6330-MX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to wait at each location for 1 minute while observing the signal strength indicator on the front of the device. Minimum cellular signal strength for proper operation is 2 bars.
3. After the optimal location has been determined, remove the battery pack and connect either the main power supply unit or PoE injector cable (see section labeled Using Remote Power for more information).

> ❗ After the optimal location has been determined, setup the 6330-MX with either the power supply unit or the PoE injector cable.

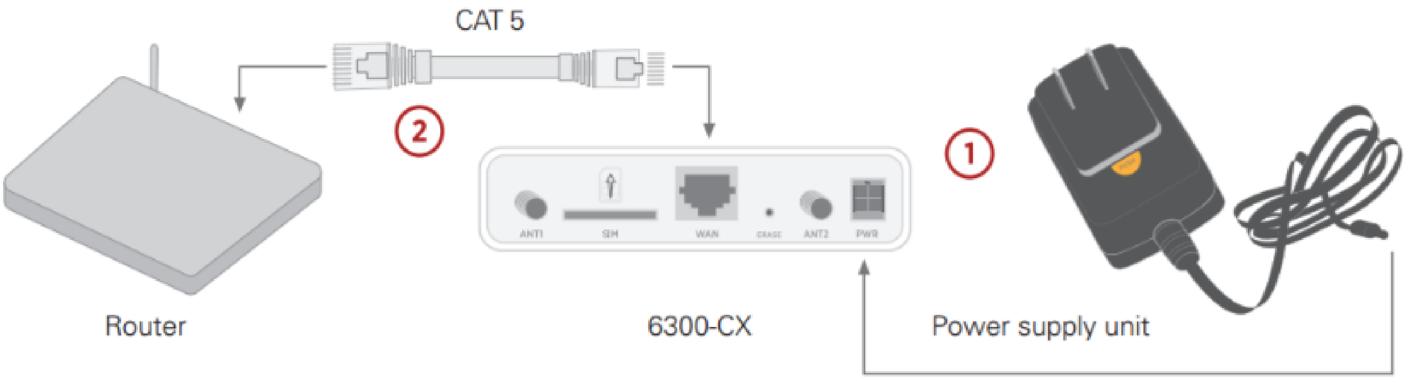
Site Survey Troubleshooting

If you are unable to verify a location with a strong cellular signal:

- Verify your SIM has been activated with your cellular operator.
- If cellular signal isn’t indicated on the Accelerated 6330-MX indoors, then take the device outdoors to verify that your cellular network operator has coverage in your location.
- If the outdoor cellular signal strength is less than 2 bars, it may be necessary to connect using a different cellular network operator. This requires an activated SIM from the alternate cellular network operator.
- Try the device/antennas in different orientations and away from other nearby electronic equipment at each test location. Note: LTE requires the use of both antennas & antennas will usually give better performance when vertical.
- Refer to the Device Status section to use Accelerated 6330-MX indicator lights to aid in diagnosis.

Physical Installation

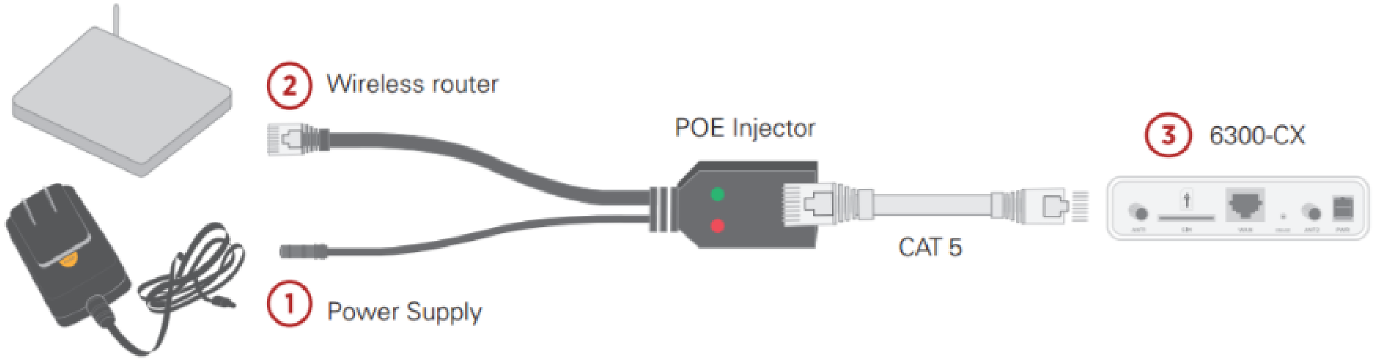
Connecting to the Site Network with Local Power



1. Plug the power supply unit into an AC power outlet
2. Connect the PSU to the MX.

Connecting to the Site Network with Remote Power

If your device needs to be positioned some distance from either the nearest AC power outlet or site network equipment, using the included passive Power-over-Ethernet (PoE) injector will simplify the installation cabling and allow for improved cellular signal strength. The POE injector cable allows the DC power and Ethernet connection to be run to the Accelerated 6330-MX via the Ethernet connection only.



1. Plug the power supply unit into an AC power outlet and connect to the PoE injector.
2. Connect an Ethernet cable from the RJ45 socket/jack on the PoE injector, (marked 'POE'), to the Ethernet port of the device.
3. Run another Ethernet cable from the PoE injector's LAN port to the client device that will be associated with the MX's first Ethernet port (marked '1/POE').

Remote Power Trouble Shooting

The LED marked **IN** will illuminate when the PoE injector is receiving power from the PSU. The LED marked **OUT** lights up green when an Ethernet connection is recognized by the MX.

If the **IN** LED is not illuminated check the following:

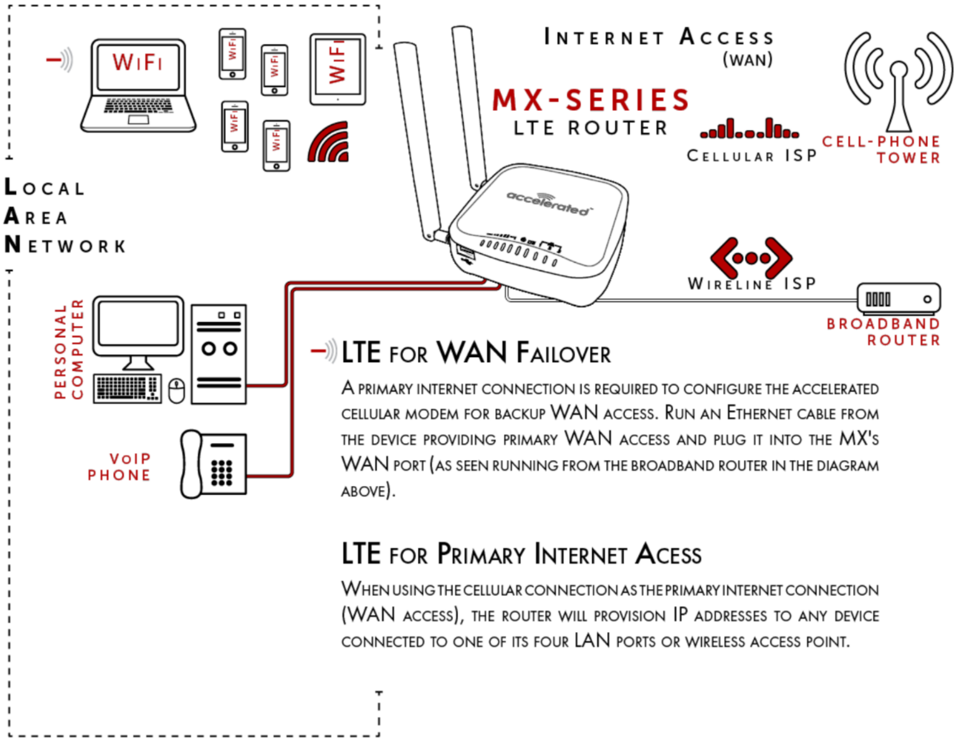
- Ensure that the PSU is plugged into an AC power outlet and is receiving power.
- Ensure that the PSU's power plug is correctly connected to the POE injector cable power input socket.

If the **OUT** LED is not illuminated after connecting to the 6330-MX, verify the integrity of the Ethernet cable.

> ❗ The PoE injector must be connected to LAN port 1 on the MX for the device to properly receive power.

POE
OUT
IN
POEINJECTOR

Network Integration



LTE for WAN Failover

A primary internet connection is required to configure the Accelerated cellular modem for backup WAN access. Run an Ethernet cable from the device providing primary WAN access and plug it into the MX's WAN port (as seen running from the broadband router in the diagram above).

LTE for Primary Internet Acess

When using the cellular connection as the primary internet connection (WAN access), the router will provision IP addresses to any device connected to one of its four LAN ports or wireless access point.

The 6330-MX is WiFi-Enabled while the 6335-MX lacks WiFi Capabilities.

A second internet connection must be available for cellular failover.

NOTE: When integrating a second Internet connection for cellular failover, connect the alternative ISP to port 3. This interface (port 3) is configured for WAN access by default though ports can be reconfigured as necessary.

Default Settings

Ethernet ports

- Ports 1 and 2 are configured as LAN ports, and will issue an IP address via DHCP to client devices.
- Port 3 is configured as a WAN port and will accept an IP address from the existing local newtwork router.

Interface Priorities

- WAN set at a metric of 1

> ❗ This metric sets the WAN port as the MX's primary network connection.

- Modem (cellular) at a metric of 3

Modem Configuration

- SIM Failover after 5 attempts
- Carrier Smart Select™ enabled

Network Settings

- LAN subnet of 192.168.2.1/24
- DHCP enabled
- Source NAT enabled (outbound traffic)

WiFi Defaults

- SSID = Accelerated 6330-MX
- Password = Accelerated!
- Channel = Automatic

WAN Failover Conditions

- Connectivity monitoring enabled for WAN
- HTTP and Ping test: 4 attempts set at a 30s interval

Security Policies

- Packet Filtering set to block all inbound traffic
- SSH, Web Admin, and Local GUI access enabled

Configuring Device

Network Managed Configuration

Your Accelerated 6330-MX has the capability to automatically sync and receive all settings from a centralized cloud management tool, Accelerated View™.

The Accelerated View management portal provides the following capabilities for your Accelerated 6330-MX.

- Monitoring details including signal strength, network connectivity details (RSRP, CNTI, RSRQ, Ec/Io, etc.), SIM card details (IMEI, IMSI, ESN, etc.), data transmitted/received, and more.
- Email notifications based on connectivity, device firmware, and signal strength.
- Remote control.
- Out of band SMS recovery.

Devices using Accelerated View typically require no additional configuration or set-up.

Local Configuration

If your Accelerated 6330-MX is not provisioned in Accelerated View, it will use a default local configuration profile which will enable basic cellular connectivity (primary or backup) to your router.

To change any default settings for an Accelerated 6330-MX not provisioned in Accelerated View refer to Managing Device Locally section.

Local Device Management

NOTE: It is recommended that Accelerated View centrally manages the MX-series router.

If you are not using the web based portal, you must manage and configure your device via the local interface.

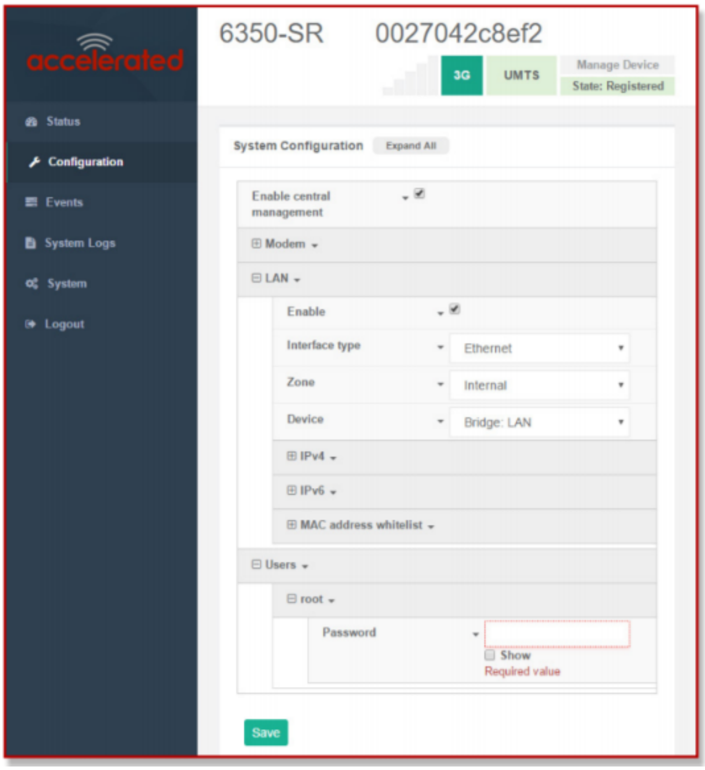
Connect to the router using its Gateway IP address: 192.168.2.1 by default.

Username: root

Password: default

The local management portal offers the same configuration options as Accelerated View, although changes made here will not sync with the cloud.

Passwords are case sensitive. (The default credentials are all lower case.)



6350-SR 0027042c8ef2

State: Registered

System Configuration

Enable central management ☑

⊞ Modem

⊟ LAN

Enable ☑

Interface type: Ethernet

Zone: Internal

Device: Bridge: LAN

⊞ IPv4

⊞ IPv6

⊞ MAC address whitelist

⊟ Users

⊟ root

Password:

□ Show

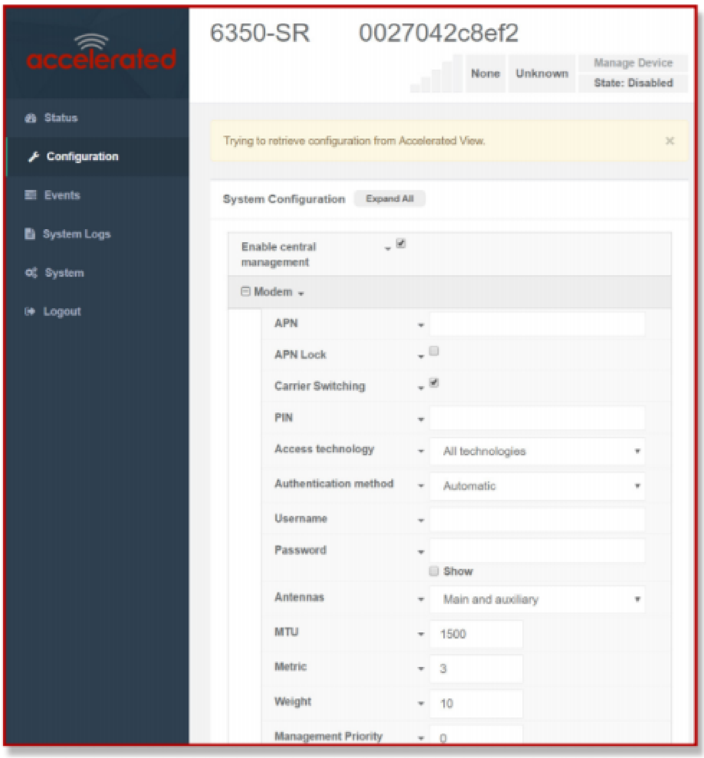
Required value

Defining a Custom APN

If your device is unable to sync with Accelerated View because the device cannot establish a cellular connection without a custom APN, it will need to be managed locally before remote configuration will be possible.

To do so:

1. Connect to the device's local UI by navigating to its default gateway address in a web browser.
2. From the **Configuration** tab, enter the name of the APN that should be associated with this device.
3. **Optional:** If the custom APN requires a specific **username** and **password**, please input those into the corresponding fields.
4. Click the **Save** button to finalize any changes.



6350-SR 0027042c8ef2

State: Disabled

Trying to retrieve configuration from Accelerated View.

System Configuration

Enable central management ☑

⊟ Modem

APN	
APN Lock	☐
Carrier Switching	☑
PIN	
Access technology	All technologies
Authentication method	Automatic
Username	
Password	 ☐ Show
Antennas	Main and auxiliary
MTU	1500
Metric	3
Weight	10
Management Priority	0

Getting Started with Accelerated View™

The following actions are typically performed by your network administrator.

Changes can be made either at the device or group level. Select override from any given menu item to edit its inherited value, or navigate to the MX's corresponding group configuration page to update the config profile shared between all devices belonging to this group.

It is recommended that Accelerated View centrally manages the 6330-MX and 6335-MX routers; only resort to local management as necessary. For any questions regarding how to access Accelerated View, please contact support@accelerated.com or your purchasing partner.

Viewing & Editing Group Configurations

To bring up a device in the configuration portal:

1. Use the **search** bar to filter devices by **MAC address**.

> ❗ The router's MAC address is on its bottom label.

2. Select the MAC address of your router and bring up its **Details** page.
3. Navigate to the **Configuration** tab of the left-side menu.
4. Follow the **Edit Group Configuration** link.
5. Adjust the necessary settings, clicking the Update button to apply any changes.

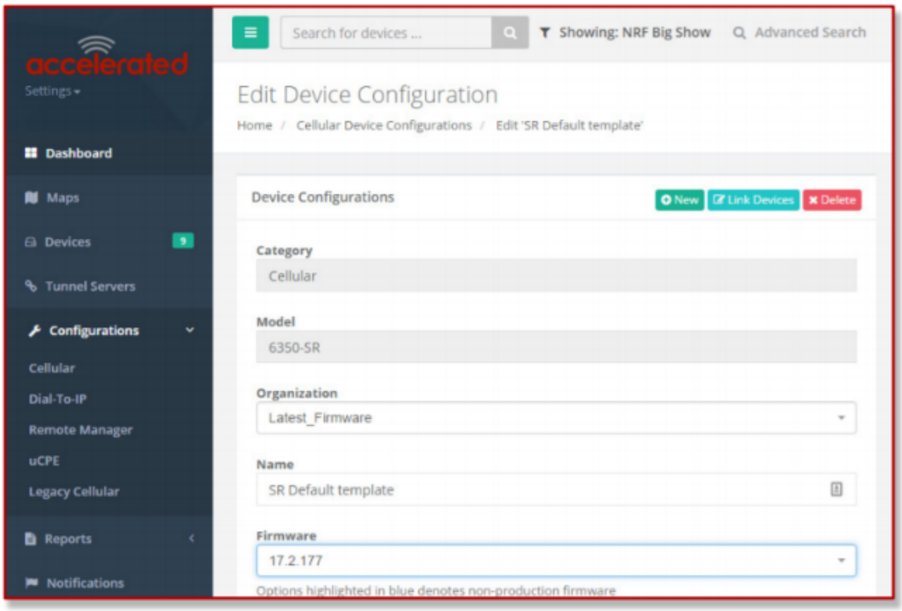
Devices will automatically apply configuration updates after the next daily sync (1am UTC by default). Refer to the Remote Commands sections for details on how to apply changes sooner.

Upgrading Firmware

> ❗ When the MX-series router is updating firmware, its LEDs will flash red and yellow. Do **NOT** remove power from the device during this process.

To view or select new firmware:

1. Navigate to the **Configuration** tab of the left-side menu.
2. Follow the **Edit Group Configuration** link.
3. Locate the **Firmware** pull-down menu.
4. Select on the intended version and wait for the settings to finish loading.
5. Click on the **Update** button at the bottom of the page to confirm firmware selection.



Edit Device Configuration

Home / Cellular Device Configurations / Edit 'SR Default template'

Device Configurations

Category: Cellular

Model: 6350-SR

Organization: Latest_Firmware

Name: SR Default template

Firmware: 17.2.177

Options highlighted in blue denotes non-production firmware

CAUTION:
IF FLASHING RED/YELLOW
DO NOT REMOVE POWER

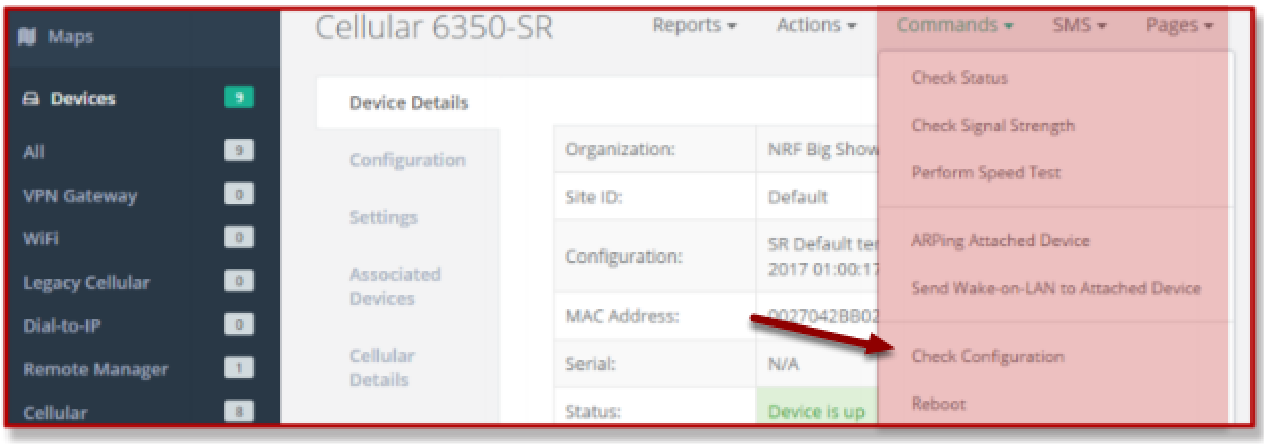
Using Remote Commands

Accelerated View maintains a connection to all online client devices registered with the service.

Using this "tunnel," network administrators can send a specific set of remote commands that will be received immediately as opposed to waiting to check in and apply any changes propagated from the cloud. The following remote commands are available:

- Check Status
- Check Signal Strength
- Perform Speed Test
- ARPing Attached Device
- Send Wake-on-LAN to Attached Device
- Check Configuration
- Reboot

Remote commands must be sent to each device in question. To do so, browse to the **Device Details** screen and select the desired option from the **Commands** pull-down.



Organization:	NRF Big Show
Site ID:	Default
Configuration:	SR Default te 2017 01:00:17
MAC Address:	0027042BB02
Serial:	N/A
Status:	Device is up

Select the **Check Configuration** menu option to update a device immediately.

Learning More

Details on using Accelerated View can be found in the Accelerated View User’s Guide.

Dual-WAN Configurations

The MX-series router is a dual-WAN device, meaning it has two interfaces capable of providing Internet access by default -- its WAN Ethernet port and the plug-in cellular modem -- though additional LAN ports may even be reconfigured for supplemental Internet access. Active WAN connections can provide both failover and load balancing per user-defined parameters

Failover

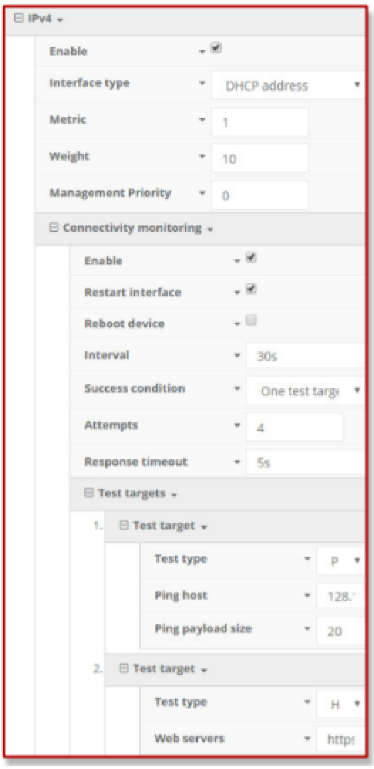
By default, this allows the plug-in modem to serve as a secondary (backup) WAN that becomes the active connection once the Ethernet WAN port is detected as offline. The router then monitors the offline connection to see when it comes back online, which prompts the backup interface to once again become inactive.

Each interface has a **Metric** value associated with its IPv4 configuration. The example on this page is associated with the WAN interface, which will take priority over all other interfaces by default (as seen by its Metric value of "1").

Connectivity Monitoring

> ❗ Both tests are set via the default group config in Accelerated View -- it is not built into the firmware.
>
> Devices that have not synced with AView will not have these tests enabled by default.

To properly trigger a failover (or failback) scenario, test parameters must be defined to monitor the primary connection. Both a Ping and HTTP test come built into the MX's WAN port configuration by default. After 4 failed attempts, the secondary connection will take over Internet access for the router. Similarly, the monitoring tests trigger the restoration of the primary WAN connection when they detect that the interface with a higher metric has come back up.



⊟ IPv4

Enable	☑
Interface type	DHCP address
Metric	1
Weight	10
Management Priority	0

⊟ Connectivity monitoring

Enable	☑
Restart interface	☑
Reboot device	□
Interval	30s
Success condition	One test targe
Attempts	4
Response timeout	5s

⊟ Test targets

1. ⊟ Test target

Test type	P
Ping host	128.'
Ping payload size	20

2. ⊟ Test target

Test type	H
Web servers	https

Carrier Smart Select™

If one of the SIM cards requires a custom or unique APN, you will need to add this APN into the router's config under the Modem > APN Option

By default, the MX-series' plug-in modem is setup for automatic SIM selection. Meaning, if the router is unable to connect with the SIM in slot 1, after a specified number of failures (5 by default) the MX will automatically switch to use the SIM in slot 2. For this setup, you will need two SIM cards enabled, provisioned, and installed in the plug-in modem's SIM slots. The two cards can be from the same carrier or from different carriers.

Load Balancing

Traffic can be balanced between the Ethernet and Cellular WAN interfaces. This feature, often referred to as "load balancing," uses an interface's **Weight** value -- this is defined under the **IPv4** expandable menu. The interfaces being balanced must share the same **Metric** value.

It is important to note that the two SIM slots cannot be leveraged simultaneously for load balancing; the load must be shared between the cellular modem and the wireline Internet connection. The Weight of an interface establishes its proportional contribution relative to the weight of its complimentary interface.

For example, setting the Ethernet WAN to a weight of "20" and the Cellular WAN to a weight of "5" establishes a 4:1 ratio -- the Ethernet interface will handle 4x the amount of data with this configuration.

Interface Configuration

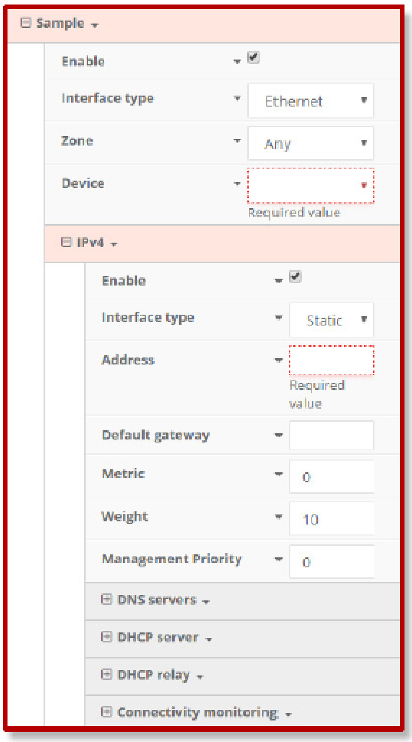
Changing the LAN Subnet

The default subnet -- 192.168.2.1/24 -- is set in the IPv4 Address field of the LAN interface, and can be adjusted to any range of private IPs by completing the following steps:

1. Expand the configuration page to **Network** > **Interfaces**.
2. Select the LAN interface that needs to be adjusted and expand its IPv4 entry.
3. The **Address** field contains the range of IPs available for assignment.

NOTE: The subnet mask must also be specified.

> ! Changes made to the IPv4 Address must also be updated in the DHCP server entry to preserve functionality.



⊟ Sample

Enable ☑

Interface type: Ethernet

Zone: Any

Device: Required value

⊟ IPv4

Enable ☑

Interface type: Static

Address: Required value

Default gateway

Metric: 0

Weight: 10

Management Priority: 0

⊞ DNS servers

⊞ DHCP server

⊞ DHCP relay

⊞ Connectivity monitoring

Creating New Interfaces

Additional interfaces may be configured to further differentiate port functionality:

1. Expand the configuration page to **Network** > **Interfaces**.
2. Name the new **Interface** using the text field at the bottom of the list, clicking the **Add** button to continue.

3. Ensure the appropriate settings are entered into the new collapsible section generated for the interface:
   - The **Enable** checkbox must remain selected.
   - **Interface Type** will stay **Ethernet**.
   - The default **Zone**, "Any," suffices unless security policies necessitate a different selection.
   - **Device** establishes which port(s) are assigned to the new interface.
   - Expand the **IPv4** category to specify the Interface type and the desired address range.
   - Additional settings for **DNS** and **DHCP** configuration can be adjusted as necessary.
   - Refer to the Failover section for information on **Connectivity Monitoring.**

❗ This assumes a static (private) IP is desired for the interface.

VLAN Management

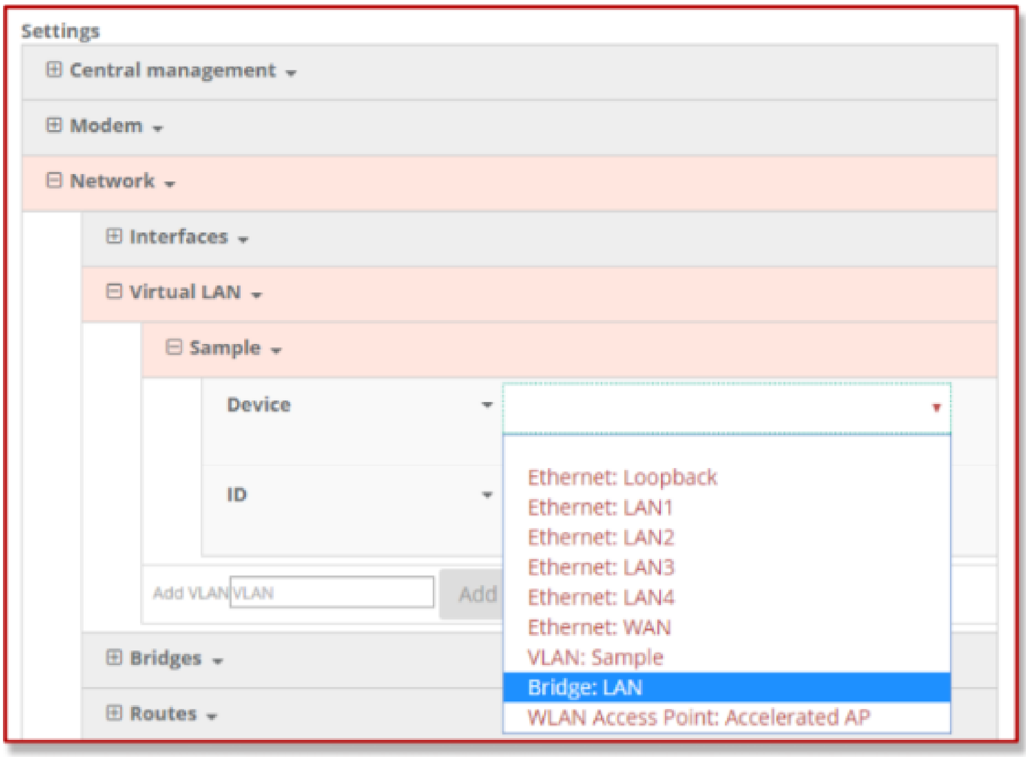
Before creating a Virtual LAN route for the MX-series router, be sure that its corresponding LAN interface has been configured (per the steps on the previous page).

The interface's **Device** must be set to only include the port(s) that will be utilizing the VLAN designation. Use the pull-down menu to specify an individual Ethernet LAN port, or choose the "**Bridge: LAN**" option to assign all four ports.

Once the interface is created, it will be selectable as a Device in the VLAN's pulldown menu.

Separate VLANs by assigning each a unique **ID** number.

❗ For guidance on how to create bridges with less than four ports, please refer to the Accelerated University knowledge article.



Settings

⊞ Central management

⊞ Modem

⊟ Network

⊞ Interfaces

⊟ Virtual LAN

⊟ Sample

Device

ID

Add VLAN VLAN Add

⊞ Bridges

⊞ Routes

WiFi Options

IMPORTANT: The 6335-MX does not have WiFi capabilities. The following information applies to the 6330-MX ONLY.

Wireless LAN

Per the default configuration profile, there will be one available SSID: "Accelerated 6330-MX."

WiFi-enabled SRs can broadcast up to a total of **8 WLAN SSIDs** simultaneously. To create additional SSIDs or to change the configuration of existing ones:

1. Navigate to the device's (or group's) **Configuration** page.
2. Expand **Network** > **Wireless LAN**.
3. Verify that **Enabled** is selected and adjust the **Channel** and **Beacon** Interval if necessary.
4. Expand the **Access Points** menu to view existing SSIDs or create new ones.
5. Each WLAN AP is listed as its own collapsable menu featuring:
    - Enabled status box
    - SSID
    - SSID Broadcast
    - Encryption type
    - Pre-shared key
6. To create a new AP, specify its name in the corresponding text field and click the **Add** button.

Client Mode

In addition to serving as an independent WLAN Access Point, the 6350-SR's WiFi can broadcast in "Client Mode" to serve as a supplemental AP to relay a wireless LAN originating from another WiFi-enabled router by entering that network's **SSID** and **Pre-shared key.**

WiFi as WAN

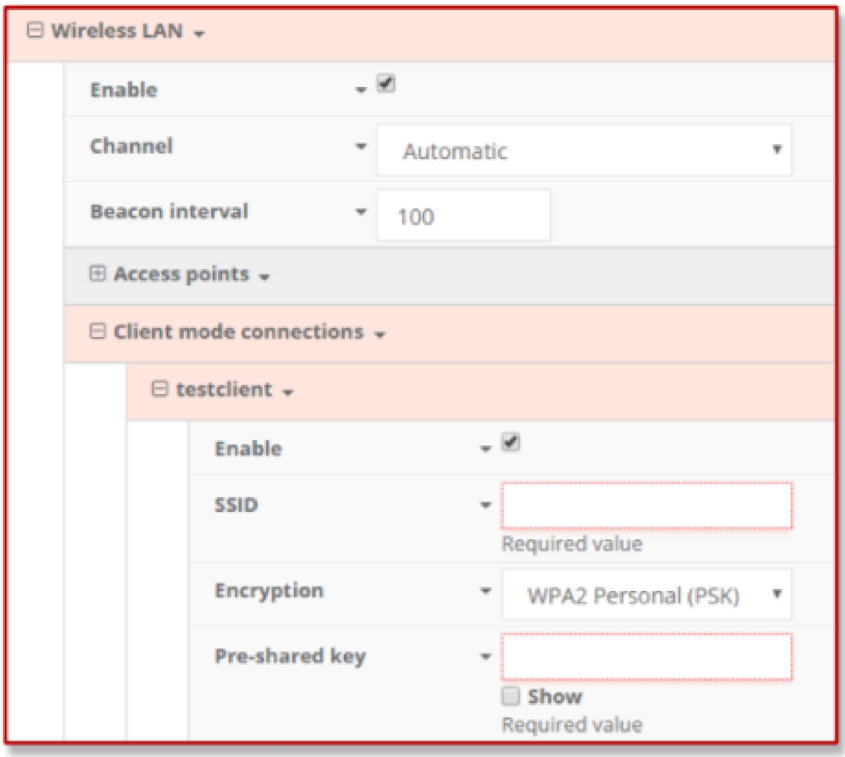
Client Mode can also be used to leverage the 6330-MX's WiFi to relay Internet access (WAN) provided by another router's wireless AP.

Before configuring the 6330-MX for WiFi-as-WAN (WaW) Client Mode, identify the SSID that the 6330-MX should connect to, including its broadcasting channel, authentication details for the SSID, and interface prioritization for the WaW connection (i.e. should it take precedence over the WAN Ethernet port).

1. Under **Network** > **Wireless LAN** > **Client mode connections**, create a new entry named "testclient." The name can be different if desired.
2. Enter the **Channel** and **authentication credentials** for the SSID of the secondary wireless router.
3. Under **Network** > **Interfaces**, create a new entry named "WiFiasWAN."

> For details on how to create new interfaces, refer to the article covering **Custom Interfaces.**

4. Set the **Zone** for the new interface to **External.**
5. Set the **Device** for the new interface to WLAN Client: testclient
6. Under **IPv4**, set **the Interface type** to **DHCP address.** NOTE: This will trigger the 6330-MX to obtain a DHCP connection to the secondary wireless router's SSID network.
7. Click **Save.**



⊟ Wireless LAN

Enable ☑

Channel: Automatic

Beacon interval: 100

⊞ Access points

⊟ Client mode connections

⊟ testclient

Enable ☑

SSID: Required value

Encryption: WPA2 Personal (PSK)

Pre-shared key: □ Show

Required value

Firewall Settings

Both the 6330-MX and 6335-MX can function as a stateful firewall. Options for the MX-series firewall configuration leverage two key security measures:

Port Forwarding

Remote computers can access applications or services hosted on a local network with the Accelerated SR-series router by setting up port forwarding. It provides mapping instructions that direct incoming traffic to the proper device on a LAN.

To configure port forwarding:

1. Under **Firewall** > **Port Forwarding**, click the Add button.
2. Select the relevant **LAN Interface**.

> ❗ Select LAN unless custom interfaces were configured.

3. The **IP version** and **Protocol** can be left at their default values unless changes are required by the request being serviced by this port-forwarding configuration.
4. Specify the public-facing **Port** for remote access.
5. In the "To" fields, specify the **port** and **IP address** associated with the intended destination device.
6. If necessary, expand the **Access Control List** to create a white list that determines which devices are authorized to leverage this particular forwarding route.

> ❗ Both individual IP addresses and entire zones may be white listed.

