6330-MX / 6335-MX

Table of Contents

User Manual

Configuration Examples

Supplemental Information

Antenna Notes and Solutions

Package Contents

6330-MX Unit

Cellular Antennas (2x)

Ethernet Cable

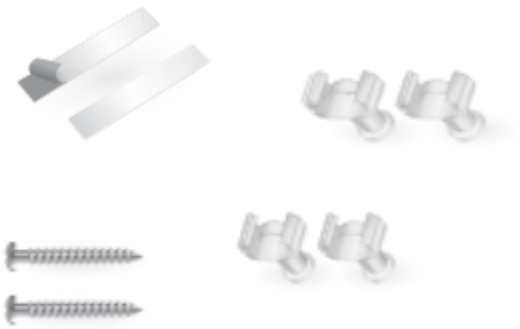
Power Supply Unit

Power-over-Ethernet (PoE) Injector

Temporary Battery Pack

Mounting Bracket

Mounting Accessories

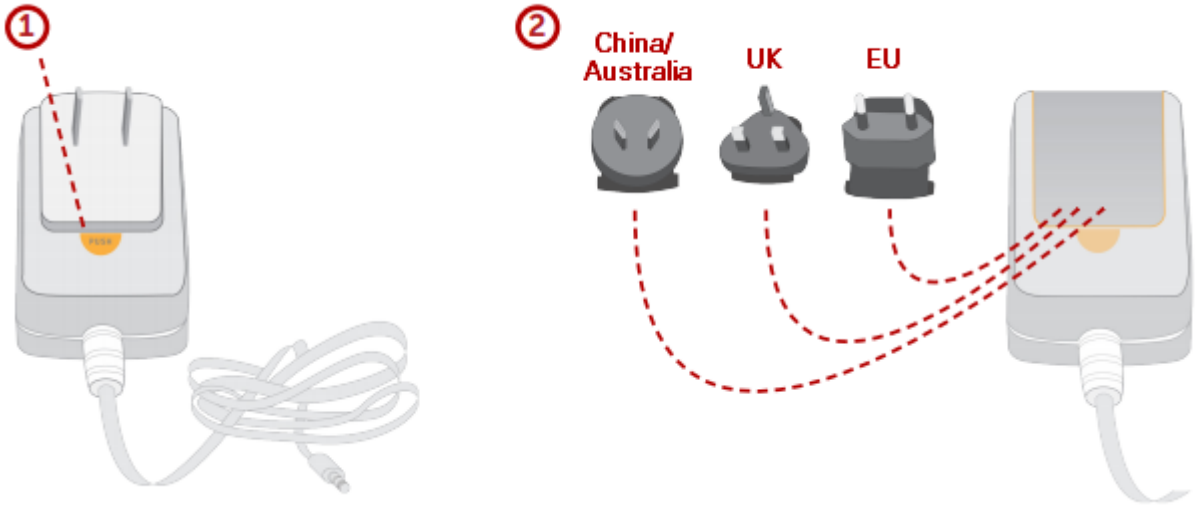


Exchanging Power Tips

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.



NOTE: *For more information regarding power-tip compatibility with global deployments, please click here.*

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** is used to perform device reset, and it has three modes. 1) Configuration reset, 2) Full device reset, 3) Firmware reversion:

1. Single pressing the ERASE button will reset the device configurations to factory default, **it will not** remove any automatically generated certificates/keys.
2. Two presses: After the device reboots from the first button press and by pressing the button again **before the device is connected** to the internet, the device configurations and generated certificates/keys will also be removed.
3. Press and hold the ERASE button and then power on the device will boot the firmware that was used prior to the current version.

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.

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.

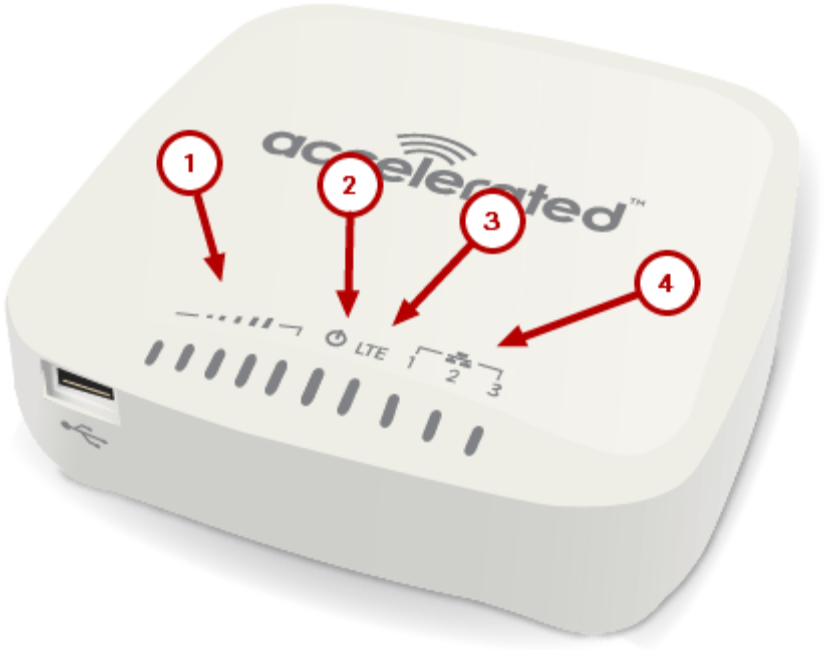
Be sure to use the plate with the cut outs for the antenna connectors.

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.

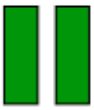
Solid Green
Connected to 2G or 3G and also has a device linked to a LAN port.

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.

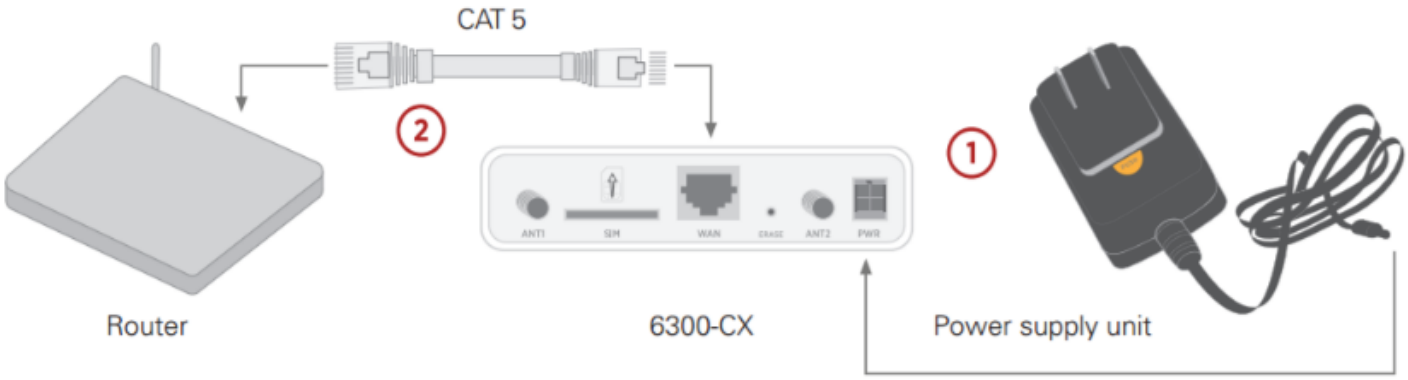
Site Survey Troubleshooting

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

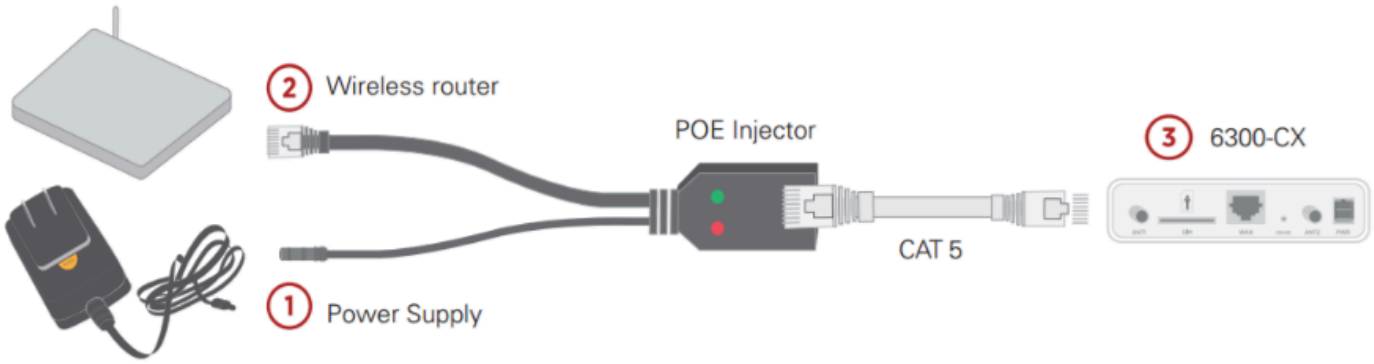
Connecting to the Site Network with Local Power



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.

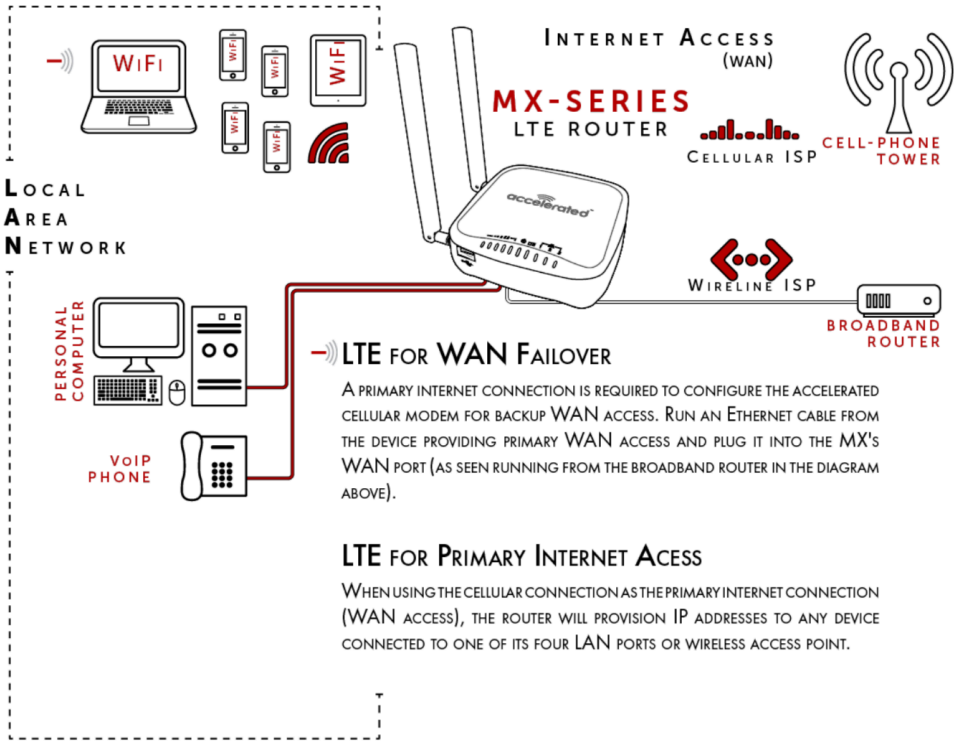
If the **IN** LED is not illuminated check the following:

- 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.

Network Integration



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 aView portal, you must manage and configure your device via the local interface.

Connect to the router using its Gateway IP address: **192.168.210.1** by default.

Username: root

Password: default

Once logged in via the local web interface, click on the ***Configuration*** link. You will initially be shown a limited set of configuration options. Start by enabling local management of the device.

1. Uncheck box next to "**Enable central management**"

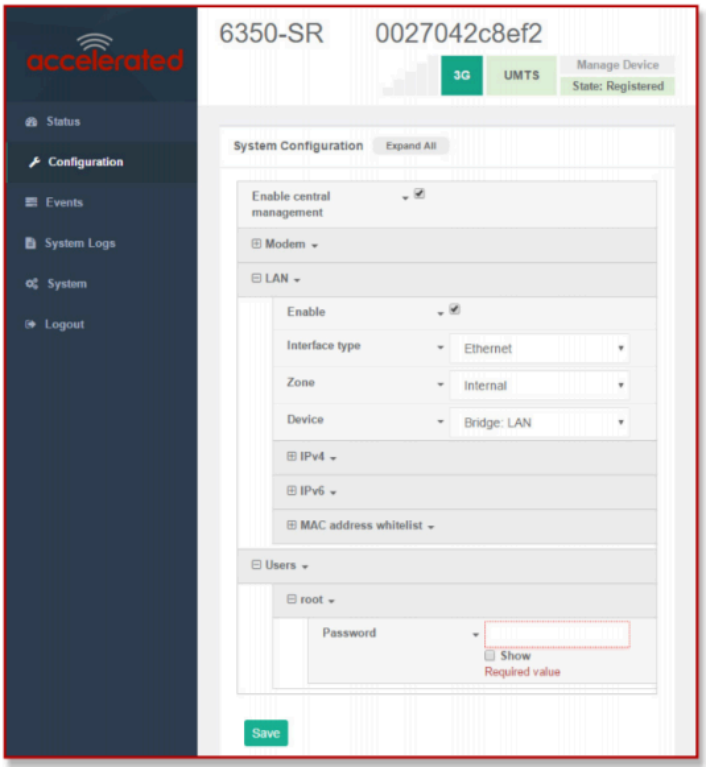
2. (optional) If this is the first time the device has been configured, you will also need to update the root user's password, under ***Users -> Root -> Password***

2. Click **Save**.

After saving the profile, the device will no longer attempt to sync with Accelerated View and a full range of available configuration options will be visible. Clicking the down arrow next to the name of a configuration option will display a pop-up providing help details about that option, including any default values.

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.)

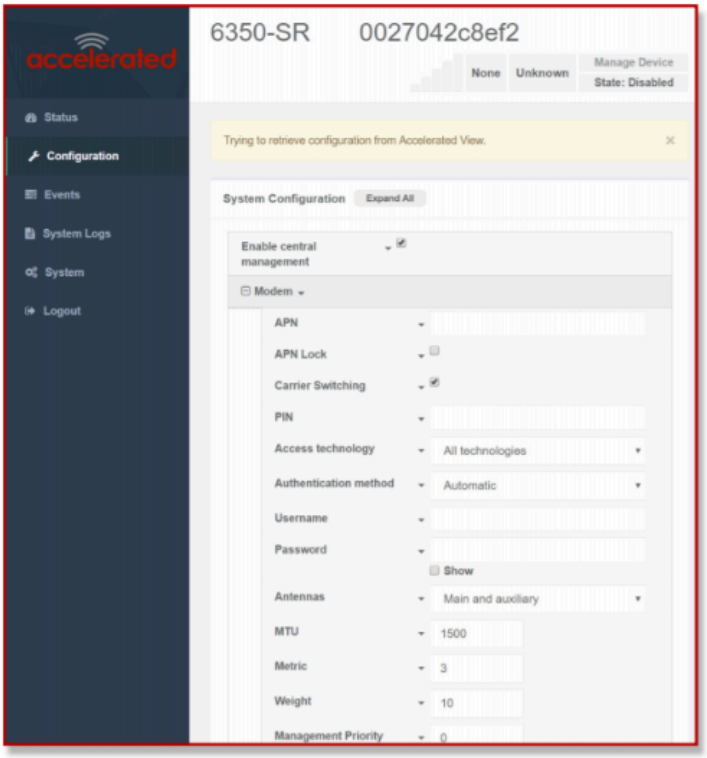


Defining a Custom APN

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.


accelerated
6350-SR
0027042c8ef2
None
Unknown
Manage Device
State: Disabled
Status
Configuration
Events
System Logs
System
Logout
Trying to retrieve configuration from Accelerated View.
System Configuration
Expand All
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.