Packet Filtering

Enabled by default, packet filtering will monitor traffic going to and from the MX-series router. The predefined settings are intended to block unauthorized inbound traffic while providing an unrestricted flow of data from LAN to WAN.

Virtual Router Redundancy Protocol

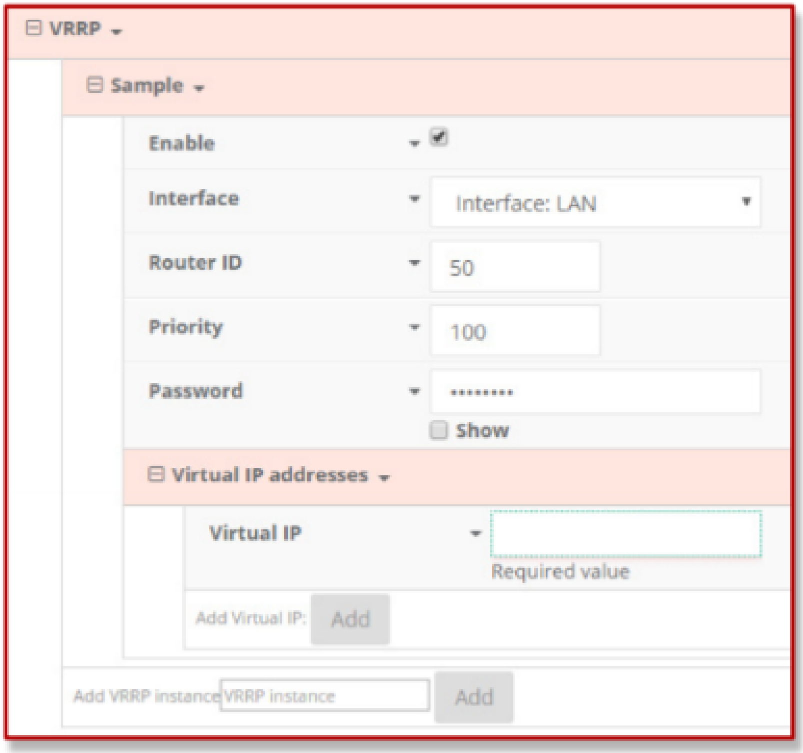
VRRP is a networking protocol used to configure devices as a "hot standby" for a primary router, where a backup device will only start routing traffic after the network detects that the primary device is offline (using parameters set by VRRP).

To link multiple devices together, each must be configured with the same Router ID within Accelerated View. Refer to the following step-by-step guidance for more information:

1. Expand **Network** > **VRRP**.
2. In the **Add** VRRP Instance text field, enter a name for the entry.
3. Enable the instance.
4. Specify an **Interface** -- this will typically be set to **LAN**, meaning all four LAN ports.
5. Set the **Router ID** to match the number designated for this instance.
6. **Priority** establishes the order in which backup devices step in for offline routers.
7. The **Password** is a shared string of characters that must be entered for each device to authorize its integration into the VRRP instance.

A higher number establishes higher priority.

Refer to the Interface Creation section of this user manual for more info on custom interfaces.



VRRP

Sample

Enable ☑

Interface: Interface: LAN

Router ID: 50

Priority: 100

Password: •••••••••

□ Show

Virtual IP addresses

Virtual IP:

Required value

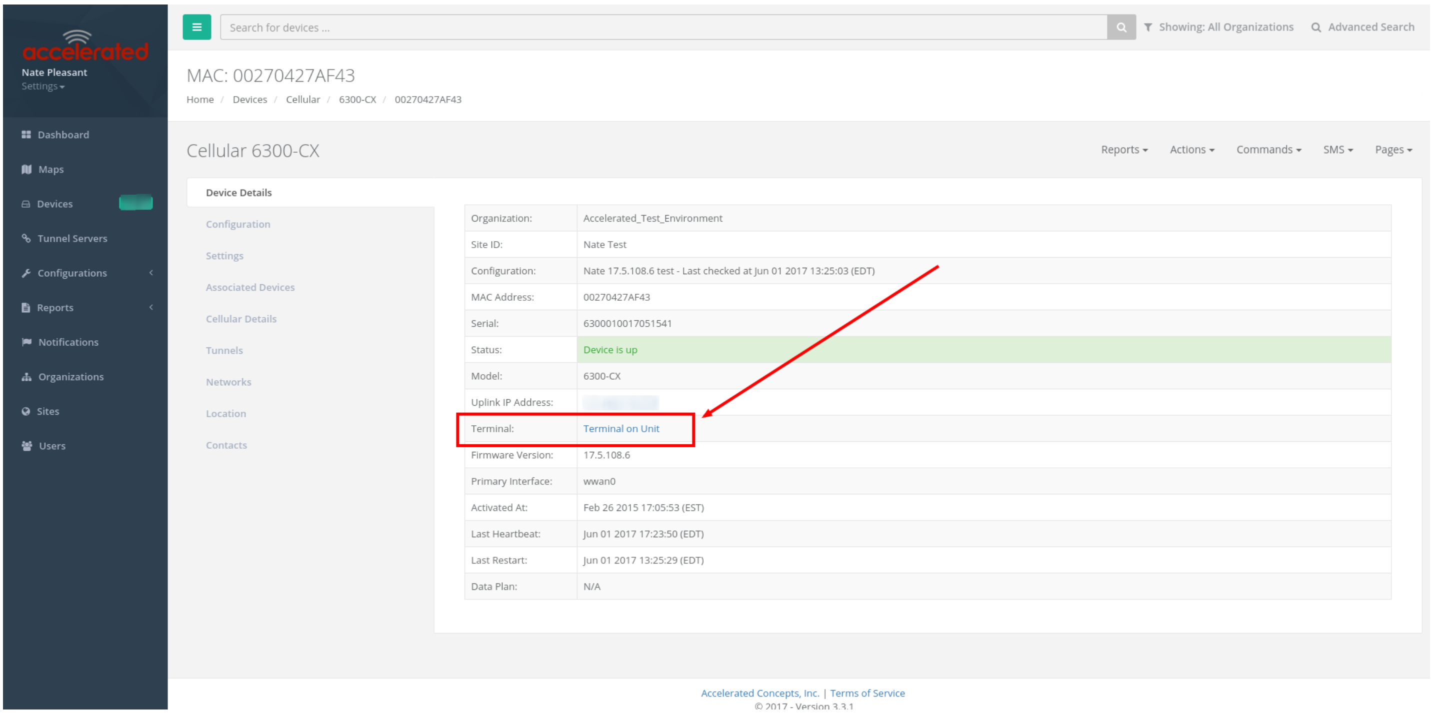
Terminal on Unit

Skill level: *Intermediate*

Goal

To access the console of an Accelerated LTE router using the *Terminal on Unit* link presented in Accelerated View for the device.

> The *Terminal on Unit* access leverages the management tunnel established between the 63xx-series router and Accelerated View. For details on the monthly data usage for this access, refer to the following article:
>
> [Data Usage Estimates]



MAC: 00270427AF43

Home / Devices / Cellular / 6300-CX / 00270427AF43

Cellular 6300-CX

Organization:	Accelerated_Test_Environment
Site ID:	Nate Test
Configuration:	Nate 17.5.108.6 test - Last checked at Jun 01 2017 13:25:03 (EDT)
MAC Address:	00270427AF43
Serial:	6300010017051541
Status:	Device is up
Model:	6300-CX
Uplink IP Address:	[redacted]
Terminal:	Terminal on Unit
Firmware Version:	17.5.108.6
Primary Interface:	wwan0
Activated At:	Feb 26 2015 17:05:53 (EST)
Last Heartbeat:	Jun 01 2017 17:23:50 (EDT)
Last Restart:	Jun 01 2017 13:25:29 (EDT)
Data Plan:	N/A

Accelerated Concepts, Inc. | Terms of Service
© 2017 - Version 3.3.1

Setup

For this setup, you will need access to Accelerated View, and a 63xx-series router online and syncing with Accelerated View. If you see the 63xx-series router listed as up (green status) in Accelerated View, you are good to go.

Details

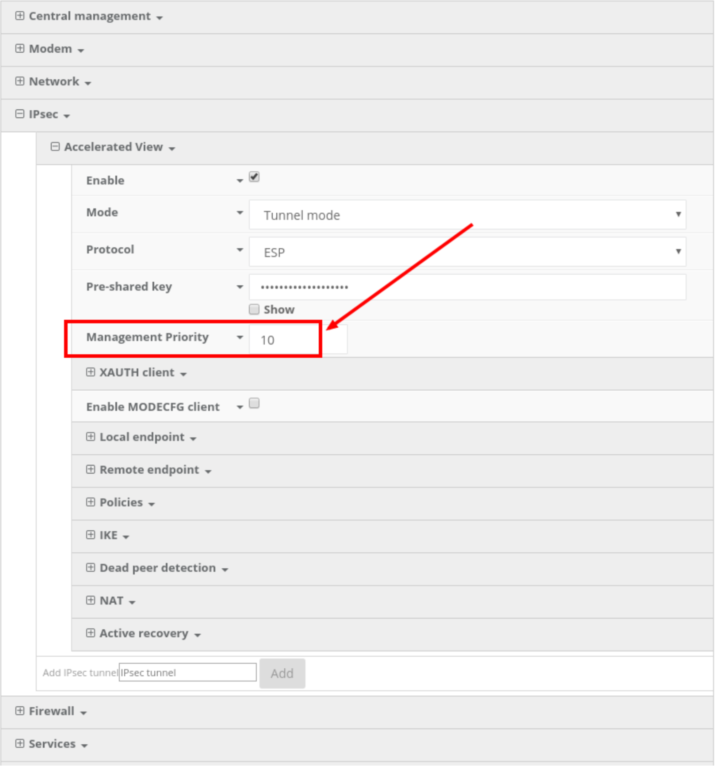
Accelerated View utilizes the IPSec tunnel the 63xx-series router establishes to remote.accns.com to provide terminal access to the console of the router.

For details on the monthly data usage for this access, refer to the following article:

Data Usage Estimates

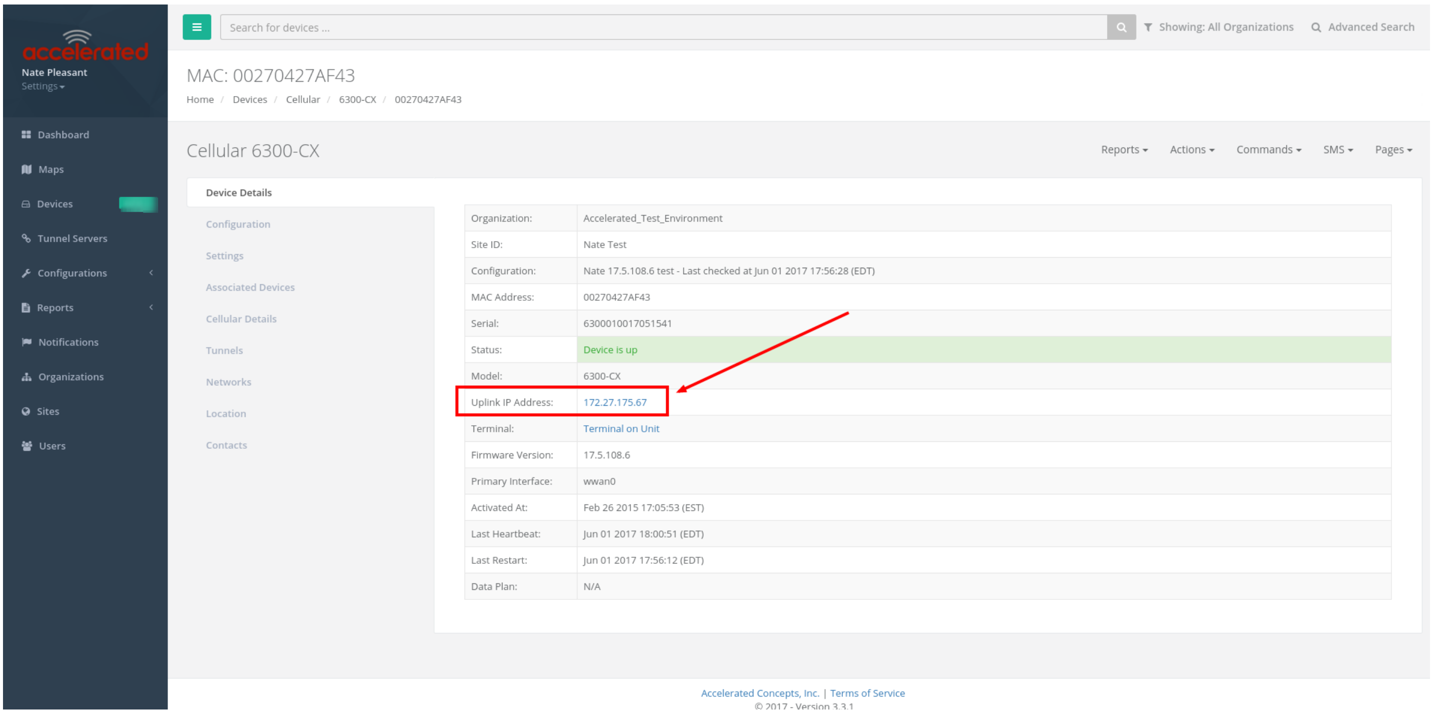
The following configuration settings will setup the Accelerated router to report its IPSec tunnel local IP address as the management IP that Accelerated View can then use to access its console.

Open the configuration profile for the 63xx-series router. Under *IPSec -> Accelerated View*, set the *Management priority* to *10*. This will tell the 63xx-series router to treat the AView IPSec tunnel as the highest priority management interface, which it then reports to Accelerated View as the IP that can be used to access its console.



⊞ Central management
⊞ Modem
⊞ Network
⊟ IPsec
⊟ Accelerated View
Enable ☑
Mode: Tunnel mode
Protocol: ESP
Pre-shared key: ••••••••••••••••••••
□ Show
Management Priority: 10
⊞ XAUTH client
Enable MODECFG client □
⊞ Local endpoint
⊞ Remote endpoint
⊞ Policies
⊞ IKE
⊞ Dead peer detection
⊞ NAT
⊞ Active recovery
Add IPsec tunnel: IPsec tunnel [Add]
⊞ Firewall
⊞ Services

Once you apply the new configuration to the 63xx-series router, reboot the 63xx-series device so it rebuilds the IPSec tunnel and reports the new IPSec local IP address to Accelerated View. You can verify that Accelerated View is using the IPSec local IP as the management IP by looking at the *Uplink IP address* on the *Device Details* tab. This value should be set to a 172.x.x.x IP address.



MAC: 00270427AF43

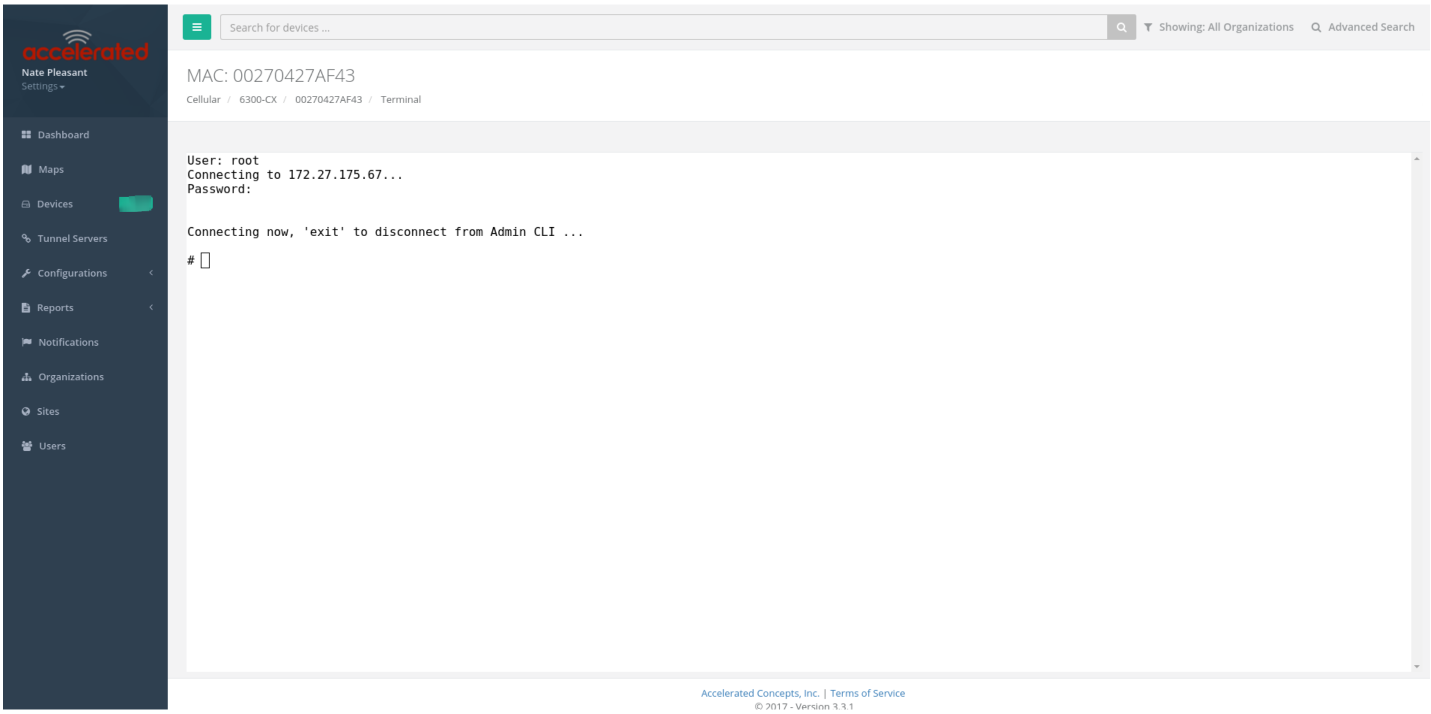
Home / Devices / Cellular / 6300-CX / 00270427AF43

Cellular 6300-CX

Organization:	Accelerated_Test_Environment
Site ID:	Nate Test
Configuration:	Nate 17.5.108.6 test - Last checked at Jun 01 2017 17:56:28 (EDT)
MAC Address:	00270427AF43
Serial:	6300010017051541
Status:	Device is up
Model:	6300-CX
Uplink IP Address:	172.27.175.67
Terminal:	Terminal on Unit
Firmware Version:	17.5.108.6
Primary Interface:	wwan0
Activated At:	Feb 26 2015 17:05:53 (EST)
Last Heartbeat:	Jun 01 2017 18:00:51 (EDT)
Last Restart:	Jun 01 2017 17:56:12 (EDT)
Data Plan:	N/A

Using the Terminal on Unit link

Once the correct management IP is reported from the 63xx-series router to Accelerated View, clicking the *Terminal on Unit* will open a page on Accelerated View to provide the user access to the console of the 63xx-series router.



MAC: 00270427AF43

Cellular / 6300-CX / 00270427AF43 / Terminal

```
User: root
Connecting to 172.27.175.67...
Password:


Connecting now, 'exit' to disconnect from Admin CLI ...

#
```

AT Command Access

To gain AT command access through the 6330-MX, the tester must have a PC/laptop connected to one of the LAN Ethernet ports of the Accelerated router. They will need to configure a static IP on the PC/laptop of 192.168.210.2/24 with a gateway of 192.168.210.1

- Open a SSH session to the 6300-CX at 192.168.210.1. Default login credentials are:
  - *username:* root
  - *password:* default

- Select **a** to access the Admin CLI. If the SSH session immediately gives you the # prompt, you are already in the Admin CLI.
- Type **atcmd** and press Enter. Type **n** when the SR prompts you if you want exclusive access. This allows you to send AT commands to the device while still allowing the device to connect, disconnect, and/or reconnect to the Sprint network.
- Example AT command access below:

```
$ ssh root@192.168.210.1
Password:

Access selection menu:

a: Admin CLI
s: Shell
q: Quit

Select access or quit [admin] : a

Connecting now, 'exit' to disconnect from Admin CLI ...

# atcmd

Do you want exclusive access to the modem? (y/n) [y]: n
Starting terminal access to modem AT commands.
Note that the modem is still in operation.

To quit enter '~.' ('~~.' if using an ssh client) and press ENTER

Connected
ati
Manufacturer: Sierra Wireless, Incorporated
Model: MC7354
Revision: SWI9X15C_05.05.16.02 r21040 carmd-fwbuild1 2014/03/17 23:49:48
MEID: 35922505082765
ESN: 12803341918, 8032FE5E
IMEI: 359225050827658
```

```
IMEI SV: 11
FSN: J8513103240310
+GCAP:
```

Troubleshooting

Resetting Your Device

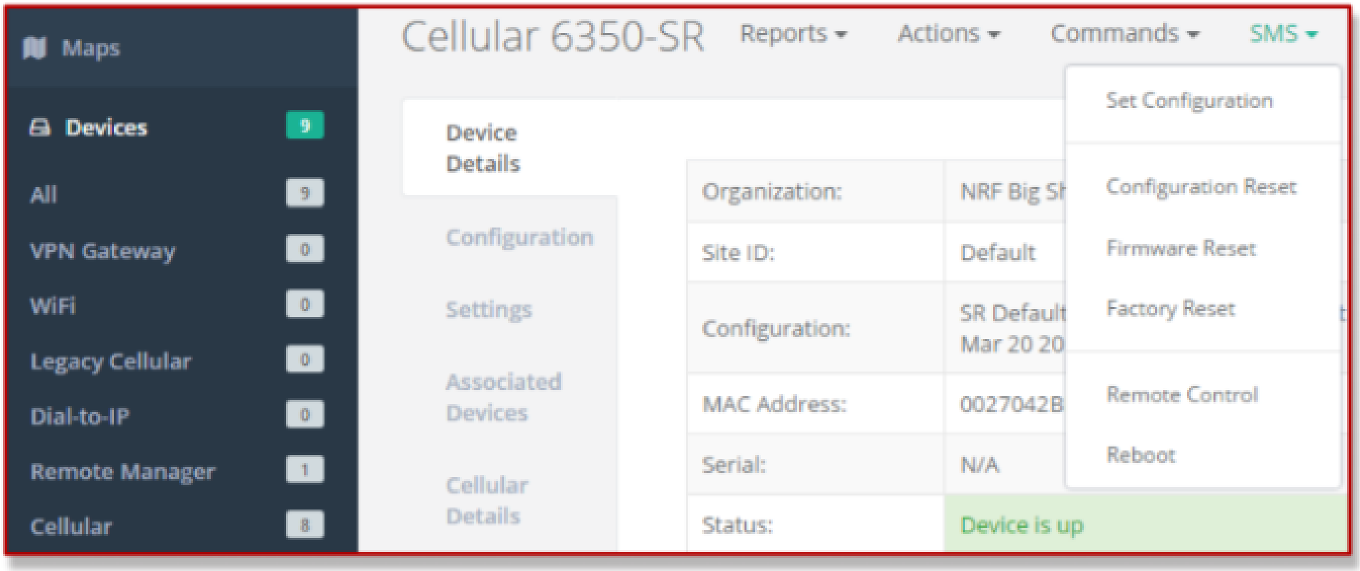
While the settings are reset, the device's firmware version remains the same.

To reset the device to factory default settings, press and release the ERASE switch once on the rear of the device when the device is switched on. This will erase all device-specific settings to their original state, and it will automatically reboot.

Out-of-Band SMS Commands

This feature is only available via Accelerated View.

A set of emergency remote commands can be sent via SMS to the device to provide Out-Of Band (OOB) recovery for the device. These SMS commands allow you to perform actions such as factory resets, reboot the device, and restore to the backup firmware partition, all without requiring the device to have an active IP (WAN) connection. Similar to the standard remote commands, these can be used to provide control over the device without any on-site interaction. To utilize this feature, SMS must be enabled for the SIM card used by the device. The complete list of SMS commands is defined in the Accelerated View™ User Manual.



Organization:	NRF Big Sh
Site ID:	Default
Configuration:	SR Default Mar 20 20
MAC Address:	0027042B
Serial:	N/A
Status:	Device is up

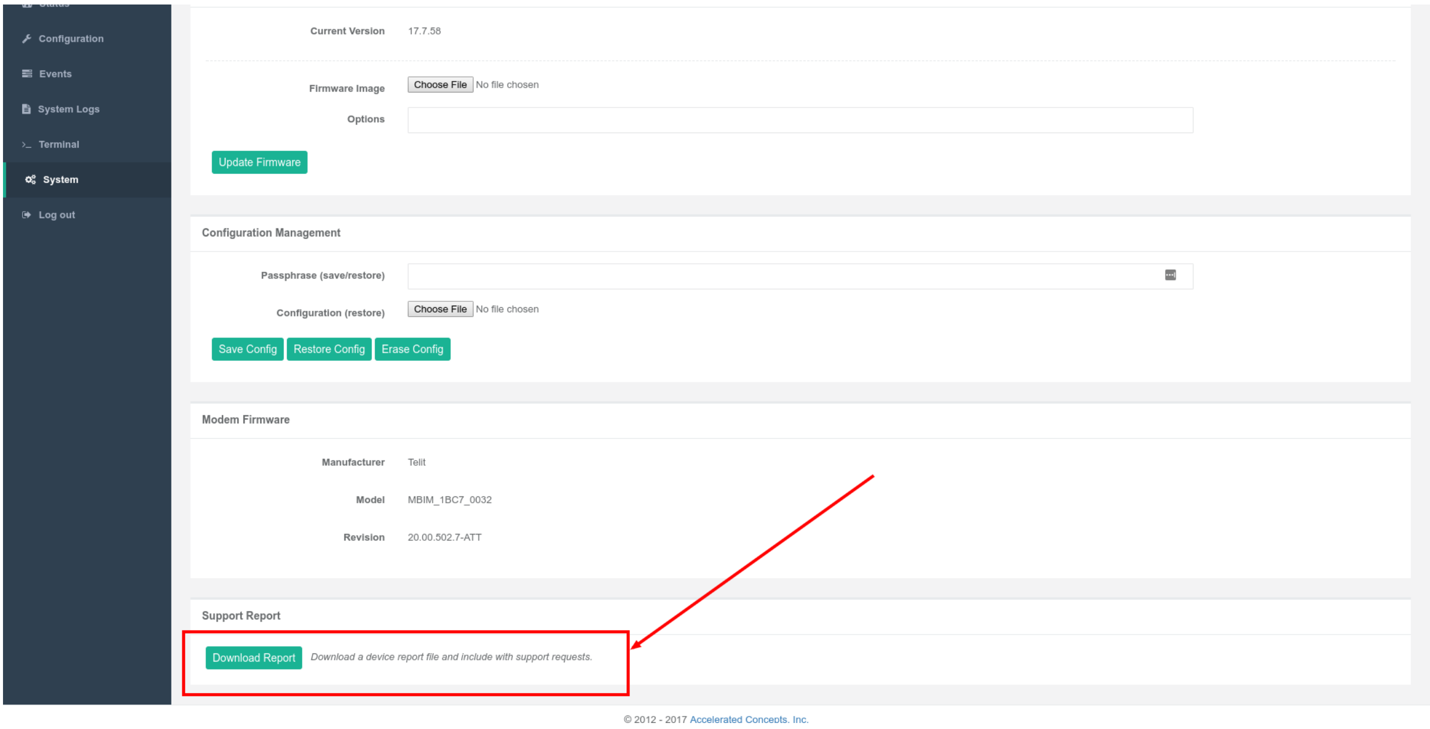
Support Report

Often times, it is beneficial to download a support report from the device to provide to technical support. This report is a zip file that contains all of the current details for the device's state, and a full record of the system logs from the device.

To obtain a support report from the device, login to the device's local web UI. To access the local web UI, the user must have a PC/laptop connected to one of the LAN Ethernet ports of the 6330-MX. They should receive an IP address via DHCP from the MX in the 192.168.2.100-250 range. If they do not receive a DHCP address, they can configure a static IP on the PC/laptop of 192.168.2.2/24 with a gateway of 192.168.2.1. Once the PC/laptop has an IP address, open the following URL in a browser on the PC:

https://192.168.2.1

Next, go to the *System* page, then click the *Download Report* button at the bottom of the page.



Current Version 17.7.58

Firmware Image No file chosen

Options

Configuration Management

Passphrase (save/restore)

Configuration (restore) No file chosen

Modem Firmware

Manufacturer Telit

Model MBIM_1BC7_0032

Revision 20.00.502.7-ATT

Support Report

Download a device report file and include with support requests.

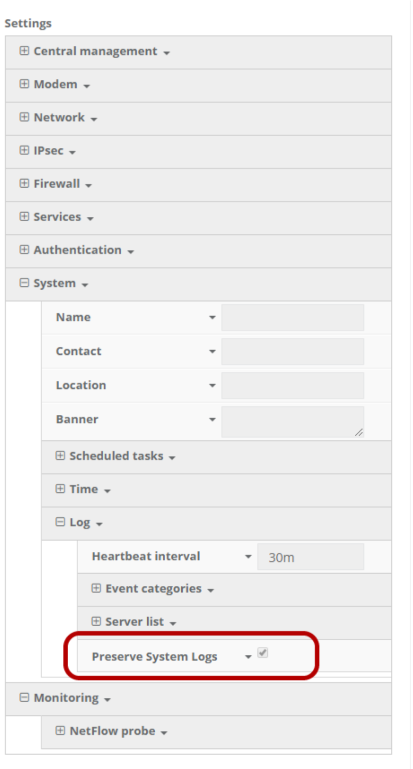
© 2012 - 2017 Accelerated Concepts, Inc.

Persistent System Logs

As of December 6th, 2017, the default behavior for all Accelerated Routers is to have persistent system logs disabled. Information logged on the device will be erased when the router is powered off/ rebooted.

Logging can be configured to persist between power cycles by enabling the **Preserve System Logs** checkbox nested under the **System** → **Log** menu option.

NOTE: Logging across reboots should be enabled only to debug issues and then disabled ASAP to avoid unnecessary wear to the flash memory.

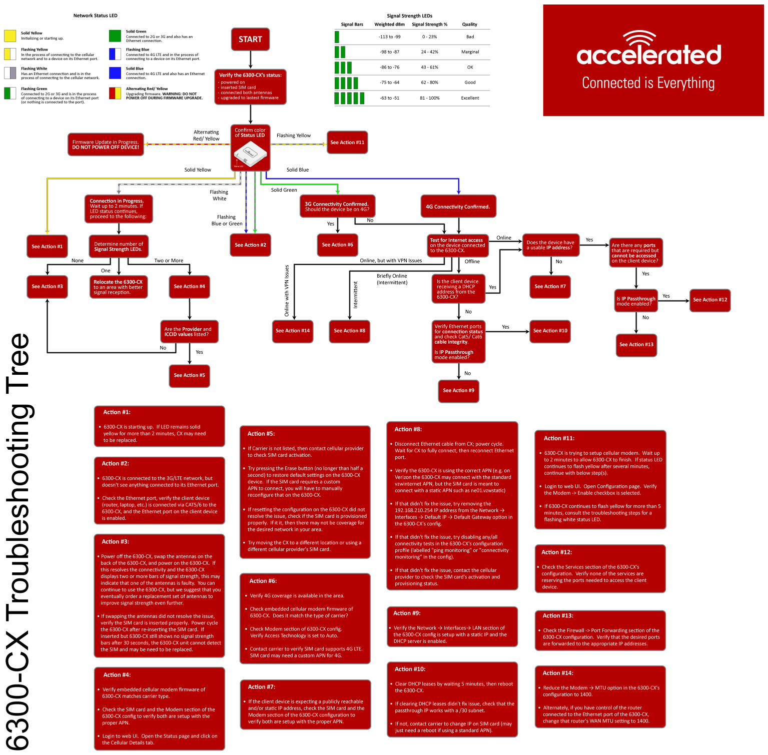


Settings

- ⊞ Central management
- ⊞ Modem
- ⊞ Network
- ⊞ IPsec
- ⊞ Firewall
- ⊞ Services
- ⊞ Authentication
- ⊟ System
  - Name
  - Contact
  - Location
  - Banner
  - ⊞ Scheduled tasks
  - ⊞ Time
  - ⊟ Log
    - Heartbeat interval: 30m
    - ⊞ Event categories
    - ⊞ Server list
    - Preserve System Logs ☑
- ⊟ Monitoring
  - ⊞ NetFlow probe

LTE Troubleshooting Tree

6300-CX_Troubleshooting_Flowchart.pdf


6300-CX Troubleshooting Tree
Network Status LED
Solid Yellow
Initializing or starting up.
Flashing Yellow
In the process of connecting to the cellular network and to a device on its Ethernet port.
Flashing White
Has an Ethernet connection and is in the process of connecting to the cellular network.
Flashing Green
Connected to 2G or 3G and is in the process of connecting to a device on its Ethernet port (or nothing is connected to the port).
Solid Green
Connected to 2G or 3G and also has an Ethernet connection.
Flashing Blue
Connected to 4G LTE and in the process of connecting to a device on its Ethernet port.
Solid Blue
Connected to 4G LTE and also has an Ethernet connection.
Alternating Red/ Yellow
Upgrading firmware. WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.
Signal Strength LEDs
Signal Bars
Weighted dBm
Signal Strength %
Quality
-113 to -99
0 - 23%
Bad
-98 to -87
24 - 42%
Marginal
-86 to -76
43 - 61%
OK
-75 to -64
62 - 80%
Good
-63 to -51
81 - 100%
Excellent
accelerated
Connected is Everything
START
Verify the 6300-CX's status:
- powered on
- inserted SIM card
- connected both antennas
- upgraded to lastest firmware
Confirm color of Status LED
Alternating Red/ Yellow
Firmware Update in Progress. DO NOT POWER OFF DEVICE!
Flashing Yellow
See Action #11
Solid Yellow
Solid Blue
Flashing White
Solid Green
Flashing Blue or Green
Connection in Progress. Wait up to 2 minutes. If LED status continues, proceed to the following:
3G Connectivity Confirmed. Should the device be on 4G?
4G Connectivity Confirmed.
See Action #1
Determine number of Signal Strength LEDs.
See Action #2
Yes
See Action #6
No
Test for Internet access on the device connected to the 6300-CX.
Online
Does the device have a usable IP address?
Yes
Are there any ports that are required but cannot be accessed on the client device?
None
One
Two or More
See Action #3
Relocate the 6300-CX to an area with better signal reception.
See Action #4
Online, but with VPN Issues
Offline
Briefly Online (Intermittent)
Is the client device receiving a DHCP address from the 6300-CX?
Yes
No
See Action #7
Yes
Is IP Passthrough mode enabled?
Yes
See Action #12
No
See Action #13
Online with VPN Issues
Intermittent
See Action #14
See Action #8
Are the Provider and ICCID values listed?
No
Yes
See Action #5
No
Verify Ethernet ports for connection status and check Cat5/ Cat6 cable integrity.
Is IP Passthrough mode enabled?
Yes
See Action #10
No
See Action #9

Action #1:

- 6300-CX is starting up. If LED remains solid yellow for more than 2 minutes, CX may need to be replaced.

Action #2:

- 6300-CX is connected to the 3G/LTE network, but doesn't see anything connected to its Ethernet port.
- Check the Ethernet port, verify the client device (router, laptop, etc.) is connected via CAT5/6 to the 6300-CX, and the Ethernet port on the client device is enabled.

Action #3:

- Power off the 6300-CX, swap the antennas on the back of the 6300-CX, and power on the 6300-CX. If this resolves the connectivity and the 6300-CX displays two or more bars of signal strength, this may indicate that one of the antennas is faulty. You can continue to use the 6300-CX, but we suggest that you eventually order a replacement set of antennas to improve signal strength even further.
- If swapping the antennas did not resolve the issue, verify the SIM card is inserted properly. Power cycle the 6300-CX after re-inserting the SIM card. If inserted but 6300-CX still shows no signal strength bars after 30 seconds, the 6300-CX unit cannot detect the SIM and may be need to be replaced.

Action #4:

- Verify embedded cellular modem firmware of 6300-CX matches carrier type.
- Check the SIM card and the Modem section of the 6300-CX config to verify both are setup with the proper APN.
- Login to web UI. Open the Status page and click on the Cellular Details tab.

Action #5:

- If Carrier is not listed, then contact cellular provider to check SIM card activation.
- Try pressing the Erase button (no longer than half a second) to restore default settings on the 6300-CX device. If the SIM card requires a custom APN to connect, you will have to manually reconfigure that on the 6300-CX.
- If resetting the configuration on the 6300-CX did not resolve the issue, check if the SIM card is provisioned properly. If it it, then there may not be coverage for the desired network in your area.
- Try moving the CX to a different location or using a different cellular provider's SIM card.

Action #6:

- Verify 4G coverage is available in the area.
- Check embedded cellular modem firmware of 6300-CX. Does it match the type of carrier?
- Check Modem section of 6300-CX config. Verify Access Technology is set to Auto.
- Contact carrier to verify SIM card supports 4G LTE. SIM card may need a custom APN for 4G.

Action #7:

- If the client device is expecting a publicly reachable and/or static IP address, check the SIM card and the Modem section of the 6300-CX configuration to verify both are setup with the proper APN.

Action #8:

- Disconnect Ethernet cable from CX; power cycle. Wait for CX to fully connect, then reconnect Ethernet port.
- Verify the 6300-CX is using the correct APN (e.g. on Verizon the 6300-CX may connect with the standard vzwinternet APN, but the SIM card is meant to connect with a static APN such as ne01.vzwstatic)
- If that didn't fix the issue, try removing the 192.168.210.254 IP address from the Network → Interfaces → Default IP → Default Gateway option in the 6300-CX's config.
- If that didn't fix the issue, try disabling any/all connectivity tests in the 6300-CX's configuration profile (labelled "ping monitoring" or "connectivity monitoring" in the config).
- If that didn't fix the issue, contact the cellular provider to check the SIM card's activation and provisioning status.