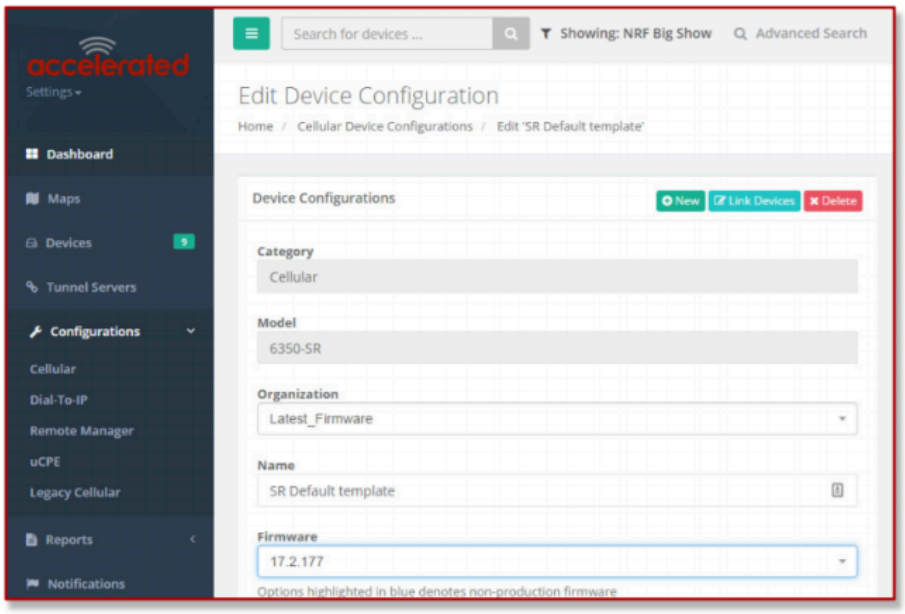
Devices will automatically apply configuration updates after the next daily sync (1am UTC by default). Refer to the **Remote Commands** sections for details on how to apply changes sooner.

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.



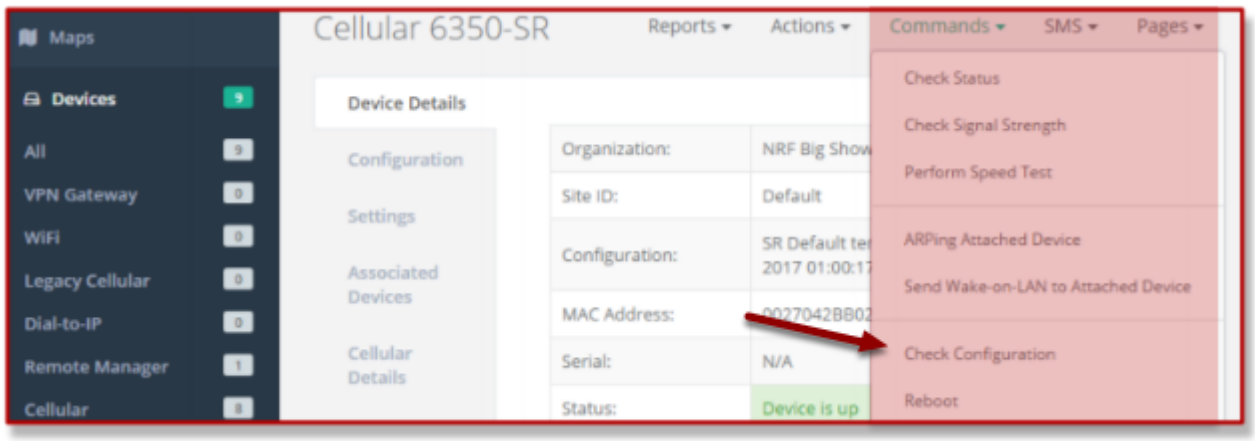
Using Remote Commands

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.



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").

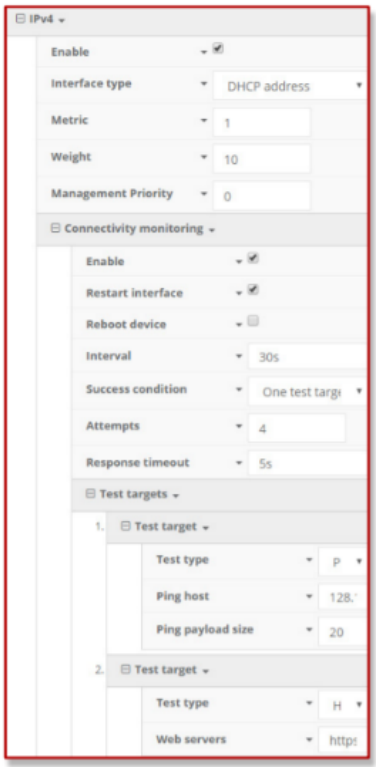
Connectivity Monitoring

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. **Note:** 2 different tests are recommended to prevent false positives.

NOTE: *Best practices dictate that redundant tests (with divergent failure conditions) will be the best way to ensure proper connectivity monitoring/active recovery. With only a single test type, false positives could be reported.*



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

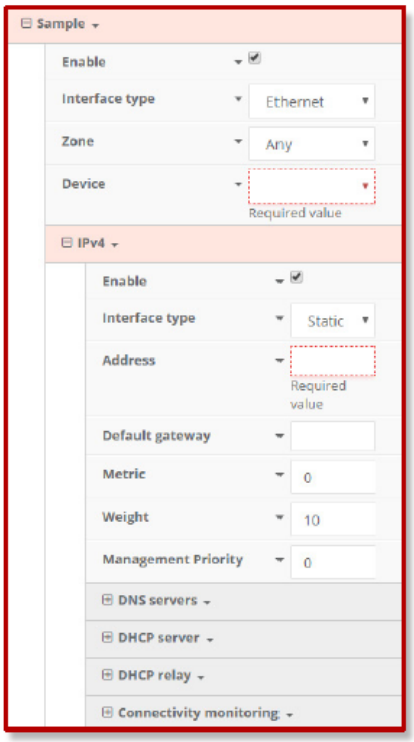
Changing the LAN Subnet

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.



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

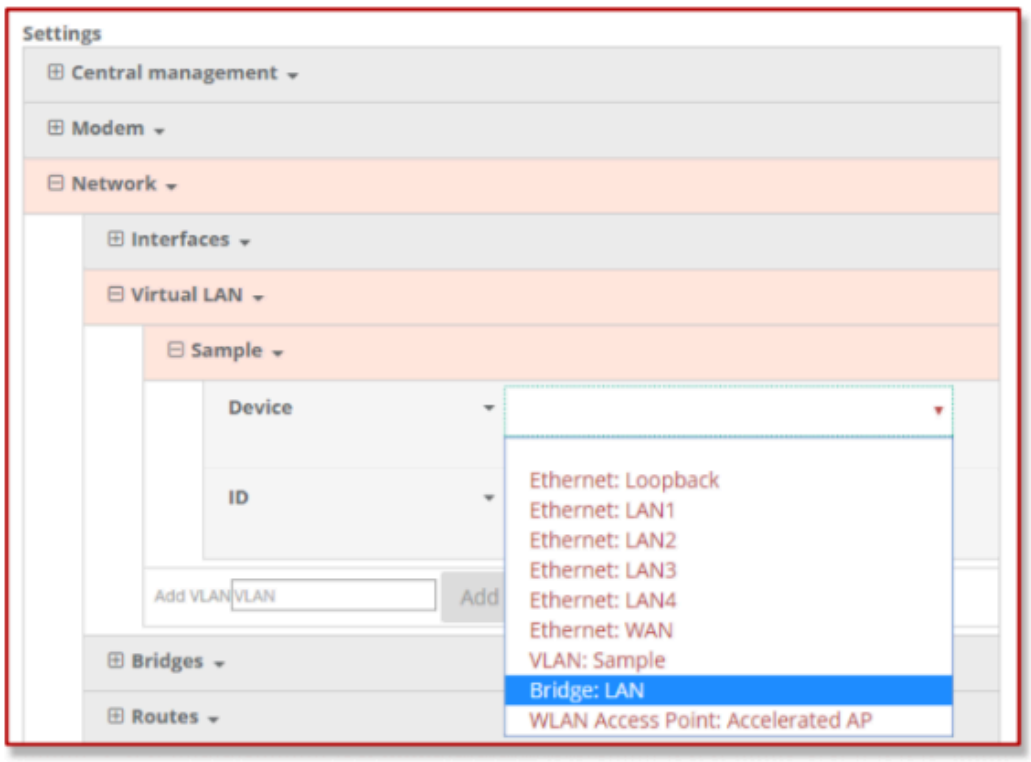
Before creating a Virtual LAN route for the MX-series router, be sure that its corresponding LAN interface has been configured (per the steps on the previous page).

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
Ethernet: Loopback
Ethernet: LAN1
Ethernet: LAN2
Ethernet: LAN3
Ethernet: LAN4
Ethernet: WAN
VLAN: Sample
Bridge: LAN
WLAN Access Point: Accelerated AP

WiFi Options

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

WiFi

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 > WiFi**.
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 WiFi originating from another WiFi-enabled router by entering that network's **SSID** and **Pre-shared key.**

WiFi as WAN

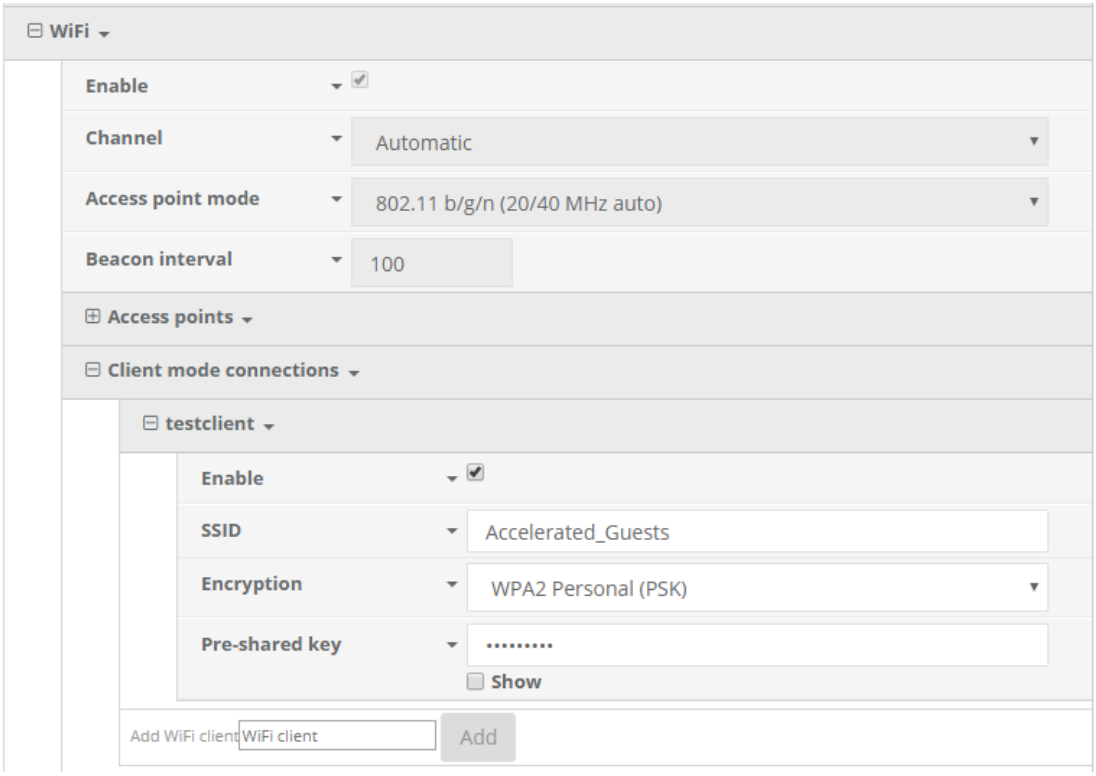
Client Mode can also be used to leverage the 6330-MX's WiFi to relay Internet access (WAN) provided by another router's wireless AP.

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 > WiFi > 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**.



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

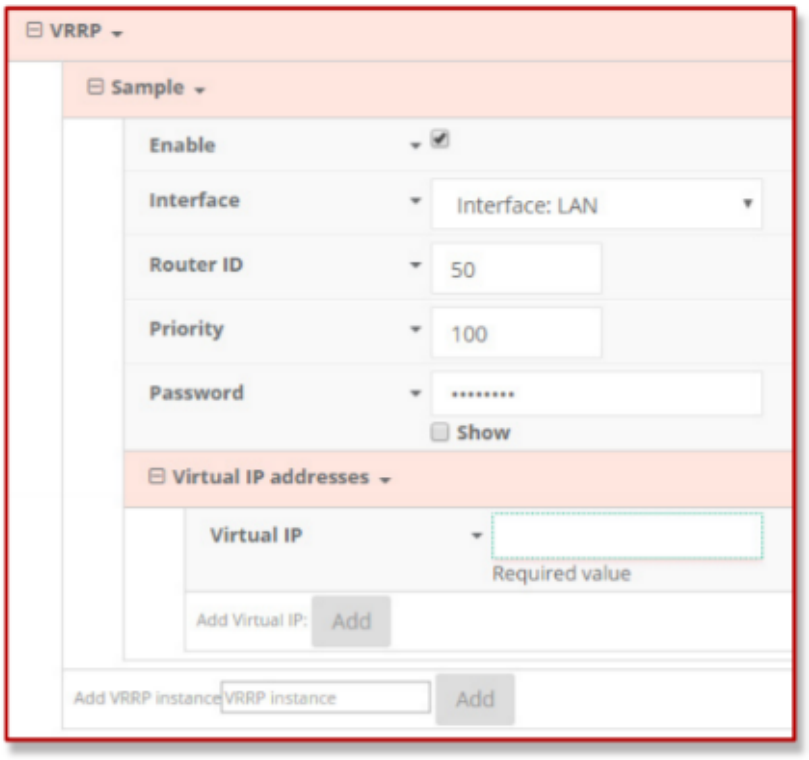
VRRP is a networking protocol used to configure devices as a "hot standby" for a primary router, where a backup device will only start routing traffic after the network detects that the primary device is offline (using parameters set by VRRP).

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.



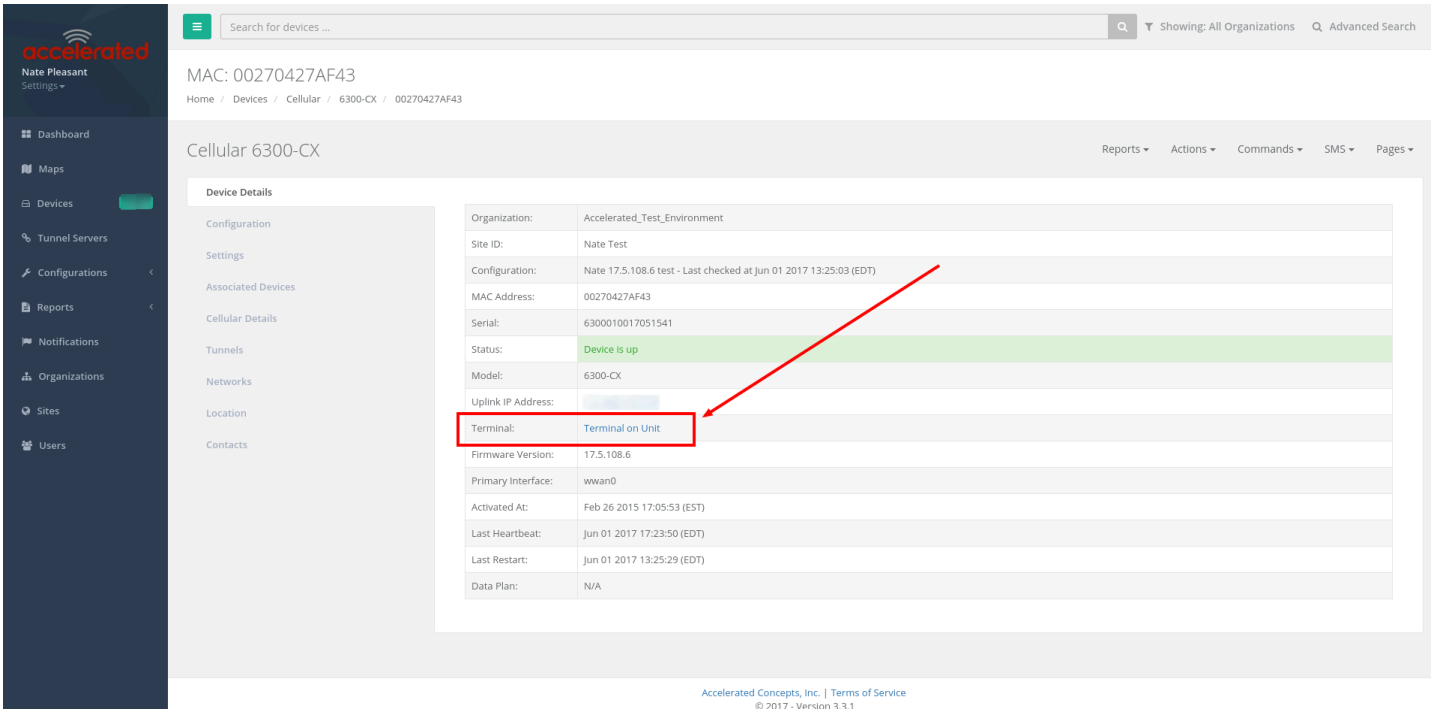
Terminal on Unit

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



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

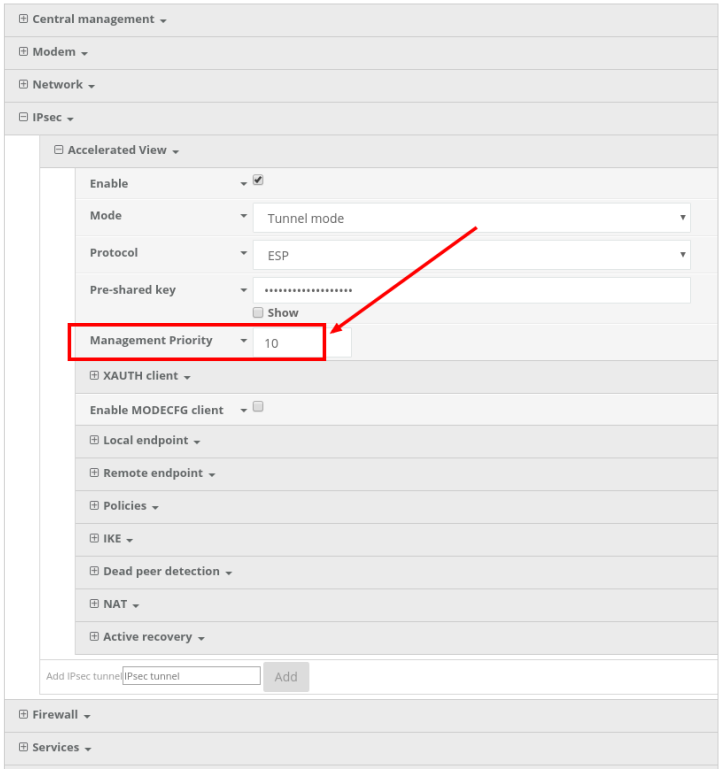
Accelerated View utilizes the IPSec tunnel the 63xx-series router establishes to remote.accns.com to provide terminal access to the console of the router.

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

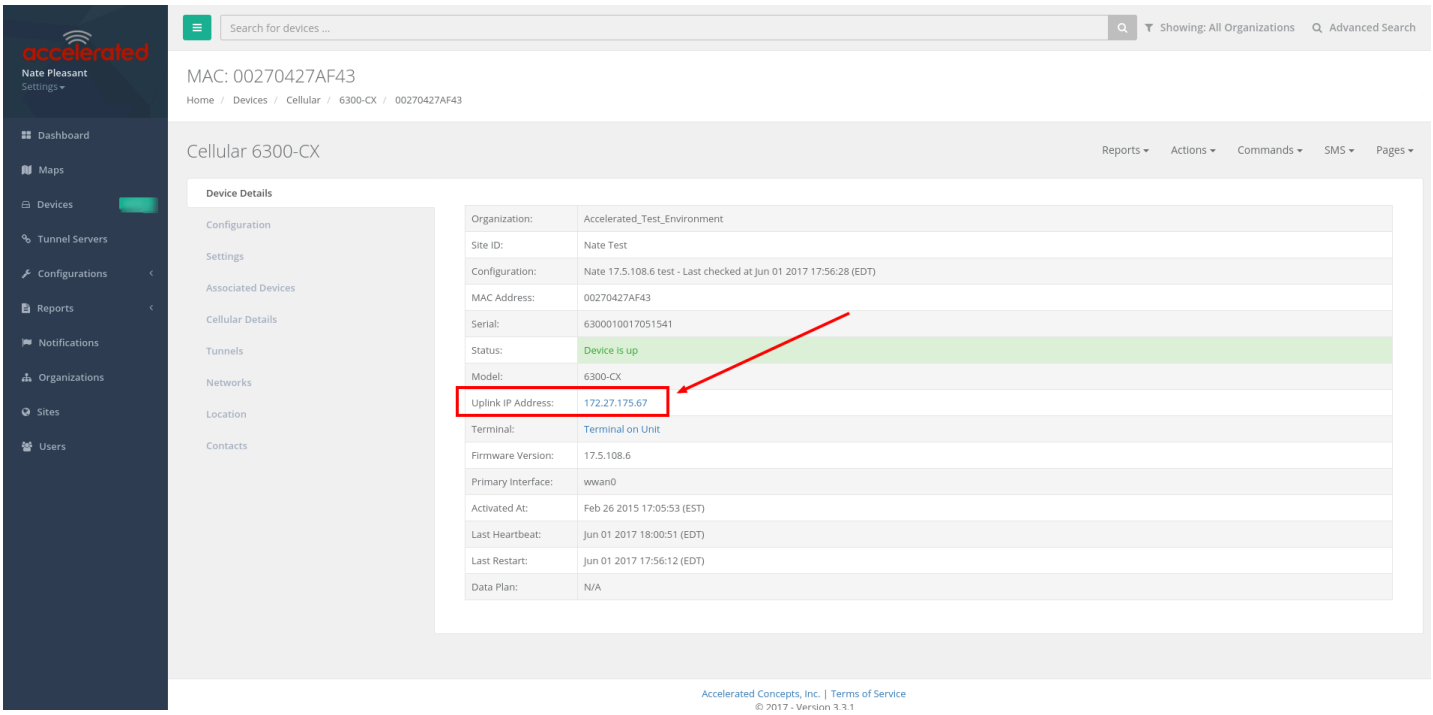
Data Usage Estimates

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.

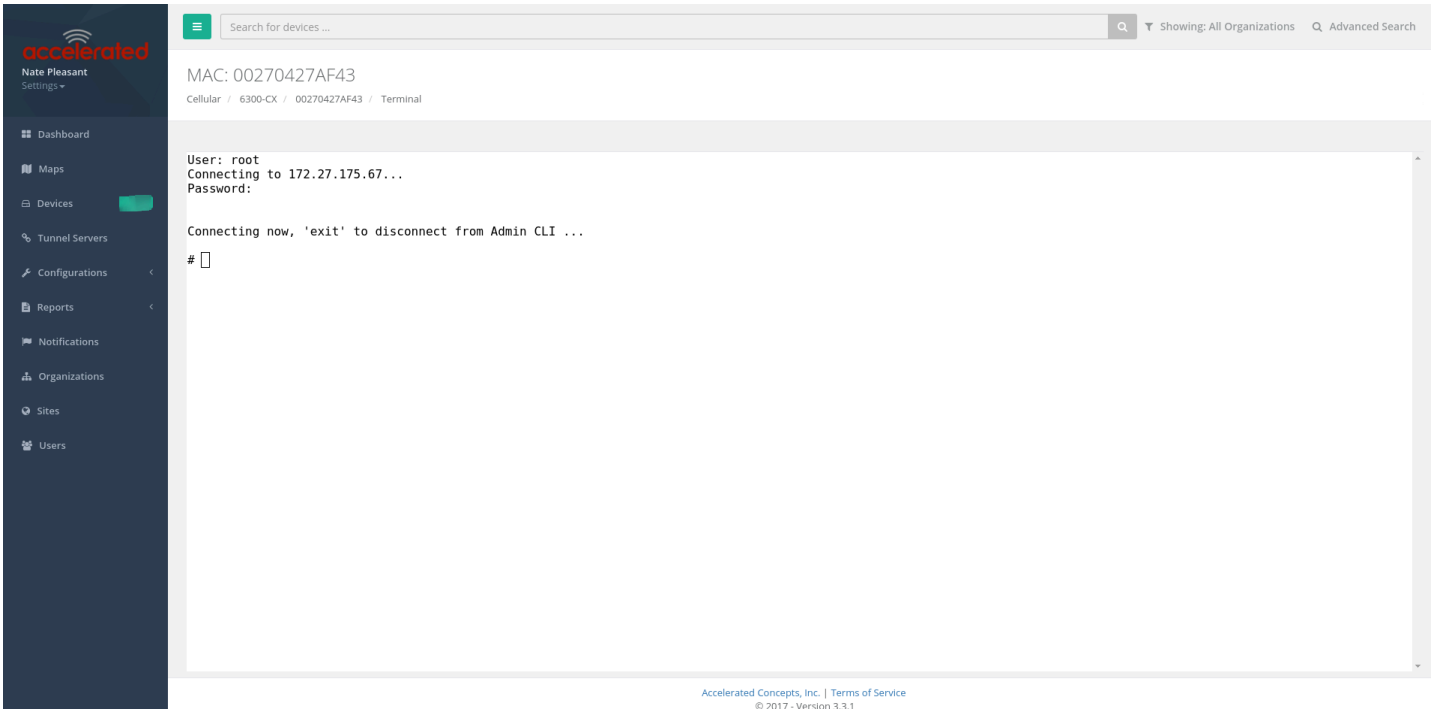


Once you apply the new configuration to the 63xx-series router, reboot the 63xx-series device so it rebuilds the IPSec tunnel and reports the new IPSec local IP address to Accelerated View. You can verify that Accelerated View is using the IPSec local IP as the management IP by looking at the ***Uplink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



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.



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

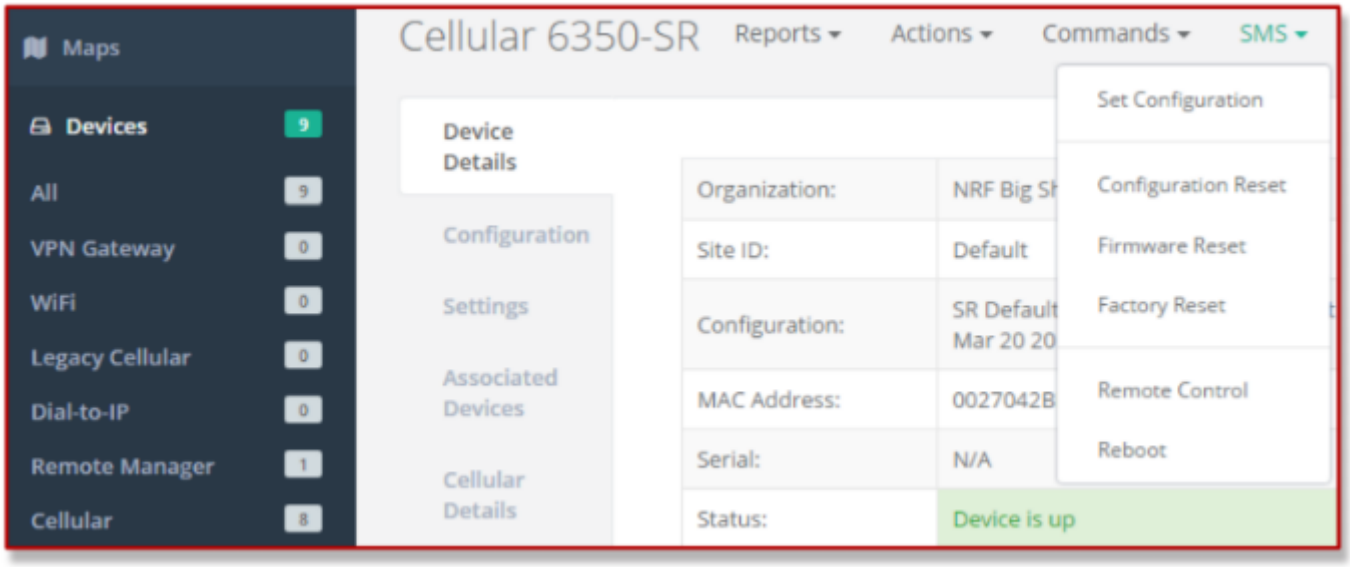
> While the settings are reset, the device's firmware version remains the same.

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 (excluding any automatically generated keys/certificates) 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**.



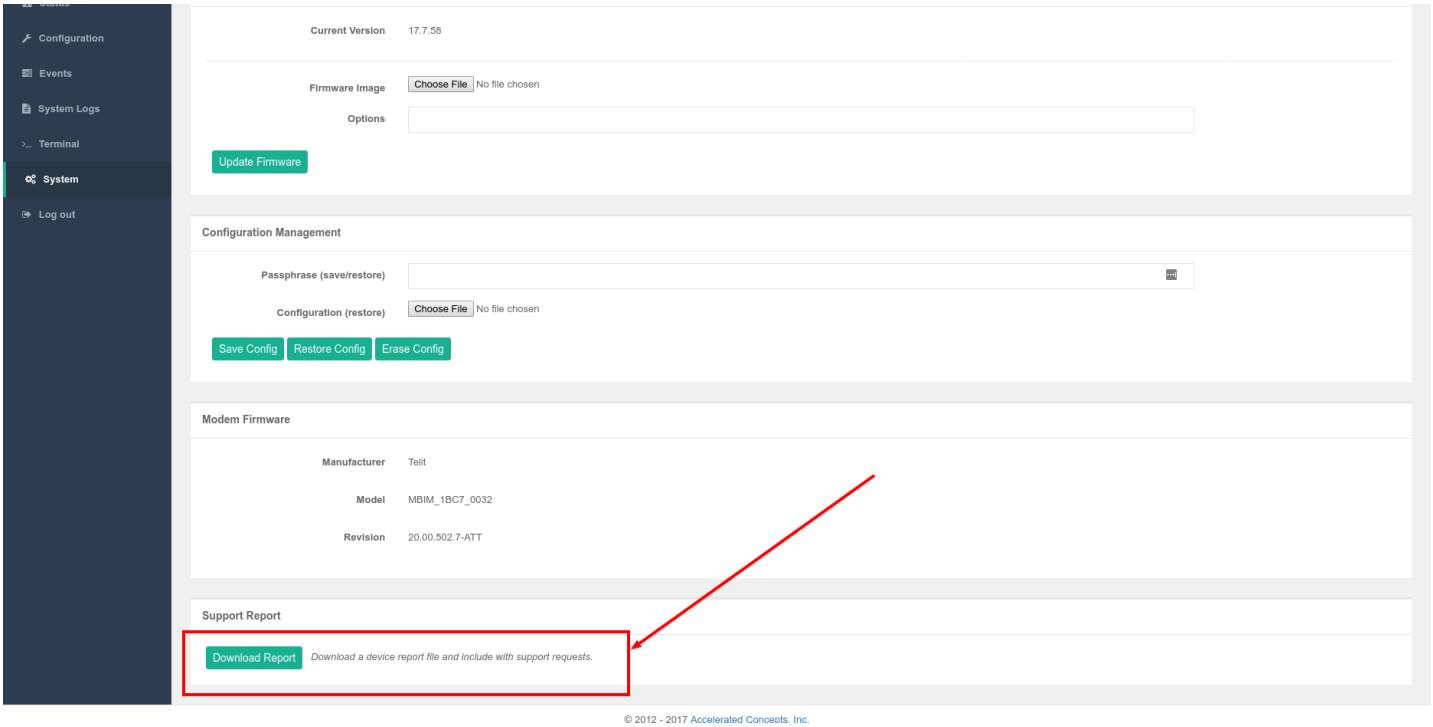
Support Report

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 192.168.210.2/24 with a gateway of 192.168.210.1. Once the PC/laptop has an IP address, open the following URL in a browser on the PC:

https://192.168.210.1

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

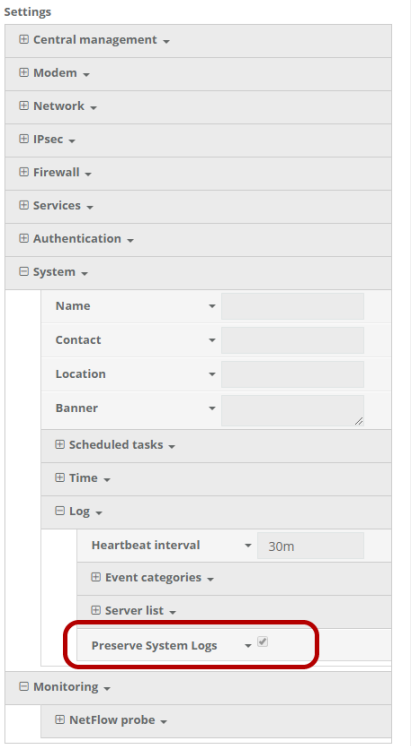


Persistent System Logs

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.