Action #9:

- Verify the Network → Interfaces→ LAN section of the 6300-CX config is setup with a static IP and the DHCP server is enabled.

Action #10:

- Clear DHCP leases by waiting 5 minutes, then reboot the 6300-CX.
- If clearing DHCP leases didn't fix issue, check that the passthrough IP works with a /30 subnet.
- If not, contact carrier to change IP on SIM card (may just need a reboot if using a standard APN).

Action #11:

- 6300-CX is trying to setup cellular modem. Wait up to 2 minutes to allow 6300-CX to finish. If status LED continues to flash yellow after several minutes, continue with below step(s).
- Login to web UI. Open Configuration page. Verify the Modem -> Enable checkbox is selected.
- If 6300-CX continues to flash yellow for more than 5 minutes, consult the troubleshooting steps for a flashing white status LED.

Action #12:

- Check the Services section of the 6300-CX's configuration. Verify none of the services are reserving the ports needed to access the client device.

Action #13:

- Check the Firewall -> Port Forwarding section of the 6300-CX configuration. Verify that the desired ports are forwarded to the appropriate IP addresses.

Action #14:

- Reduce the Modem → MTU option in the 6300-CX's configuration to 1400.
- Alternately, if you have control of the router connected to the Ethernet port of the 6300-CX, change that router's WAN MTU setting to 1400.

Network Status LED

🟨 **Solid Yellow**
Initializing or starting up.

🟨⬜ **Flashing Yellow**
In the process of connecting to the cellular network and to any device on its LAN port(s).

⬜▨ **Flashing White**
Established LAN connection(s) and is in the process of connecting to the cellular network.

🟩⬜ **Flashing Green**
Connected to 2G or 3G and is in the process of connecting to any device on its LAN port(s), or nothing is connected to the port.

🟩 **Solid Green**
Connected to 2G or 3G and also has a device linked to a LAN port.

🟦⬜ **Flashing Blue**
Connected to 4G LTE and in the process of connecting to a device on its LAN port(s).

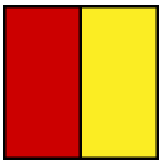
🟦 **Solid Blue**
Connected to 4G LTE and also has a LAN connection.

🟥🟨 **Alternating Red/ Yellow**
Upgrading firmware. **WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.**

Signal Strength LEDs

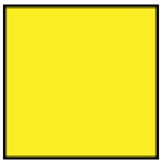
Signal Bars	Weighted dBm	Signal Strength %	Quality
▮	-113 to -99	0 - 23%	Bad
▮▮	-98 to -87	24 - 42%	Marginal
▮▮▮	-86 to -76	43 - 61%	OK
▮▮▮▮	-75 to -64	62 - 80%	Good
▮▮▮▮▮	-63 to -51	81 - 100%	Excellent

Alternating Red/ Yellow



Firmware Update in Progress: DO NOT POWER OFF DEVICE!

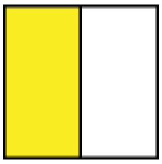
Solid Yellow



6300-CX is starting up.

If LED remains solid yellow for more than 2 minutes, CX may need to be replaced.

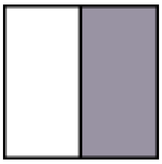
Flashing Yellow



6300-CX is trying to setup cellular modem. Wait up to 2 minutes to allow the process to finish. If status LED continues to flash yellow after several minutes, continue with below step(s):

1. Login to web UI. Open Configuration page. Verify the Modem -> Enable check box is selected.
2. If the 6300-CX continues to flash yellow for more than 5 minutes, consult the troubleshooting steps for a flashing white status LED.

Flashing White



Ethernet link detected, connection is in progress.

Wait up to 2 minutes. If LED status continues, determine the number of Signal Strength LEDs:

None

- Power off the 6300-CX, swap the antennas on the back of the 6300-CX, and power on the 6300-CX. If this resolves the connectivity and the 6300-CX displays two or more bars of signal strength, this may indicate that one of the antennas is faulty. You can continue to use the 6300-CX, but we suggest that you eventually order a replacement set of antennas to improve signal strength even further.
- If swapping the antennas did not resolve the issue, verify the SIM card is inserted properly. Power cycle the 6300-CX after re-insterting the SIM card. Wait 30 to 60 seconds. If the problem persists, the 6300-CX unit cannot detect the SIM and the router may need to be replaced.

One

Relocate the 6300-CX to an area with better signal reception.

Two or More

Verify that the embedded cellular modem firmware of the 6300-CX matches carrier type.

Check the SIM card and the Modem section of the 6300-CX config to verify both are setup with the proper APN.

Login to the web UI. Open the Status page and click on the Cellular Details Tab. Are the **Provider** and **ICCID** values listed?

No

- If the proper Carrier is not listed, contact the cellular provider to verify SIM card activation.
- Try pressing the Erase button (no longer than half a second) to restore default settings on the 6300-CX device. If the SIM card requires a custom APN to connect, you will have to manually reconfigure that on the 6300-CX
- If resetting the configuration on the CX did not resolve the issue, check if the SIM card is provisioned properly. If it is, then there may not be coverage for the desired network in your area.
- Try moving the CX to a different location or using a different cellular provider's SIM card.

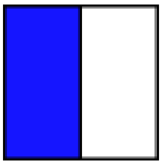
Yes

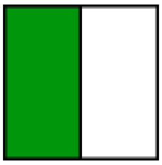
- Power off the 6300-CX, swap the antennas on the back of the 6300-CX, and power on the 6300-CX. If this resolves the connectivity and the 6300-CX displays two or more bars of signal strength, this may indicate that one of the antennas is faulty. You can continue to use the

6300-CX, but we suggest that you eventually order a replacement set of antennas to improve signal strength even further.

- If swapping the antennas did not resolve the issue, verify the SIM card is inserted properly. Power cycle the 6300-CX after re-insterting the SIM card. Wait 30 to 60 seconds. If the problem persists, the 6300-CX unit cannot detect the SIM and the router may need to be replaced.

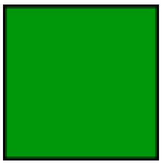
Flashing Blue or Green





6300-CX is connected to the 3G/LTE network, but doesn't see anything connected to its Ethernet port. Check the Ethernet port, verify the client device (router, laptop, etc.) is connected via CAT5/6 to the 6300-CX, and the Ethernet port on the client device is enabled

Solid Green



3G connectivity confirmed

Should the device be on 4G?

Yes

- Verify 4G coverage is available in the area.
- Check embedded cellular modem firmware of 6300-CX. Does it match the type of carrier?
- Check Modem section of 6300-CX config. Verify Access Technology is set to Auto.
- Contact carrier to verify SIM card supports 4G LTE. SIM card may need a custom APN for 4G.

No

Test for Internet access on the device connected to the 6300-CX.

Online

Does the device has a usable IP Address?

- **If no**, see if the client device is expecting a publicly reachable and/or static IP address, check the SIM card and the Modem section of the 6300-CX configuration to verify both are setup with the proper APN.

Are there any ports that are required but cannot be accessed on the client device? Also check if the IP Passthrough has been enabled.

- **If yes**, check the Services section of the 6300-CX's configuration. Verify none of the services are reserving the ports needed to access the client device.
- **If no**, check the Firewall -> Port Forwarding section of the 6300-CX configuration. Verify that the desired ports are forwarded to the appropriate IP addresses.

Offline

Is the client device receiving a DHCP address from the 6300-CX?

- **If yes**, check if the IP Passthrough has been enabled.
  - If yes, are there any ports that are required but cannot be accessed on the client device? Also check if the IP Passthrough has been enabled.
    - If yes, check the Services section of the 6300-CX's configuration. Verify none of the services are reserving the ports needed to access the client device.
    - If no, check the Firewall -> Port Forwarding section of the 6300-CX configuration. Verify that the desired ports are forwarded to the appropriate IP addresses.
  - If no, see if the client device is expecting a publicly reachable and/or static IP address, check the SIM card and the Modem section of the 6300-CX configuration to verify both are setup with the proper APN.
- **If no**, verify Ethernet ports for connection status and check Cat5/ Cat6 cable integrity. Is IP Passthrough mode enabled?
  - If yes, clear DHCP leases by waiting 5 minutes, then reboot the 6300-CX. If clearing DHCP leases didn't fix issue, check that the passthrough IP works with a /30 subnet. If not, contact carrier to change IP on SIM card (may just need a reboot if using a standard APN).
  - If no, verify the Network → Interfaces→ LAN section of the 6300-CX config is setup with a static IP and the DHCP server is enabled.

Online, but with VPN issues

Reduce the Modem → MTU option in the 6300-CX's configuration to 1400. Alternately, if you have control of the router connected to the Ethernet port of the 6300-CX, change that router's WAN MTU seting to 1400.

Briefly Online

1. Disconnect Ethernet cable from CX; power cycle. Wait for CX to fully connect, then reconnect Ethernet port.
2. Verify the 6300-CX is using the correct APN (e.g. on Verizon the 6300-CX may connect with the standard vzwinternet APN, but the SIM card is meant to connect with a static APN such as ne01.vzwstatic)
3. If that didn't fix the issue, try removing the 192.168.210.254 IP address from the Network → Interfaces → Default IP → Default Gateway option in the 6300-CX's config.
4. If that didn't fix the issue, try disabling any/all connectivity tests in the 6300-CX's configuration profile (labelled "ping monitoring" or "connectivity monitoring" in the config).
5. If that didn't fix the issue, contact the cellular provider to check the SIM card's activation and provisioning status.

Solid Blue

🟦

4G connectivity Confirmed

Test for Internet access on the device connected to the 6300-CX.

Online

Does the device has a usable IP Address?

- **If no**, see if the client device is expecting a publicly reachable and/or static IP address, check the SIM card and the Modem section of the 6300-CX configuration to verify both are setup with the proper APN.

Are there any ports that are required but cannot be accessed on the client device? Also check if the IP Passthrough has been enabled.

- If yes, check the Services section of the 6300-CX's configuration. Verify none of the services are reserving the ports needed to access the client device.
- If no, check the Firewall -> Port Forwarding section of the 6300-CX configuration. Verify that the desired ports are forwarded to the appropriate IP addresses.

Offline

Is the client device receiving a DHCP address from the 6300-CX?

- *If yes*, check if the IP Passthrough has been enabled.
  - If yes, are there any ports that are required but cannot be accessed on the client device? Also check if the IP Passthrough has been enabled.
    - *If yes*, check the Services section of the 6300-CX's configuration. Verify none of the services are reserving the ports needed to access the client device.
    - *If no*, check the Firewall -> Port Forwarding section of the 6300-CX configuration. Verify that the desired ports are forwarded to the appropriate IP addresses.
  - If no, see if the client device is expecting a publicly reachable and/or static IP address, check the SIM card and the Modem section of the 6300-CX configuration to verify both are setup with the proper APN.
- *If no*, verify Ethernet ports for connection status and check Cat5/ Cat6 cable integrity. Is IP Passthrough mode enabled?
  - If yes, clear DHCP leases by waiting 5 minutes, then reboot the 6300-CX. If clearing DHCP leases didn't fix issue, check that the passthrough IP works with a /30 subnet. If not, contact carrier to change IP on SIM card (may just need a reboot if using a standard APN).
  - If no, verify the Network → Interfaces→ LAN section of the 6300-CX config is setup with a static IP and the DHCP server is enabled.

Online, but with VPN issues

Reduce the Modem → MTU option in the 6300-CX's configuration to 1400. Alternately, if you have control of the router connected to the Ethernet port of the 6300-CX, change that router's WAN MTU seting to 1400.

Briefly Online

1. Disconnect Ethernet cable from CX; power cycle. Wait for CX to fully connect, then reconnect Ethernet port.
2. Verify the 6300-CX is using the correct APN (e.g. on Verizon the 6300-CX may connect with the standard vzwinternet APN, but the SIM card is meant to connect with a static APN such as ne01.vzwstatic)
3. If that didn't fix the issue, try removing the 192.168.210.254 IP address from the Network → Interfaces → Default IP → Default Gateway option in the 6300-CX's config.

4. If that didn't fix the issue, try disabling any/all connectivity tests in the 6300-CX's configuration profile (labelled "ping monitoring" or "connectivity monitoring" in the config).
5. If that didn't fix the issue, contact the cellular provider to check the SIM card's activation and provisioning status.

FAQs

How do I factory reset the Accelerated 6330-MX?

1. Ensure that the device has been powered on for at least 30 seconds.
2. Briefly press the Erase button located on the back of the device.

What subnet does the Accelerated 6330-MX use?

By default, the Accelerated 6330-MX provisions IP addresses using DHCP over the LAN subnet of 192.168.2.1/24.

What size SIM card does the Accelerated 6330-MX use?

All Accelerated devices support standard mini-SIMs (2FF).

Does the Accelerated 6330-MX fail back to 3G?

Yes, if the Accelerated 6330-MX doesn't recognize a 4G/LTE network available, the device will automatically fallback to the highest available 3G network. Supported networks include DC-HSPA+, HSPA+, HSPA, EDGE, GPRS, GSM and CDMA.

Does the Accelerated 6330-MX support IPv6?

Yes. In passthrough mode, when the 6330-MX receives an IPv6 prefix from the cellular network, it uses SLAAC to pass the prefix to the client device connected to its Ethernet port. The 6330-MX will also pass the IPv6 DNS server using the SLAAC RDNSS option and stateless DHCPv6.

Regulatory Guide

FCC

THIS EQUIPMENT HAS BEEN TESTED AND FOUND TO COMPLY WITH THE LIMITS FOR A CLASS A DIGITAL DEVICE, PURSUANT TO PART 15 OF THE FCC RULES. THESE LIMITS ARE DESIGNED TO PROVIDE REASONABLE PROTECTION AGAINST HARMFUL INTERFERENCE WHEN THE EQUIPMENT IS OPERATED IN A COMMERCIAL ENVIRONMENT. THIS EQUIPMENT GENERATES, USES, AND CAN RADIATE RADIO FREQUENCY ENERGY AND, IF NOT INSTALLED AND USED IN ACCORDANCE WITH THE INSTRUCTION MANUAL, MAY CAUSE HARMFUL INTERFERENCE TO RADIO COMMUNICATIONS. OPERATION OF THIS EQUIPMENT IN A RESIDENTIAL AREA IS LIKELY TO CAUSE HARMFUL INTERFERENCE IN WHICH CASE THE USER WILL BE REQUIRED TO CORRECT THE INTERFERENCE AT HIS OWN EXPENSE. INDUSTRY CANADA - CAN ICES-3(A)/NMB-3(A) THIS PRODUCT IS INTENDED FOR OPERATION IN A COMMERCIAL OR INDUSTRIAL ENVIRONMENT AND SHOULD NOT BE USED IN A RESIDENTIAL ENVIRONMENT. THIS PRODUCT HAS BEEN TESTED AND FOUND TO COMPLY WITH THE REQUIREMENTS OF: ICES-003 - INFORMATION TECHNOLOGY EQUIPMENT - LIMITS AND METHODS OF MEASUREMENT ISSUE 5, AUGUST 2012.

European Union

THIS PRODUCT MAY CAUSE INTERFERENCE IF USED IN RESIDENTIAL AREAS. SUCH USE MUST BE AVOIDED UNLESS THE USER TAKES SPECIAL MEASURES TO REDUCE ELECTROMAGNETIC EMISSIONS TO PREVENT INTERFERENCE TO THE RECEPTION OF RADIO AND TELEVISION BROADCASTS.

Supported Countries

FOR A FULL LIST OF CERTIFIED COUNTRIES GO TO: WWW.ACCELERATED.COM/PRODUCTS/6330_MX_LTE_ROUTER

End User Agreement

ACCELERATED CONCEPTS, INC. END USER AGREEMENT (v20160613.01)

USE OF THIS PRODUCT IS YOUR ACCEPTANCE TO THE ACCELERATED CONCEPTS, INC. END USER AGREEMENT FOUND AT: HTTPS://ACCELERATED.COM/ENDUSERAGREEMENT

LIMITED WARRANTY

Accelerated Concepts, Inc. (“ACI”) provides the Limited Warranty set forth herein on ACI’s VPN and Cellular products (“Product” or “Products”) to the original purchaser (hereinafter referred to as the “End User”) who purchased Products directly from ACI or one of its authorized resellers. This Limited Warranty does not apply to Products purchased from third-parties who falsely claim to be ACI resellers. Please visit our web site if you have questions about authorized resellers.

This Limited Warranty becomes invalid once the End User no longer owns the Product, if the Product or its serial number is altered in any manner, or if any repair or modification to the Product is made by anyone other than an ACI approved agent.

This Limited Warranty covers the Product against defects in materials and workmanship encountered in normal use of the Product as set forth in the Product’s Users Guide for one (1) year from the date of purchase. This Limited Warranty is not intended to include damage relating to shipping, delivery, installation, applications and uses for which the Product was not intended; cosmetic damage or damage to the Product’s exterior finish; damages resulting from accidents, abuse, neglect, fire, water, lighting or other acts of nature; damage resulting from equipment, systems, utilities, services, parts, supplies, accessories, wiring, or software applications not provided by ACI for use with the Product; damage cause by incorrect electrical line voltage, fluctuations, surges; customer adjustments, improper cleaning or maintenance, or a failure to follow any instruction provided in the Product’s Users Guide. This list is not intended to cover every possible limitation to this Limited Warranty. ACI does not warrant against totally uninterrupted or error-free operation of its Products.

In order to obtain warranty service under this Limited Warranty during the Limited Warranty period as set forth above, you must submit a valid claim through ACI’s return merchandise authorization (“RMA”) process as follows:

End User must request an RMA number either from Accelerated support or by sending an e-mail to RMA@accelerated.com with the following information:

1. Your name, address and e-mail address
2. The Product model number and serial number
3. A copy of your receipt
4. A description of the problem

ACI will review your request and e-mail you either an RMA number and shipping instructions or a reason why your request was rejected. Properly pack and ship the Product to ACI with the RMA number written on the outside of each package. ACI will not accept any returned Products which are not accompanied by an RMA number. ACI will use commercially reasonable efforts to ship a replacement device within ten (10) working days after receipt of the Product. Actual delivery times may vary depending on shipment location. Products returned to ACI must conform in quantity and serial number to the RMA request. End User will be notified by e-mail by ACI in the event of any incomplete RMA shipments.

Products presented for repair under this Limited Warranty may be replaced by refurbished goods of the same type rather than being repaired. Refurbished or used parts may be used to repair a Product covered by this Limited Warranty. If ACI, by its sole determination, is unable to replace a Product covered by this Limited Warranty, it will refund the depreciated purchase price of the Product.

LIMITED LIABILITY

EXCEPT AS PROVIDED IN THE LIMITED WARRANTY AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, UNDER NO CIRCUMSTANCES WILL ACI BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING, BUT NOT LIMITED TO, COMPENSATION, REIMBURSEMENT OR DAMAGES ON ACCOUNT OF THE LOSS OF PRESENT OR PROSPECTIVE PROFITS, EXPENDITURES, INVESTMENTS OR COMMITMENTS, WHETHER MADE IN THE ESTABLISHMENT, DEVELOPMENT OR MAINTENANCE OF BUSINESS REPUTATION OR GOODWILL, FOR LOSS OR DAMAGE OF RECORDS OR DATA, COST OF SUBSTITUTE PRODUCTS, COST OF CAPITAL, THE CLAIMS OF ANY THIRDPARTY, OR FOR ANY OTHER REASON WHATSOEVER.

ACI'S LIABILITY, IF ANY, AND THE END USER'S SOLE AND EXCLUSIVE REMEDY FOR DAMAGES FOR ANY CLAIM OF ANY KIND WHATSOEVER REGARDLESS OF THE LEGAL THEORY, SHALL NOT BE GREATER THAN THE PRODUCT'S ACTUAL PURCHASE PRICE.

THIS LIMITATION OF LIABILITY IS APPLICABLE EVEN IF ACI IS INFORMED IN ADVANCE OF THE POSSIBILITY OF DAMAGES BEYOND THE PRODUCT'S ACTUAL PURCHASE PRICE.

SOFTWARE LICENSE

ACI software is copyrighted and is licensed to the End User solely for use with the Product.

Some software components are licensed under the GNU General Public License, version 2. Please visit http://www.gnu.org/licenses/old-licenses/gpl-2.0.en. html for more details regarding GNU GPL version 2.

These GNU General Public License, version 2 software components are available as a CD or download. The CD may be obtained for an administration fee by contacting Accelerated support at support@accelerated.com.

Change Port 3 from WAN to LAN

Difficulty level: *intermediate*

Goal

To change the functionality of the 633x-MX router's port #3 from a WAN connection to be a part of LAN.

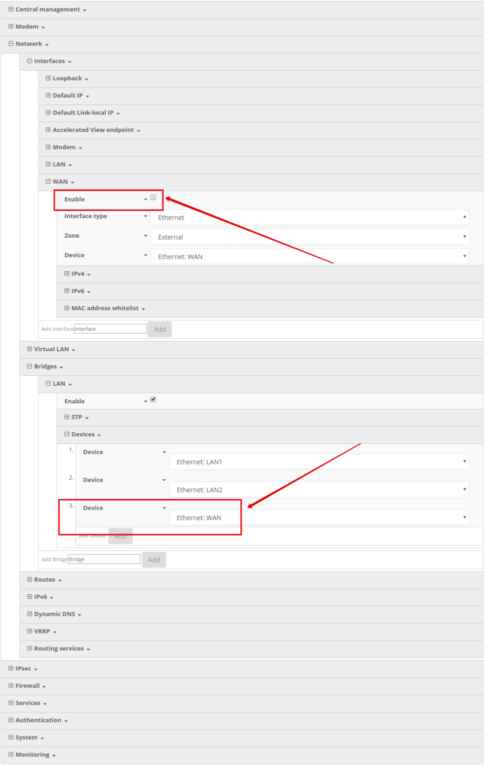
Setup

This article assumes the 633x-MX router is operating under default settings, which provide DHCP connectivity to devices connected ports 1 and 2 of the 633x-MX. For more details on the default settings of the 633x-MX, see the Default Settings section of the 6330-MX User's Manual. Also, refer to the Getting started with Accelerated View for details on how to configure a 6330-MX (or the Local device management section, if you are managing the device without Accelerated View).

Configuration Steps

Open the configuration profile for the 6330-MX and make the following changes.

1. Under *Network -> Interfaces -> WAN*, de-select the *Enabled* checkbox.
2. Under *Network -> Bridges -> LAN -> Devices*, click *Add* and select *Ethernet: WAN* from the drop-down.



- ⊞ Central management
- ⊞ Modem
- ⊟ Network
  - ⊟ Interfaces
    - ⊞ Loopback
    - ⊞ Default IP
    - ⊞ Default Link-local IP
    - ⊞ Accelerated View endpoint
    - ⊞ Modem
    - ⊞ LAN
    - ⊟ WAN
      - Enable □
      - Interface type: Ethernet
      - Zone: External
      - Device: Ethernet: WAN
      - ⊞ IPv4
      - ⊞ IPv6
      - ⊞ MAC address whitelist
    - Add Interface: Interface [Add]
  - ⊞ Virtual LAN
  - ⊟ Bridges
    - ⊟ LAN
      - Enable ☑
      - ⊞ STP
      - ⊟ Devices
        1. Device: Ethernet: LAN1
        2. Device: Ethernet: LAN2
        3. Device: Ethernet: WAN
        - Add Device: [Add]
    - Add Bridge: Bridge [Add]
  - ⊞ Routes
  - ⊞ IPv6
  - ⊞ Dynamic DNS
  - ⊞ VRRP
  - ⊞ Routing services
- ⊞ IPsec
- ⊞ Firewall
- ⊞ Services
- ⊞ Authentication
- ⊞ System
- ⊞ Monitoring

Configure DHCP Server for PXE Booting

Difficulty level: *advanced*

Goal

To set up the 633x-MX router to hand out Trivial File Transfer Protocol (TFTP) server information via Dynamic Host Configuration Protocol (DHCP), allowing the client devices that supports Preboot Environment Execution (PXE) booting to take advantage of the advanced DHCP server settings.

Setup

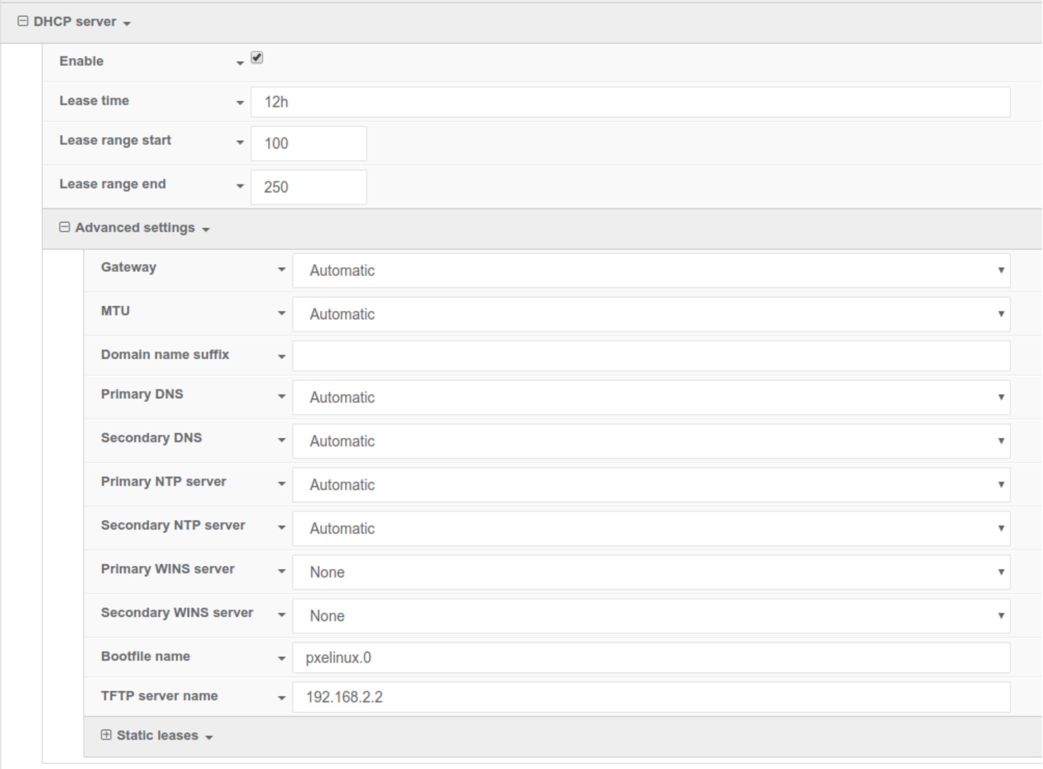
This article assumes the 633x-MX router is operating under default settings, all relevant PXE boot files and TFTP server processes are in place ready to be connected, and the client device is in a state ready for PXE boot.

A generic Linux distribution is used as an example for the set up, and no operating system installations will be covered.

Configuration Steps

Open the configuration profile for the 633x-MX and make the following changes.

1. Navigate to *Network -> Interfaces -> LAN -> IPv4 -> DHCP server -> Advanced settings*.
2. Under field *Bootfile name*, insert: *pxelinux.0* (this depends on the desired file name. If the file is not directly under */tftpboot/*, ensure the relative file path is also included).
3. Under field *TFTP server name*, insert: *192.168.2.x* where '*x*' is the last octet of the TFTP server IP address (assume using subnet /24).
4. Save the configuration.



⊟ DHCP server

Enable	☑
Lease time	12h
Lease range start	100
Lease range end	250

⊟ Advanced settings

Gateway	Automatic
MTU	Automatic
Domain name suffix	
Primary DNS	Automatic
Secondary DNS	Automatic
Primary NTP server	Automatic
Secondary NTP server	Automatic
Primary WINS server	None
Secondary WINS server	None
Bootfile name	pxelinux.0
TFTP server name	192.168.2.2

⊞ Static leases

WiFi as WAN

Difficulty level: *Intermediate*

Goal

To use a separate wireless router's SSID network as a WAN internet connection on the 63xx-series router.

Setup

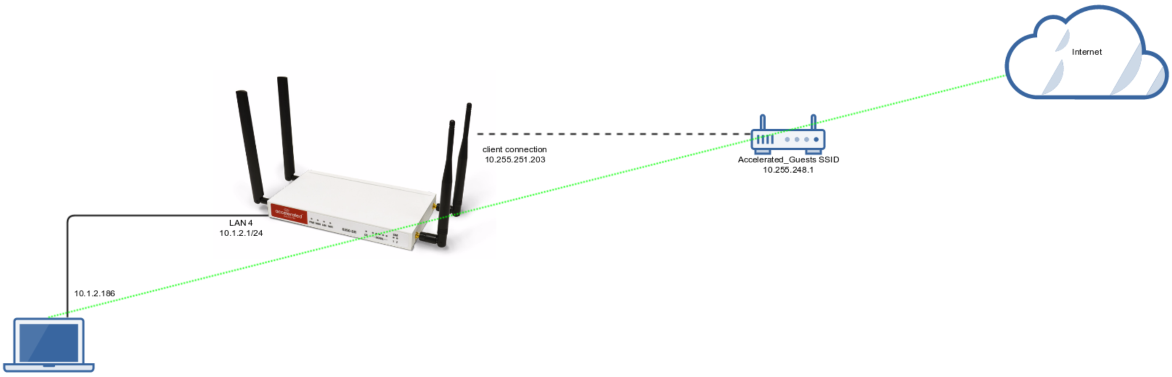
This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 63xx-series router's LAN ports. For more details on the default settings of the 63xx-series router, see the *Default Settings* section of the User Manual.

You will need to establish the following details before configuring the 63xx-series router.

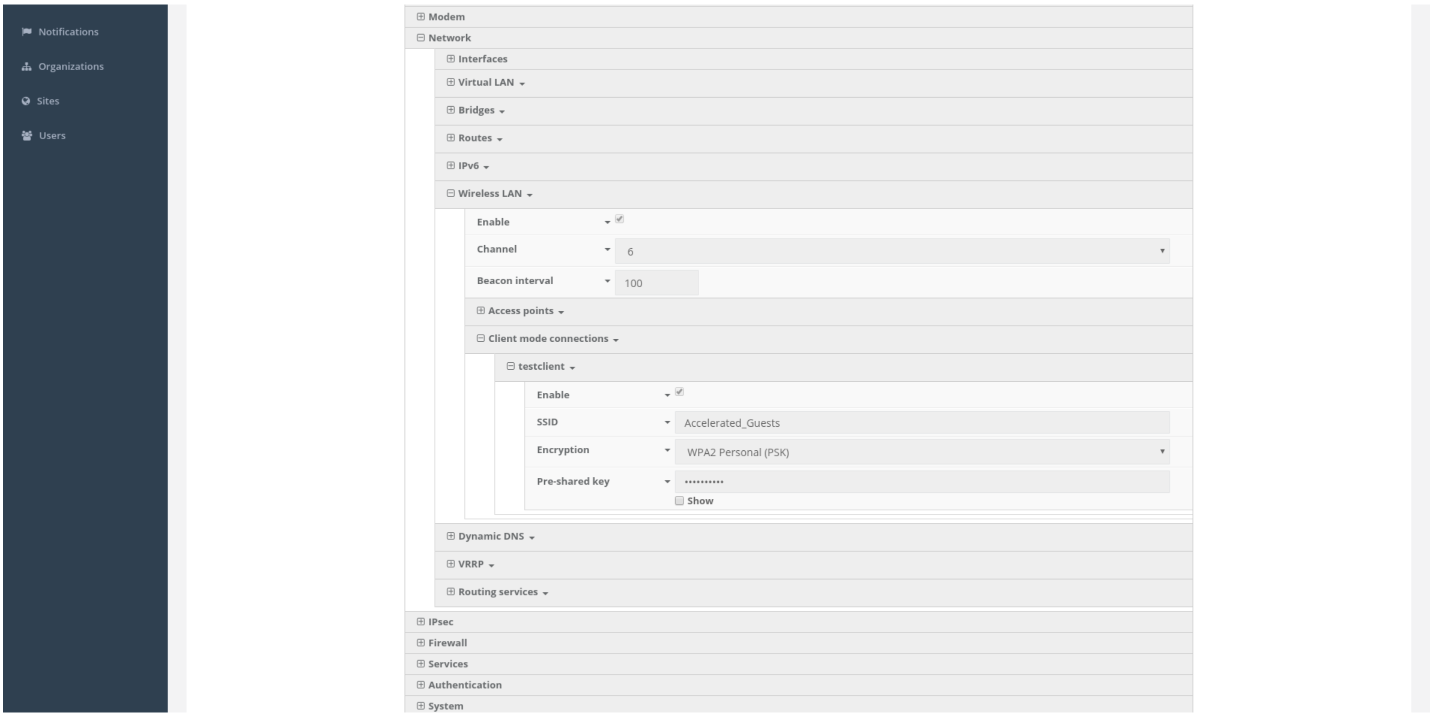
- The SSID you want the 63xx-series router to connect to, including the wireless channel the SSID is broadcasted on.
- The authentication credentials for the SSID.
  - Supported encryption types for WiFi as WAN are open (unencrypted), WPA, and WPA2 PSK
- The priority of the *WiFi as WAN* interface (i.e. should it take precedence over the WAN Ethernet port).

Sample

The following diagram shows a sample setup of a 63xx-series router establishing a client connection to a separate wireless router's SSID (Accelerated Guests), and then using that interface for a *WiFi as WAN* connection. A laptop is shown connected to one of the LAN Ethernet ports of the 63xx-series router as an example end-user device utilizing the *WiFi as WAN* connection.



Sample Configuration



Enable ☑

Channel 6

Beacon interval 100

Enable ☑

SSID Accelerated_Guests

Encryption WPA2 Personal (PSK)

Pre-shared key ••••••••••

□ Show

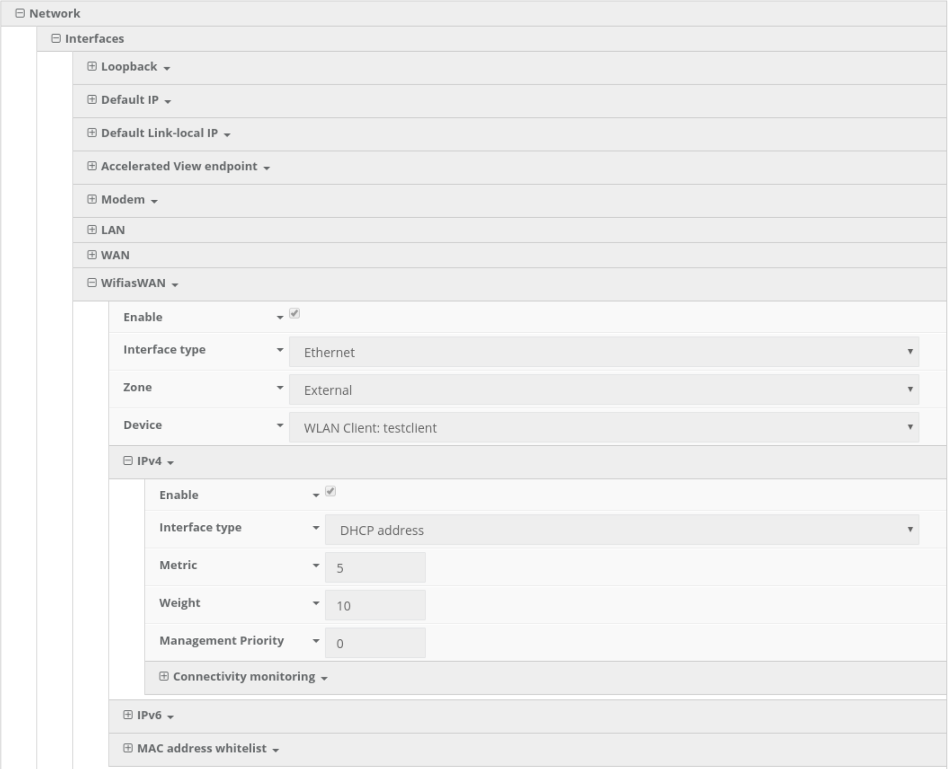
Open the configuration profile for the 63xx-series router and make the following changes.

1. Under *Network -> Wireless LAN -> Channel*, select the channel used by the secondary wireless router's SSID. Note that if you only are establishing one *WiFi as WAN* connection, and disable any AP-mode SSIDs under the Accelerated device's *Network -> Wireless LAN -> Access points* config options, you do not need to specify a specific wireless channel, and can instead leave this *Channel* option set to *Automatic.*
2. Under *Network -> Wireless LAN -> Client mode connections*, create a new entry named *testclient*. The name can be different if desired.
3. Under the new client mode connection entry, enter in the SSID and authentication credentials for the SSID of the secondary wireless router.

Next, under *Network -> Interfaces*, create a new entry named *WiFiasWAN*.

1. Set the *Zone* for the new interface to *External*.
2. Set the *Device* for the new interface to *WLAN Client: testclient*
3. Under *IPv4*, set the *Interface type* to *DHCP address*.
   1. *NOTE:* This will trigger the 63xx-series router to obtain a DHCP connection to the secondary wireless router's SSID network.

4. *Optional*: Set the *Metric* to *0* to make this the primary WAN interface. Doing so will make both the WAN Ethernet and cellular modem (if used) backup WAN connections.
5. Click *Save*.