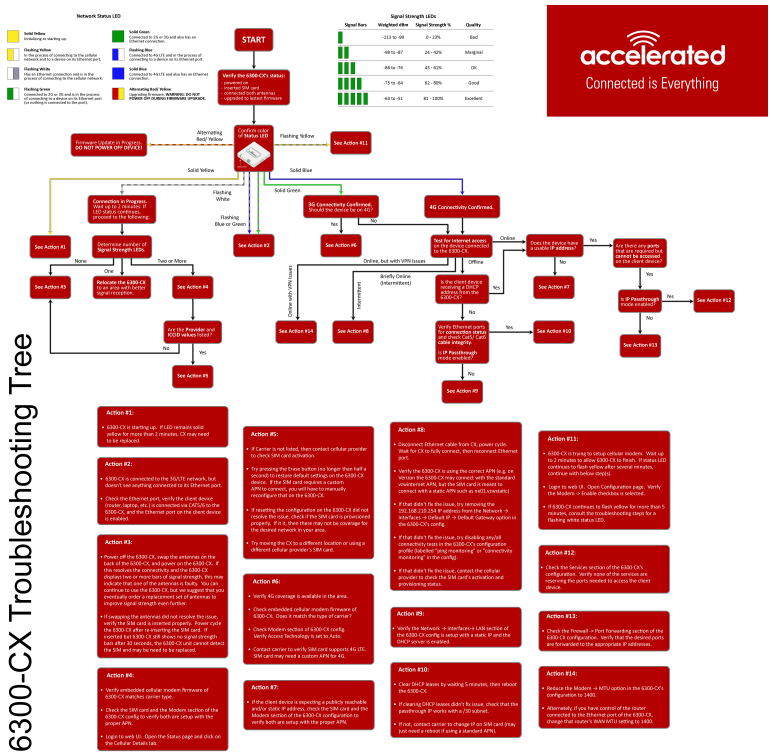
Logging can be configured to persist between power cycles by enabling the **Preserve System Logs** checkbox nested under the **System** → **Log** menu option.

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



LTE Troubleshooting Tree

6300-CX_Troubleshooting_Flowchart.pdf



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).

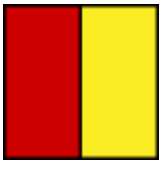
Solid Blue
Connected to 4G LTE and also has a LAN connection.

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

Signal Strength LEDs

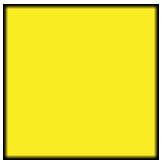
Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

Alternating Red/ Yellow



Firmware Update in Progress: DO NOT POWER OFF DEVICE!

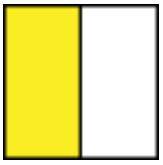
Solid Yellow



6300-CX is starting up.

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

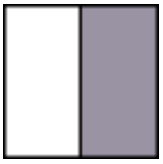
Flashing Yellow



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.

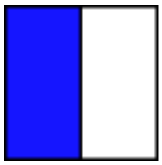
Yes

- 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.

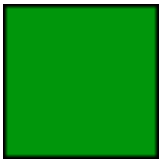
- If swapping the antennas did not resolve the issue, verify the SIM card is inserted properly. Power cycle the 6300-CX after re-insterting the SIM card. Wait 30 to 60 seconds. If the problem persists, the 6300-CX unit cannot detect the SIM and the router may need to be replaced.

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.

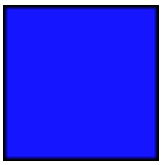
Online, but with VPN issues

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.

Accessing Admin CLI

Skill level: ***Beginner***

Goal

To show how to access Admin CLI using ***Terminal on Unit or SSH.***

Setup

For ***Terminal on Unit***, you will need either:

a) Direct SSH access to the ACL device

b) Access to the management portal, and an cellular extender online and syncing with the management portal. If you see the cellular extender listed as up (green status) in the management portal, you are good to go.

For more information on how to access ***Terminal on Unit or SSH***, please see the below link.

Remote_Access

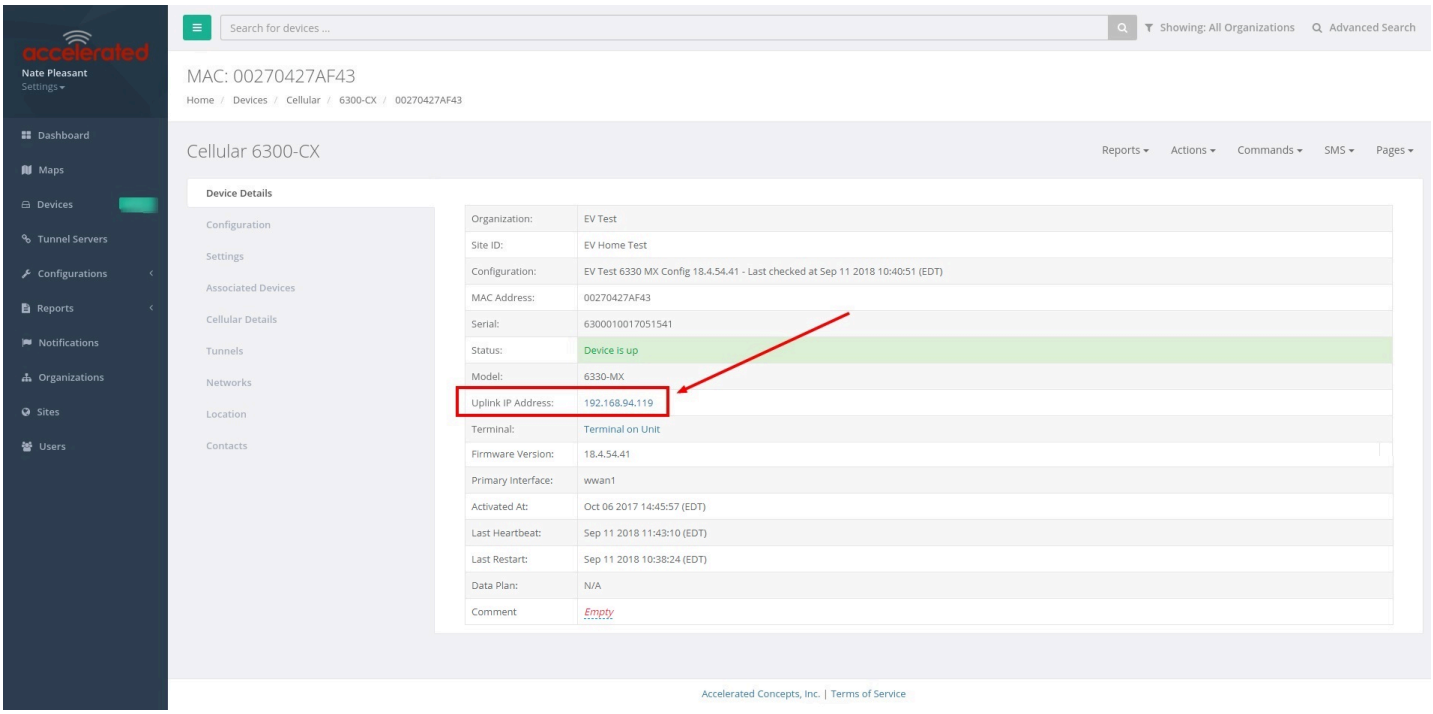
Details

The management portal utilizes the IPSec tunnel the cellular extender establishes to ipsec.accns.com (or remote.accns.com) to provide terminal access to the console of the device.

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

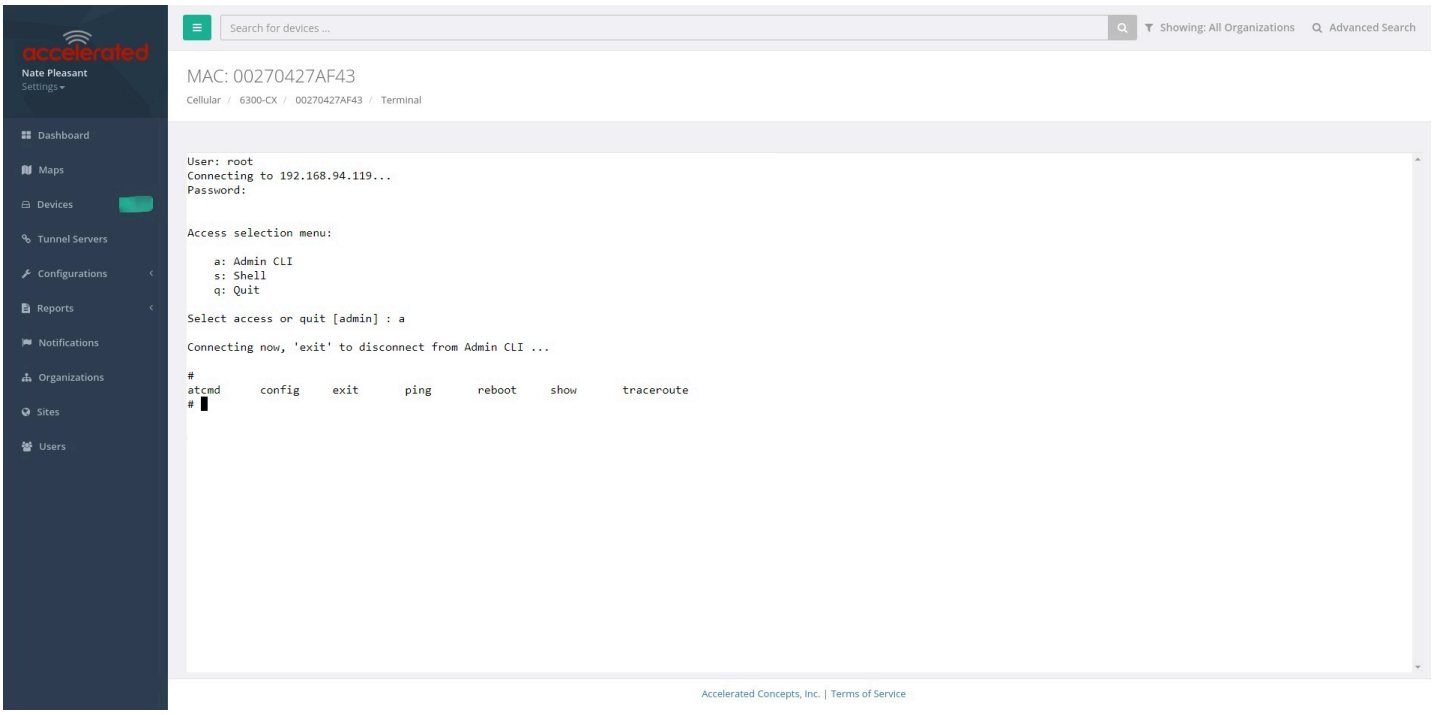
Data Usage Estimates

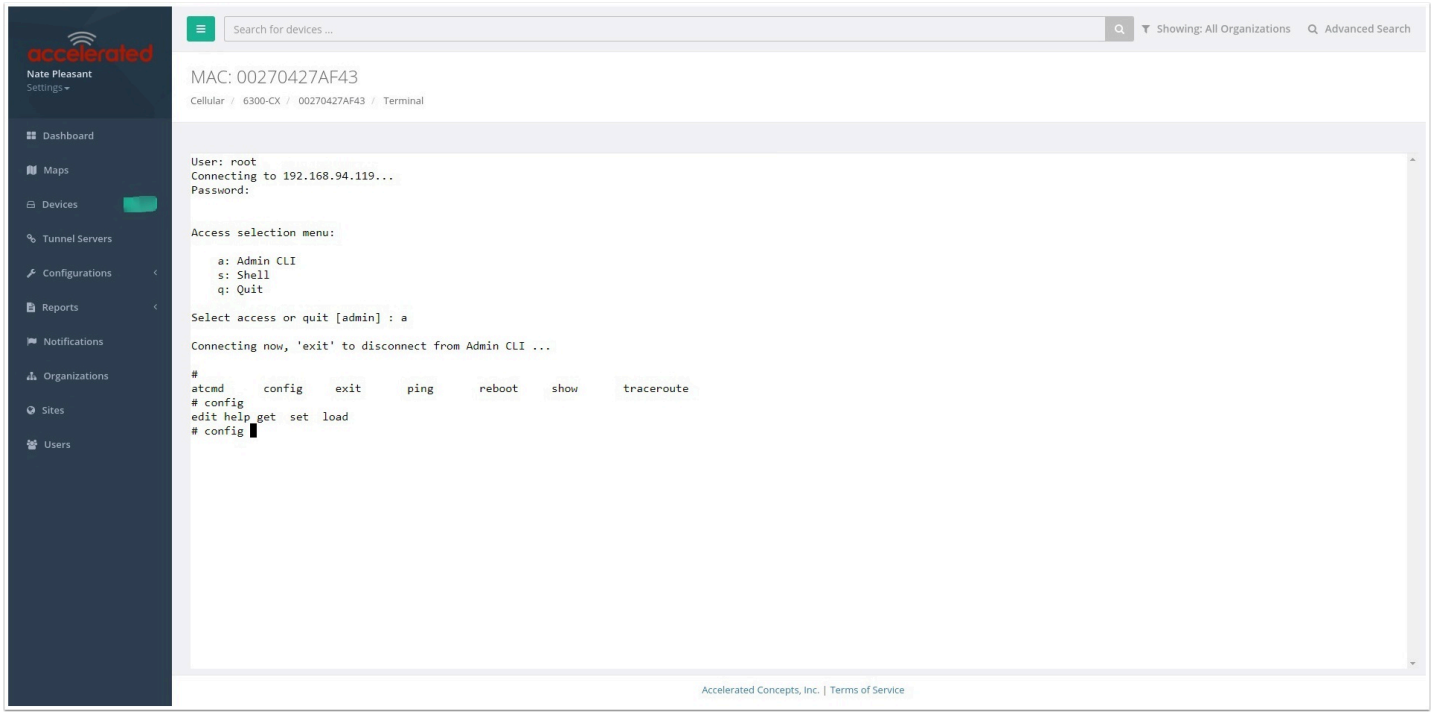
If a new configuration is applied to an Accelerated cellular extender, reboot the Accelerated cellular device so it rebuilds the IPSec tunnel and reports the new IPSec local IP address to the management portal. You can verify that the management portal is using the IPSec local IP as the management IP by looking at the ***Uplink IP address*** on the ***Device Details*** tab. This value should be set to a 192.x.x.x IP address (when using ipsec.accns.com or 172.x.x.x for remote.accns.com).



Using the Terminal on Unit link

1. Once the correct management IP is reported from the cellular extender to the management portal, clicking ***Terminal on Unit*** will open a page on the management portal to provide the user access to the console of the 63xx-series device.
2. Type in the ***User*** and ***Password*** for the device and hit enter.
3. At the prompt, type ***a*** for ***Admin CLI*** and hit enter. (If typing in the user and password brings you directly to the ***# prompt***, you are already in the ***Admin CLI.***)
4. At the ***# prompt,*** hit tab and the possible commands will be presented. The same is true for typing one of the commands followed by a space then hitting tab. This will show the available options within that command. (See command break down below)





Direct SSH access

SSH access can be gained through a local connection to the ACL device. You can access the cellular extender on its LAN IP address (default 192.168.2.1) or its default 192.168.210.1 IP address. Below is an example SSH login process.