⊟ Network
⊟ Interfaces
⊞ Loopback
⊞ Default IP
⊞ Default Link-local IP
⊞ Accelerated View endpoint
⊞ Modem
⊞ LAN
⊞ WAN
⊟ WifiasWAN
Enable ☑
Interface type: Ethernet
Zone: External
Device: WLAN Client: testclient
⊟ IPv4
Enable ☑
Interface type: DHCP address
Metric: 5
Weight: 10
Management Priority: 0
⊞ Connectivity monitoring
⊞ IPv6
⊞ MAC address whitelist

Port Forwarding

Difficulty level: *Easy*

Goal

To access a client device on the LAN port of a 63xx-series router using a specific port and the external IP address of the 63xx-series router.

Setup

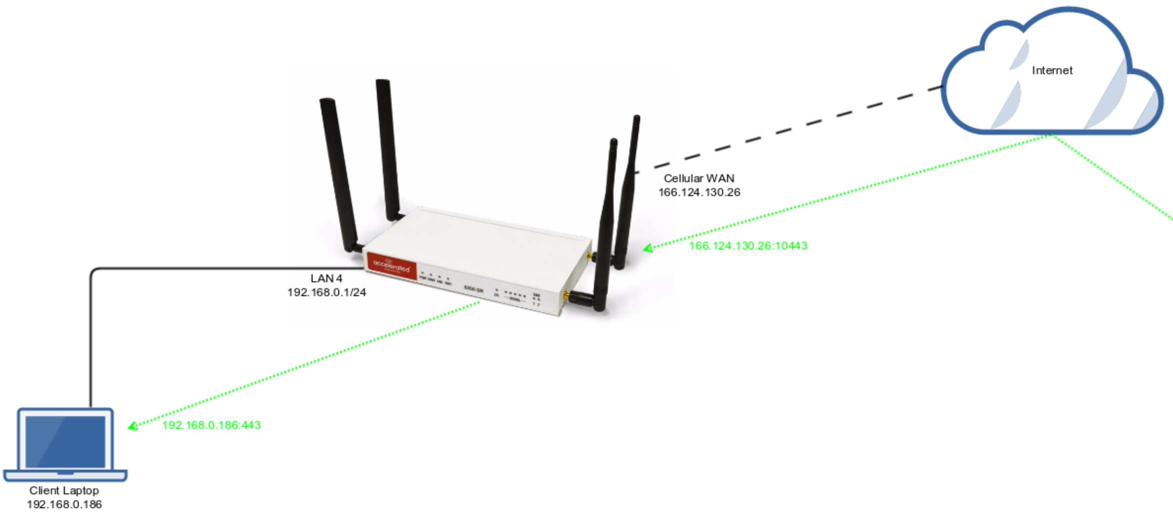
This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 63xx-series router's LAN ports. For more details on the default settings of the 63xx-series router, see the ***Default Settings*** section of the User's Manual.

You will need to establish the following details before configuring the 63xx-series router.

- The IP address of the client device on the LAN port.
- The external port you want to forward to the client device.
- The port you want to access the client device on.

Sample

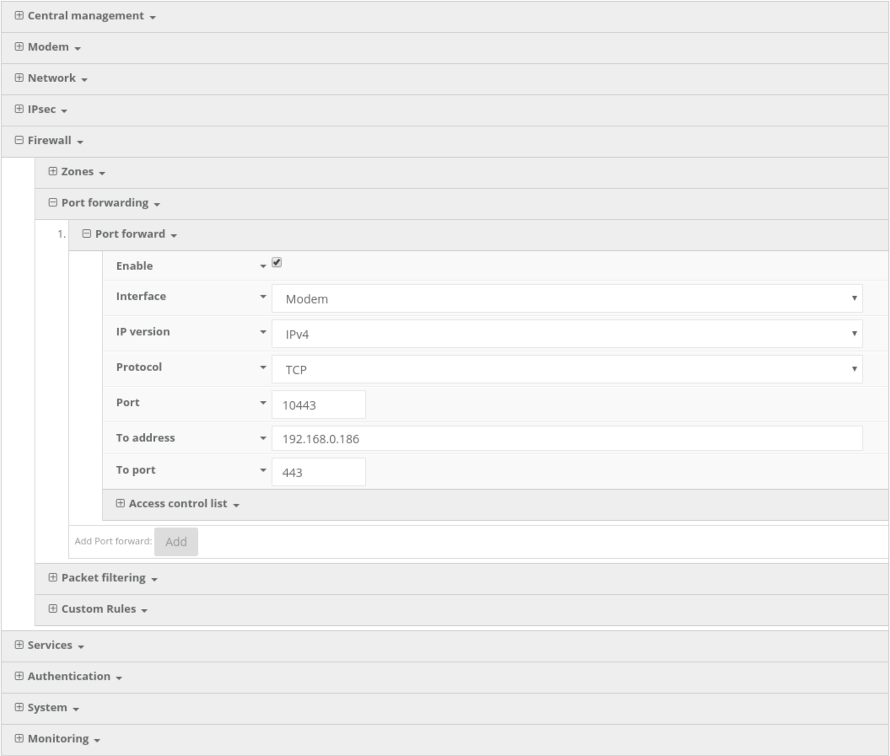
The following diagram shows a sample setup of a 63xx-series router with a cellular WAN connection and a client's laptop connected to LAN port 4. In this setup, we want to access TCP port 443 of the client laptop from the external IP address of the 63xx-series router's cellular WAN connection. We will be configuring the 63xx-series router with a port forwarding rule to forward external port 10443 to port 443 of the client device's LAN IP.



Sample Configuration

Open the configuration profile for the 63xx-series router and make the following changes. Under *Firewall -> Port Forwarding*, click *Add* to create a new entry. Set the following options under the new port forwarding rule.

- *Interface:* Modem
- *Prototol:* TCP
- *Port:* 10443
- *To Address:* 192.168.0.186
- *To Port:* 443



⊞ Central management
⊞ Modem
⊞ Network
⊞ IPsec
⊟ Firewall
⊞ Zones
⊟ Port forwarding
1. ⊟ Port forward

Enable	☑
Interface	Modem
IP version	IPv4
Protocol	TCP
Port	10443
To address	192.168.0.186
To port	443

⊞ Access control list

Carrier (SIM) Smart Select

Difficulty level: *Intermediate*

Goal

To use the 63xx-series router's dual SIM modem to provide internet connectivity with one SIM, and failover to the other SIM slot if the first SIM's connection dies.

Setup

For this setup, you will need two SIM cards enabled, provisioned, and installed in the 63xx-series router's pluggable cellular modem's SIM slots. The two SIM cards can be from the same provider (e.g. two Verizon SIMs), or can be from different carriers.

> *Note:* If one of the SIM cards requires a custom or unique APN, you will need to add this APN into the 63xx- series router's configuration, under the *Modem -> APN* option.

Sample

By default, the 63xx-series router is setup for automatic SIM selection. Meaning, if the 63xx-series router is unable to connect with the SIM in slot 1, after a specified number of failures the 63xx-series router will automatically switch to use the SIM in slot 2.

We will leverage this automatic SIM failover, along with a connectivity monitor, to setup the 63xx-series router to failover between SIM cards if either SIM is unable to establish a cellular connection.

In the sample configuration below, the 63xx-series router is setup to test the cellular network connection once every two minutes. If three sequential tests fail, then the 63xx-series router will restart the cellular connection, attempting to connect with the same SIM card. If the SIM card fails to connect after five attempts (each attempt takes from 10-30 seconds), the 63xx-series router will switch to the secondary SIM slot.

Summed up, if a SIM's cellular connection fails, with the below configuration the 63xx-series router will failover to the secondary SIM in under 10 minutes.

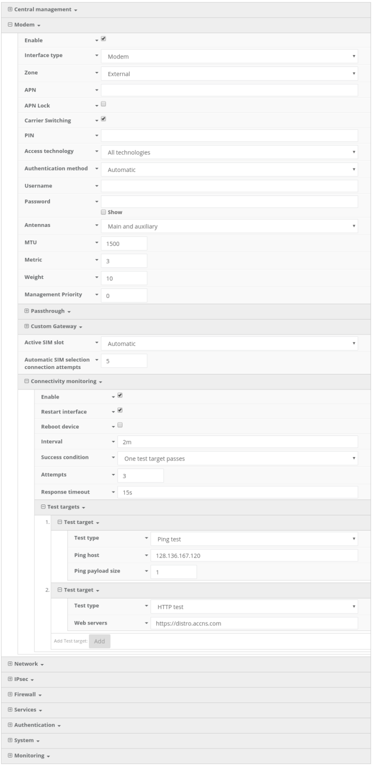
Sample Configuration

Open the configuration profile for the 63xx-series router and make the following changes. Under *Modem*, set the following options.

- Active SIM slot: Automatic
- Automatic SIM selection connection attempts: 5

Next, open the *Modem -> Connectivity Monitoring* section and make the following changes.

- **Enabled:** checked
- **Restart interface:** checked
- **Interval:** 2m
- **Attempts:** 3
- **Test targets:** a ping test to *128.136.167.120* and a HTTP test to *distro.accns.com*



⊞ Central management

⊟ Modem

Enable ☑

Interface type: Modem

Zone: External

APN:

APN Lock ☐

Carrier Switching ☑

PIN:

Access technology: All technologies

Authentication method: Automatic

Username:

Password:

☐ Show

Antennas: Main and auxiliary

MTU: 1500

Metric: 3

Weight: 10

Management Priority: 0

⊞ Passthrough

⊞ Custom Gateway

Active SIM slot: Automatic

Automatic SIM selection connection attempts: 5

⊟ Connectivity monitoring

Enable ☑

Restart interface ☑

Reboot device ☐

Interval: 2m

Success condition: One test target passes

Attempts: 3

Response timeout: 15s

⊟ Test targets

1. ⊟ Test target

Test type: Ping test

Ping host: 128.136.167.120

Ping payload size: 1

2. ⊟ Test target

Test type: HTTP test

Web servers: https://distro.accns.com

Add Test target: Add

⊞ Network

⊞ IPsec

⊞ Firewall

⊞ Services

⊞ Authentication

⊞ System

⊞ Monitoring

Failover

Difficulty level: *Beginner*

Goal

To use the 63xx-series router's cellular modem as a backup WAN connection for the primary WAN Ethernet port. The 63xx-series router will use the WAN Ethernet port as its main Internet connection, and will fail over to the cellular modem if the primary connection goes down.

Setup

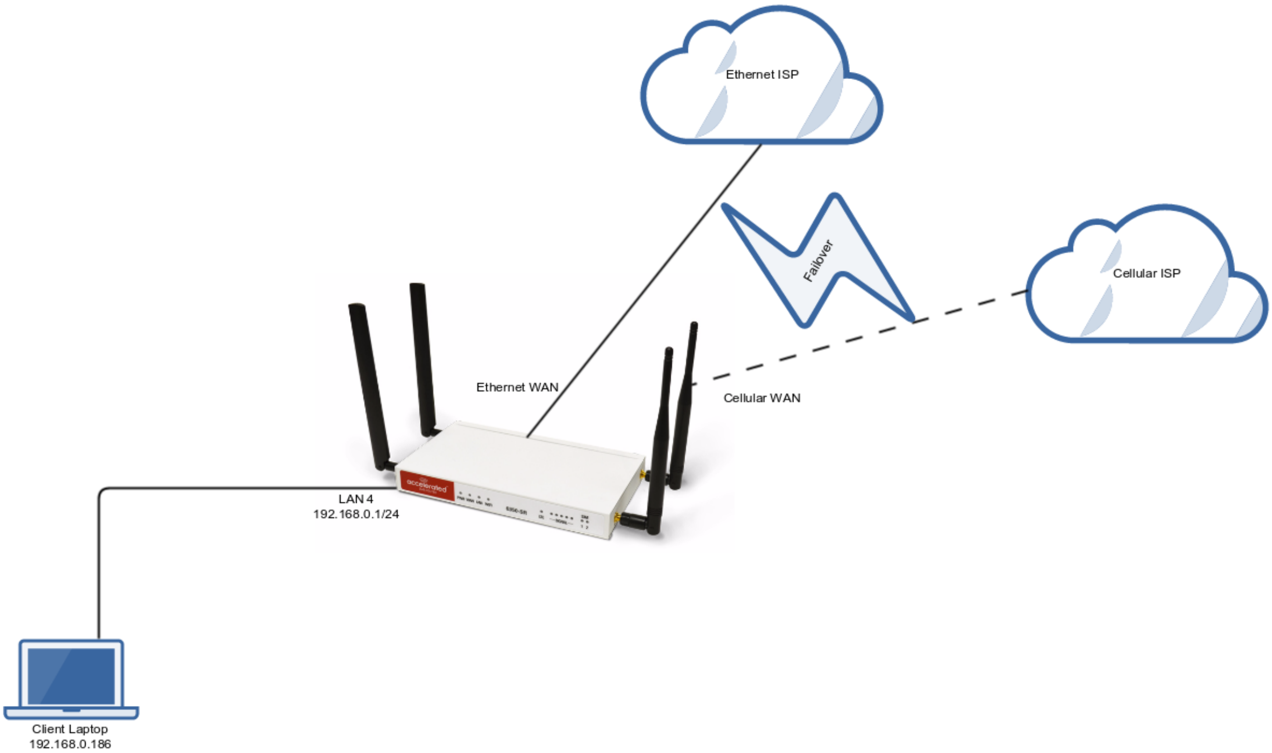
This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 63xx-series router's LAN ports. For more details on the default settings of the 63xx-series router, see the ***Default Settings*** section of the SR User's Manual.

For this setup, you will need the 63xx-series router with both a primary WAN Ethernet connection, and a cellular modem connection.

Sample

The sample configuration below shows a 63xx-series router with two internet connections. The WAN Ethernet interface will be used as the primary Internet connection. The 63xx-series router is setup to test the WAN Ethernet connection twice every minute. If three sequential tests fail, then the 63xx-series router will restart the WAN Ethernet connection, and failover to the cellular modem's Internet connection until the WAN Ethernet connection is re-established.

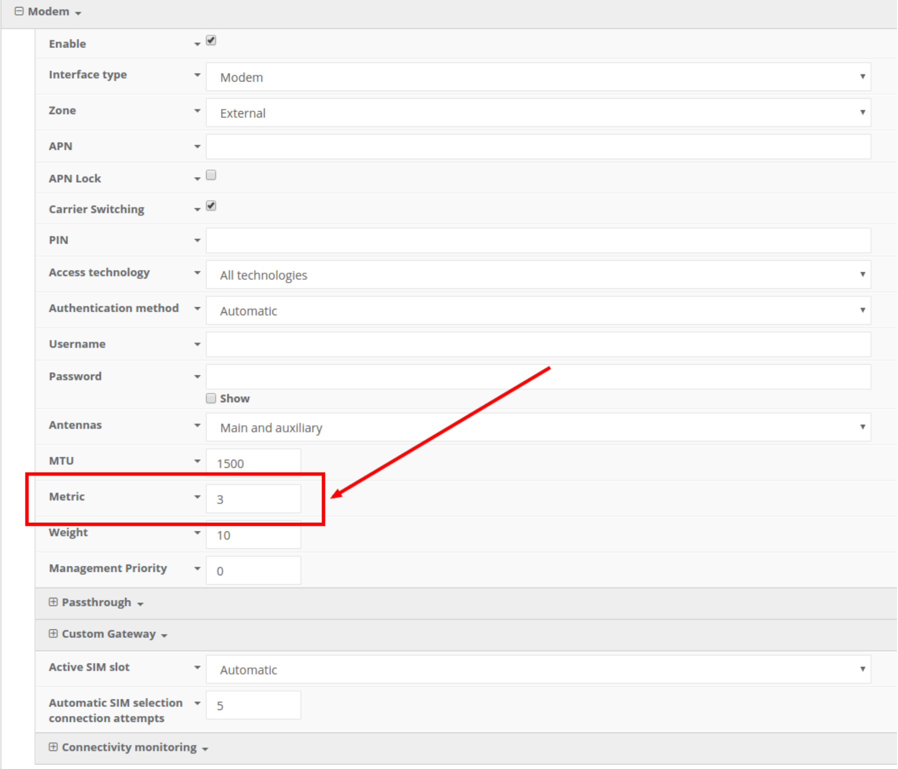
Summed up, if a 63xx-series router's primary WAN connection fails, with the below configuration the 63xx-series router will failover to the cellular modem in under 2 minutes.



Sample Configuration

Open the configuration profile for the 63xx-series router and make the following changes.

In the *Modem -> Metric entry*, ensure the value is set to a number higher than the the value in *Network -> Interfaces -> WAN -> IPv4 -> Metric*. The interface with the lower metric takes higher precedence. By default, the cellular modem metric should be 3 and the WAN Ethernet's metric should be 1, making WAN Ethernet the primary and the cellular modem the backup Internet connection.



⊟ Modem

Enable	☑
Interface type	Modem
Zone	External
APN	
APN Lock	□
Carrier Switching	☑
PIN	
Access technology	All technologies
Authentication method	Automatic
Username	
Password	 □ Show
Antennas	Main and auxiliary
MTU	1500
Metric	3
Weight	10
Management Priority	0

⊞ Passthrough

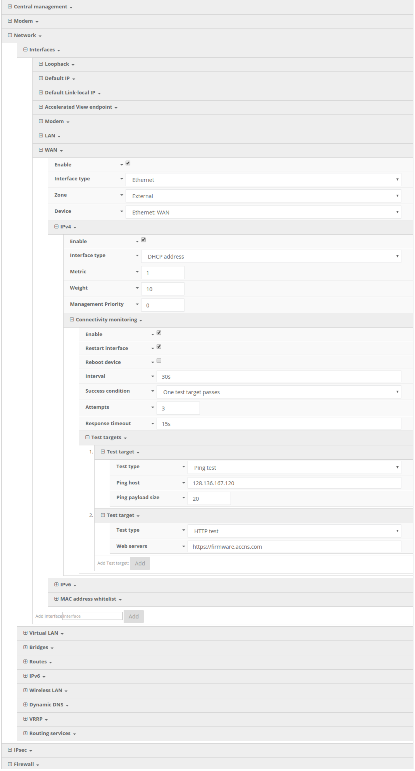
⊞ Custom Gateway

Active SIM slot	Automatic
Automatic SIM selection connection attempts	5

⊞ Connectivity monitoring

Next, open the *Network -> Interfaces -> WAN -> IPv4 -> Connectivity Monitoring* section and make the following changes.

- Enabled: checked
- Restart interface: checked
- Interval: 30s
- Attempts: 3
- Test targets: a ping test to *128.136.167.120* and a HTTP test to *firmware.accns.com*



- ⊞ Central management
- ⊞ Modem
- ⊟ Network
  - ⊟ Interfaces
    - ⊞ Loopback
    - ⊞ Default IP
    - ⊞ Default Link-local IP
    - ⊞ Accelerated View endpoint
    - ⊞ Modem
    - ⊞ LAN
    - ⊟ WAN
      - Enable ☑
      - Interface type: Ethernet
      - Zone: External
      - Device: Ethernet: WAN
      - ⊟ IPv4
        - Enable ☑
        - Interface type: DHCP address
        - Metric: 1
        - Weight: 10
        - Management Priority: 0
        - ⊟ Connectivity monitoring
          - Enable ☑
          - Restart interface ☑
          - Reboot device □
          - Interval: 30s
          - Success condition: One test target passes
          - Attempts: 3
          - Response timeout: 15s
          - ⊟ Test targets
            1. ⊟ Test target
               - Test type: Ping test
               - Ping host: 128.136.167.120
               - Ping payload size: 20
            2. ⊟ Test target
               - Test type: HTTP test
               - Web servers: https://firmware.accns.com

            Add Test target: Add
      - ⊞ IPv6
      - ⊞ MAC address whitelist

    Add Interface Interface Add
  - ⊞ Virtual LAN
  - ⊞ Bridges
  - ⊞ Routes
  - ⊞ IPv6
  - ⊞ Wireless LAN
  - ⊞ Dynamic DNS
  - ⊞ VRRP
  - ⊞ Routing services
- ⊞ IPsec
- ⊞ Firewall

Load Balancing

Difficulty level: *Easy*

Goal

To configure additional WAN interfaces on the 63xx-series router in tandem with its primary WAN uplink such that all interfaces share the network load for Internet connectivity.

> NOTE: The cellular plug-in module is available as a WAN interface by default, though additional interfaces can be configured. For more information please refer to the configuration example for *Dual WAN Ethernet Ports*.

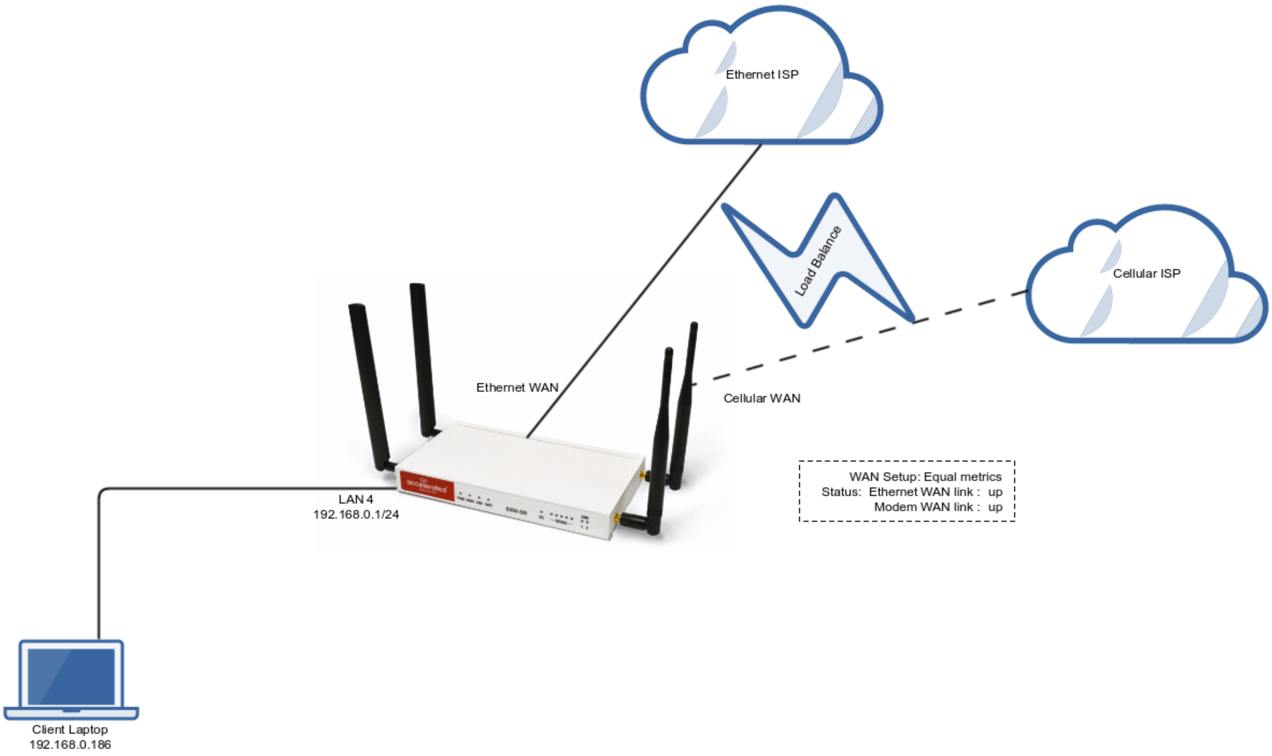
Setup

This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 63xx-series router's LAN ports. For more details on the default settings of the 6350-SR, see the *Default Settings* section of the User Manual.

For this setup, you will need the 63xx-series router with both a primary WAN Ethernet connection and a secondary means of WAN access.

Sample

The sample configuration below shows a 6350-SR with two Internet connections: a cellular-based WAN connection through the 6350-SR's modem, and a broadband-based WAN connection through the 6350-SR's WAN Ethernet port. Both WAN interfaces will be utilized equally, sharing 50% of the WAN network traffic.

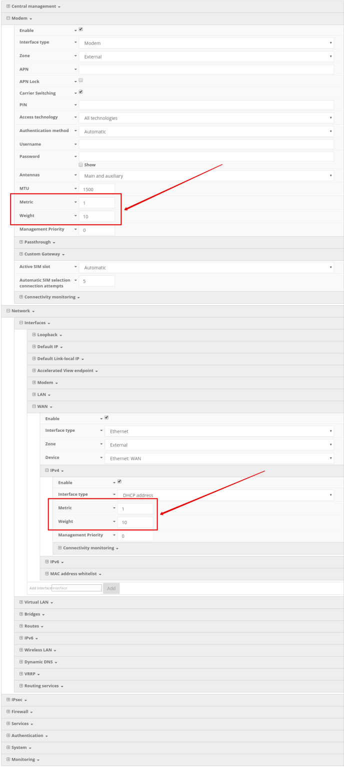


Sample Configuration

Open the configuration profile for the 63xx-series router and make the following changes.

1. In the *Modem -> Metric* entry, ensure the value is set to the same number set in the *Network -> Interfaces -> WAN -> IPv4 -> Metric* setting.
2. In the *Modem -> Weight* entry, ensure the value is set to the same number set in the *Network -> Interfaces -> WAN -> IPv4 -> Weight* setting. This will set a 1:1 ratio between the two WAN interfaces, so each interface is handling 50% of the WAN network traffic.

NOTE: The *weight* setting can be adjusted if you prefer to weigh the WAN traffic differently. For example, if you instead want 75% of the WAN traffic to go through the Ethernet WAN interface, and only 25% to go through the cellular modem's WAN interface (i.e. a 1:4 ratio), you would set the weight of the *Modem* interface to *3* and the weight of the *WAN -> IPv4* interface to *12* (or any 1:4 ratio of numbers, such as *1* and *4*, or *2* and *8*).



⊞ Central management

⊟ Modem

Enable ☑

Interface type: Modem

Zone: External

APN:

APN Lock □

Carrier Switching ☑

PIN:

Access technology: All technologies

Authentication method: Automatic

Username:

Password:

□ Show

Antennas: Main and auxiliary

MTU: 1500

Metric: 1

Weight: 10

Management Priority: 0

⊞ Passthrough

⊞ Custom Gateway

Active SIM slot: Automatic

Automatic SIM selection connection attempts: 5

⊞ Connectivity monitoring

⊟ Network

⊟ Interfaces

⊞ Loopback

⊞ Default IP

⊞ Default Link-local IP

⊞ Accelerated View endpoint

⊞ Modem

⊞ LAN

⊟ WAN

Enable ☑

Interface type: Ethernet

Zone: External

Device: Ethernet: WAN

⊟ IPv4

Enable ☑

Interface type: DHCP address

Metric: 1

Weight: 10

Management Priority: 0

⊞ Connectivity monitoring

⊞ IPv6

⊞ MAC address whitelist

Add Interface: Interface

Add

⊞ Virtual LAN

⊞ Bridges

⊞ Routes

⊞ IPv6

⊞ Wireless LAN

⊞ Dynamic DNS

⊞ VRRP

⊞ Routing services

⊞ IPsec

⊞ Firewall

⊞ Services

⊞ Authentication

⊞ System

⊞ Monitoring

Add a New SSID

Difficulty level: *Beginner*

Goal

To add a new SSID that WiFi-enabled client devices can connect to for Internet access.

Setup

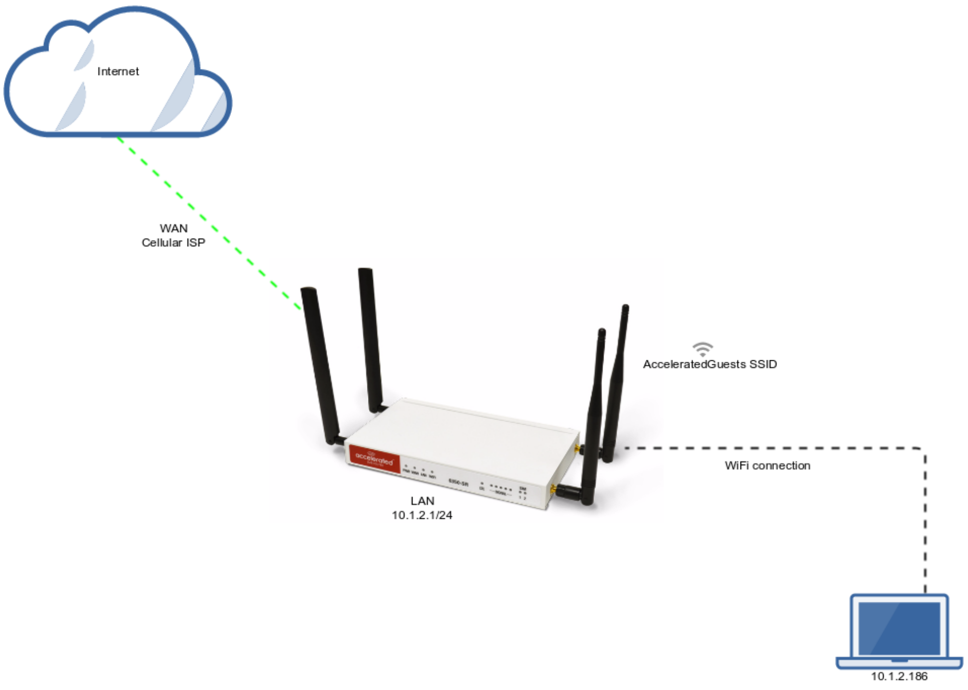
You will need to establish the following details before configuring the 63xx-series router.

- The name of the SSID you want the 63xx-series router to broadcast.
- The authentication credentials for the SSID.

Sample

The following diagram shows a sample setup of a 6350-SR broadcasting a SSID named AcceleratedGuests. The SSID is encrypted with WPA2 security, with a passphrase of *testing123*

Clients connected to that SSID can access the Internet through the 6350-SR's cellular ISP connection. A laptop is shown connected to the AcceleratedGuests SSID as an example end-user device utilizing the connection.

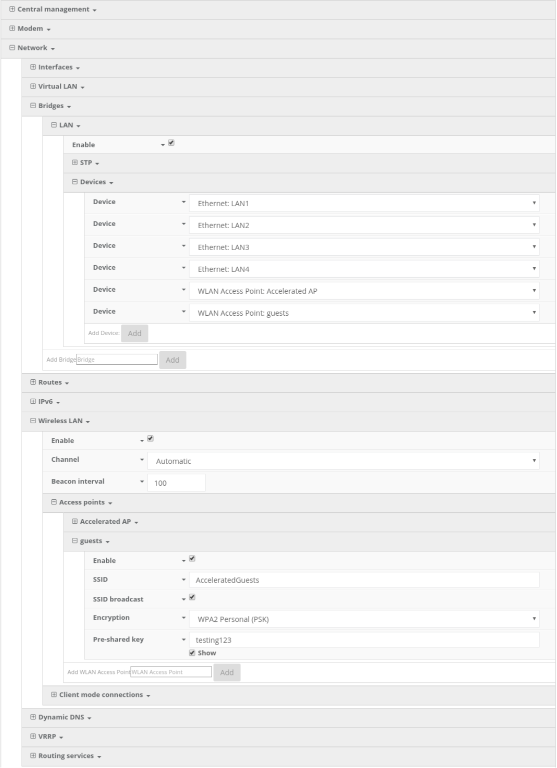


Sample Configuration

Open the configuration profile for the 63xx-series router and make the following changes.

1. Under *Network -> Wireless LAN -> Access points*, create a new entry named *guests*. The name can be different if desired.
2. Enter in the desired SSID name and authentication credentials.
3. Under *Network -> Bridges -> LAN -> Devices*, click *Add* and select *WLAN Access Point: guests* from the drop-down.

4. Click *Save*.



Enable ☑

Device: Ethernet: LAN1

Device: Ethernet: LAN2

Device: Ethernet: LAN3

Device: Ethernet: LAN4

Device: WLAN Access Point: Accelerated AP

Device: WLAN Access Point: guests

Enable ☑

Channel: Automatic

Beacon interval: 100

Enable ☑

SSID: AcceleratedGuests

SSID broadcast ☑

Encryption: WPA2 Personal (PSK)

Pre-shared key: testing123

☑ Show

Individual LAN port setup (VLAN)

Difficulty level: *Expert*

Goal

To setup a VLAN to separate network traffic on one LAN port from all other LAN interfaces.

Setup

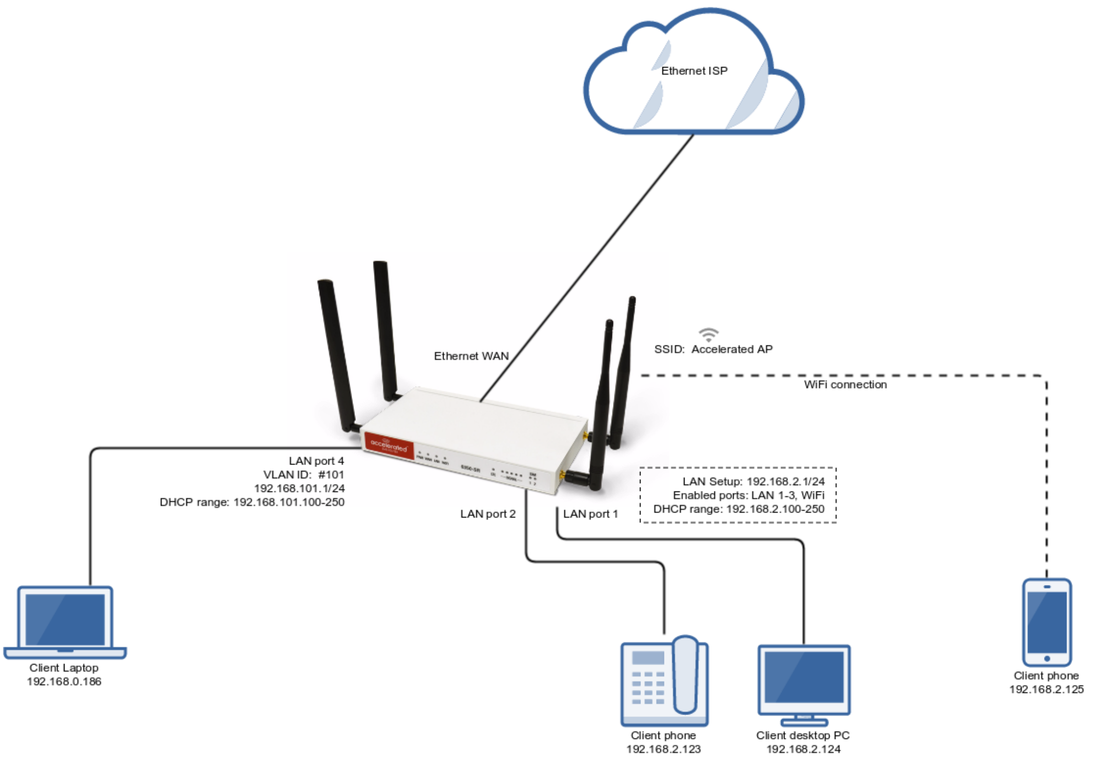
This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 6350-SR's LAN ports. For more details on the default settings of the 6350-SR, see the ***Default Settings*** section of the 6350-SR User's Manual.

You will need to establish the following details before configuring the 6350-SR.

- The IP address range for the VLAN subnet.
- The LAN Ethernet port or SSID you want to separate onto the VLAN interface.

Sample

The following diagram shows a sample setup of a 6350-SR with LAN port 4 separated from the other LAN ports, and placed in a VLAN with ID #101. VLAN 101 is configured to hand out IP addresses within the 192.168.101.100 - 192.168.101.250 range, with a gateway IP of 192.168.101.1/24



Sample Configuration

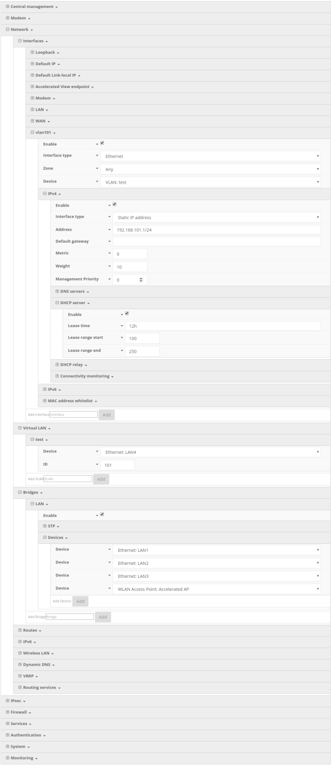
Open the configuration profile for the 6350-SR and make the following changes. Under *Network -> Virtual LAN*, perform the following:

1. Create a new entry named *test.* The name can be different if desired.
2. Select the desired LAN interface under the *Device* drop-down.
3. Type in the desired VLAN ID number in the *ID* field.

Next, under *Network -> Interfaces*, perform the following:

1. Create a new entry named *vlan##*, where *##* is the number of the VLAN ID. The name can be different if desired.
2. Select the *VLAN: test* option in the *Device* drop-down.
3. Type in the desired IP address and subnet in the *Address* field.
4. Under *DHCP server* , ensure the *Enabled* option is checked, and the DHCP lease range *start* and *end* values match the desired DHCP range.

Finally, under *Network -> Bridges -> LAN -> Devices*, remove *Ethernet: LAN4* device from the LAN bridge.