1. SSH to the ACL device at its LAN IP address (default 192.168.2.1) or its default 192.168.210.1 IP address.

2. Type in the ***User*** and ***Password*** for the device and hit enter.
3. At the prompt, type ***a*** for ***Admin CLI*** and hit enter. (If typing in the user and password brings you directly to the ***# prompt***, you are already in the ***Admin CLI.***)
4. At the ***# prompt,*** hit tab and the possible commands will be presented. The same is true for typing one of the commands followed by a space then hitting tab. This will show the available options within that command. (See command break down below)

```
$ ssh root@192.168.2.1
$ 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 ...

#
```

Command Breakdown

1. ***atcmd*** - run AT commands to cellular modem in the device
2. ***config*** - make config changes on the device, one at a time
3. ***exit*** - exit from the ***Admin CLI*** console
4. ***ping*** - ping an IP address or domain (Ctrl+c to stop)
5. ***reboot*** - reboot the device
6. ***show*** - display network or device version details
7. ***traceroute*** - perform traceroute to an IP address or domain

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.

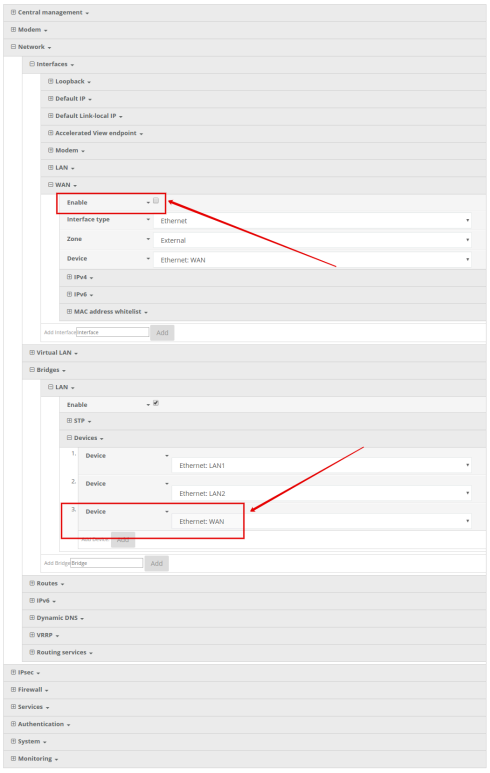
Setup

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.



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

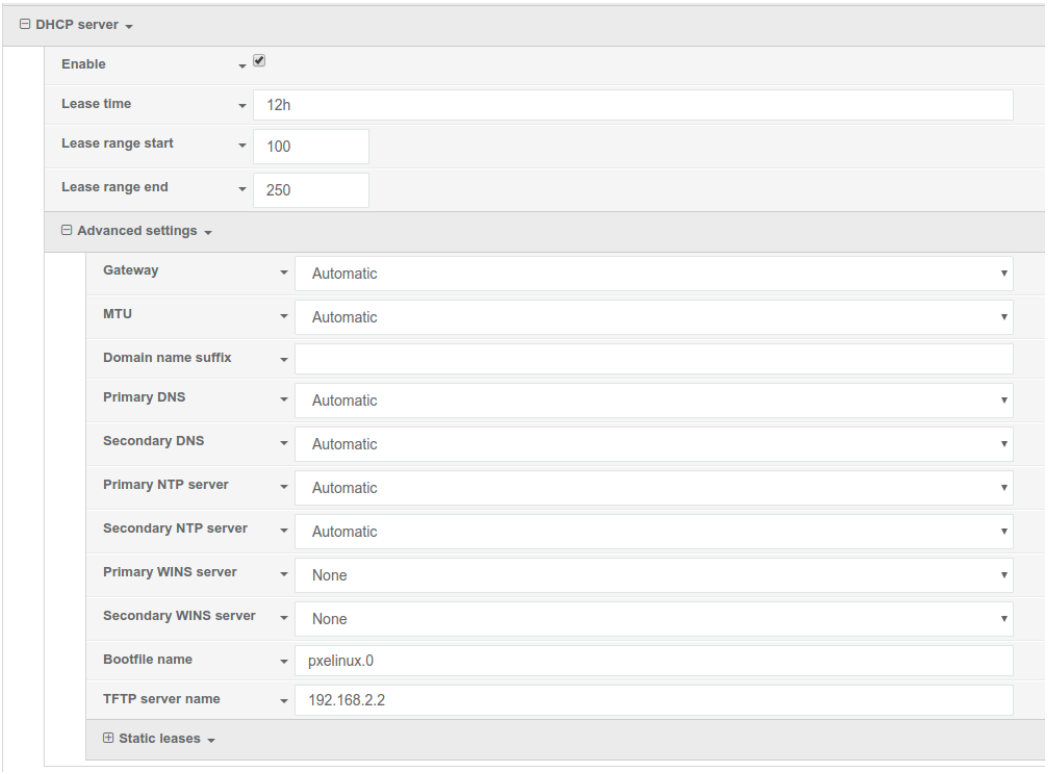
This article assumes the 633x-MX router is operating under default settings, all relevant PXE boot files and TFTP server processes are in place ready to be connected, and the client device is in a state ready for PXE boot.

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.

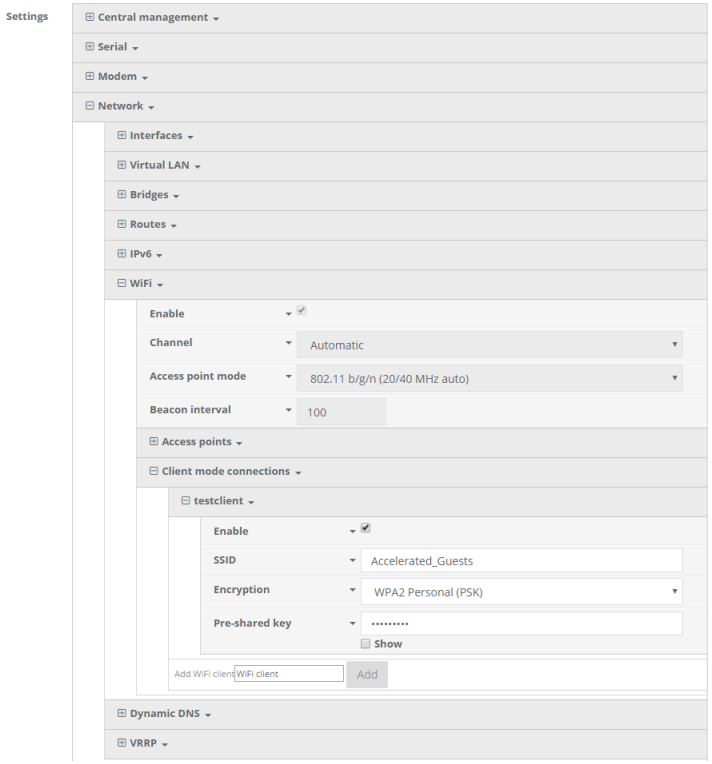
You will need to establish the following details before configuring the 63xx-series router.

- 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



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

1. Under ***Network -> WiFi -> 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 -> WiFi -> 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 -> WiFi -> 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***.

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

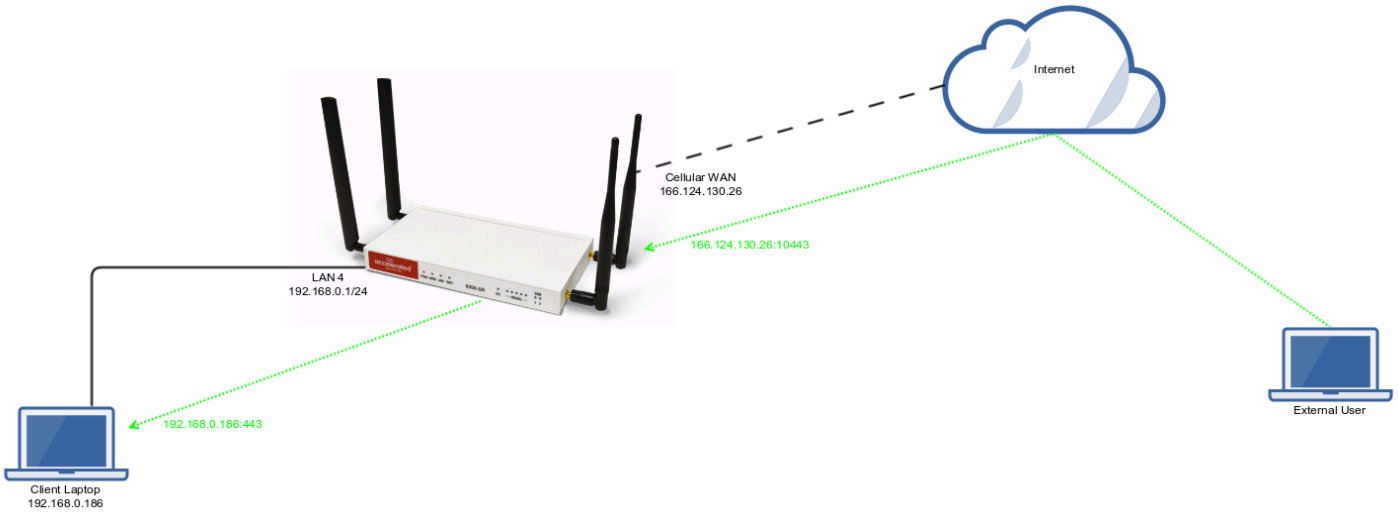
This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 63xx-series router's LAN ports. For more details on the default settings of the 63xx-series router, see the ***Default Settings*** section of the User's Manual.

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

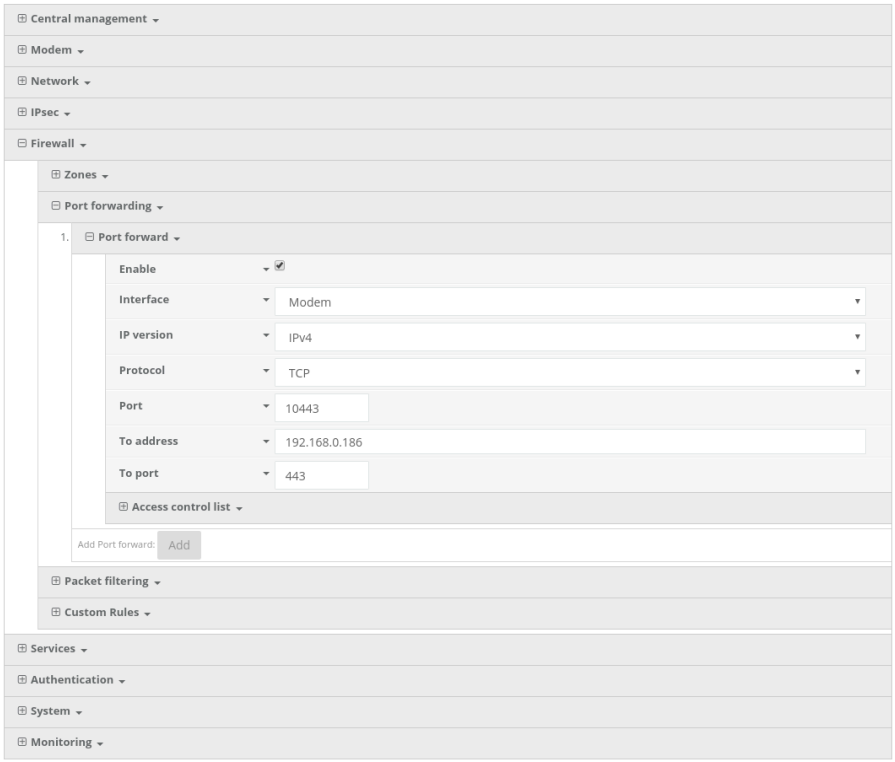
The following diagram shows a sample setup of a 63xx-series router with a cellular WAN connection and a client's laptop connected to LAN port 4. In this setup, we want to access TCP port 443 of the client laptop from the external IP address of the 63xx-series router's cellular WAN connection. We will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



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*** or ***Modem -> APN list*** options.

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 for firmwares 18.4.54.41 and newer

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

- **Connection attempts before SIM failover:** 5

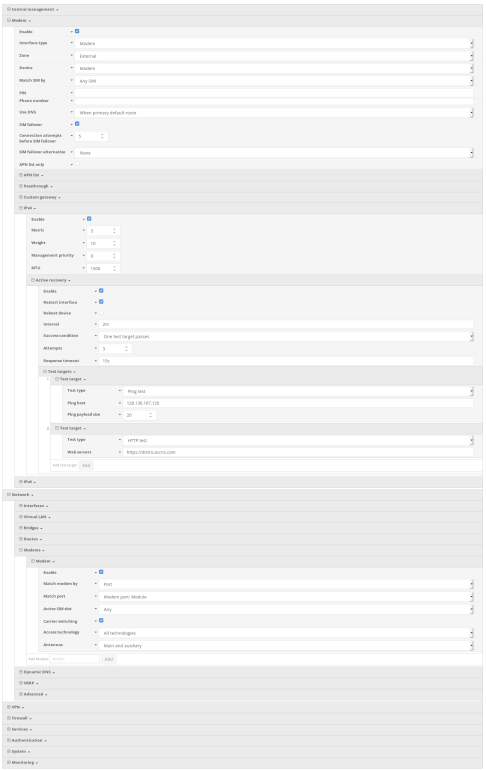
Next, open the ***Modem -> IPv4 -> Active recovery*** section and make the following changes.

- **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***
  Note: 2 different tests are recommended to prevent false positives

Next, open the ***Network -> Modems -> Modem*** section and set the following options.

- **Active SIM slot:** Any

> ***NOTE:*** *Best practices dictate that redundant tests (with divergent failure conditions) will be the best way to ensure proper connectivity monitoring/active recovery. With only a single test type, false positives could be reported.*



Sample Configuration firmware 18.1.29.41 and older

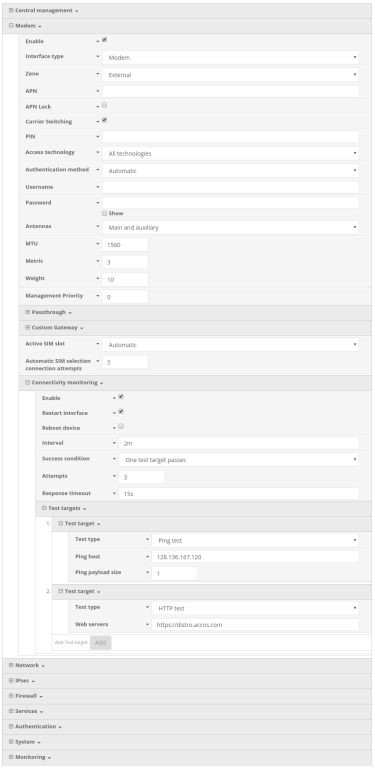
Open the configuration profile for the 63xx-series router and make the following changes.
Under ***Modem***, set the following options.

- **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***
  Note: 2 different tests are recommended to prevent false positives

NOTE: *Best practices dictate that redundant tests (with divergent failure conditions) will be the best way to ensure proper connectivity monitoring/active recovery. With only a single test type, false positives could be reported.*



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

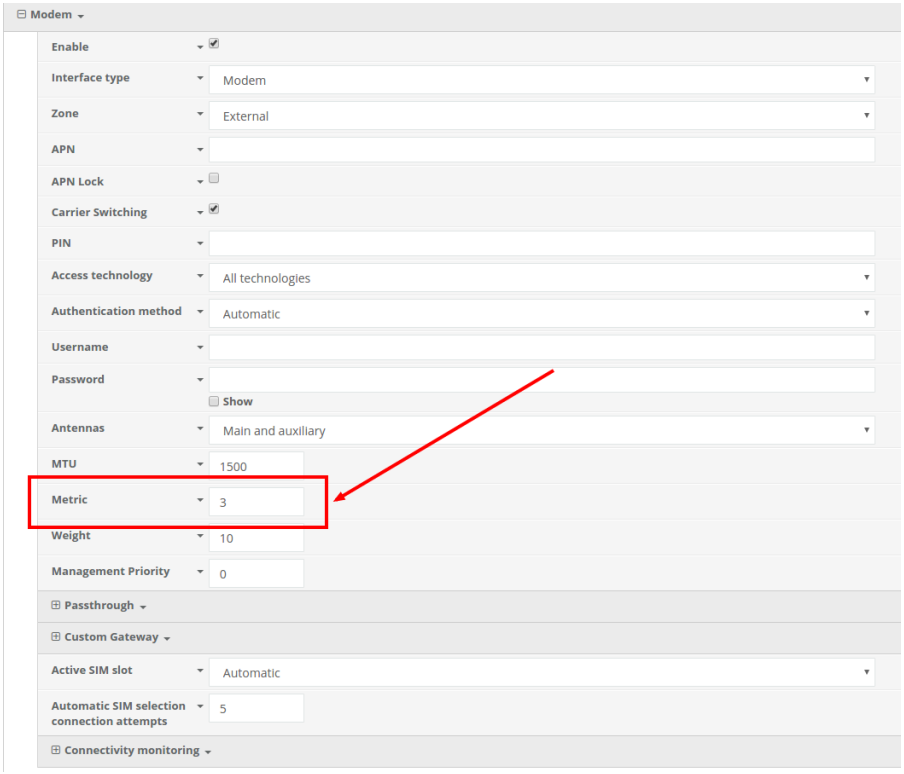
The sample configuration below shows a 63xx-series router with two internet connections. The WAN Ethernet interface will be used as the primary Internet connection. The 63xx-series router is setup to test the WAN Ethernet connection twice every minute. If three sequential tests fail, then the 63xx-series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

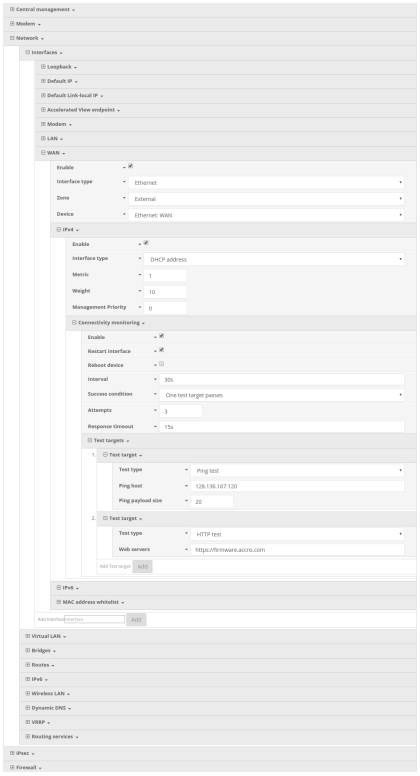
In the ***Modem -> Metric entry***, ensure the value is set to a number higher than the the value in ***Network -> Interfaces -> WAN -> IPv4 -> Metric***. The interface with the lower metric takes higher precedence. By default, the cellular modem metric should be 3 and the WAN Ethernet's metric should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



Next, open the ***Network -> Interfaces -> WAN -> IPv4 -> Active Recovery*** 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***
  Note: 2 different tests are recommended to prevent false positives

NOTE: *Best practices dictate that redundant tests (with divergent failure conditions) will be the best way to ensure proper connectivity monitoring/active recovery. With only a single test type, false positives could be reported.*


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***.

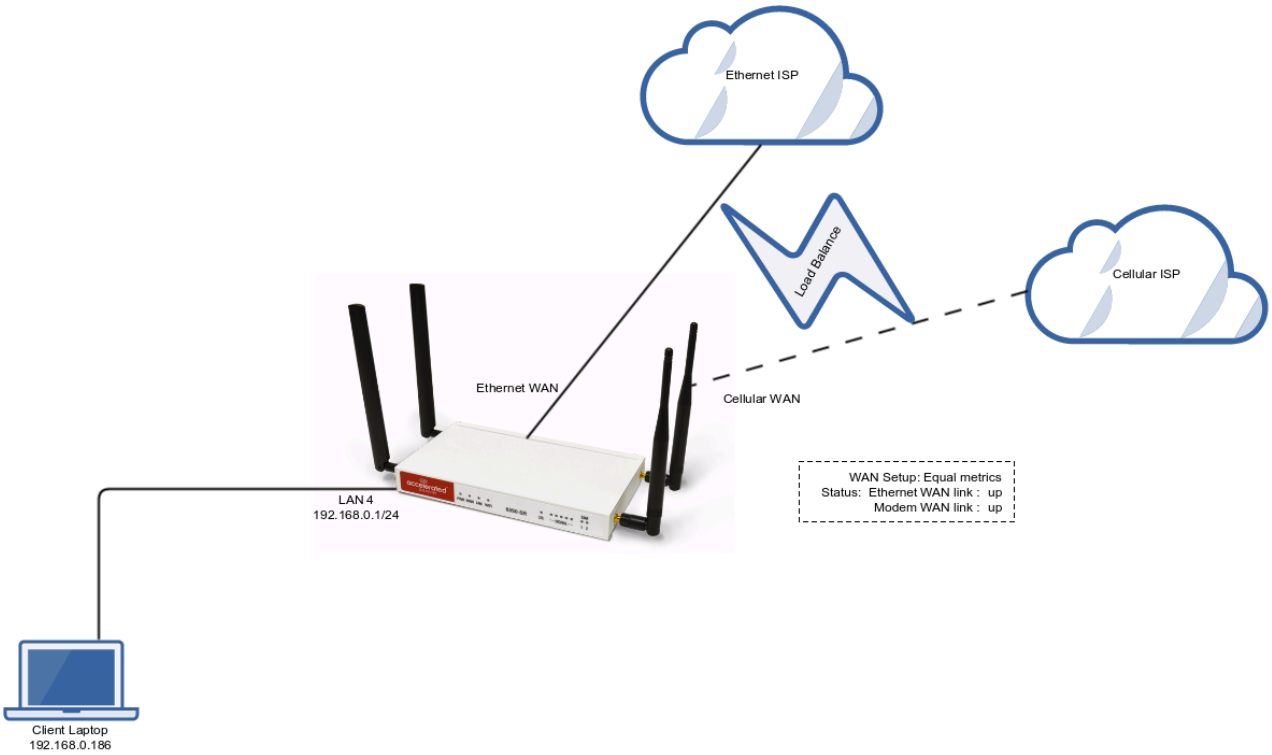
Setup

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.

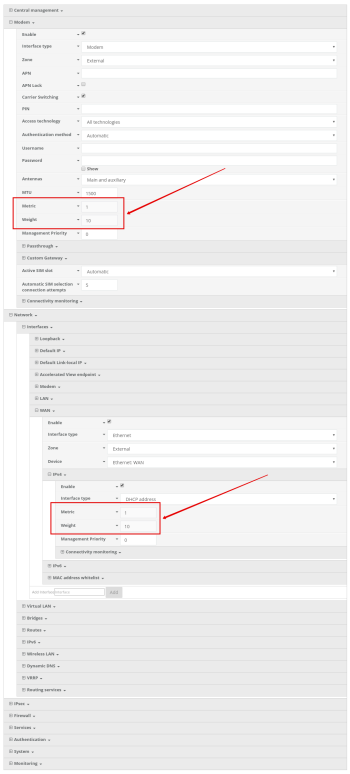


Sample Configuration

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***).



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

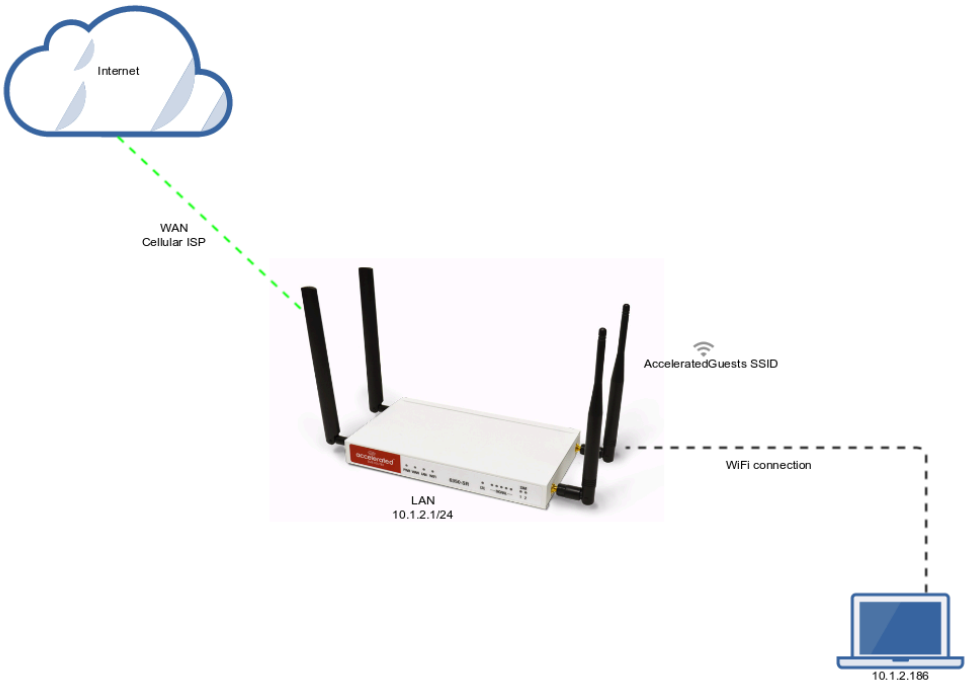
You will need to establish the following details before configuring the 63xx-series router.

- 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.



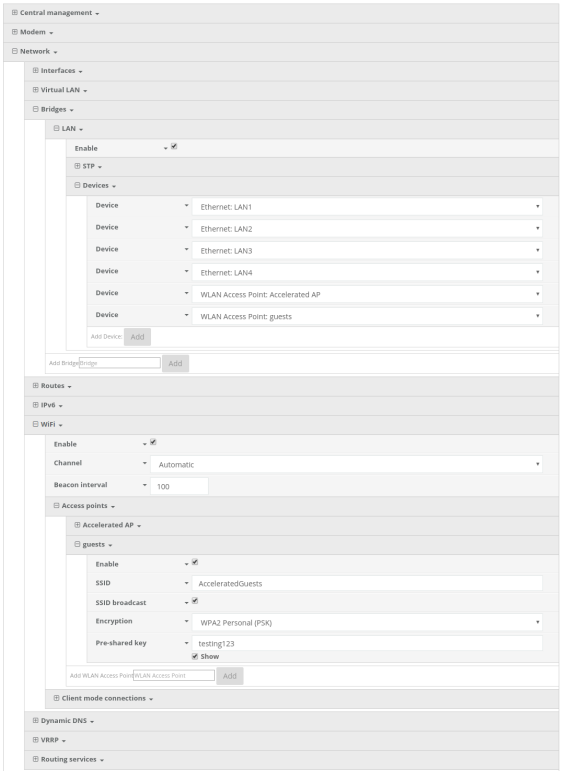
Sample Configuration

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

1. Under ***Network -> WiFi -> 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.

Under ***Network -> Bridges -> LAN -> Devices***, click ***Add*** and select ***WLAN Access Point: guests*** from the drop-down.

Click ***Save***.



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

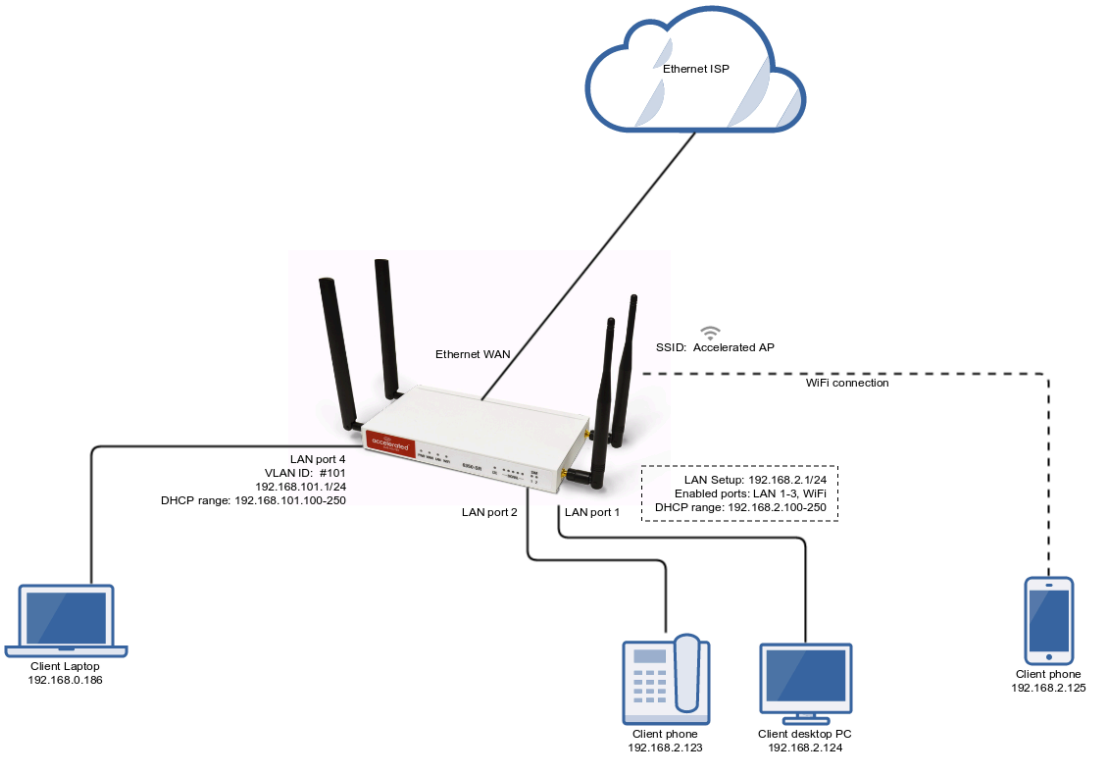
This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 6350-SR's LAN ports. For more details on the default settings of the 6350-SR, see the ***Default Settings*** section of the 6350-SR User's Manual.

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.

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.

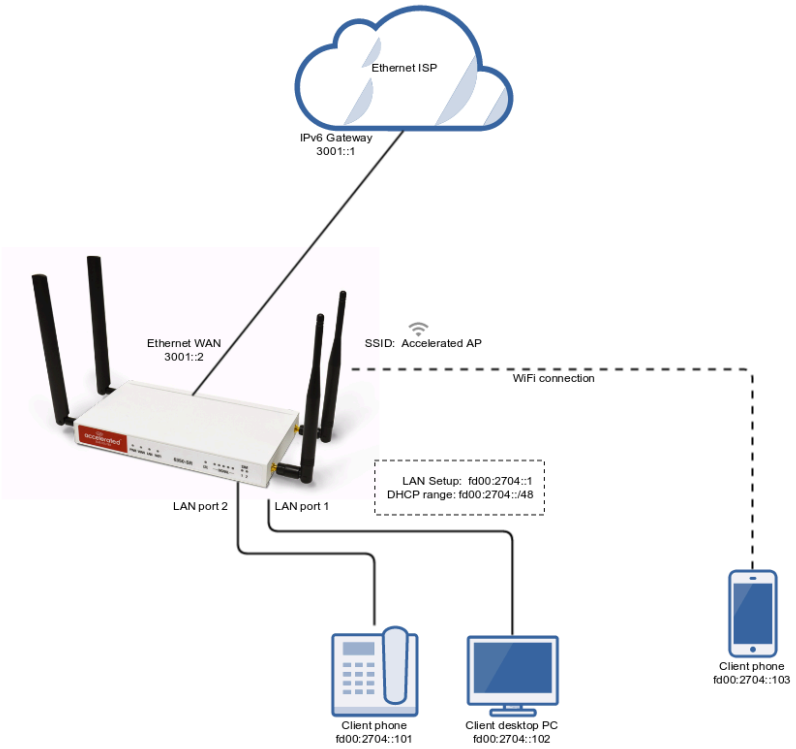
Setup

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.***

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.