- ⊞ Central management
- ⊞ Modem
- ⊟ Network
  - ⊟ Interfaces
    - ⊞ Loopback
    - ⊞ Default IP
    - ⊞ Default Link-local IP
    - ⊞ Accelerated View endpoint
    - ⊞ Modem
    - ⊞ LAN
    - ⊞ WAN
    - ⊟ vlan101
      - Enable ☑
      - Interface type: Ethernet
      - Zone: Any
      - Device: VLAN: test
      - ⊟ IPv4
        - Enable ☑
        - Interface type: Static IP address
        - Address: 192.168.101.1/24
        - Default gateway:
        - Metric: 0
        - Weight: 10
        - Management Priority: 0
        - ⊞ DNS servers
        - ⊟ DHCP server
          - Enable ☑
          - Lease time: 12h
          - Lease range start: 100
          - Lease range end: 250
        - ⊞ DHCP relay
        - ⊞ Connectivity monitoring
      - ⊞ IPv6
      - ⊞ MAC address whitelist
    - Add Interface: Interface [Add]
  - ⊟ Virtual LAN
    - ⊟ test
      - Device: Ethernet: LAN4
      - ID: 101
    - Add VLAN: VLAN [Add]
  - ⊟ Bridges
    - ⊟ LAN
      - Enable ☑
      - ⊞ STP
      - ⊟ Devices
        - Device: Ethernet: LAN1
        - Device: Ethernet: LAN2
        - Device: Ethernet: LAN3
        - Device: WLAN Access Point: Accelerated AP
        - Add Device: [Add]
    - Add Bridge: Bridge [Add]
  - ⊞ Routes
  - ⊞ IPv6
  - ⊞ Wireless LAN
  - ⊞ Dynamic DNS
  - ⊞ VRRP
  - ⊞ Routing services
- ⊞ IPsec
- ⊞ Firewall
- ⊞ Services
- ⊞ Authentication
- ⊞ System
- ⊞ Monitoring

IPv6

Difficulty level: *Intermediate*

Goal

To setup IPv6 connectivity on the Ethernet WAN of the 6350-SR, and setup a IPv6 DHCP server for client connectivity on the 6350-SR's LAN Ethernet ports and WiFi SSIDs.

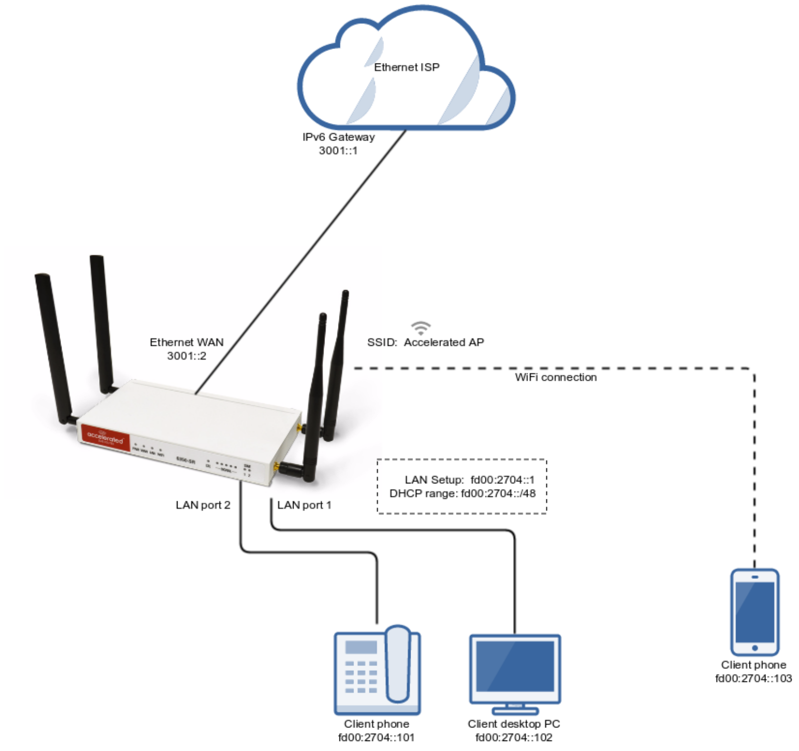
Setup

You will need to establish the following details before configuring the 6350-SR.

- The IPv6 address range for the LAN network.

Sample

The following diagram shows a sample setup of a 6350-SR with an IPv6 DHCP server running on its LAN ports and WiFi, and the 6350-SR has a DHCP IPv6 connection on its WAN Ethernet port. The 6350-SR runs an IPv6 DHCP server to hand out IP addresses in the fd00:2704::/48 range, with a gateway IP of fd00:2704::1



Sample Configuration

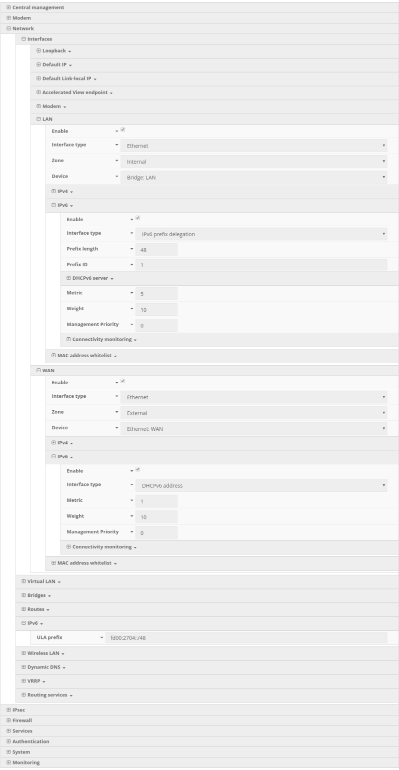
Open the configuration profile for the 6350-SR and make the following changes:

To enable the IPv6 DHCP server on the LAN and WiFi SSIDs.

1. Under *Network -> IPv6*, set the *ULA prefix* to *fd00:2704::/48*
2. Under *Network -> Interfaces -> LAN -> IPv6*, set the *Interface type* to *IPv6 prefix delegation*.
3. Under *Network -> Interfaces -> LAN -> IPv6*, set the *Prefix length* to *48*.
4. Under *Network -> Interfaces -> LAN -> IPv6*, enable the *DHCPv6 server.*
5. *Optional:* for complete LAN IPv6 connectivity without IPv4, uncheck *Network -> Interfaces -> LAN -> IPv4 -> Enable.*

To enable WAN IPv6 via DHCP.

1. Under *Network -> Interfaces -> WAN -> IPv6*, set the *Interface type* to *DHCPv6 address*.
2. *Optional:* for complete WAN IPv6 connectivity without IPv4, uncheck *Network -> Interfaces -> WAN -> IPv4 -> Enable.*



```
⊞ Central management
⊞ Modem
⊟ Network
    ⊟ Interfaces
        ⊞ Loopback
        ⊞ Default IP
        ⊞ Default Link-local IP
        ⊞ Accelerated View endpoint
        ⊞ Modem
        ⊟ LAN
            Enable                ☑
            Interface type        Ethernet
            Zone                  Internal
            Device                Bridge: LAN
            ⊞ IPv4
            ⊟ IPv6
                Enable                ☑
                Interface type        IPv6 prefix delegation
                Prefix length         48
                Prefix ID             1
                ⊞ DHCPv6 server
                Metric                5
                Weight                10
                Management Priority   0
                ⊞ Connectivity monitoring
            ⊞ MAC address whitelist
        ⊟ WAN
            Enable                ☑
            Interface type        Ethernet
            Zone                  External
            Device                Ethernet: WAN
            ⊞ IPv4
            ⊟ IPv6
                Enable                ☑
                Interface type        DHCPv6 address
                Metric                1
                Weight                10
                Management Priority   0
                ⊞ Connectivity monitoring
            ⊞ MAC address whitelist
    ⊞ Virtual LAN
    ⊞ Bridges
    ⊞ Routes
    ⊟ IPv6
        ULA prefix            fd00:2704::/48
    ⊞ Wireless LAN
    ⊞ Dynamic DNS
    ⊞ VRRP
    ⊞ Routing services
⊞ IPsec
⊞ Firewall
⊞ Services
⊞ Authentication
⊞ System
⊞ Monitoring
```

Dual WAN Policy-based Routing

Difficulty: *Intermediate*

Minimum firmware version: *17.11.125*

Goal

To use the 635xx-series router's cellular modem in tandem with its primary WAN Ethernet port, but direct certain IP addresses destinations to go always through the cellular modem's Internet connection.

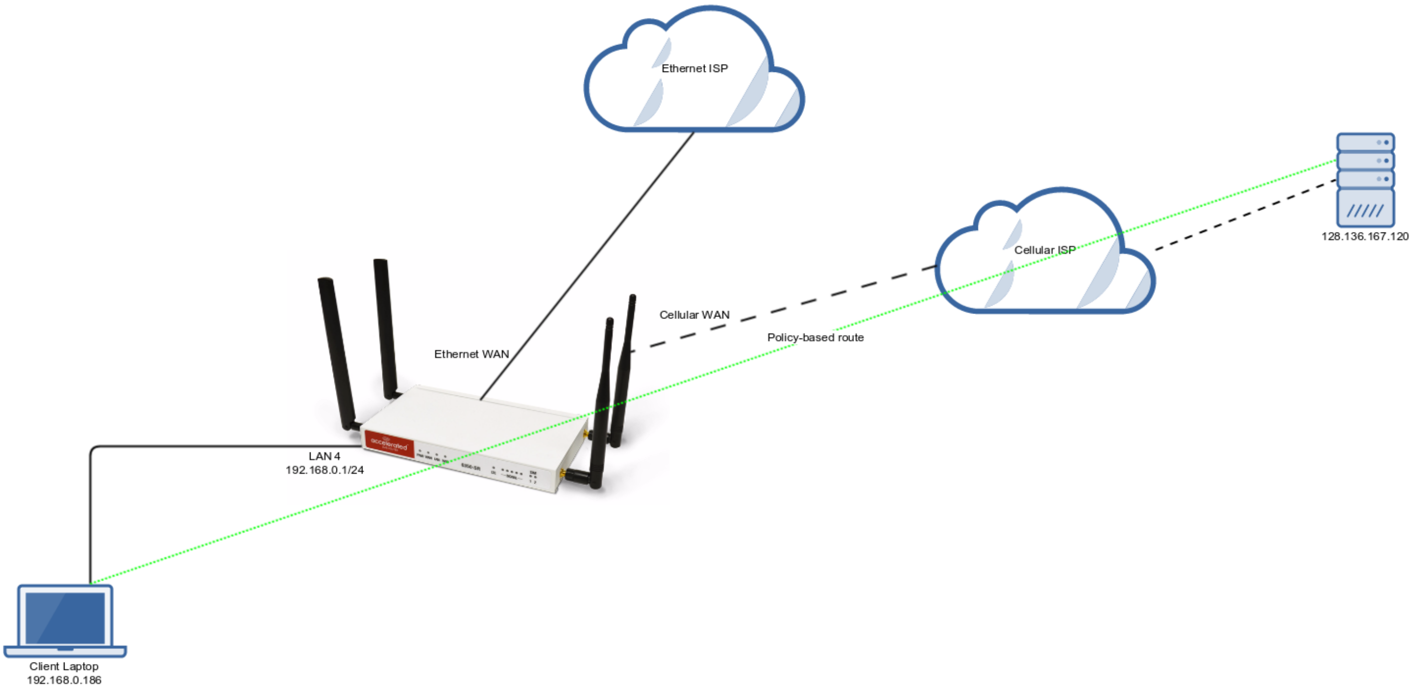
Setup

This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 63xx-series router's LAN ports. For more details on the default settings of the 63xx-series router, see the ***Default Settings*** section of the User's Manual.

For this setup, you will need the 63xx-series router with both a primary WAN Ethernet connection, and a cellular modem connection.

Sample

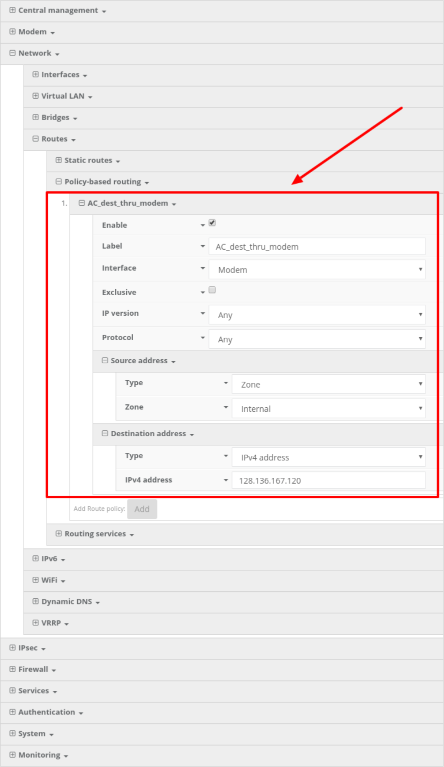
The sample configuration below shows a 63xx-series router with two Internet connections: a cellular-based WAN connection through the 63xx-series router's modem, and a broadband-based WAN connection through the 63xx-series router's WAN Ethernet port. The 63xx-series router's cellular WAN connection will be used to provide access to the 128.136.167.120 IP address, while all other access will be sent through the primary WAN Ethernet connection.



Sample Configuration

Under *Network -> Routes -> Policy-based routing*, setup a new policy with the following settings:

1. *Interface:* Modem
2. *Source address -> Type:* Zone
3. *Source address -> Zone:* Internal
4. *Destination address -> Type:* IPv4 address
5. *Destination address -> IPv4 address:* 128.136.167.120



1. ⊟ AC_dest_thru_modem

Enable	☑
Label	AC_dest_thru_modem
Interface	Modem
Exclusive	☐
IP version	Any
Protocol	Any

⊟ Source address

Type	Zone
Zone	Internal

⊟ Destination address

Type	IPv4 address
IPv4 address	128.136.167.120

Add Route policy: Add

Per-device Policy-based Routing with Dual WAN

Difficulty: *Expert*

Goal

To use the 6350-SR's cellular modem in tandem with its primary WAN Ethernet port, but only allow certain IP addresses access to the cellular modem's Internet connection.

Setup

This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 6350-SR's LAN ports. For more details on the default settings of the 6350-SR, see the ***Default Settings*** section of the 6350-SR User's Manual.

For this setup, you will need the 6350-SR with both a primary WAN Ethernet connection, and a cellular modem connection.

You will also need to configure a static IP address on any client devices you want to allow access to the cellular modem connection.

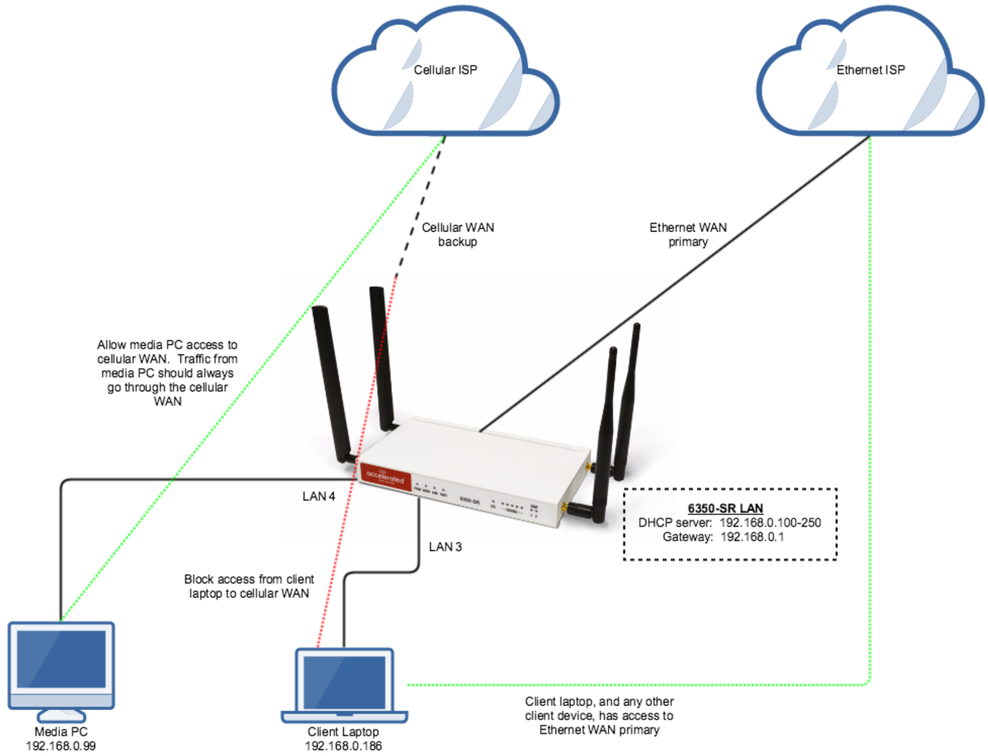
Sample

The sample configuration below shows a 6350-SR with two Internet connections: a cellular-based WAN connection through the 6350-SR's modem, and a broadband-based WAN connection through the 6350-SR's WAN Ethernet port.

This set setup shows two client devices on a 6350-SR's LAN ports, a media PC and a laptop. The media PC is configured with a static IP address of 192.168.0.99, and the laptop is getting its IP address via DHCP from the 6350-SR.

The policy-based routing we are going to setup will accomplish the following.

1. The 6350-SR uses the Ethernet WAN as its primary interface.
2. The 6350-SR has a cellular modem connection, used as a secondary WAN interface.
3. All traffic from the media PC will always go through the cellular modem WAN interface.
4. Any traffic from other LAN devices should go through the Ethernet WAN connection.
5. If the Ethernet WAN connection is down, the 6350-SR should drop any packets from LAN devices, excluding packets from the media PC, and prevent them from going out the cellular modem interface.


Cellular ISP
Ethernet ISP
Cellular WAN backup
Ethernet WAN primary
Allow media PC access to cellular WAN. Traffic from media PC should always go through the cellular WAN
LAN 4
LAN 3
6350-SR LAN
DHCP server: 192.168.0.100-250
Gateway: 192.168.0.1
Block access from client laptop to cellular WAN
Media PC
192.168.0.99
Client Laptop
192.168.0.186
Client laptop, and any other client device, has access to Ethernet WAN primary

Sample Configuration

Open the configuration profile for the 6350-SR and make the following changes.

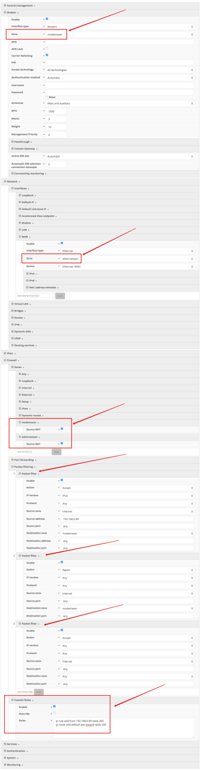
1. Under *Firewall* -> *Zones*, add two new zones, one labelled *modemwan*, and another labelled *ethernetwan*. Ensure the *source NAT* option is selected for both new zones.
2. Under *Modem*, set the *Zone* to *modemwan*.
3. Under *Network* -> *Interfaces* -> *WAN*, set the *Zone* to *ethernetwan*.
4. Under *Firewall* -> *Packet filtering*, setup three rules rules to accomplish the following:
   1. allow packets from the media device (192.168.0.99) to go out the cellular modem
   2. reject all other LAN packets on the cellular modem interface
   3. allow LAN packets to go through the Ethernet WAN interface

5. Under *Firewall* -> *Custom Rules*, select the *Enable* checkbox and add the following three lines to the *Rules*.

```
ip rule add from 192.168.0.99 table 200 priority 32766
```

```
ip route add default dev wwan0 table 200
```

```
ip route flush cache
```



⊟ Central management

⊟ Modem

Enable ☑

Interface type: Modem

Zone: modemwan

APN:

APN Lock ☐

Carrier Switching ☑

PIN:

Access technology: All technologies

Authentication method: Automatic

Username:

Password:

☐ Show

Antennas: Main and auxiliary

MTU: 1500

Metric: 3

Weight: 10

Management Priority: 0

⊟ Passthrough

⊟ Custom Gateway

Active SIM slot: Automatic

Automatic SIM selection connection attempts: 5

⊟ Connectivity monitoring

⊟ Network

⊟ Interfaces

⊟ Loopback

⊟ Default IP

⊟ Default Link-local IP

⊟ Accelerated View endpoint

⊟ Modem

⊟ LAN

⊟ WAN

Enable ☑

Interface type: Ethernet

Zone: ethernetwan

Device: Ethernet: WAN

⊟ IPv4

⊟ IPv6

⊟ MAC address whitelist

Add Interface Interface Add

⊟ Virtual LAN

⊟ Bridges

⊟ Routes

⊟ IPv6

⊟ Dynamic DNS

⊟ VRRP

⊟ Routing services

⊟ IPsec

⊟ Firewall

⊟ Zones

⊟ Any

⊟ Loopback

⊟ Internal

⊟ External

⊟ Setup

⊟ IPsec

⊟ Dynamic routes

⊟ modemwan

Source NAT ☑

⊟ ethernetwan

Source NAT ☑

Add Zone Zone Add

⊟ Port forwarding

⊟ Packet filtering

1. ⊟ Packet filter

Enable ☑

Action: Accept

IP version: IPv4

Protocol: Any

Source zone: Internal

Source address: 192.168.0.99

Source port: any

Destination zone: modemwan

Destination address: any

Destination port: any

2. ⊟ Packet filter

Enable ☑

Action: Reject

IP version: Any

Protocol: Any

Source zone: Internal

Source port: any

Destination zone: modemwan

Destination port: any

3. ⊟ Packet filter

Enable ☑

Action: Accept

IP version: Any

Protocol: Any

Source zone: Internal

Source port: any

Destination zone: Any

Destination port: any

Add Packet filter Add

⊟ Custom Rules

Enable ☑

Override ☐

Rules:

```
ip rule add from 192.168.0.99 table 200
ip route add default dev wwan0 table 200
```

⊟ Services

⊟ Authentication

⊟ System

⊟ Monitoring

VPN Access with IPSec tunnels

Skill level: *Expert* (requires knowledge of IPSec tunnel setup)

Goal

To build an IPSec tunnel through the 63xx router's WAN internet connection, and use that IPSec tunnel to access endpoints inside a VPN.

Setup

For this setup, the 63xx series router will need an active WAN internet connection (cellular for the 6300-series, cellular or Ethernet for the 635x-SR series).

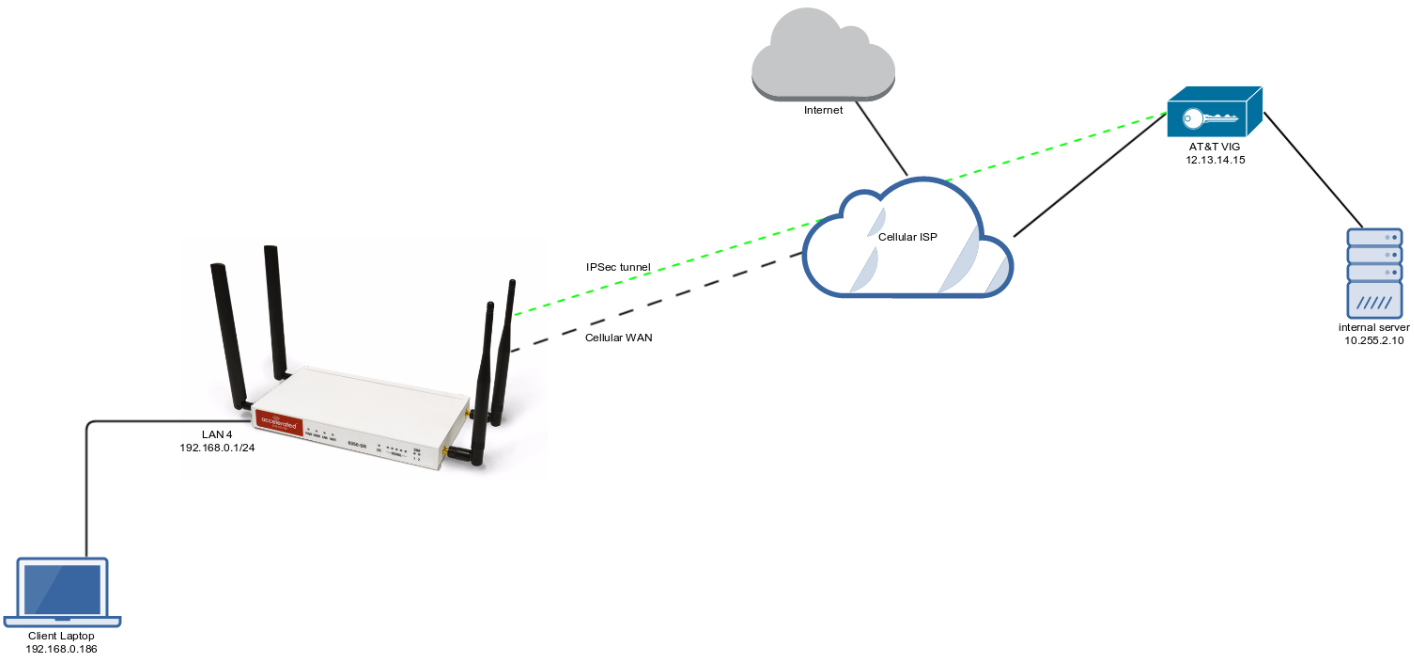
You will also need to know the IPSec credentials and settings needed to build a tunnel to the IPSec endpoint.

! NOTE: the 63xx series of routers support building IPSec tunnels to the following endpoints:

- AT&T SIGs
- AT&T VIGs
- Sonicwall routers
- strongswan IPSec servers
- other 63xx series routers. See the site-to-site tunnel article for an example.

Sample

The sample configuration below shows a 6350-SR building a tunnel to an AT&T VIG at 12.13.14.15 through it's cellular modem. The client laptop connected to the LAN Ethernet port of the 6350-SR can then use that IPSec tunnel to access any IP address in the 10.255.0.0/16 range behind the VIG's IPSec server. Any traffic not destined for 10.255.0.0/16 will instead go through the cellular modem straight to the Internet.



Sample Configuration

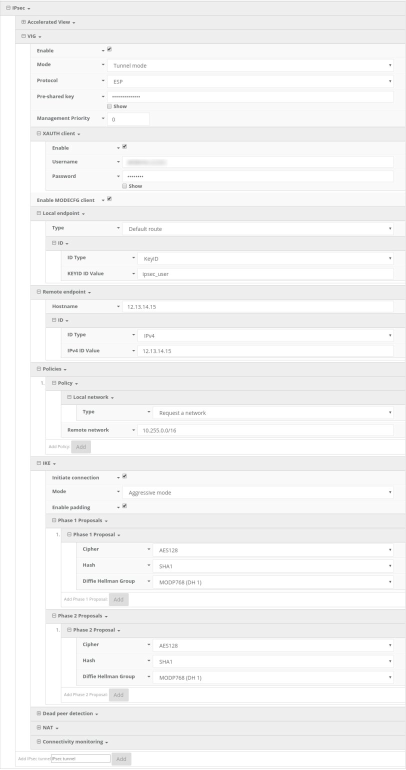
Open the configuration profile for the 6350-SR. Under *IPSec*, create a new entry titled *VIG*, and add your IPSec settings to the new entry. The following settings reflect the sample setup in the diagram above.

1. Enter in the PSK into the *Pre-shared key.*
2. (*optional; required for AT&T VIGs*) In *XAUTH client*, check the *Enable* box and enter in the account, username, and password.
3. Check the *Enable MODECFG client* box.
4. Change *Local endpoint -> ID -> ID type* to *KeyID*
5. Set the local ID in *Local endpoint -> ID -> KEYID ID Value*
6. *(optional)* Set *Local endpoint -> type* to *Interface*,and set *Local endpoint -> Interface* to *Modem.* This configures the 63xx-series router to only build the tunnel through the cellular modem WAN interface. Leaving *Local endpoint -> type* to *Interface* as *Default route* will allow the tunnel to be built through any available WAN interface.
7. Change *Remote endpoint -> ID -> ID type* to *IPv4*
8. Set the IP address of the IPSec server in *Remote endpoint -> Hostname* and *Remote endpoint -> ID -> IPv4 ID Value*. In the example, this is 12.13.14.15
9. Set *IKE -> Mode* to *Aggressive mode*.
10. Set *IKE -> Phase 1 Proposals* and *IKE -> Phase 2 Proposals* to match the IKE settings required by the IPSec server. In this example, both proposals are set to AES128, SHA1, MOD768.

Under *Policies*, click *Add* to create a new policy, and enter the following settings:

1. Set *Policy -> Local network -> Type* to *Request a network.*
2. Set *Policy -> Remote network* to the IPv4 network you wish to access through the tunnel. In the sample, this is 10.255.0.0/16

(alternative) If you would instead like to have all outbound traffic go through this tunnel, set *Policy -> Remote network* to *0.0.0.0/0*



⊟ IPsec

⊞ Accelerated View

⊟ VIG

Enable ☑

Mode: Tunnel mode

Protocol: ESP

Pre-shared key: ••••••••••••••
□ Show

Management Priority: 0

⊟ XAUTH client

Enable ☑

Username: [redacted]

Password: ••••••••
□ Show

Enable MODECFG client ☑

⊟ Local endpoint

Type: Default route

⊟ ID

ID Type: KeyID

KEYID ID Value: ipsec_user

⊟ Remote endpoint

Hostname: 12.13.14.15

⊟ ID

ID Type: IPv4

IPv4 ID Value: 12.13.14.15

⊟ Policies

1. ⊟ Policy

⊟ Local network

Type: Request a network

Remote network: 10.255.0.0/16

⊟ IKE

Initiate connection ☑

Mode: Aggressive mode

Enable padding ☑

⊟ Phase 1 Proposals

1. ⊟ Phase 1 Proposal

Cipher: AES128

Hash: SHA1

Diffie Hellman Group: MODP768 (DH 1)

⊟ Phase 2 Proposals

1. ⊟ Phase 2 Proposal

Cipher: AES128

Hash: SHA1

Diffie Hellman Group: MODP768 (DH 1)

Add Phase 2 Proposal: Add
⊞ Dead peer detection
⊞ NAT
⊞ Connectivity monitoring
Add IPsec tunnel IPsec tunnel Add

Dual WAN Ethernet Ports

Difficulty level: *Beginner*

Goal

Reconfigure an existing LAN port on the 63xx-series router to serve as a WAN interface.

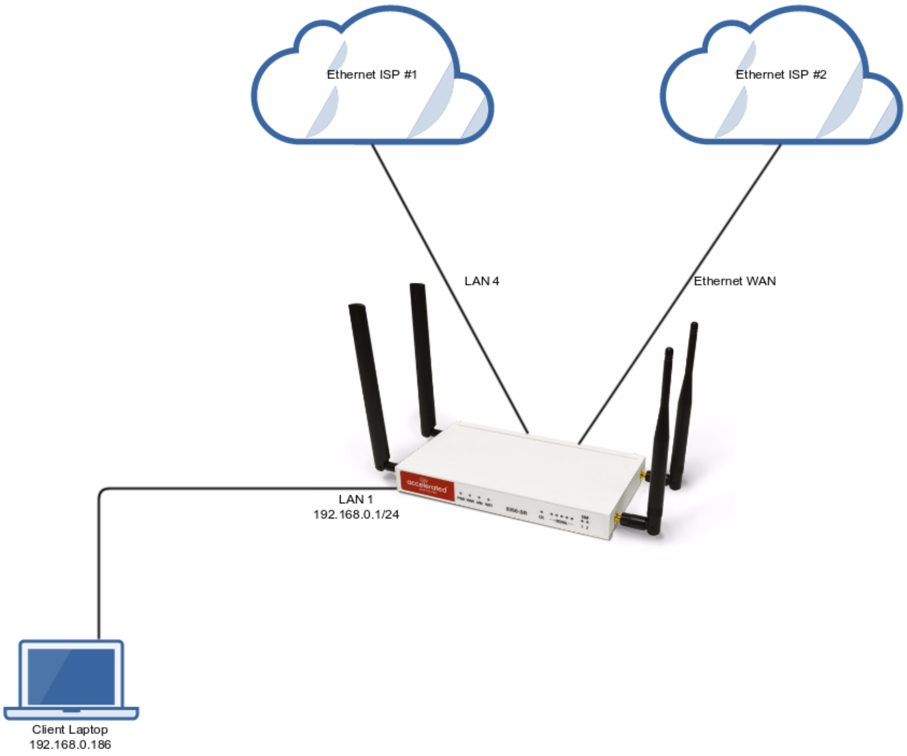
Setup

This article assumes that a second Internet connection is available from an Ethernet cable, and that a primary connection is established via an Ethernet connection in the WAN port. Prior to reconfiguring the LAN port, all interfaces should be operating under default settings, which provide DHCP conenctivity to client devices. For more details on the default settings of the 63xx-series routers, see the *Default Settings* section of the User Manual.

Sample

The sample configuration below shows a 63xx-series router with two Internet connections established via Ethernet cables. Ethernet ISP #1 is connected to the reconfigured LAN (port 4) interface, and Ethernet ISP #2 is connected to the WAN Ethernet port.

! The additional WAN interface can then be used in conjunction with other WAN interfaces when configuring failover, load balancing, or other advanced routing policies.

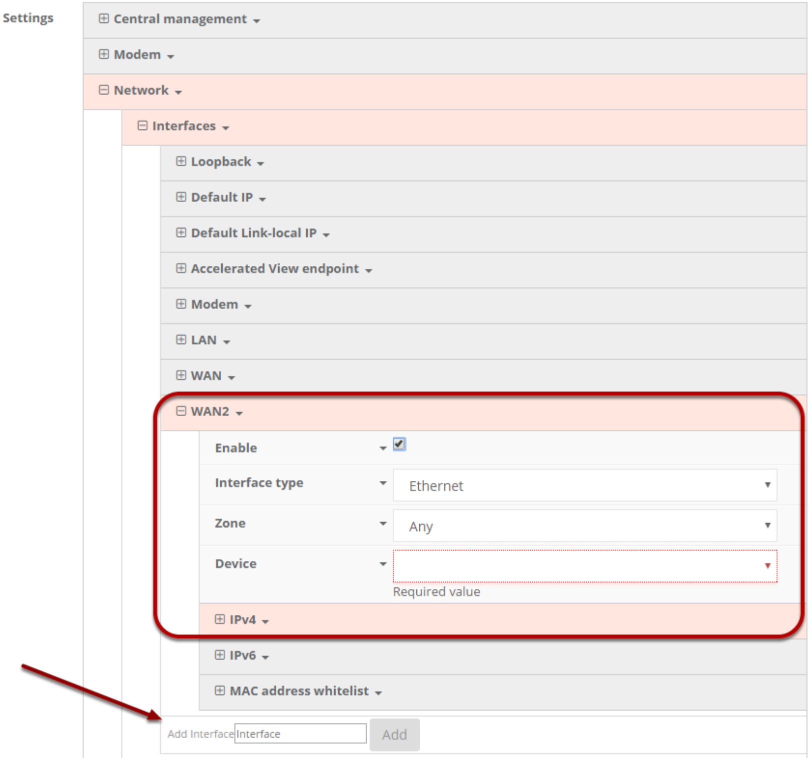


Sample Configuration

Open the configuration profile for the 63xx-series router and make the following changes:

1. In the *Network -> Interfaces* section, specify a name for the new interface and click *Add*.
2. Ensure **Enable** is selected and adjust the *Interface type* if necessary.
3. Specify the *Device* that should be associated with the new WAN interface. (Per the sample above, this will be LAN 4.)
4. Set the *Zone* to *External*.
5. In the *Network -> Bridges* section, expand the *LAN* entry.
6. Using the pull-down menu next to the *Device* indicating LAN 4, select *Delete*.

The LAN port is now reconfigured to serve as a WAN interface.



Settings

⊞ Central management

⊞ Modem

⊟ Network

⊟ Interfaces

⊞ Loopback

⊞ Default IP

⊞ Default Link-local IP

⊞ Accelerated View endpoint

⊞ Modem

⊞ LAN

⊞ WAN

⊟ WAN2

Enable	☑
Interface type	Ethernet
Zone	Any
Device	Required value

⊞ IPv4

⊞ IPv6

⊞ MAC address whitelist

Add Interface Interface

LAN port with IP passthrough

Difficulty level: *Intermediate*

Goal

To setup a device attached to a specific LAN Ethernet port to receive the passthrough IP address of the 63xx-series router's cellular modem connection.

Setup

This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 63xx-series router's LAN ports. For more details on the default settings of the 63xx-series router, see the ***Default Settings*** section of the User's Manual.

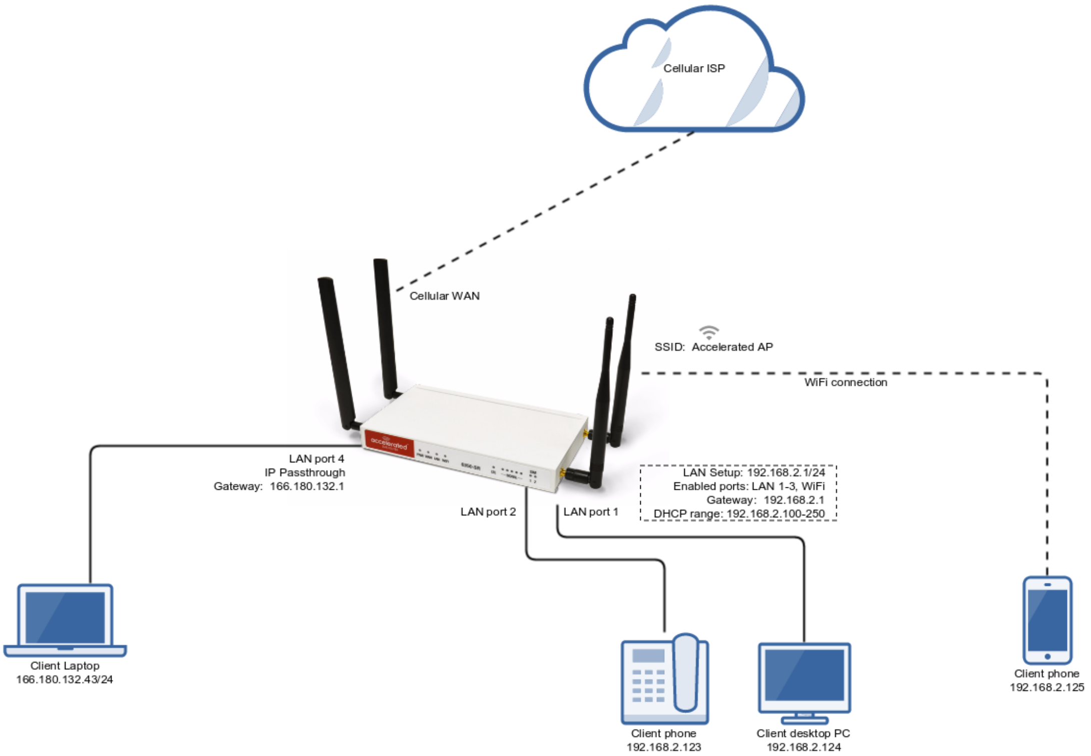
You will need to establish the following details before configuring the 63xx-series router.