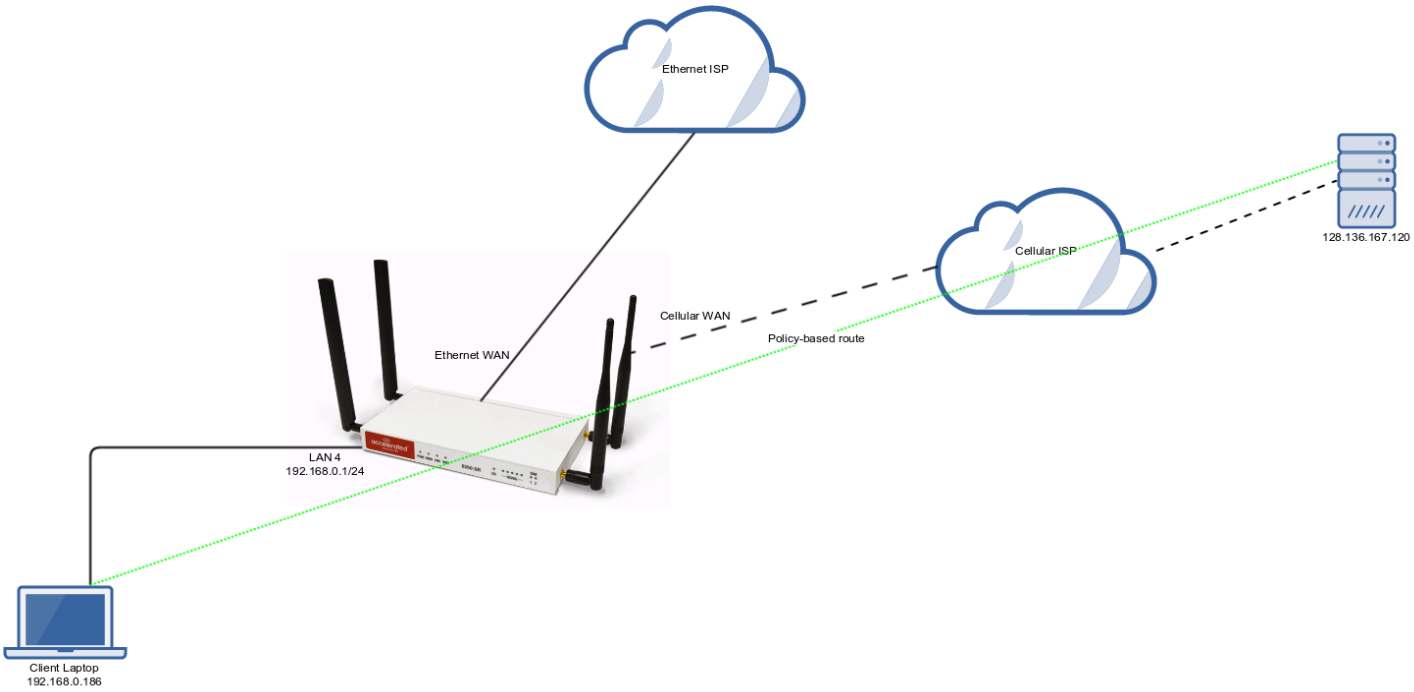
Setup

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

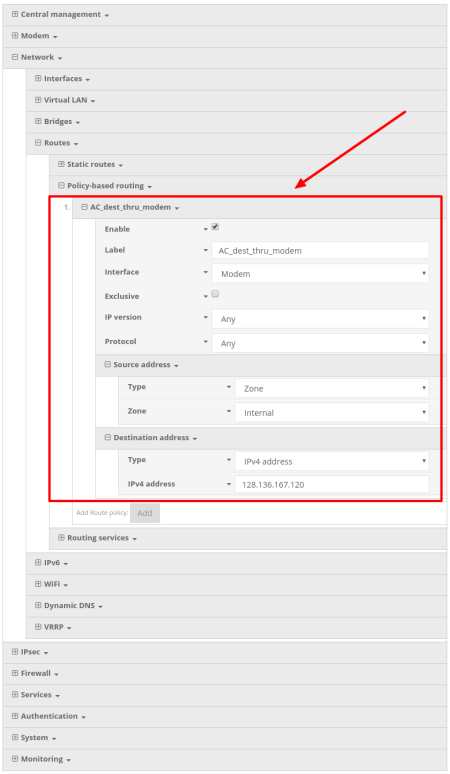
The sample configuration below shows a 63xx-series router with two Internet connections: a cellular-based WAN connection through the 63xx-series router's modem, and a broadband-based WAN connection through the 63xx-series router's WAN Ethernet port. The 63xx-series router's cellular WAN connection will 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


Central management
Modem
Network
Interfaces
Virtual LAN
Bridges
Routes
Static routes
Policy-based routing
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
Routing services
IPv6
WiFi
Dynamic DNS
VRRP
IPsec
Firewall
Services
Authentication
System
Monitoring

Per-device Policy-based Routing with Dual WAN

Difficulty: ***Expert***

Minimum firmware version: ***18.1.29***

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.

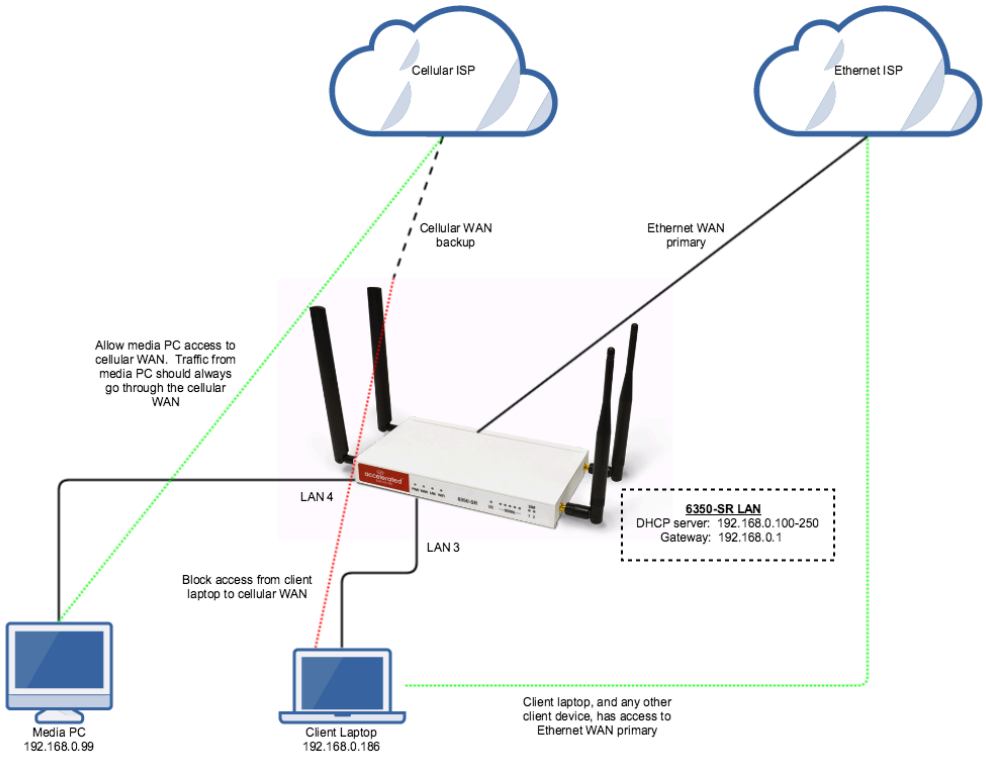
Sample

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.



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 ***Network -> Routes -> Policy-based routing***, setup a new policy with the following settings:
    1. ***Interface:*** Modem
    2. ***Source address -> Type:*** IPv4 address
    3. ***Source address -> IPv4 address:*** 192.168.0.99
    4. ***Destination address -> Type:*** Zone
    5. ***Destination address -> Zone:*** ethernetwan

VPN Access with IPSec tunnels

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

Goal

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

Setup

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

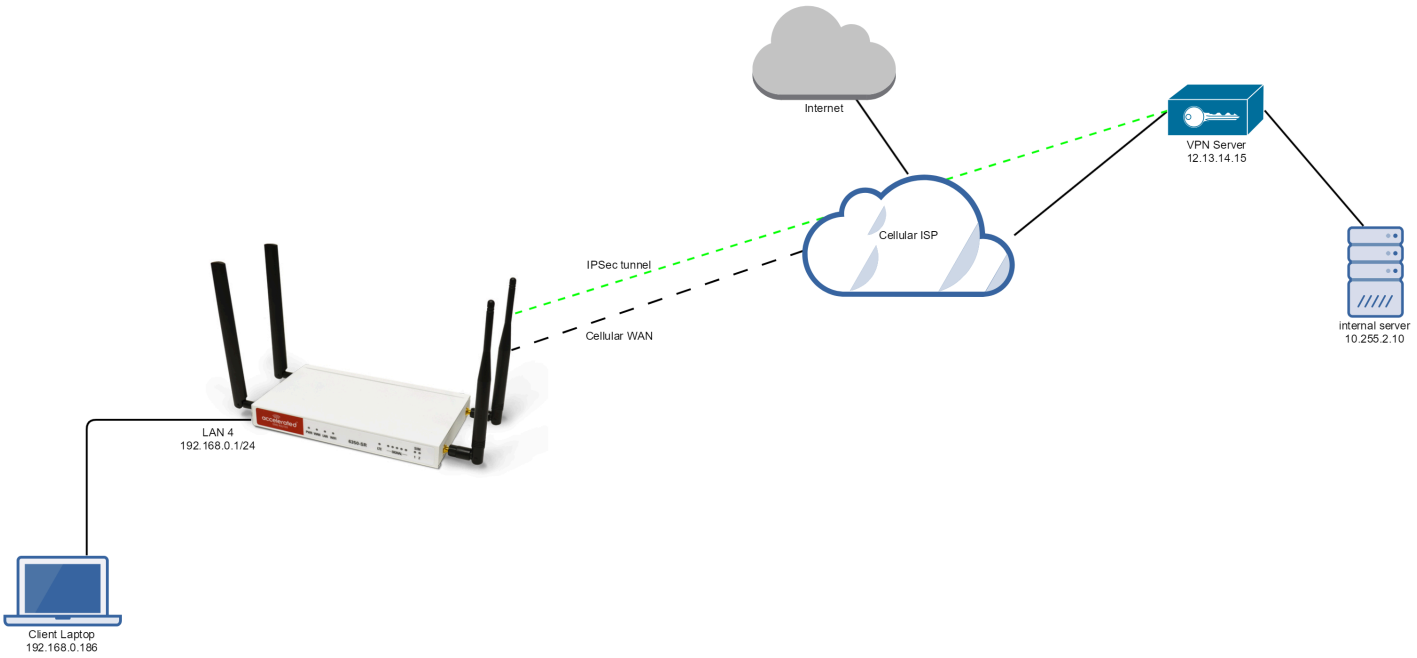
You will also need to know the IPSec credentials and settings needed to build a tunnel to the IPSec endpoint.

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

- SonicWall routers
- strongswan IPSec servers
- OpenVPN IPSec servers
- other 63xx series devices. See the site-to-site tunnel article for an example.

Sample

The sample configuration below shows a 6350-SR building a tunnel to a VPN server 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 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

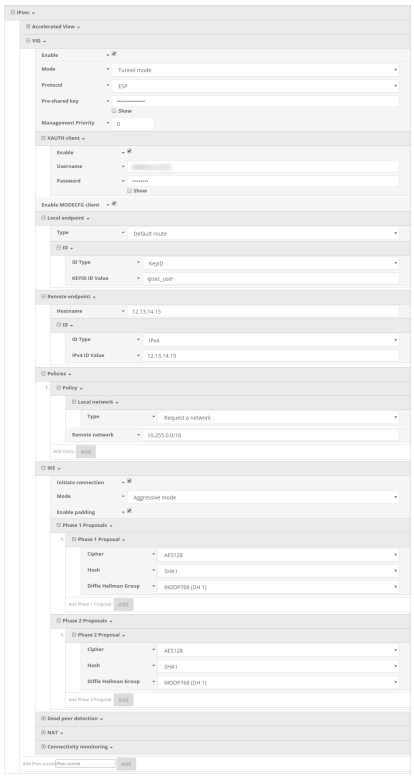
Open the configuration profile for the 6350-SR. Under ***IPSec***, create a new entry titled ***Tunnel***, and add your IPSec settings to the new entry. The following settings reflect the sample setup in the diagram above.

1. Enter in the PSK into the ***Pre-shared key***.
2. (*optional*) 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 device 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***



Dual WAN Ethernet Ports

Difficulty level: ***Beginner***

Goal

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

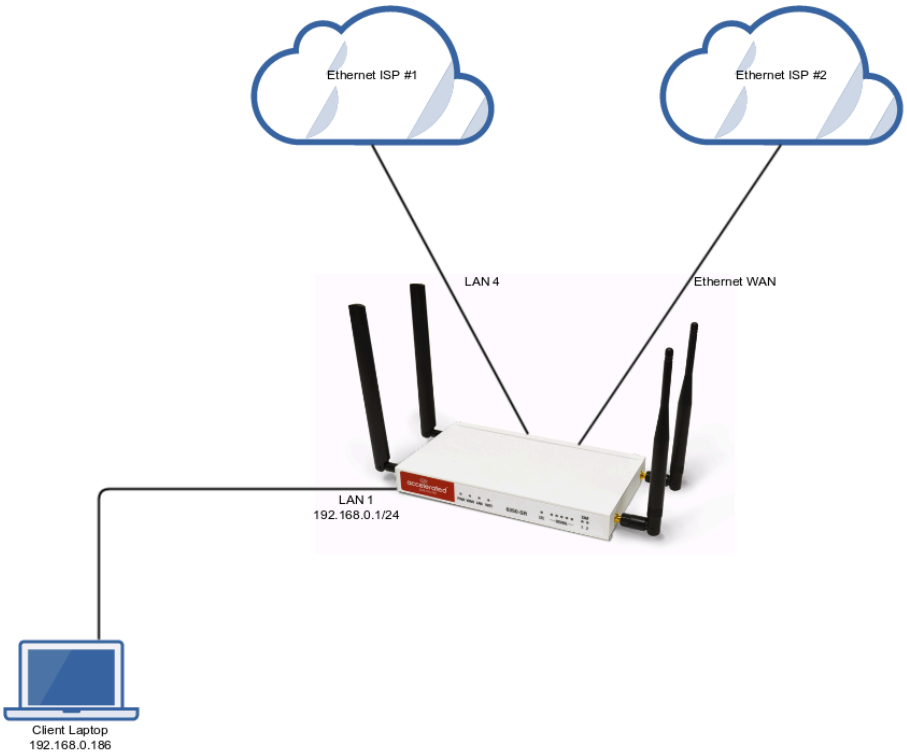
Setup

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.

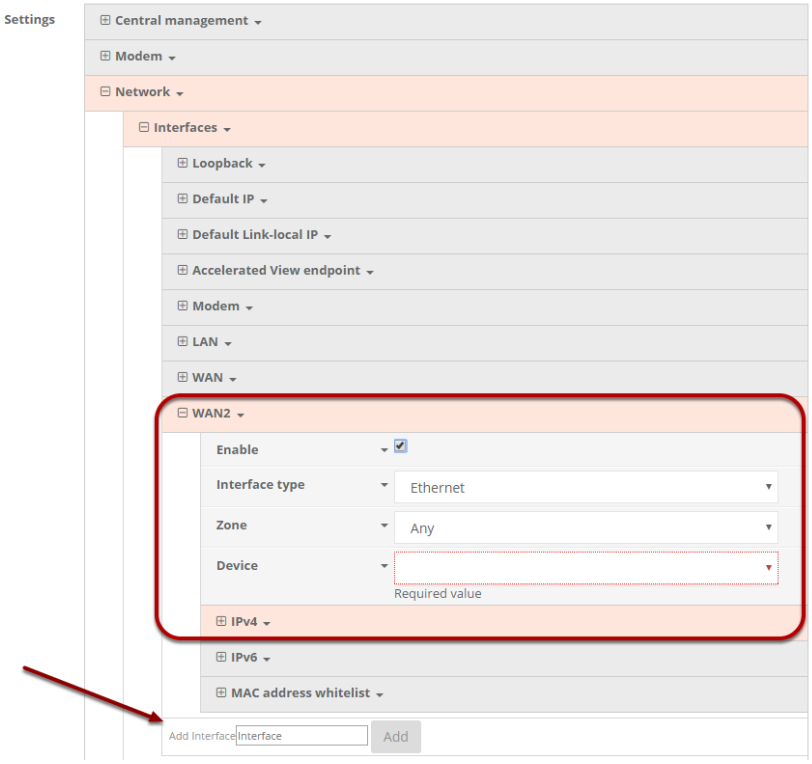


Sample Configuration

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
Add

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.