- The 63xx-series router must be running firmware version 17.5.86 or higher.
- The LAN Ethernet port you want to connect your client device to so it receives the passthrough IP address.

Sample

The following diagram shows a sample setup of a 63xx-series router with LAN port 4 setup to provide the IP address of the cellular modem connection as a passthrough to the client device connected to port 4. Client devices connected to LAN ports of the 63xx-series router or its WiFi networks will receive a DHCP address in the 192.168.0.x/24 range from the router like normal.

Important: The client device receiving the passthrough IP will only be able to use the 63xx's cellular WAN connection. Meaning, if the 63xx-series router has a second WAN connection through its WAN Ethernet port, the client device with the passthrough IP will not be able to send traffic through the 63xx's WAN Ethernet interface.



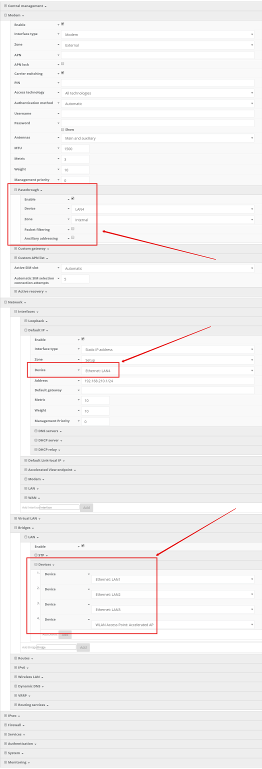
Sample Configuration

Open the configuration profile for the 63xx-series router and make the following changes.

1. Under *Modem -> Passthrough*, check the *Enabled* box and select the desired LAN interface under the *Device* drop-down. For this example, we are selecting *LAN1*.

2. Ensure the same LAN interface is selected under *Network -> Interfaces -> Default IP -> Device*.

3. Under *Network -> Bridges -> LAN -> Devices*, remove the LAN interface you selected for passthrough mode in step 1 above. Removing the LAN interface from this section of the config is done by selecting the down-arrow to the left of the LAN number, and select *Delete.* In this sample config, we are removing *Ethernet: LAN1* from the LAN bridge.
4. Save and apply the new configuration settings to the device.



⊞ Central management

⊟ Modem

- Enable: ☑
- Interface type: Modem
- Zone: External
- APN:
- APN lock: □
- Carrier switching: ☑
- PIN:
- Access technology: All technologies
- Authentication method: Automatic
- Username:
- Password: □ Show
- Antennas: Main and auxiliary
- MTU: 1500
- Metric: 3
- Weight: 10
- Management priority: 0

⊟ Passthrough

- Enable: ☑
- Device: LAN4
- Zone: Internal
- Packet filtering: □
- Ancillary addressing: □

⊞ Custom gateway

⊞ Custom APN list

- Active SIM slot: Automatic
- Automatic SIM selection connection attempts: 5

⊞ Active recovery

⊟ Network

⊟ Interfaces

⊞ Loopback

⊟ Default IP

- Enable: ☑
- Interface type: Static IP address
- Zone: Setup
- Device: Ethernet: LAN4
- Address: 192.168.210.1/24
- Default gateway:
- Metric: 10
- Weight: 10
- Management Priority: 0

⊞ DNS servers

⊞ DHCP server

⊞ DHCP relay

⊞ Default Link-local IP

⊞ Accelerated View endpoint

⊞ Modem

⊞ LAN

⊞ WAN

Add Interface Interface Add

⊞ Virtual LAN

⊟ Bridges

⊟ LAN

- Enable: ☑

⊞ STP

⊟ Devices

1. Device: Ethernet: LAN1
2. Device: Ethernet: LAN2
3. Device: Ethernet: LAN3
4. Device: WLAN Access Point: Accelerated AP

Add Device: Add

Add Bridge Bridge Add

⊞ Routes

⊞ IPv6

⊞ Wireless LAN

⊞ Dynamic DNS

⊞ VRRP

⊞ Routing services

⊞ IPsec

⊞ Firewall

⊞ Services

⊞ Authentication

⊞ System

⊞ Monitoring

Site-to-Site VPN Access with two 63xx Series Routers

Skill level: *Expert* (requires knowledge of IPSec tunnel setup)

Goal

To build an IPSec tunnel through the 63xx router's cellular WAN Internet connection to another 63xx, and use that IPSec tunnel to access endpoints inside a VPN.

Setup

For this setup, you will need two 63xx series routers. Both 63xx routers must be on firmware version 17.5.108.6 or higher. The 63xx series routers will need an active WAN Internet connection.

The main site's 63xx series router will need a publicly reachable IP address, so the remote 63xx series router can reach the IP and build a tunnel.

You will also need to decide on the IPSec credentials and settings needed to build a tunnel between the 63xx series routers.

> ❗ If configuring a 6300-CX for Site-to-Site VPN Access, it must be in router mode.

Sample

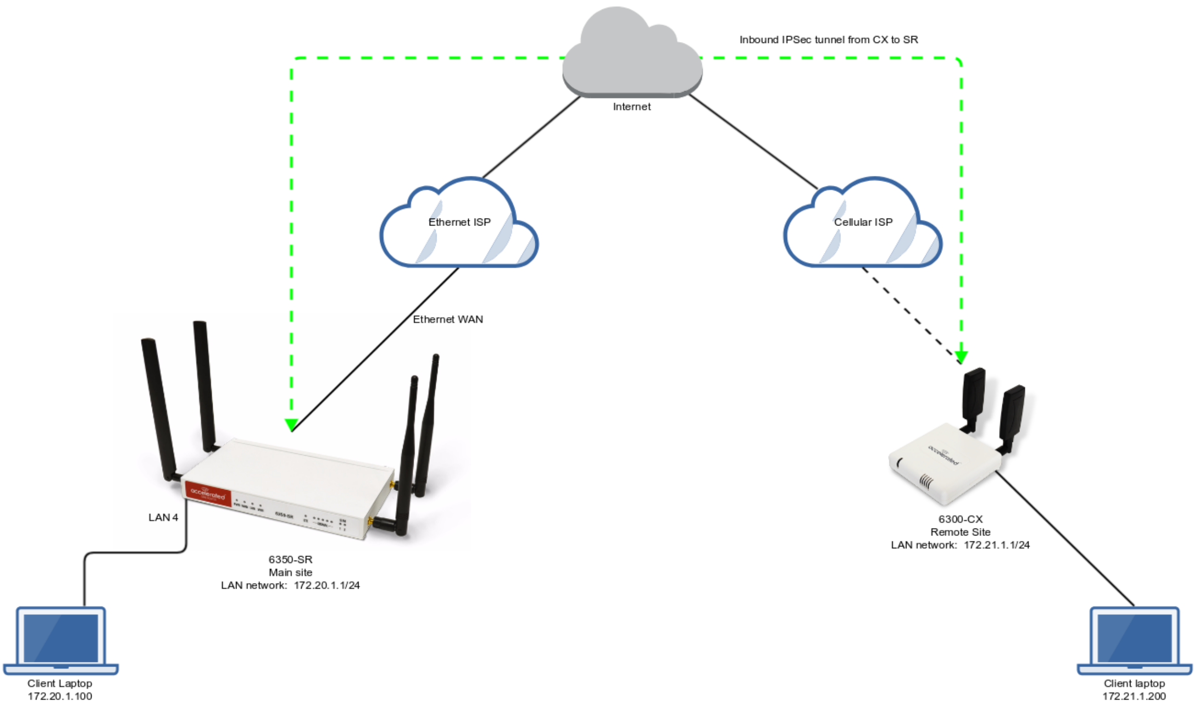
The sample configuration below shows a 6300-CX building a tunnel to a 6350-SR through its cellular modem. The client laptop connected to the LAN Ethernet port of the 6300-CX can then use that IPSec tunnel to access any IP address in the 172.20.1.1/24 range behind the 6350-SR. Any traffic not destined for 172.20.1.1/24 will instead go through the cellular modem straight to the Internet.

This tunnel will also allow the client laptop connected to the LAN 4 port of the 6350-SR to access any IP address in the 172.21.1.1/24 range behind the 6300-CX. Any traffic not destined for 172.20.1.1/24 will instead go through the Ethernet WAN of the 6350-SR straight to the Internet.

Both the 6350-SR and 6300-CX will need to be configured with a new IPSec tunnel, using matching authentication settings, in order for the 6300-CX to build the tunnel to the 6350-SR. Sample configuration settings for both devices are listed below.

Additional 63xx series routers can build IPSec tunnels to this 6350-SR. Each 63xx series router will need a unique local address range (e.g. 172.21.2.1/24 or 172.21.100.1/24) so the various remote sites do not conflict with each other. Also, the *remote network* and *NAT* settings of the main site's 6350-SR will need to be expanded to account for the additional ranges (e.g. 172.21.1.1/16).

NOTE: Be sure a value greater than 0 is specified for the local address ranges' fourth octet (i.e. X.X.X.1/24 is valid, X.X.X.0/24 is not).



6350-SR Sample Configuration

Open the configuration profile for the 6350-SR. Under *IPSec*, create a new entry titled *N6300* (the name is arbitrary), and add your IPSec settings to the new entry. The following settings reflect the sample setup in the diagram above.

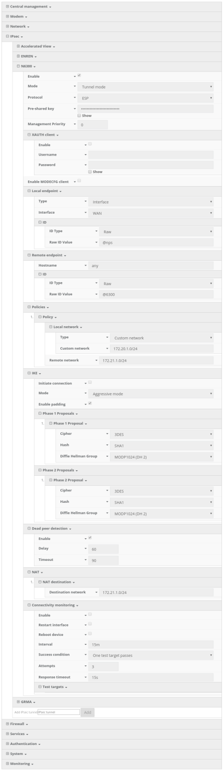
1. Enter in the PSK into the *Pre-shared key*.
2. Change *Local endpoint -> ID -> ID type* to *Raw*
3. Set the local ID in *Local endpoint -> ID -> Raw ID Value*, e.g. *@nps*
4. Set *Local endpoint -> type* to *Interface*,and set *Local endpoint -> Interface* to *WAN*, or whichever interface you want to allow the inbound tunnel to connect through.
5. Change *Remote endpoint -> ID -> ID type* to *Raw*
6. Set the remote ID in *Remote endpoint -> ID -> Raw ID Value*, e.g. *@6300*.
7. Set the *Remote endpoint -> Hostname* to *any*. This allows the 6300-CX to have any IP address. If you know the public IP address of the 6350-CX and wish to lock down the

6350-SR's settings so it only allows inbound tunnels from that IP, input the 6300-CX's public IP address here.

8. Set *IKE -> Mode* to *Aggressive mode*.
9. Uncheck the *IKE -> Initiate connection* option.
10. Set *IKE -> Phase 1 Proposals* and *IKE -> Phase 2 Proposals*. In this example, both proposals are set to 3DES, SHA1, MODP1024.
11. Under NAT, add a destination that corresponds to the local address range of the *remote* device. (In this example, it'd be 172.21.1.1/24.)

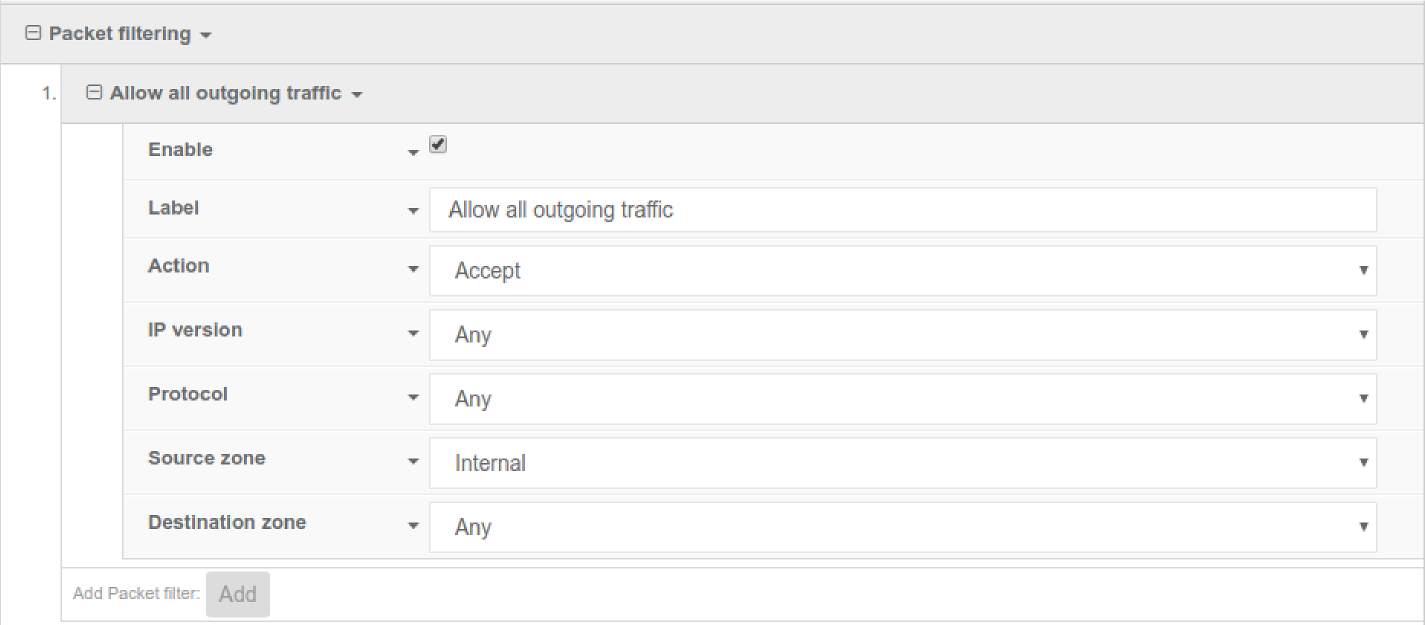
Under *Policies*, click *Add* to create a new policy, and enter the following settings:

1. Set *Policy -> Local network -> Type* to *Custom network.*
2. Set *Policy -> Local network -> Custom network* to the IPv4 network you wish to have on the LAN side of the 6300-CX. In the sample, this is 172.20.1.1/24
3. Set *Policy -> Remote network* to the IPv4 network you wish to access through the tunnel. (In the sample, this is 172.21.1.1/24)



```
⊞ Central management
⊞ Modem
⊞ Network
⊟ IPsec
  ⊞ Accelerated View
  ⊞ ENREN
  ⊟ N6300
    Enable                  ☑
    Mode                    Tunnel mode
    Protocol                ESP
    Pre-shared key          ••••••••••••••••••••••••••
                            □ Show
    Management Priority     0
    ⊟ XAUTH client
      Enable                □
      Username
      Password
                            □ Show
    Enable MODECFG client   □
    ⊟ Local endpoint
      Type                  Interface
      Interface             WAN
      ⊟ ID
        ID Type             Raw
        Raw ID Value        @nps
    ⊟ Remote endpoint
      Hostname              any
      ⊟ ID
        ID Type             Raw
        Raw ID Value        @6300
    ⊟ Policies
      1. ⊟ Policy
        ⊟ Local network
          Type              Custom network
          Custom network    172.20.1.0/24
        Remote network      172.21.1.0/24
    ⊟ IKE
      Initiate connection   □
      Mode                  Aggressive mode
      Enable padding        ☑
      ⊟ Phase 1 Proposals
        1. ⊟ Phase 1 Proposal
          Cipher                3DES
          Hash                  SHA1
          Diffie Hellman Group  MODP1024 (DH 2)
      ⊟ Phase 2 Proposals
        1. ⊟ Phase 2 Proposal
          Cipher                3DES
          Hash                  SHA1
          Diffie Hellman Group  MODP1024 (DH 2)
    ⊟ Dead peer detection
      Enable                ☑
      Delay                 60
      Timeout               90
    ⊟ NAT
      1. ⊟ NAT destination
        Destination network 172.21.1.0/24
    ⊟ Connectivity monitoring
      Enable                □
      Restart interface     □
      Reboot device         □
      Interval              15m
      Success condition     One test target passes
      Attempts              3
      Response timeout      15s
      ⊟ Test targets
  ⊞ GRMA
  Add IPsec tunnel [IPsec tunnel] Add
⊞ Firewall
⊞ Services
⊞ Authentication
⊞ System
⊞ Monitoring
```

Under *Firewall*, click *Packet Filtering* to ensure *Allow all outgoing traffic* item exists and enabled.



⊟ Packet filtering

1. ⊟ Allow all outgoing traffic

Enable	☑
Label	Allow all outgoing traffic
Action	Accept
IP version	Any
Protocol	Any
Source zone	Internal
Destination zone	Any

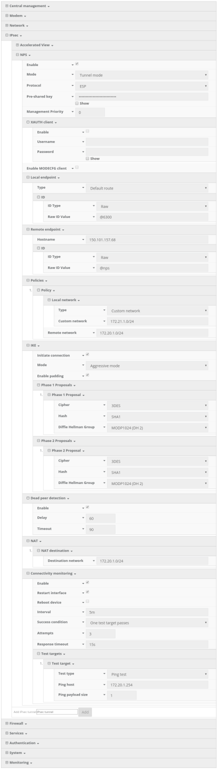
6300-CX Sample Configuration

Open the configuration profile for the 6350-SR. Under *IPSec*, create a new entry titled *NPS* (the name is arbitrary), and add your IPSec settings to the new entry. The following settings reflect the sample setup in the diagram above.

1. Enter in the PSK into the *Pre-shared key*.
2. Change *Local endpoint -> ID -> ID type* to *Raw*
3. Set the local ID in *Local endpoint -> ID -> Raw ID Value*, e.g. *@6300.*
4. *(optional)* Set *Local endpoint -> type* to *Interface*,and set *Local endpoint -> Interface* to *Modem.* This configures the 63xx-series router to only build the tunnel through the cellular modem WAN interface. Leaving *Local endpoint -> type* to *Interface* as *Default route* will allow the tunnel to be built through any available WAN interface.
5. Change *Remote endpoint -> ID -> ID type* to *Raw*
6. Set the remote ID in *Remote endpoint -> ID -> Raw ID Value*, e.g. *@nps*.
7. Set the *Remote endpoint -> Hostname* to the public IP address of the 6350-SR's WAN Ethernet.
8. Set *IKE -> Mode* to *Aggressive mode*.
9. Set *IKE -> Phase 1 Proposals* and *IKE -> Phase 2 Proposals* to match the IKE settings required by the 6350-SR. In this example, both proposals are set to 3DES, SHA1, MODP1024.

Under *Policies*, click *Add* to create a new policy, and enter the following settings:

1. Set *Policy -> Local network -> Type* to *Custom network.*
2. Set *Policy -> Local network -> Custom network* to the IPv4 network you wish to have on the LAN side of the 6300-CX. In the sample, this is 172.21.1.0/24
3. Set *Policy -> Remote network* to the IPv4 network you wish to access through the tunnel. In the sample, this is 172.20.1.0/24



- ⊞ Central management
- ⊞ Modem
- ⊞ Network
- ⊟ IPsec
  - ⊞ Accelerated View
  - ⊟ NPS
    - Enable: ☑
    - Mode: Tunnel mode
    - Protocol: ESP
    - Pre-shared key: •••••••••••••••••••••••••• □ Show
    - Management Priority: 0
    - ⊟ XAUTH client
      - Enable: □
      - Username:
      - Password: □ Show
    - Enable MODECFG client: □
    - ⊟ Local endpoint
      - Type: Default route
      - ⊟ ID
        - ID Type: Raw
        - Raw ID Value: @6300
    - ⊟ Remote endpoint
      - Hostname: 150.101.157.68
      - ⊟ ID
        - ID Type: Raw
        - Raw ID Value: @nps
    - ⊟ Policies
      1. ⊟ Policy
         - ⊟ Local network
           - Type: Custom network
           - Custom network: 172.21.1.0/24
         - Remote network: 172.20.1.0/24
    - ⊟ IKE
      - Initiate connection: ☑
      - Mode: Aggressive mode
      - Enable padding: ☑
      - ⊟ Phase 1 Proposals
        1. ⊟ Phase 1 Proposal
           - Cipher: 3DES
           - Hash: SHA1
           - Diffie Hellman Group: MODP1024 (DH 2)
      - ⊟ Phase 2 Proposals
        1. ⊟ Phase 2 Proposal
           - Cipher: 3DES
           - Hash: SHA1
           - Diffie Hellman Group: MODP1024 (DH 2)
    - ⊟ Dead peer detection
      - Enable: ☑
      - Delay: 60
      - Timeout: 90
    - ⊟ NAT
      1. ⊟ NAT destination
         - Destination network: 172.20.1.0/24
    - ⊟ Connectivity monitoring
      - Enable: ☑
      - Restart interface: ☑
      - Reboot device: □
      - Interval: 5m
      - Success condition: One test target passes
      - Attempts: 3
      - Response timeout: 15s
      - ⊟ Test targets
        1. ⊟ Test target
           - Test type: Ping test
           - Ping host: 172.20.1.254
           - Ping payload size: 1
  - Add IPsec tunnel: IPsec tunnel [Add]
- ⊞ Firewall
- ⊞ Services
- ⊞ Authentication
- ⊞ System
- ⊞ Monitoring

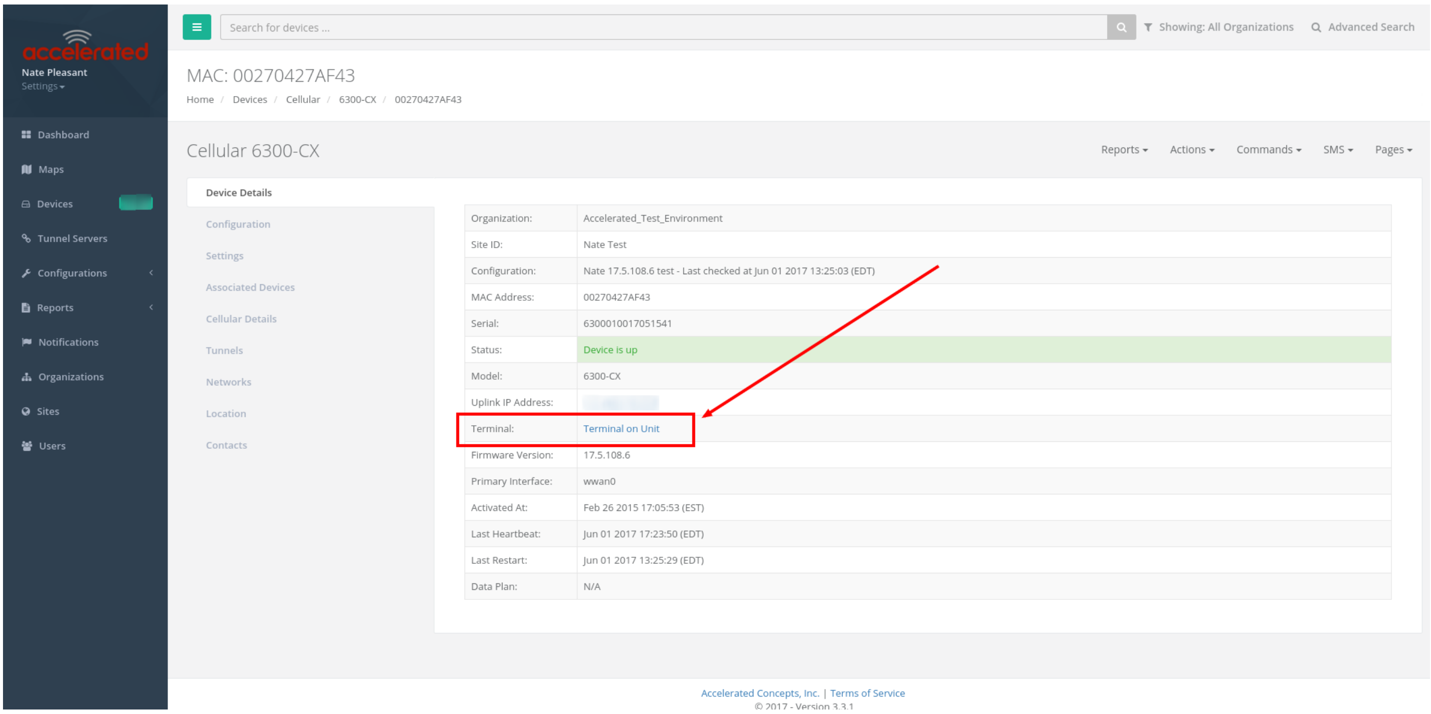
Terminal on Unit

Skill level: *Intermediate*

Goal

To access the console of an Accelerated LTE router using the *Terminal on Unit* link presented in Accelerated View for the device.

> The *Terminal on Unit* access leverages the management tunnel established between the 63xx-series router and Accelerated View. For details on the monthly data usage for this access, refer to the following article:
>
> Data Usage Estimates



MAC: 00270427AF43

Home / Devices / Cellular / 6300-CX / 00270427AF43

Cellular 6300-CX

Organization:	Accelerated_Test_Environment
Site ID:	Nate Test
Configuration:	Nate 17.5.108.6 test - Last checked at Jun 01 2017 13:25:03 (EDT)
MAC Address:	00270427AF43
Serial:	6300010017051541
Status:	Device is up
Model:	6300-CX
Uplink IP Address:	[redacted]
Terminal:	Terminal on Unit
Firmware Version:	17.5.108.6
Primary Interface:	wwan0
Activated At:	Feb 26 2015 17:05:53 (EST)
Last Heartbeat:	Jun 01 2017 17:23:50 (EDT)
Last Restart:	Jun 01 2017 13:25:29 (EDT)
Data Plan:	N/A

Accelerated Concepts, Inc. | Terms of Service
© 2017 - Version 3.3.1

Setup

For this setup, you will need access to Accelerated View, and a 63xx-series router online and syncing with Accelerated View. If you see the 63xx-series router listed as up (green status) in Accelerated View, you are good to go.

Details

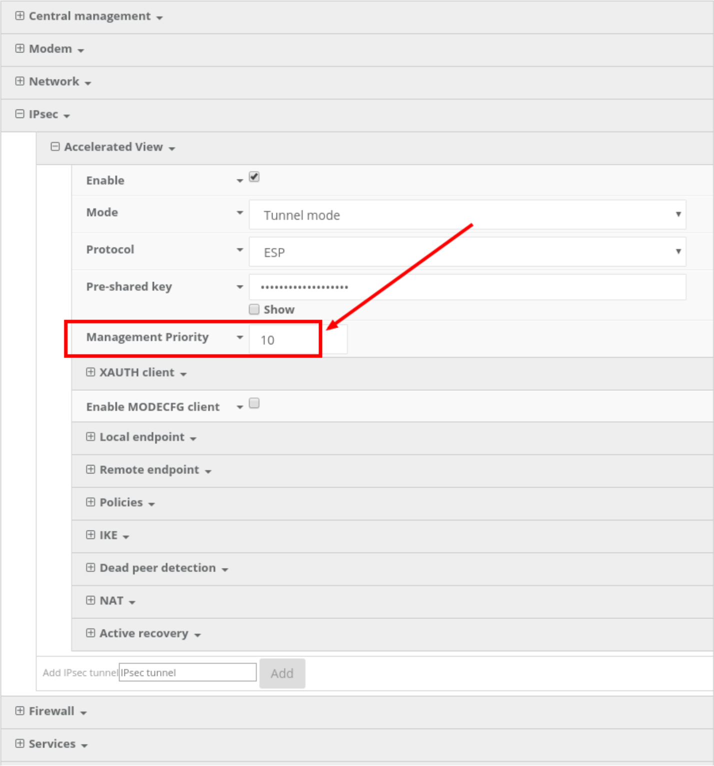
Accelerated View utilizes the IPSec tunnel the 63xx-series router establishes to remote.accns.com to provide terminal access to the console of the router.

For details on the monthly data usage for this access, refer to the following article:

Data Usage Estimates

The following configuration settings will setup the 6300-CX to report its IPSec tunnel local IP address as the management IP that Accelerated View can then use to access its console.

Open the configuration profile for the 63xx-series router. Under *IPSec -> Accelerated View*, set the *Management priority* to *10*. This will tell the 63xx-series router to treat the AView IPSec tunnel as the highest priority management interface, which it then reports to Accelerated View as the IP that can be used to access its console.



Enable ☑

Mode: Tunnel mode

Protocol: ESP

Pre-shared key: ••••••••••••••••••••

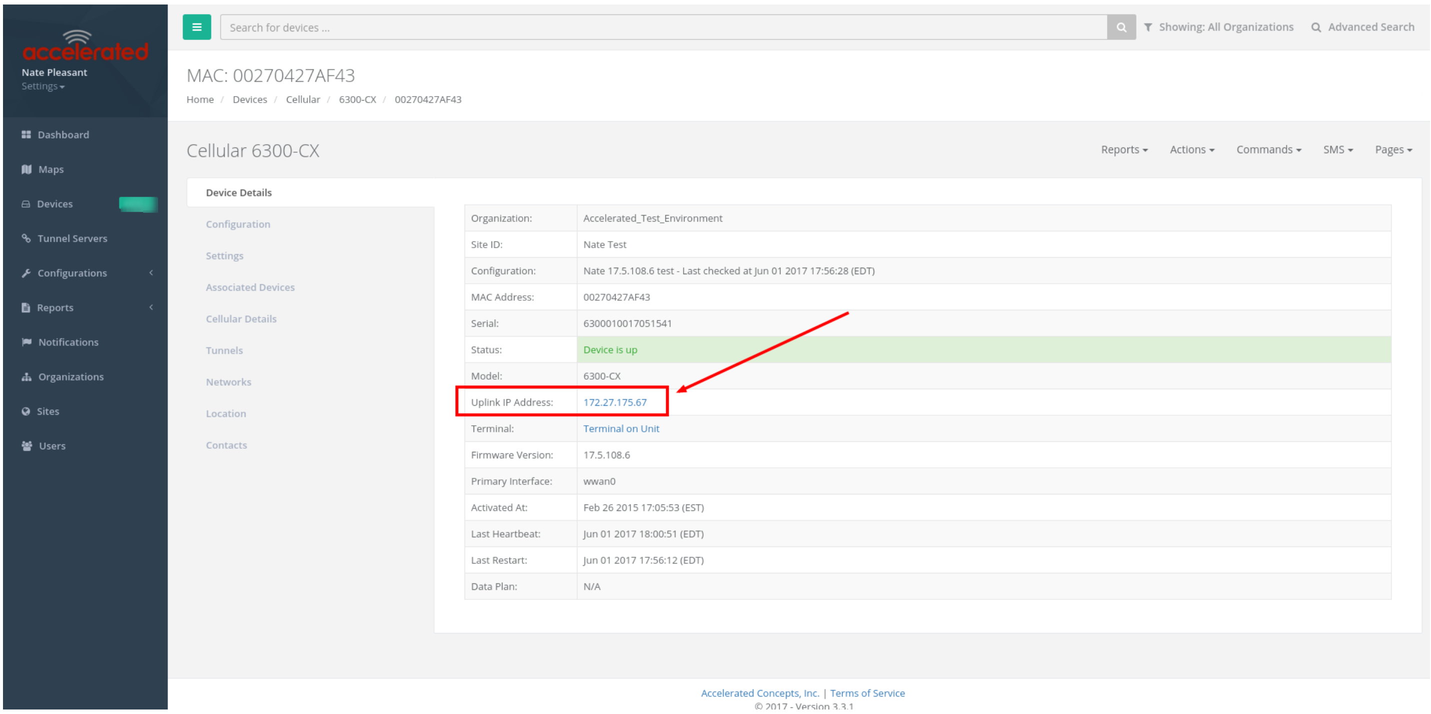
□ Show

Management Priority: 10

Enable MODECFG client □

Add IPsec tunnel: IPsec tunnel

Once you apply the new configuration to the 63xx-series router, reboot the 63xx-series device so it rebuilds the IPSec tunnel and reports the new IPSec local IP address to Accelerated View. You can verify that Accelerated View is using the IPSec local IP as the management IP by looking at the *Uplink IP address* on the *Device Details* tab. This value should be set to a 172.x.x.x IP address.



MAC: 00270427AF43

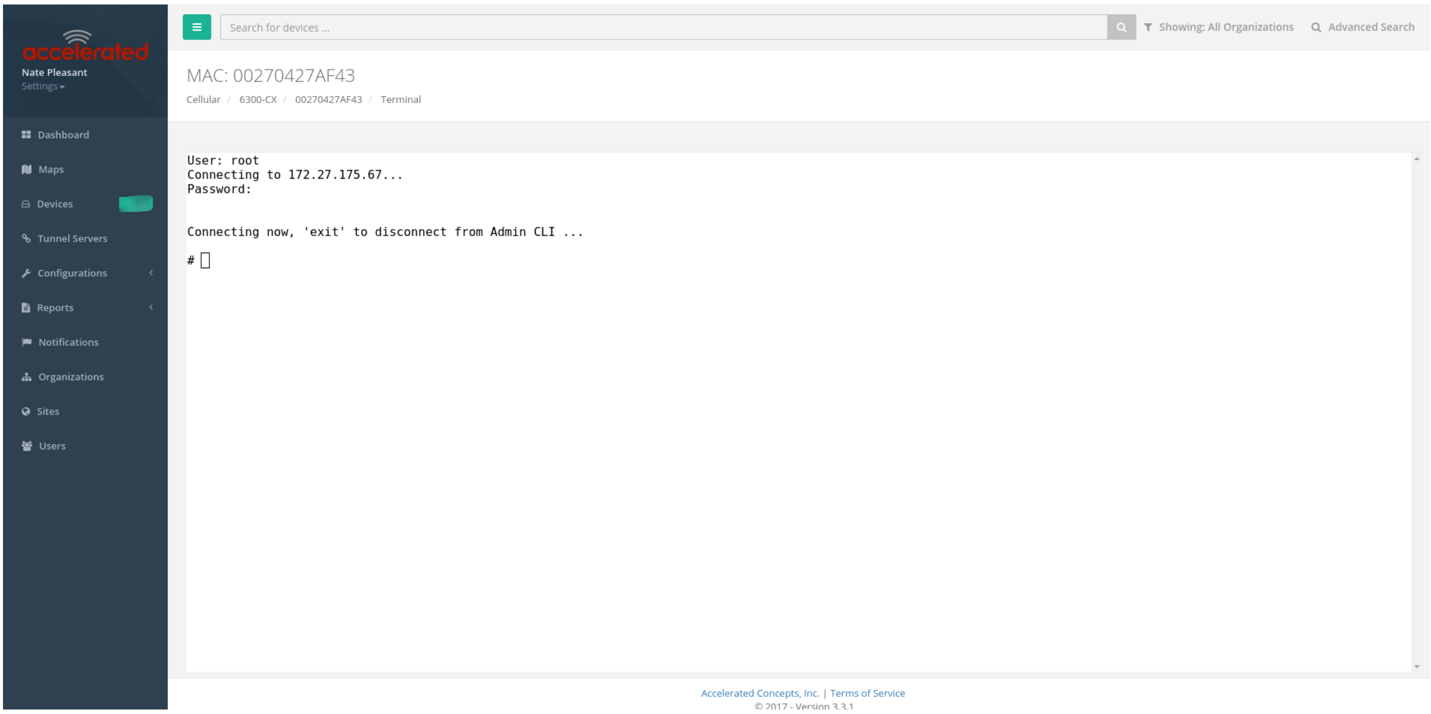
Home / Devices / Cellular / 6300-CX / 00270427AF43

Cellular 6300-CX

Organization:	Accelerated_Test_Environment
Site ID:	Nate Test
Configuration:	Nate 17.5.108.6 test - Last checked at Jun 01 2017 17:56:28 (EDT)
MAC Address:	00270427AF43
Serial:	6300010017051541
Status:	Device is up
Model:	6300-CX
Uplink IP Address:	172.27.175.67
Terminal:	Terminal on Unit
Firmware Version:	17.5.108.6
Primary Interface:	wwan0
Activated At:	Feb 26 2015 17:05:53 (EST)
Last Heartbeat:	Jun 01 2017 18:00:51 (EDT)
Last Restart:	Jun 01 2017 17:56:12 (EDT)
Data Plan:	N/A

Using the Terminal on Unit link

Once the correct management IP is reported from the 63xx-series router to Accelerated View, clicking the *Terminal on Unit* will open a page on Accelerated View to provide the user access to the console of the 63xx-series router.



MAC: 00270427AF43

Cellular / 6300-CX / 00270427AF43 / Terminal

```
User: root
Connecting to 172.27.175.67...
Password:


Connecting now, 'exit' to disconnect from Admin CLI ...

# 
```

Custom Speed Test Server

Skill level: *Intermediate*

Goal

To setup a custom speed test server and have your Accelerated 63xx-series router perform speed tests to it.

> ❗ The *Speed test* command leverages the management tunnel established between the 63xx-series router and Accelerated View. For details on the monthly data usage for this access, refer to the following article:
>
> Data Usage Estimates

Setup

For this setup, you will need access to Accelerated View, and a 63xx-series router online and syncing with Accelerated View. If you see the 63xx-series router listed as up (green status) in Accelerated View, you are good to go.

Details

Accelerated View utilizes the IPSec tunnel the 63xx-series router establishes to remote.accns.com to send remote commands to the device. One of the available commands a user can run is the *Perform Speed Test* command. This will trigger the 63xx-series router to perform a speed test to the speedtest server specified in its configuration settings. The default speed test server is speedtest.accns.com.

> ❗ *Note:* In order to minimize the speed test's impact on cellular data consumption, the results are an estimation of the available throughput of the device, and may not represent the full network speed available.

This article will detail setting up a separate speed test server that a 63xx-series router can use as an alternative to the default speed test server.

Speed Test server setup

The speed test server utilizes the nuttcp tool in Linux. This setup was tested using nuttcp version 6.1.2 on an Ubuntu 16.04 server with 1GB of RAM and a 30GB hard drive. The nuttcp tool used approximately 150kB of disk space, and consumed an average of 100MB of RAM.

Run the following command to install the nuttcp package.

```
sudo apt-get install nuttcp
```

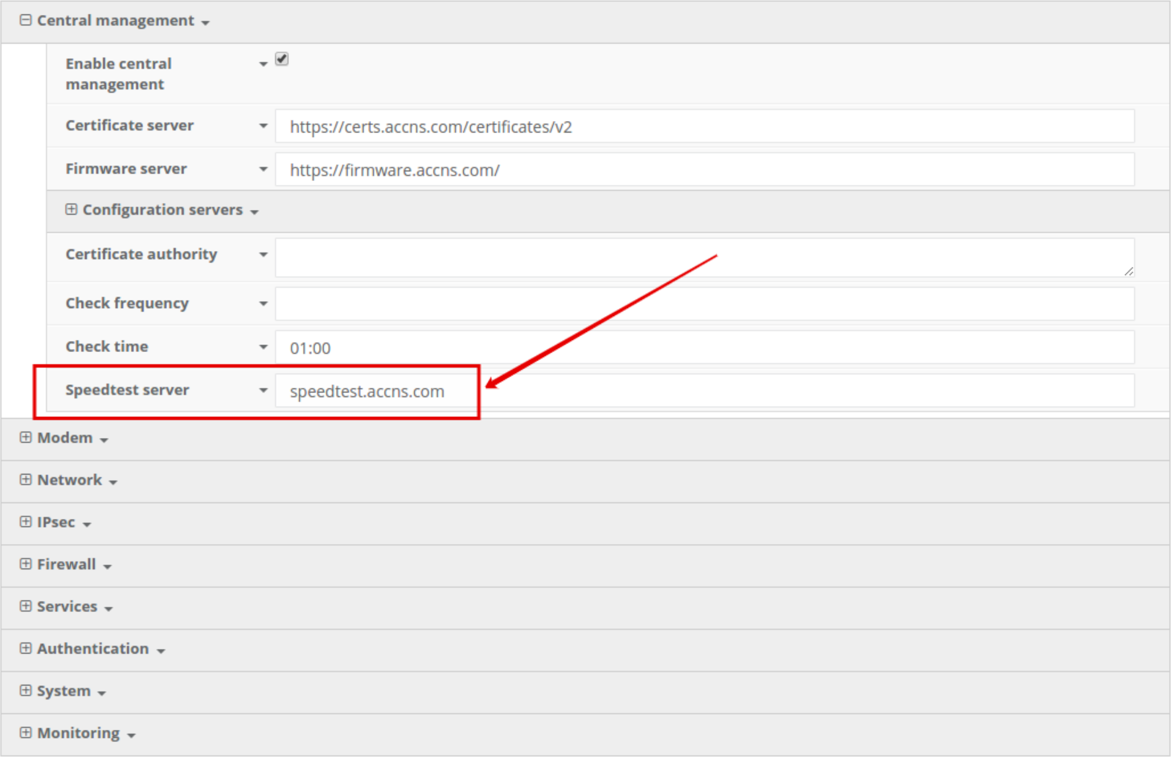
Then start the nuttcp speed test server with the following command:

```
nuttcp -S
```

The 63xx-series router will need access to this server on UDP ports 5000 and 5001. Please ensure proper firewalls are opened to allow access to the IP address of the speed test server and its respective ports.

Using the new speed test server

Once the new speed test server is running, add the IP address to the 63xx-series router's configuration profile under *Central management -> speedtest server* and apply the configuration to the device.



⊟ Central management

Enable central management ☑

Certificate server: https://certs.accns.com/certificates/v2

Firmware server: https://firmware.accns.com/

⊞ Configuration servers

Certificate authority:

Check frequency:

Check time: 01:00

Speedtest server: speedtest.accns.com

⊞ Modem

⊞ Network

⊞ IPsec

⊞ Firewall

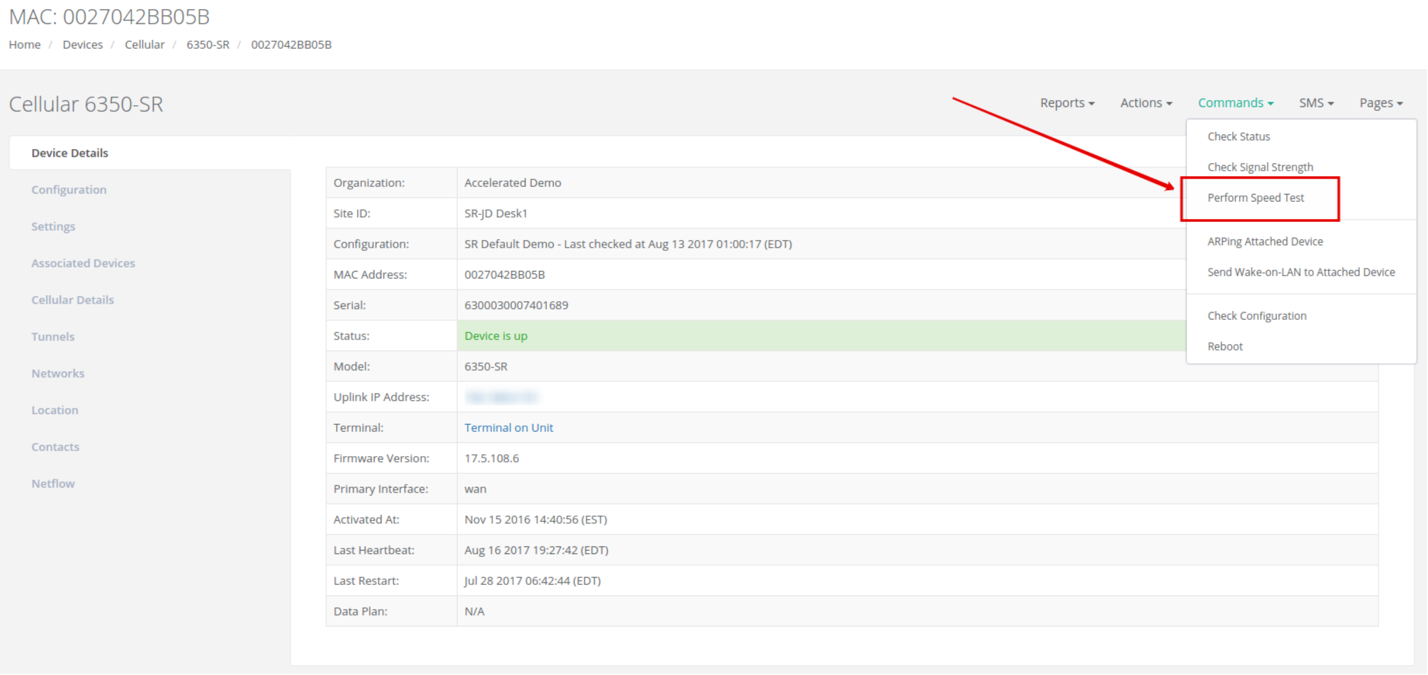
⊞ Services

⊞ Authentication

⊞ System

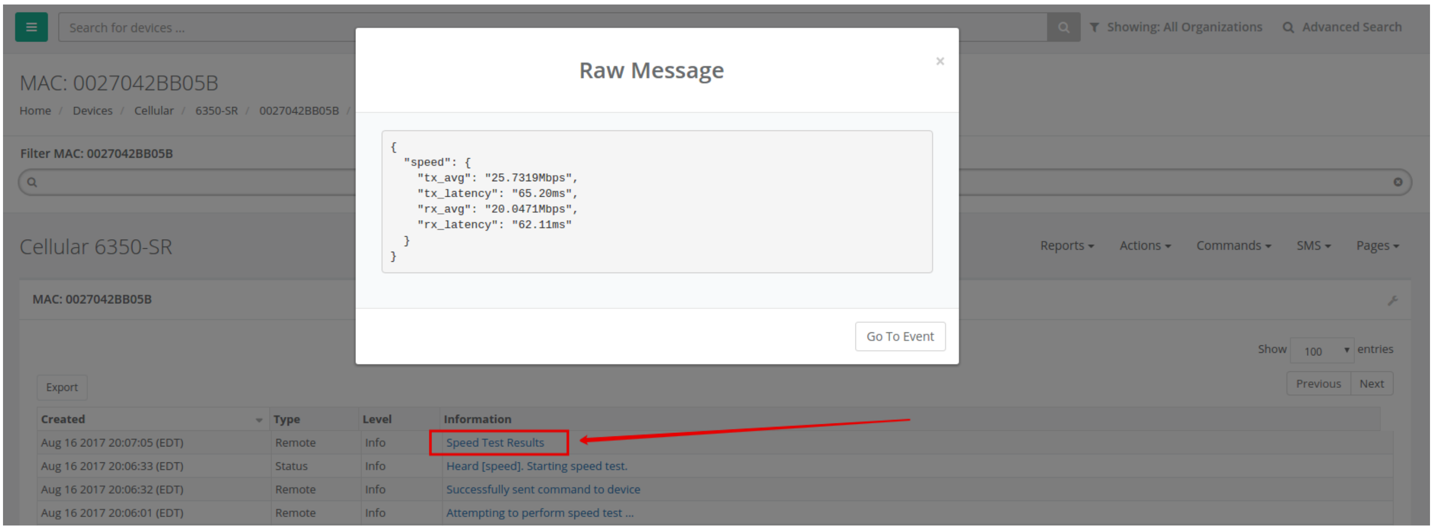
⊞ Monitoring

To run a speed test, select the *Perform Speed Test* option under the *Commands* drop-down listed on the device's details page in Accelerated View.



Organization:	Accelerated Demo
Site ID:	SR-JD Desk1
Configuration:	SR Default Demo - Last checked at Aug 13 2017 01:00:17 (EDT)
MAC Address:	0027042BB05B
Serial:	6300030007401689
Status:	Device is up
Model:	6350-SR
Uplink IP Address:	[redacted]
Terminal:	Terminal on Unit
Firmware Version:	17.5.108.6
Primary Interface:	wan
Activated At:	Nov 15 2016 14:40:56 (EST)
Last Heartbeat:	Aug 16 2017 19:27:42 (EDT)
Last Restart:	Jul 28 2017 06:42:44 (EDT)
Data Plan:	N/A

The 63xx-series router will acknowledge the request to perform the speed test, and will send another event to Accelerated View once the speed test completes. Clicking on the speed test results will display a window with the upload and downloads speeds observed in the test.



```
{
  "speed": {
    "tx_avg": "25.7319Mbps",
    "tx_latency": "65.20ms",
    "rx_avg": "20.0471Mbps",
    "rx_latency": "62.11ms"
  }
}
```

Created	Type	Level	Information
Aug 16 2017 20:07:05 (EDT)	Remote	Info	Speed Test Results
Aug 16 2017 20:06:33 (EDT)	Status	Info	Heard [speed]. Starting speed test.
Aug 16 2017 20:06:32 (EDT)	Remote	Info	Successfully sent command to device
Aug 16 2017 20:06:01 (EDT)	Remote	Info	Attempting to perform speed test ...

Remote Access

Skill Level: *Moderate* (assumes familiarity with SSH sessions)

Goal

To SSH into an Accelerated device remotely, using the terminal available via Accelerated View and a publicly reachable IP address.

If your device does not have a publicly reachable IP address, you can still leverage the Terminal on Unit via the Accelerated View IPSec Tunnel.

Setup

Devices can be managed over SSH so long as the external zone is enabled for remote SSH and web UI access.

The default credentials are:

Username: *root*

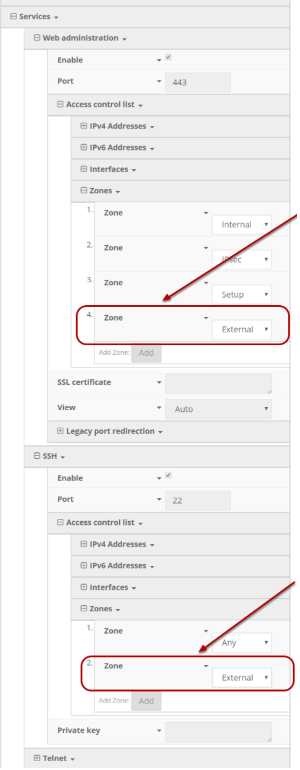
Password: *default*

NOTE: The configuration steps outlined below will open external access to your Accelerated device. It is imperative that the default password is changed to a more secure key to prevent intrusions.

Sample Configuration

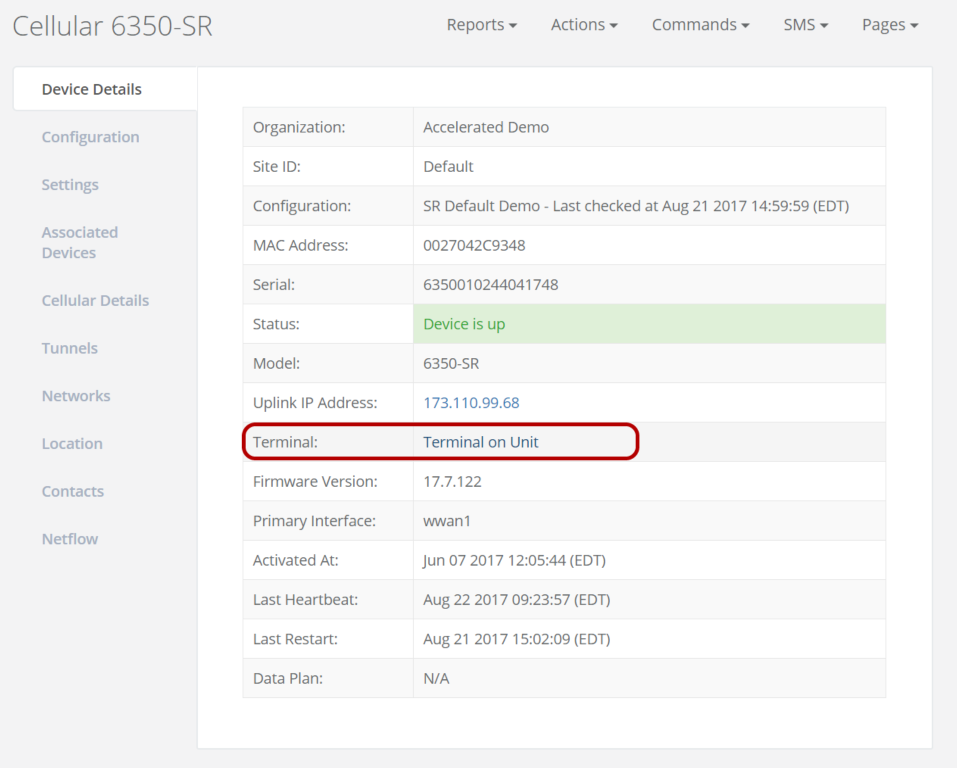
Open the configuration profile of the device and expand *Services*. Under *Web Administration*, expand *Access Control List* and *Zones* to create a new entry for "External." Repeat this process for the *Zones* associated with the *Access Control List* under the *SSH* menu heading. The following steps reflect the sample setup indicated in the screenshot below:

1. Under *Services -> Web Administration -> Access Control List*, expand *Zones*.
2. Add a new entry for "External."
3. Under *Services -> SSH -> Access Control List*, expand *Zones*.
4. Add a new entry for "External."



⊟ Services
- ⊟ Web administration
  - Enable: ☑
  - Port: 443
  - ⊟ Access control list
    - ⊞ IPv4 Addresses
    - ⊞ IPv6 Addresses
    - ⊞ Interfaces
    - ⊟ Zones
      1. Zone: Internal
      2. Zone: IPsec
      3. Zone: Setup
      4. Zone: External
      - Add Zone: Add
  - SSL certificate:
  - View: Auto
  - ⊞ Legacy port redirection
- ⊟ SSH
  - Enable: ☑
  - Port: 22
  - ⊟ Access control list
    - ⊞ IPv4 Addresses
    - ⊞ IPv6 Addresses
    - ⊞ Interfaces
    - ⊟ Zones
      1. Zone: Any
      2. Zone: External
      - Add Zone: Add
  - Private key:
- ⊞ Telnet

Once the configuration has been updated, click the *Terminal on Unit* hyperlink available from the *Device Details* screen.



Organization:	Accelerated Demo
Site ID:	Default
Configuration:	SR Default Demo - Last checked at Aug 21 2017 14:59:59 (EDT)
MAC Address:	0027042C9348
Serial:	6350010244041748
Status:	Device is up
Model:	6350-SR
Uplink IP Address:	173.110.99.68
Terminal:	Terminal on Unit
Firmware Version:	17.7.122
Primary Interface:	wwan1
Activated At:	Jun 07 2017 12:05:44 (EDT)
Last Heartbeat:	Aug 22 2017 09:23:57 (EDT)
Last Restart:	Aug 21 2017 15:02:09 (EDT)
Data Plan:	N/A

MAC address-based Policy Routing with Dual WAN

Difficulty: *Expert*

Goal

To use the 6350-SR's cellular modem in tandem with its primary WAN Ethernet port, but only allow devices with certain MAC addresses access to the cellular modem's Internet connection.

Setup

This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 6350-SR's LAN ports. For more details on the default settings of the 6350-SR, see the ***Default Settings*** section of the 6350-SR User's Manual.

For this setup, you will need the 6350-SR with both a primary WAN Ethernet connection, and a cellular modem connection.

You will also need to the MAC address of any client devices you want to always use the cellular modem connection.

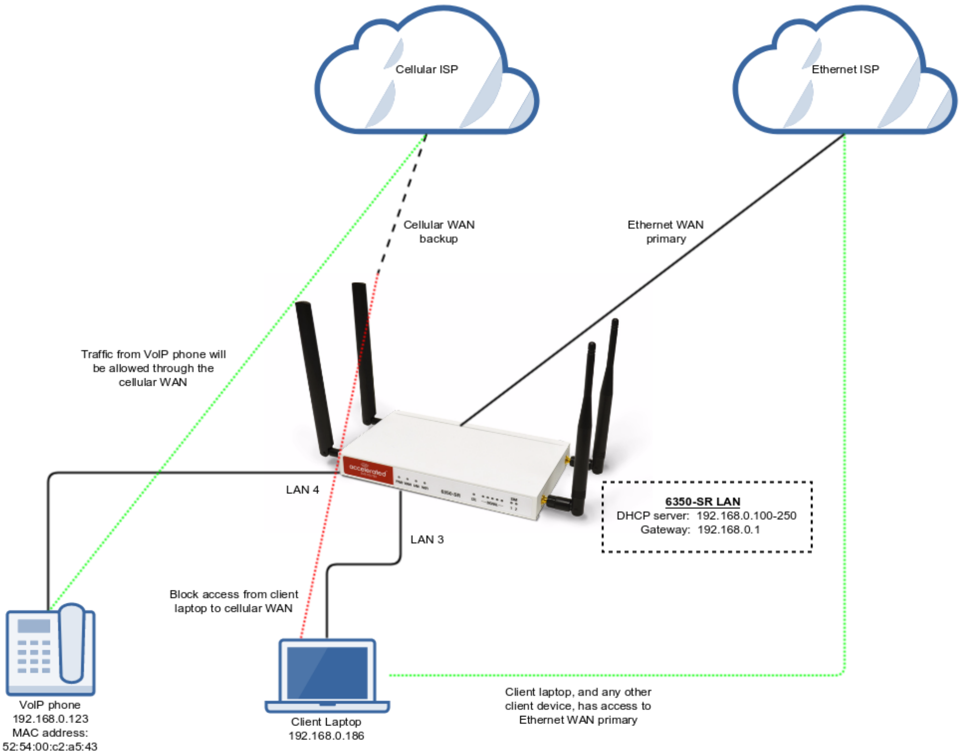
Sample

The sample configuration below shows a 6350-SR with two Internet connections: a cellular-based WAN connection through the 6350-SR's modem, and a broadband-based WAN connection through the 6350-SR's WAN Ethernet port.

This setup shows two client devices on a 6350-SR's LAN ports, a VoIP phone and a laptop. The VoIP phone and the laptop receive their IP address via DHCP from the 6350-SR.

The policy-based routing we are going to setup will accomplish the following.

1. The 6350-SR uses the Ethernet WAN as its primary interface.
2. The 6350-SR has a cellular modem connection, used as a secondary WAN interface.
3. The 6350-SR will drop any packets from LAN devices, excluding packets from the media PC, and prevent them from going out the cellular modem interface.


Cellular ISP
Ethernet ISP
Cellular WAN backup
Ethernet WAN primary
Traffic from VoIP phone will be allowed through the cellular WAN
LAN 4
LAN 3
6350-SR LAN
DHCP server: 192.168.0.100-250
Gateway: 192.168.0.1
Block access from client laptop to cellular WAN
VoIP phone
192.168.0.123
MAC address:
52:54:00:c2:a5:43
Client Laptop
192.168.0.186
Client laptop, and any other client device, has access to Ethernet WAN primary

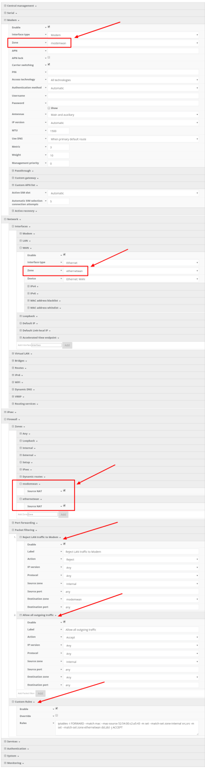
Sample Configuration

Open the configuration profile for the 6350-SR and make the following changes.

1. Under *Firewall* -> *Zones*, add two new zones, one labelled *modemwan*, and another labelled *ethernetwan*. Ensure the *source NAT* option is selected for both new zones.
2. Under *Modem*, set the *Zone* to *modemwan*.
3. Under *Network* -> *Interfaces* -> *WAN*, set the *Zone* to *ethernetwan*.
4. Under *Firewall* -> *Packet filtering*, setup two rules rules to accomplish the following:
   1. reject all other LAN packets on the cellular modem interface
   2. allow LAN packets to go through the Ethernet WAN interface

5. Under *Firewall* -> *Custom Rules*, select the *Enable* checkbox and add the following line to the *Rules* entry. If you would like to apply the same MAC-based policy route to multiple client devices, copy the line below and replace the MAC address with the MAC address of the desired device.

```
iptables -I FORWARD --match mac --mac-source 52:54:00:c2:a5:43 -m set --ma
```



⊞ Central management
⊞ Serial
⊟ Modem
Enable ☑
Interface type Modem
Zone modemwan
APN
APN lock ☐
Carrier switching ☑
PIN
Access technology All technologies
Authentication method Automatic
Username
Password
☐ Show
Antennas Main and auxiliary
IP version Automatic
MTU 1500
Use DNS When primary default route
Metric 3
Weight 10
Management priority 0
⊞ Passthrough
⊞ Custom gateway
⊞ Custom APN list
Active SIM slot Automatic
Automatic SIM selection connection attempts 5
⊞ Active recovery
⊟ Network
⊟ Interfaces
⊞ Modem
⊞ LAN
⊟ WAN
Enable ☑
Interface type Ethernet
Zone ethernetwan
Device Ethernet: WAN
⊞ IPv4
⊞ IPv6
⊞ MAC address blacklist
⊞ MAC address whitelist
⊞ Loopback
⊞ Default IP
⊞ Default Link-local IP
⊞ Accelerated View endpoint
Add Interface Interface Add
⊞ Virtual LAN
⊞ Bridges
⊞ Routes
⊞ IPv6
⊞ WiFi
⊞ Dynamic DNS
⊞ VRRP
⊞ Routing services
⊞ IPsec
⊟ Firewall
⊟ Zones
⊞ Any
⊞ Loopback
⊞ Internal
⊞ External
⊞ Setup
⊞ IPsec
⊞ Dynamic routes
⊟ modemwan
Source NAT ☑
⊟ ethernetwan
Source NAT ☑
Add Zone Zone Add
⊞ Port forwarding
⊟ Packet filtering
1. ⊟ Reject LAN traffic to Modem
Enable ☑
Label Reject LAN traffic to Modem
Action Reject
IP version Any
Protocol Any
Source zone Internal
Source port any
Destination zone modemwan
Destination port any
2. ⊟ Allow all outgoing traffic
Enable ☑
Label Allow all outgoing traffic
Action Accept
IP version Any
Protocol Any
Source zone Internal
Source port any
Destination zone Any
Destination port any
Add Packet filter Add
⊟ Custom Rules
Enable ☑
Override ☐
Rules

```
iptables -I FORWARD --match mac --mac-source 52:54:00:c2:a5:43 -m set --match-set zone-internal src,src -m set --match-set zone-ethernetwan dst,dst -j ACCEPT
```

⊞ Services
⊞ Authentication
⊞ System
⊞ Monitoring

Data Usage Estimates

The 63xx LTE Routers are designed to be sensitive to the data usage on a customer's wireless data plan. Careful consideration was applied to add reporting, alerting, and remote control features through the best-of-breed Accelerated View™ cloud management system. Please note that even though the service was designed with standard reporting/ control intervals these values can be adjusted downward to obtain near-zero data utilization or, conversely, remote services can be tuned up for more aggressive monitoring at the expense of additional data utilization. The current Accelerated View architecture requires that all devices have a minimum of 1 publicly reachable IP address to access cloud-based features (see below).

NOTE: These values are estimates to be used for planning purposes -- the actual carrier data measurement may vary.

Data Consumption for Accelerated View Services

Service/ Function	Status/ Interval	Usage	Notes
Cloud-based Reporting/ Configuration	Standard (every 30 min)	3MB (per month)	Includes one startup sequence

Service/ Function	Status/ Interval	Usage	Notes
Remote Control (IPSec tunnel)	Central management is enabled by default	25MB (per month)	Minimum keep-alive traffic

❗ For deployments with heightened sensitivity toward data usage, the IPSec remote control tunnel can be disabled. Cloud-based reporting and configuration can still be accomplished via SMS commands that are not subject usage metering on mobile data plans. Please consult Accelerated for more information before leveraging this approach, "Option 2" in the table below.

NOTE: Charges for SMS messages may apply. Please consult your cellular carrier for billing details.

Service/ Function	Status/ Interval	Usage	Notes
Option 2 (Contact Accelerated for help)	IPSec disabled	2MB	Uses SMS on demand

Itemized Breakdown of Services via Accelerated View

Service/ Function	Status/ Interval	Usage	Notes
Syslog check-in	Every 30 minutes	1KB	Used for reporting and alerts
Configuration check-in	Once nightly -- 1am (UTC)	12KB	Recommended for remote management
Boot-up sequence	Each device reboot	24KB	Used for reporting and remote management
Device firmware upgrade	As needed (~8 releases per year)	10MB	Updates device firmware upon new release
Modem firmware upgrade	As needed (less frequent than device firmware updates)	60MB	Updates firmware on the embedded cellular modem

Accelerated View Ports and URL Access

IP Address

128.136.167.120 with Ports (UDP: 123, 514 TCP: 443, 500/4500 IPsec)

URLs

time.accns.com; logs.accns.com; syslog.accns.com; certs.accns.com; configuration.accns.com; remote.accns.com

Optional IP

8.8.8.8 with UDP Port 53 – DNS backup and ping testing (customer can customize this value)

Signal Bars Explained

The cellular signal strength bars of Accelerated LTE routers are calculated using various algorithms based on the network type it is connected to. For 4G LTE, the RSRP, SNR, and RSSI values are all factored in to determine the reported signal strength bars. For 3G networks (including HSPA+) and 2G networks, the signal strength bars are determined by the RSSI value.

4G LTE algorithm

Determine RSRP, SNR, and RSSI values separately, using the following

```
RSRP > -85, rsrp_bars=5
-95 < RSRP <= -85, rsrp_bars=4
-105 < RSRP <= -95, rsrp_bars=3
-115 < RSRP <= -105, rsrp_bars=2
-199 < RSRP <= -115, if we're connected to the cellular network, rsrp_bars=1, if not
rsrp_bars=0
```

If RSRP <= -199, then use RSSI as the value and run it through the same algorithm described above.

```
SNR >= 13, snr_bars=5
4.5 <= SNR < 13, snr_bars=4
1 <= SNR < 4, snr_bars=3
-3 < SNR < 1, snr_bars=2
-99 < SNR <= -3, if we're connected to the cellular network, snr_bars=1, if not
snr_bars=0
```

Once the snr_bars and rsrp_bars are determined, use the lesser of the two. That is the reported signal strength bars.

3G algorithm

Determine RSSI signal strength.

```
RSSI > -80, bars=5
-90 < RSSI <= -80, bars=4
-100 < RSSI <= -90, bars=3
-106 < RSSI <= -100, bars=2
RSSI <= -106, if we're connected to the cellular network, bars=1, if not bars=0
```

bars is then reported as the signal strength bars.

2G algorithm

Determine RSSI signal strength.

```
RSSI > -80, bars=5
-89 < RSSI <= -80, bars=4
-98 < RSSI <= -89, bars=3
-104 < RSSI <= -98, bars=2
RSSI <= -104, if we're connected to the cellular network, bars=1, if not bars=0
```

bars is then reported as the signal strength bars.

WiFi Capabilities

The 6350-SR broadcasts WiFi in compliance with the 802.11b/g/n standard.

Range of Access

A wireless access point's range varies depending upon the presence of potential obstructions and/ or sources of interference in the surrounding area. The 802.11b/g standard supports a range from **150 feet (46 meters)** for typical indoor use to a maximum of around **300 feet (92 meters)**. 802.11n-compatible devices typically have twice the range of 802.11b/g devices.

Note that these figures represent a theoretical range that anticipates standard construction materials at the location in question. Actual results may vary from site to site.

Number of Supported Users

There is no limit to the number of client devices that may connect to one of the 6350-SR's SSIDs. However, the available bandwidth will eventually become a limiting factor as additional equipment generates an increasing amount of throughput.

Testing has indicated that **32 users** is the upper limit of reliable, simultaneous connections on a 2.4 GHz WiFi network -- this assumes all of those devices are generating standard internet traffic concurrently.

Firewall Capabilities

Number of Supported Firewall Rules

There is no software-defined limit to the number of rules that may be created. A safe upper limit, due to potential hardware constraints, would be **25,000 lines.**

Encrypted Throughput Capacity

AES-128 was used for testing encrypted throughput on Accelerated LTE routers, yielding the following results:

	Download	Upload
CX Series	150 Mbps	50 Mbps
SR Series	100 Mbps	50 Mbps

Concurrent Sessions

Default settings allow **8,192 concurrent sessions** though this value can be adjusted via custom configuration.

The maximum is 65,536 -- though this assumes sessions are short lived and/ or low-bandwidth -- a good upper limit is 10,000.

New Sessions per Second

No limit exists in the software, though a safe upper limit would be **150** sessions.

Wildcard IP Support

Wildcard IPs are supported via **custom firewall rules** (iptables), which leverage CIDR networking to set up a range of IPs (e.g. 192.168.0.1/24).

FQDN Support

FQDN is supported via **custom firewall rules** (iptables).

However, the FQDN is resolved at the time of process/applying the firewall rule, not with each packet inspected. Meaning, if the IP of a domain changes, the firewall rule will not apply to the new IP address. You would have to reload the firewall for the device to resolve the domain to the new IP. It is better to stick with IP addresses in firewall rules instead of FQDNs.

Sprint Activation

SIM Setup

Sprint grants devices access to their network using specific SIM cards that correspond to the LTE modem being used, as well as the category of that modem. Special attention should be paid to matching up the SIM card to the type of modem.

The Cat-3 Sierra MC7354 modem uses a USIM card and the Cat-6 Sierra MC7455 modem uses the ISIM card. The part number printed on the SIM card indicates its type (see chart below for reference).

The **6300-CX LTE Router** and **1002-CM03 Plug-in Modem** use the *Sierra MC7354* and the **1002-CM06 Plug-in Modem** uses the *Sierra MC7455*.

NOTE: It is not recommended to move an active Sprint SIM card between modems because the Sprint network may disconnect the connection due to a mismatch between the SIM and the device ID. SIMs should always be activated to the unique device being used. The ID used to identify the device is the IMEI, which should be printed on the device. If the MEID is required instead, this can be calculated by removing the last digit from the IMEI.

❗ Accelerated products support the 2FF SIM standard.

MC7354 module's UICC cards (USIM)

	2FF	3FF
SKU	CZ2100LWR	CZ2102LWR
OEM Part No.	SIMGLW106R	SIMGLW206R
UPC	760494000091	760492013536

MC7455 module's UICC cards (ISIM)

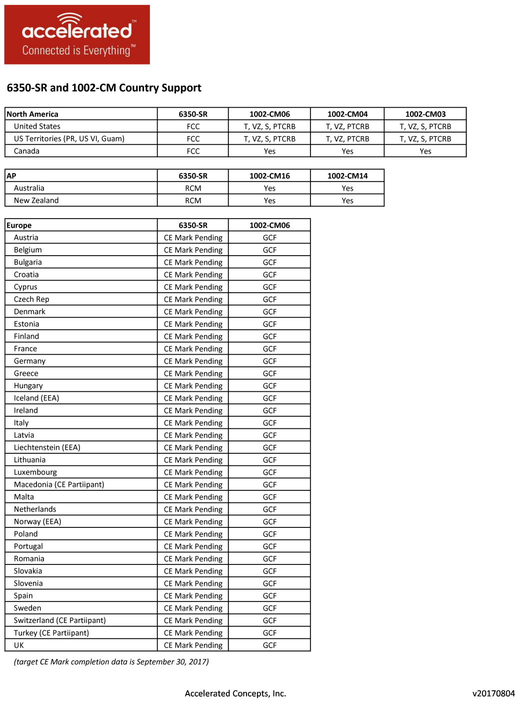
	2FF	3FF
SKU	CZ2100LWQ	CZ2112LWQ
OEM Part No.	SIMGLW106Q	SIMGLW216Q
UPC	019962040740	019962040948

Default LTE APNs

r.ispsn

n.ispsn

Cellular Support Info by Country



accelerated™
Connected is Everything™

6350-SR and 1002-CM Country Support

North America	6350-SR	1002-CM06	1002-CM04	1002-CM03
United States	FCC	T, VZ, S, PTCRB	T, VZ, PTCRB	T, VZ, S, PTCRB
US Territories (PR, US VI, Guam)	FCC	T, VZ, S, PTCRB	T, VZ, PTCRB	T, VZ, S, PTCRB
Canada	FCC	Yes	Yes	Yes

AP	6350-SR	1002-CM16	1002-CM14
Australia	RCM	Yes	Yes
New Zealand	RCM	Yes	Yes

Europe	6350-SR	1002-CM06
Austria	CE Mark Pending	GCF
Belgium	CE Mark Pending	GCF
Bulgaria	CE Mark Pending	GCF
Croatia	CE Mark Pending	GCF
Cyprus	CE Mark Pending	GCF
Czech Rep	CE Mark Pending	GCF
Denmark	CE Mark Pending	GCF
Estonia	CE Mark Pending	GCF
Finland	CE Mark Pending	GCF
France	CE Mark Pending	GCF
Germany	CE Mark Pending	GCF
Greece	CE Mark Pending	GCF
Hungary	CE Mark Pending	GCF
Iceland (EEA)	CE Mark Pending	GCF
Ireland	CE Mark Pending	GCF
Italy	CE Mark Pending	GCF
Latvia	CE Mark Pending	GCF
Liechtenstein (EEA)	CE Mark Pending	GCF
Lithuania	CE Mark Pending	GCF
Luxembourg	CE Mark Pending	GCF
Macedonia (CE Partiipant)	CE Mark Pending	GCF
Malta	CE Mark Pending	GCF
Netherlands	CE Mark Pending	GCF
Norway (EEA)	CE Mark Pending	GCF
Poland	CE Mark Pending	GCF
Portugal	CE Mark Pending	GCF
Romania	CE Mark Pending	GCF
Slovakia	CE Mark Pending	GCF
Slovenia	CE Mark Pending	GCF
Spain	CE Mark Pending	GCF
Sweden	CE Mark Pending	GCF
Switzerland (CE Partiipant)	CE Mark Pending	GCF
Turkey (CE Partiipant)	CE Mark Pending	GCF
UK	CE Mark Pending	GCF

(target CE Mark completion data is September 30, 2017)

Accelerated Concepts, Inc. v20170804

PDF 6350-SR_1002-CM_Country_Certifications_Public_(vNTM).pdf

Verizon SIM with static APN registers but doesn't connect [SOLVED]

Problem

A newly activated Verizon SIM with a static APN (e.g. ne01.vzwstatic) is inserted into a 63xx-series router. The 63xx-series router is able to detect the SIM and seeing an available Verizon network, but the 63xx-series router is unable to establish a cellular connection. The LED behavior on the front of the 63xx-series router will be a flashing white status/LTE LED, and intermittent 5 bars of signal strength.

Background

It can sometimes take longer than the 63xx-series router anticipates for the Verizon SIM to finish its registration process on the Verizon network. As a result, the 63xx-seris router tries establishing a cellular connection before this SIM finishes registering, which results in a failed connection. The 63xx-series router interprets this failed connection as it not using the correct APN, so it resorts to its fallback list of APNs to try alternate Verizon APNs with the SIM. Since the correct APN was already tried, this fallback list of APNs will try APNs that are not provisioned with the SIM. The result is the 63xx-series router gets stuck trying a fallback list of APNs, of which none will work with the given SIM.

Solution

Firmware versions 17.8.128.37 or higher resolves the connectivity issues. You can use the following instructions to upgrade the 63xx-series router to the new 17.8.128.37 firmware:

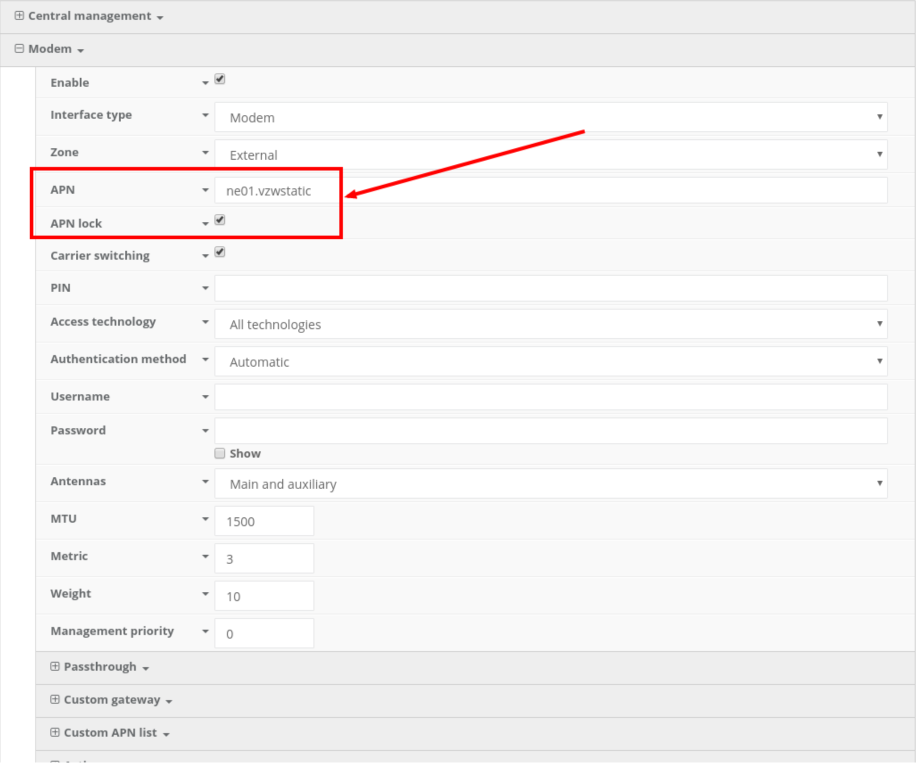
http://kb.accelerated.com/m/67105/l/729960-getting-started-with-accelerated-view#UpgradingFirmware

Manual Solution

Users can lock the 63xx-series router to keep trying the same APN. This allows the 63xx-series router to retry the same APN that the SIM card is provisioned with. Even if the 63xx-series router cannot establish a cellular connection with the SIM initially, it will keep trying with the same APN until it connects.

To implement this manual solution, update the configuration profile of the Accelerated 63xx-series router with the following configuration changes:

1. In *Modem -> APN*, set the appropriate static APN (e.g. *ne01.vzwstatic*).
2. Enable the *Modem -> APN lock* checkbox.



⊞ Central management

⊟ Modem

Enable	☑
Interface type	Modem
Zone	External
APN	ne01.vzwstatic
APN lock	☑
Carrier switching	☑
PIN	
Access technology	All technologies
Authentication method	Automatic
Username	
Password	 □ Show
Antennas	Main and auxiliary
MTU	1500
Metric	3
Weight	10
Management priority	0

⊞ Passthrough

⊞ Custom gateway

⊞ Custom APN list

Upgrading Modem Firmware

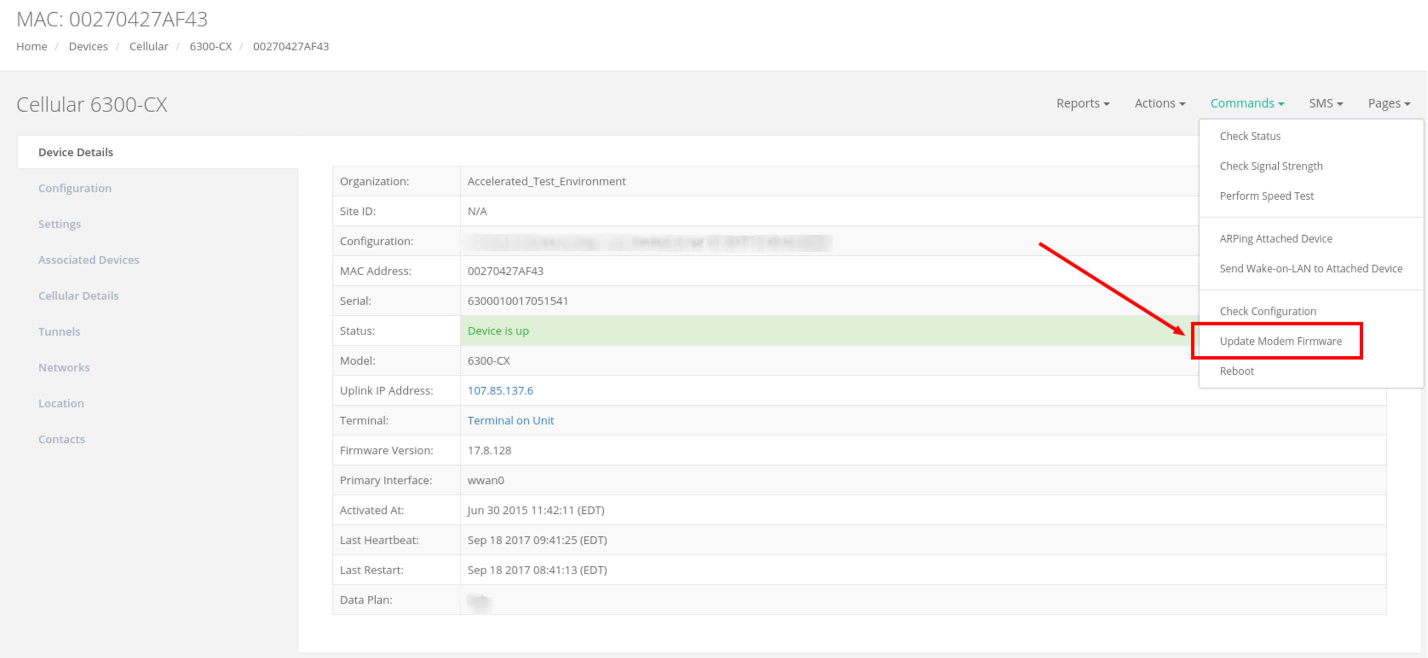
There are several options for upgrading the firmware on the modem inside your 63xx-series router. Users can upgrade the firmware on this modem either through the Accelerated View portal or the local web UI of the 63xx-series router, depending on the level of access and network connectivity the LTE router has and how the user has chosen to manage their devices.

OTA Update using Accelerated View

Upgrading the modem firmware using either of the options below requires the device to be online and in sync with Accelerated View.

Option 1 - OTA command

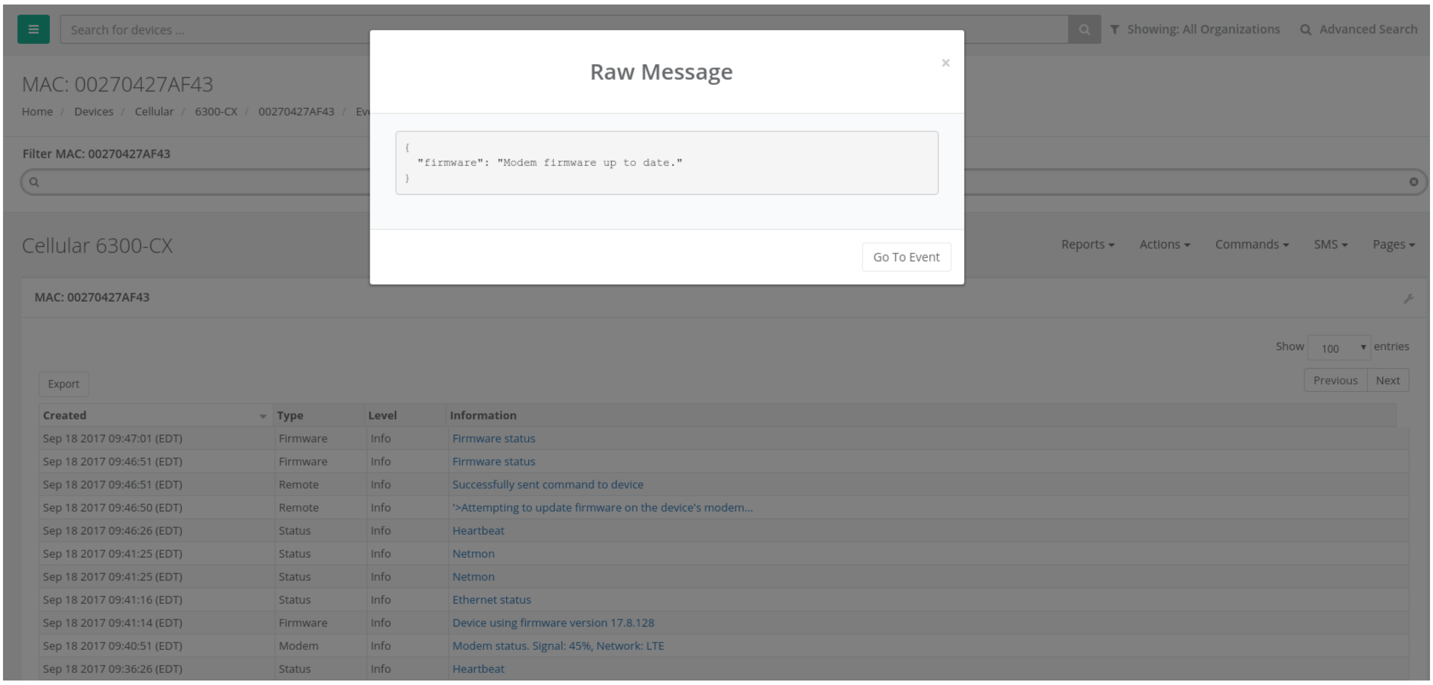
If the 63xx-series router is on firmware version 17.8.128 or higher, users can send the *Update Modem Firmware* command from Accelerated View. Details on how to send a remote command from Accelerated View to a 63xx-series router can be found here.



Organization:	Accelerated_Test_Environment
Site ID:	N/A
Configuration:	[redacted]
MAC Address:	00270427AF43
Serial:	6300010017051541
Status:	Device is up
Model:	6300-CX
Uplink IP Address:	107.85.137.6
Terminal:	Terminal on Unit
Firmware Version:	17.8.128
Primary Interface:	wwan0
Activated At:	Jun 30 2015 11:42:11 (EDT)
Last Heartbeat:	Sep 18 2017 09:41:25 (EDT)
Last Restart:	Sep 18 2017 08:41:13 (EDT)
Data Plan:	[redacted]

This command will trigger the 63xx-series router to query the Accelerated firmware server. If a newer modem firmware version is found for the current carrier-specific firmware used on the modem in the 63xx-series router, the 63xx-series router will automatically download the new firmware and flash it onto the modem.

If no new firmware is found, the 63xx-series router will send an event to Accelerated View stating that the modem firmware is up to date.



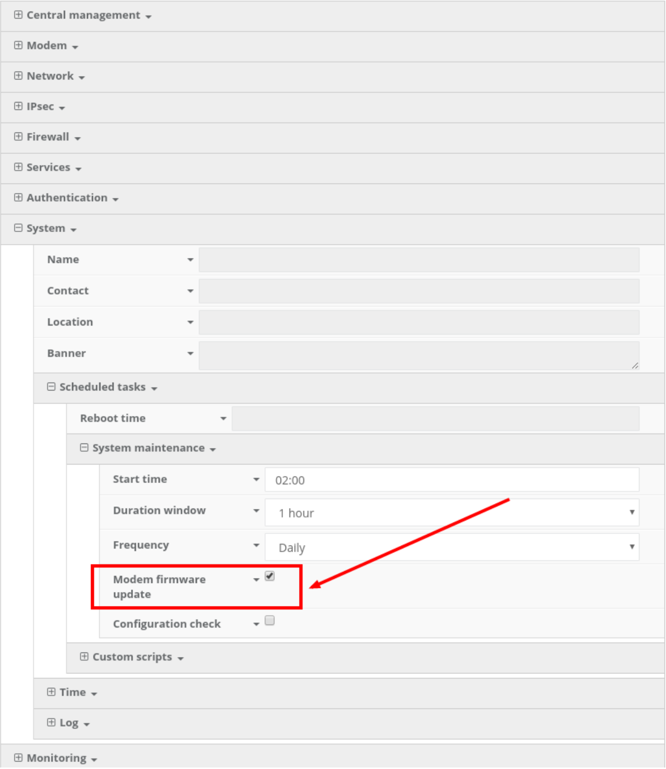
Raw Message

```
{
  "firmware": "Modem firmware up to date."
}
```

Created	Type	Level	Information
Sep 18 2017 09:47:01 (EDT)	Firmware	Info	Firmware status
Sep 18 2017 09:46:51 (EDT)	Firmware	Info	Firmware status
Sep 18 2017 09:46:51 (EDT)	Remote	Info	Successfully sent command to device
Sep 18 2017 09:46:50 (EDT)	Remote	Info	'>Attempting to update firmware on the device's modem...
Sep 18 2017 09:46:26 (EDT)	Status	Info	Heartbeat
Sep 18 2017 09:41:25 (EDT)	Status	Info	Netmon
Sep 18 2017 09:41:25 (EDT)	Status	Info	Netmon
Sep 18 2017 09:41:16 (EDT)	Status	Info	Ethernet status
Sep 18 2017 09:41:14 (EDT)	Firmware	Info	Device using firmware version 17.8.128
Sep 18 2017 09:40:51 (EDT)	Modem	Info	Modem status. Signal: 45%, Network: LTE
Sep 18 2017 09:36:26 (EDT)	Status	Info	Heartbeat

Option 2 - Scheduled OTA check/update

If the 63xx-series router is on firmware version 17.8.128 or higher, users can configure the router to check for modem firmware updates at a scheduled interval. This option is found under the *System -> Scheduled tasks -> System maintenance* section of the 63xx-series router's configuration profile. Details on configuring your 63xx-series router using Accelerated View can be found here.



Once the *Modem firmware update* scheduled task is enabled, the 63xx-series router will query the Accelerated firmware server at the specified timeframe. If a newer modem firmware version is found for the current carrier-specific firmware used on the modem in the 63xx-series router, the 63xx-series router will automatically download the new firmware and flash it onto the modem.

Manual Upgrade using the Local Web UI

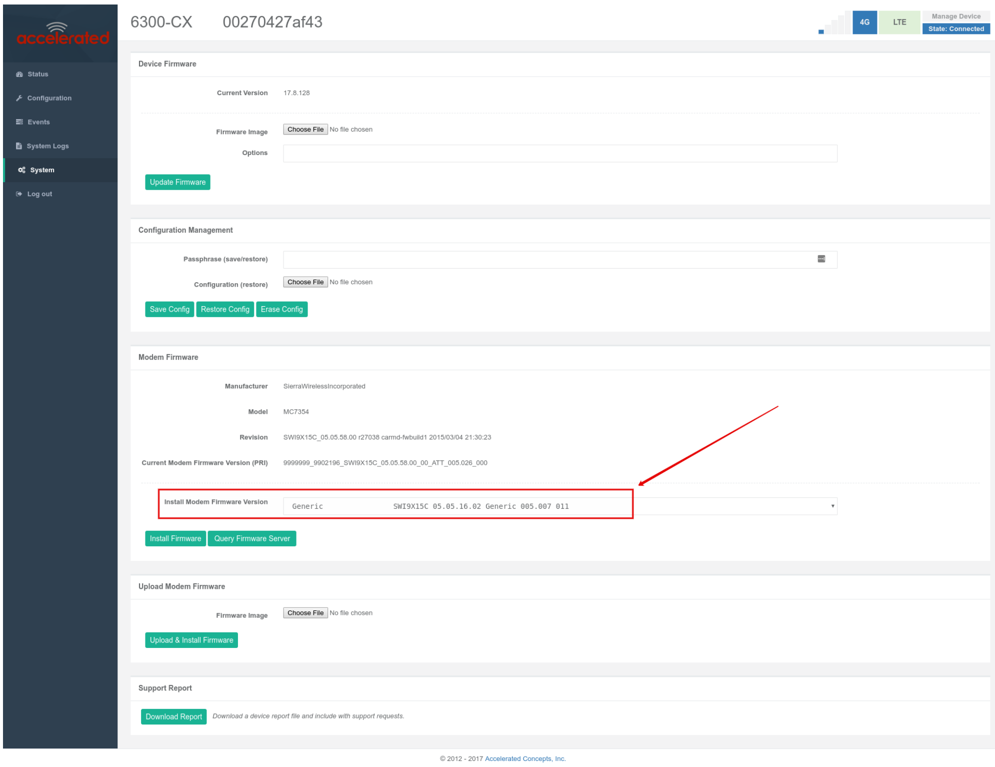
> Upgrading the modem firmware using any of the following options requires the user to directly access the web UI of the 63xx-series router.

Option 1 - Select from pre-loaded firmware list

The Category 3 series of cellular modems have smaller firmwares that our 63xx-series routers have pre-loaded inside their flash memory. Users can update the modem in their 63xx-series router to one of these pre-loaded firmwares using the following steps:

1. Login to the web UI of the 63xx-series router.
2. Click on the *System* link on the left navigation bar of the site.
3. Under the *Modem firmware* section of the page, click the drop-down next to *Install Modem Firmware Version* and select the desired carrier firmware.

4. Click *Install Firmware*. A progress bar will appear indicating the status of the modem's firmware upgrade. Once the upgrade completes, the 63xx-series router will automatically reconnect to the cellular network.



6300-CX 00270427af43

Device Firmware

Current Version 17.8.128

Firmware Image No file chosen

Options

Configuration Management

Passphrase (save/restore)

Configuration (restore) No file chosen

Modem Firmware

Manufacturer SierraWirelessIncorporated

Model MC7354

Revision SWI9X15C_05.05.58.00 r27038 carmd-fwbuild1 2015/03/04 21:30:23

Current Modem Firmware Version (PRI) 9999999_9902196_SWI9X15C_05.05.58.00_00_ATT_005.026_000

Install Modem Firmware Version Generic SWI9X15C 05.05.16.02 Generic 005.007 011

Upload Modem Firmware

Firmware Image No file chosen

Support Report

Download a device report file and include with support requests.

© 2012 - 2017 Accelerated Concepts, Inc.

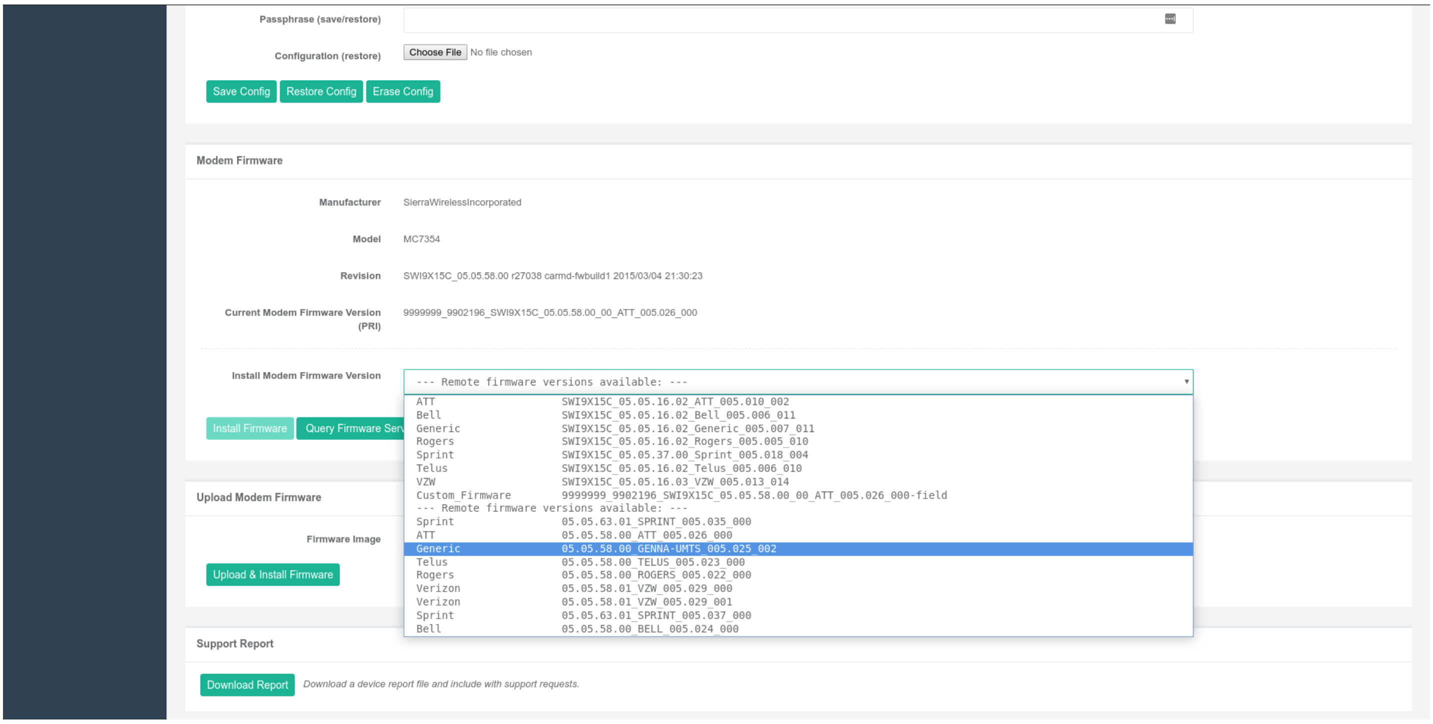
Option 2 - Query Firmware Server

If the desired modem firmware version is not listed in the pre-loaded firmware drop-down mentioned in option 1 above, users can query the Accelerated firmware server for additional firmwares for the modem inside the 63xx-seris router.

Note, your 63xx-series router must be online and have access to the Accelerated firmware.accns.com server in order for this query to work. As part of this process, the 63xx-series router will download the new firmware file over the Internet (approximately 30-60MB) and onto the device.

To perform this query and upgrade the firmware on the modem:

1. Click on the *Query Firmware Server* button.
2. Once the query completes, the drop-down will list the available remote firmware versions.
3. Select the desired firmware version from the list
4. Click the *Install Firmware* button. A progress bar will appear indicating the status of the modem's firmware upgrade. Once the upgrade completes, the 63xx-series router will automatically reconnect to the cellular network.



Passphrase (save/restore)

Configuration (restore): No file chosen

Modem Firmware

Manufacturer: SierraWirelessIncorporated

Model: MC7354

Revision: SWI9X15C_05.05.58.00 r27038 carmd-fwbuild1 2015/03/04 21:30:23

Current Modem Firmware Version (PRI): 9999999_9902196_SWI9X15C_05.05.58.00_00_ATT_005.026_000

Install Modem Firmware Version: --- Remote firmware versions available: ---

```
ATT                 SWI9X15C_05.05.16.02_ATT_005.010_002
Bell                SWI9X15C_05.05.16.02_Bell_005.006_011
Generic             SWI9X15C_05.05.16.02_Generic_005.007_011
Rogers              SWI9X15C_05.05.16.02_Rogers_005.005_010
Sprint              SWI9X15C_05.05.37.00_Sprint_005.018_004
Telus               SWI9X15C_05.05.16.02_Telus_005.006_010
VZW                 SWI9X15C_05.05.16.03_VZW_005.013_014
Custom_Firmware     9999999_9902196_SWI9X15C_05.05.58.00_00_ATT_005.026_000-field
--- Remote firmware versions available: ---
Sprint              05.05.63.01_SPRINT_005.035_000
ATT                 05.05.58.00_ATT_005.026_000
Generic             05.05.58.00_GENNA-UMTS_005.025_002
Telus               05.05.58.00_TELUS_005.023_000
Rogers              05.05.58.00_ROGERS_005.022_000
Verizon             05.05.58.01_VZW_005.029_000
Verizon             05.05.58.01_VZW_005.029_001
Sprint              05.05.63.01_SPRINT_005.037_000
Bell                05.05.58.00_BELL_005.024_000
```

Upload Modem Firmware

Firmware Image

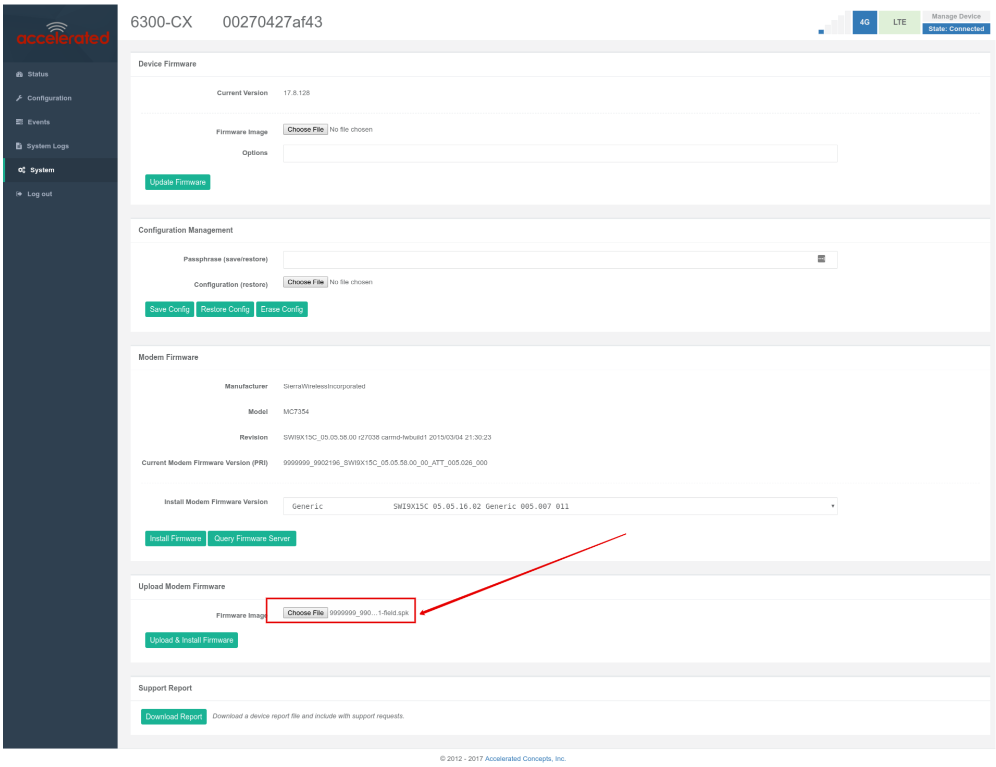
Support Report

Download a device report file and include with support requests.

Option 3 - Manual Firmware Upload

Some vendors supply direct firmware images for their cellular modems. If you have a specific firmware file you would like to apply to the modem, you can use the *Upload Modem Firmware* section on the 63xx-series router's *System* web UI page to upload the firmware onto the modem. To manually upload a firmware file onto the modem inside a 63xx-series router:

1. Select the *Choose File* button under the *Upload Modem Firmware* section.
2. Select the desired firmware file from your file system.
3. Click *Upload & Install Firmware*. A progress bar will appear indicating the status of the modem's firmware upgrade. Once the upgrade completes, the 63xx-series router will automatically reconnect to the cellular network.



6300-CX 00270427af43

Device Firmware

Current Version 17.8.128

Firmware Image No file chosen

Options

Configuration Management

Passphrase (save/restore)

Configuration (restore) No file chosen

Modem Firmware

Manufacturer SierraWirelessIncorporated

Model MC7354

Revision SWI9X15C_05.05.58.00 r27038 carmd-fwbuild1 2015/03/04 21:30:23

Current Modem Firmware Version (PRI) 9999999_9902196_SWI9X15C_05.05.58.00_00_ATT_005.026_000

Install Modem Firmware Version Generic SWI9X15C 05.05.16.02 Generic 005.007 011

Upload Modem Firmware

Firmware Image 9999999_990…1-field.spk

Support Report

Download a device report file and include with support requests.

© 2012 - 2017 Accelerated Concepts, Inc.

Antenna Terminology

Electronics require antennas to convert data into RF signals (and vice versa). They are coupled with radio transmitters and/or receivers to process the information that is carried over cellular bands. Antenna design and functionality has evolved over time:

Internal Antennas: An antenna can be concealed within the casing of a device, as seen with most smart phones. Internal antennas are potentially more prone to interference due to the close grouping of electrical components.

External Antennas: Situating antennas further away from the rest of the circuit board can help alleviate this problem by maximizing a device's natural reach. Instead of sitting inside the device directly next to the modem or transceiver, they screw into place using SMA connectors and protrude from the equipment (think "rabbit ears").

MIMO: Multiple-Input and Multiple-Output (MIMO) technology expands the throughput capacity of a transceiver by leveraging multiple antennas to simultaneously convert RF signals into data (or vice versa), providing faster transfer speeds as a result. Think of it (loosely) as Carrier Aggregation for antennas -- once again combining individual lanes into a single, coordinated superhighway. Networks must leverage MIMO antenna transmission to be technically considered 4G.

Physical Specifications

Accelerated LTE Routers use industry-standard, female SMA connectors to affix antennas to the internal cellular radio. External antennas improve clarity when compared to internal antennas, which are prone to electromagnetic interference. An extension coaxial cable can also enhance the reach of a device; however, that cabling causes **attenuation** -- or a degradation in signal quality -- due to the distance the signal travels. Significant attenuation typically begins at 30 feet of cabling.

Certain Accelerated products, e.g. the 6300-CX and 6330-MX LTE Routers, are designed to provide the ability to place the cellular router where reception is best (moving the "radio" is always preferred). This allows the device to "capture" optimal Radio Frequency (RF) before converting it to IP packets and transmit data via Ethernet cabling, an approach that yields increased performance and cost savings over coax cabling. Accelerated can also provide a battery pack for site surveys, creative mounting options, and a (passive) Power-over-Ethernet injector to provide an efficient, flexible deployment at the lowest possible cost. Most Accelerated clients will not require third-party antennas unless deploying a more traditional LTE router (without PoE). It is always preferred to mount a PoE router on an external wall via Ethernet and use the shortest coax cable required to run the external antenna to the outside of a building.

❗ CRITICAL NOTE: Please test the signal strength outside of the building to ensure you have cellular coverage in the area prior to any cabling work. (Tip: Use the site survey battery to do this.)

Best Practices for PoE Deployments

Most LTE specifications recommend (or even require) the use of dual antennas for a MIMO configuration. Many antennas include a MIMO configuration in a single antenna housing, which can be confirmed if there are two cellular coax connections running from the housing. A single-housing MIMO antenna would also require the use of dual coax extension cables. If you select a non-MIMO antenna it is recommended that two separate antennas are used, though this configuration doubles the cost of the antenna unit itself as well as the coax extension cabling. It is typically recommended to include some “separation” when mounting antennas to prevent interference (the antenna manufacturer may provide a recommendation but 18 to 24 inches should be sufficient).

Please consider the following when mounting your PoE LTE Router or third-party antennas:

1. Maximize Ethernet vs. coax extensions (e.g. inside vs. outside the building)
2. Avoid mounting inside metal enclosures or even near large metal objects
3. Within reason, maximize the distance from any other electronic equipment
4. Mount the device near an exterior wall or window (or run the antenna outdoors)
5. If possible, mount to the ceiling vs. the wall (the wall can introduce interference)
6. Generally mounting higher is better (but consider future serviceability)
7. Try to always use a MIMO antenna solution for the best results / RF performance

Accelerated has tested the following antenna solutions for performance and compatibility purposes. Please use this information as a reference to assist in determining the right antenna solution for your specific use case. It is important to test the antennas you select in your specific application environment (meaning your deployment site).

Please note that a booster, repeater, or amplifier may be another strategy to improve RF sensitivity. However, these technologies can also introduce issues because they may “amplify” bad signal. The focus of this chapter is on antennas but more information on boosters can be found on-line.

Antennas Tested by Accelerated

PLEASE NOTE: The below information has been compiled by Accelerated to assist clients in finding and sourcing an antenna solution to best meet their application and business needs. The information on availability and pricing is for planning purposes only and may vary. Clients should test and validate their own applications prior to selecting an antenna for their project.

These antennas are "Omni-Directional" or offer the ability to send/receive signals from any direction. Directional antennas may improve RF sensitivity, but they will require an expert knowledge to find a specific cellular tower and maintain the ongoing fine-tuning that may be required to keep the antenna positioned properly. Due to the challenges of directional antennas, Accelerated typically focuses on *MIMO omni-directional models*.

Extra-Small IoT "Paddle" Antennas

Manufacturer: Taoglas Antennas Solutions

Product: TG.08.0113 and the Product Datasheet

Sample Retailers: Accelerated; Digi-Key; Mouser; Tessco

MSRP: $12 per antenna ($24 for a pair)

NOTE: Use of 2 antennas is recommend for full MIMO Operation

Deployment Notes:

This is an antenna recommended for consideration when a project requires antennas with a small form factor (e.g. digital signage, small enclosures, rack mounted, in-vehicle, etc). The performance of these antennas is surprisingly good considering the size. Although testing has shown they may slightly underperform compared to the antennas included with your Accelerated router, these smaller may provide the perfect balance between form factor and performance in your IoT application.

Large External MIMO Antenna (Outdoor Rated)

Manufacturer: EAD

Product: LMO7270 and the Product Datasheet

Sample Retailers: Accelerated

MSRP: $129 with dual 5M coax cabling (sold for use with Accelerated Routers)

Deployment Notes:

This is a hardened antenna designed to be mounted outdoors. This is a MIMO antenna with two short “pig tail” connectors and the overall dimensions are 187 mm in height and 106 mm at the base. Accelerated will typically provide this antenna with a kit including dual coax cables at 5M in length. If you are using this antenna with an Accelerated PoE router (e.g. the 6300-CX LTE Router) we typically recommend you mount the Accelerated router on the inside and run the “short” 5M cables to the outside. Meaning you save costs and eliminate attenuation (signal loss) by running Ethernet as far as possible and minimize the coax cable length. Accelerated testing of this antenna reveals performance gain.

Flat MIMO Antenna #1

Manufacturer: Taoglas Antennas Solutions

Product: Gemini LMA100 and the Product Datasheet

Sample Retailers: Accelerated

MSRP: $99 with dual 5M cables

Deployment Notes:

This is an easy-to-use MIMO antenna. It offers a low-profile form factor that accommodates simple mounting. This model is manufactured by Taoglas and showed solid RF performance in our testing. The antenna has a square shape, sized at 164 mm x 164 mm x 36.5 mm. The antenna cabling is built into the antenna, and typically reaches only one meter, but it can be built (sized) to order (lead time can take up to 8 weeks). This antenna typically includes a stand that can be used instead of mounting. The pricing above is based on 5M cables (~15 feet) and the antenna is rated for indoor and outdoor use.

Flat MIMO Antenna #2

Manufacturer: Mobile Mark

Product: PNM2-LTE and the Product Datasheet

Sample Retailers: Sold through Distribution

MSRP: PNM2-LTE-1C1C-WHT-180 (includes Cabling @ 15 feet) $176.40

Deployment Notes:

This is an additional easy-to-use MIMO antenna with a low-profile form factor and simple mounting. This model is manufactured by Mobile Mark and showed solid RF performance in our testing. With a square form factor of 146 mm x 146 mm x 18 mm, the antenna cabling is built into the antenna and can be sized to order (typically lead time from the manufacturer is 2 weeks).

Paddle Extender

Built for Accelerated

Product SKU:

Sample Retailers: Sold through [Accelerated]

Deployment Notes:

This unique product (termed "the paddle extender") is designed to “move” the standard LTE router antennas to a more optimal spot to obtain better RF connectivity. A typical use can may be where the router is installed in a metal enclosure or rack (think of a data center or digital signage enclosure). The “paddle antennas” can be mounted to the top SMA connector, escaping the limitations of having to stay affixed to the device's chassis. Remote mounting is then simplified thanks to the paddle extender's magnetic base (diameter of 48mm [1.9 inches]). The length of the cable 50cm (19.7 inches).