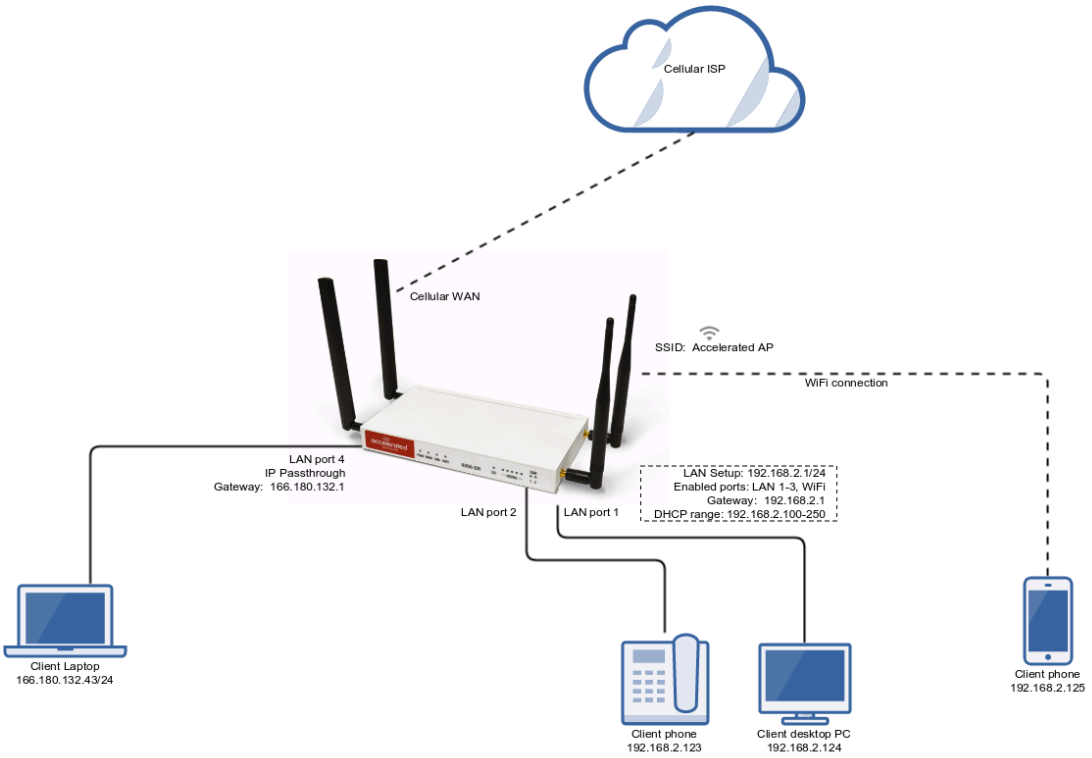
You will need to establish the following details before configuring the 63xx-series router.

- **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.



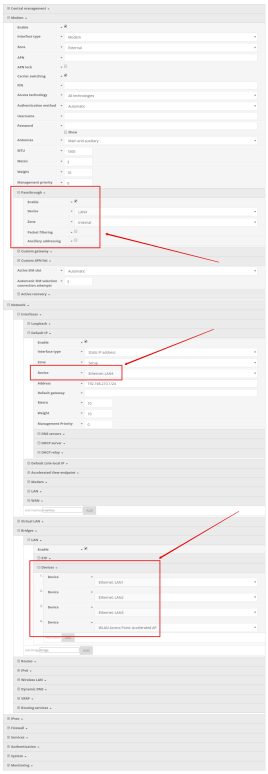
Sample Configuration

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

Under ***Modem -> Passthrough***, check the ***Enabled*** box and select the desired LAN interface under the ***Device*** drop-down. For this example, we are selecting ***LAN4***.

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

1. 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: LAN4*** from the LAN bridge.
2. Save and apply the new configuration settings to the device.



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

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

Goal

To build an IPSec tunnel through the 63xx device'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 devices. Both 63xx devices must be on firmware version 17.5.108.6 or higher. The 63xx series devices will need an active WAN Internet connection.

The main site's 63xx series device will need a publicly reachable IP address, so the remote 63xx series device 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 devices.

If configuring a 6300-CX or 6310-DX for Site-to-Site VPN Access, it must be in **router mode**.

Sample

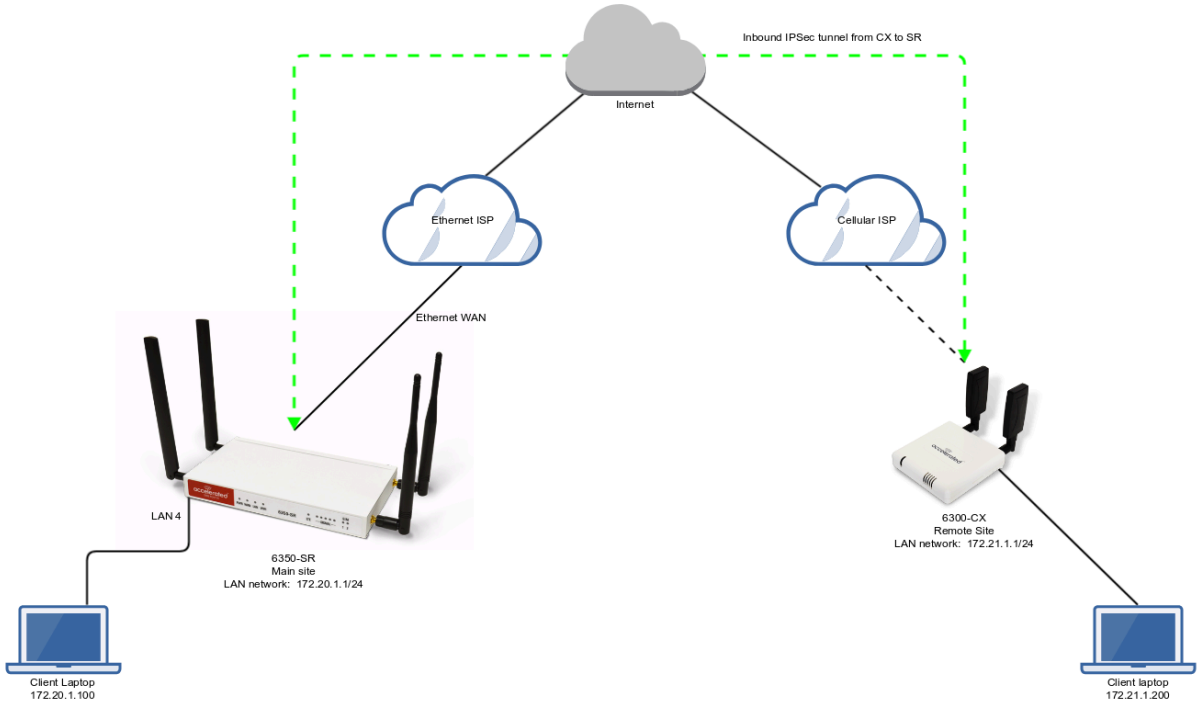
The sample configuration below shows a 6300-CX building a tunnel to a 6350-SR through its cellular modem. The client laptop connected to the LAN Ethernet port of the 6300-CX can then use that IPSec tunnel to access any IP address in the 172.20.1.1/24 range behind the 6350-SR. Any traffic not destined 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 devices can build IPSec tunnels to this 6350-SR. Each 63xx series device 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

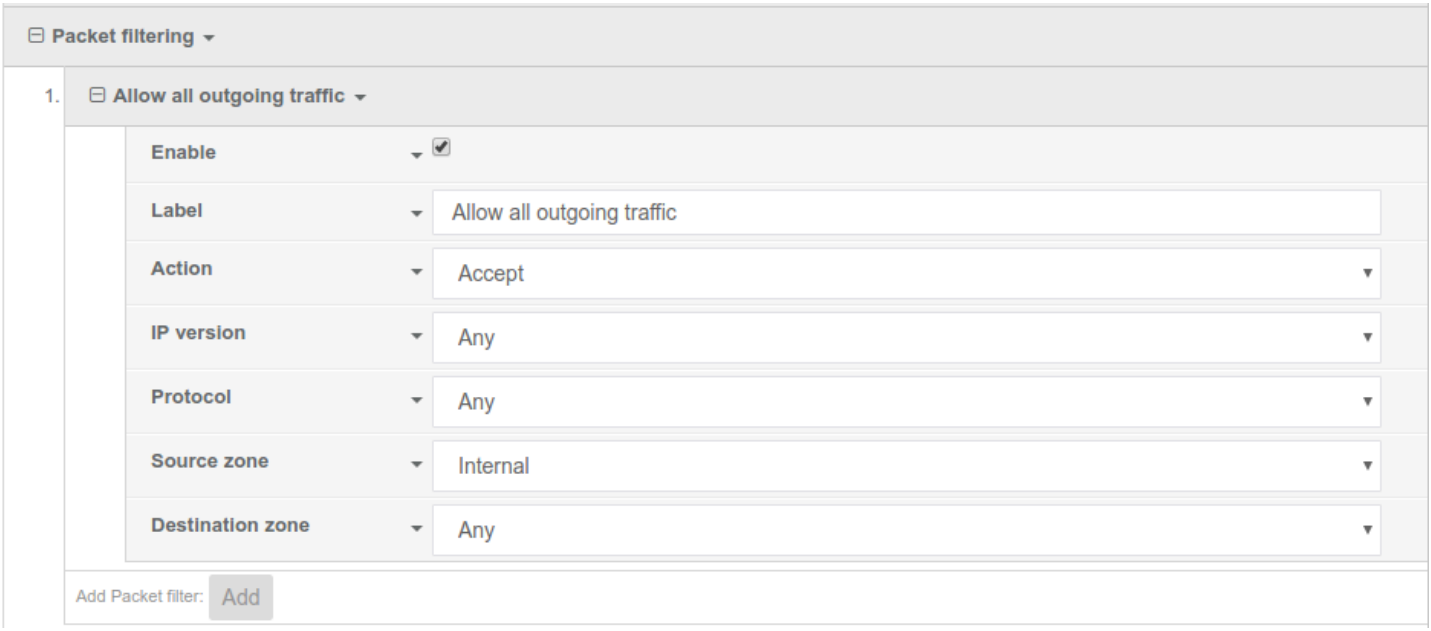
6350-SR's settings so it only allows inbound tunnels from that IP, input the 6300-CX's public IP address here.

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.)

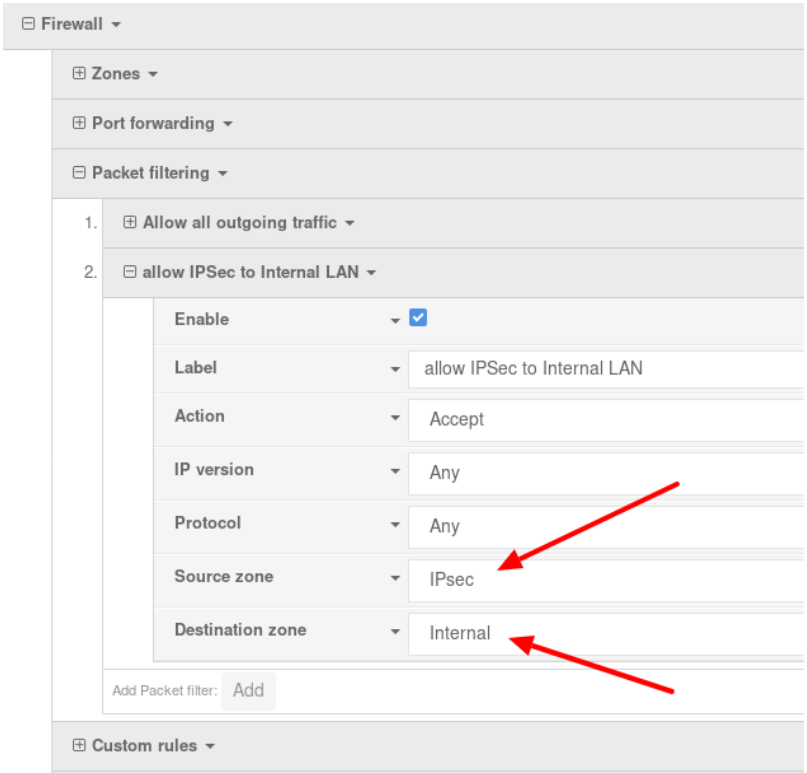
Under ***Policies***, click ***Add*** to create a new policy, and enter the following settings:

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)

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



If assigning the local network of this tunnel to a LAN port for client devices, you will also want to create a second firewall rule to allow incoming traffic on the IPSec tunnel through to the internal zone of the LAN, that way devices on the remote end of the IPSec tunnel can access client devices on the local LAN of the 6350-SR. See image below for reference.



6300-CX Sample Configuration

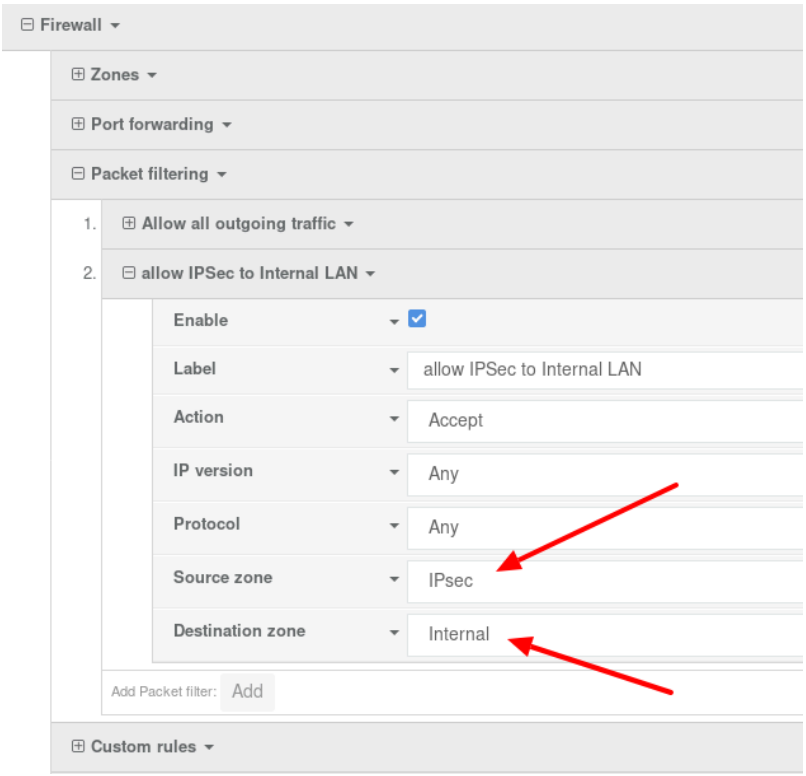
Open the configuration profile for the 6350-SR. Under ***IPSec***, create a new entry titled ***NPS*** (the name is arbitrary), and add your IPSec settings to the new entry. The following settings reflect the sample setup in the diagram above.

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 device 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

If assigning the local network of this tunnel to a LAN port for client devices, you will also want to create a second firewall rule to allow incoming traffic on the IPSec tunnel through to the internal zone of the LAN, that way devices on the remote end of the IPSec tunnel can access client devices on the local LAN of the 6300-CX. See image below for reference.



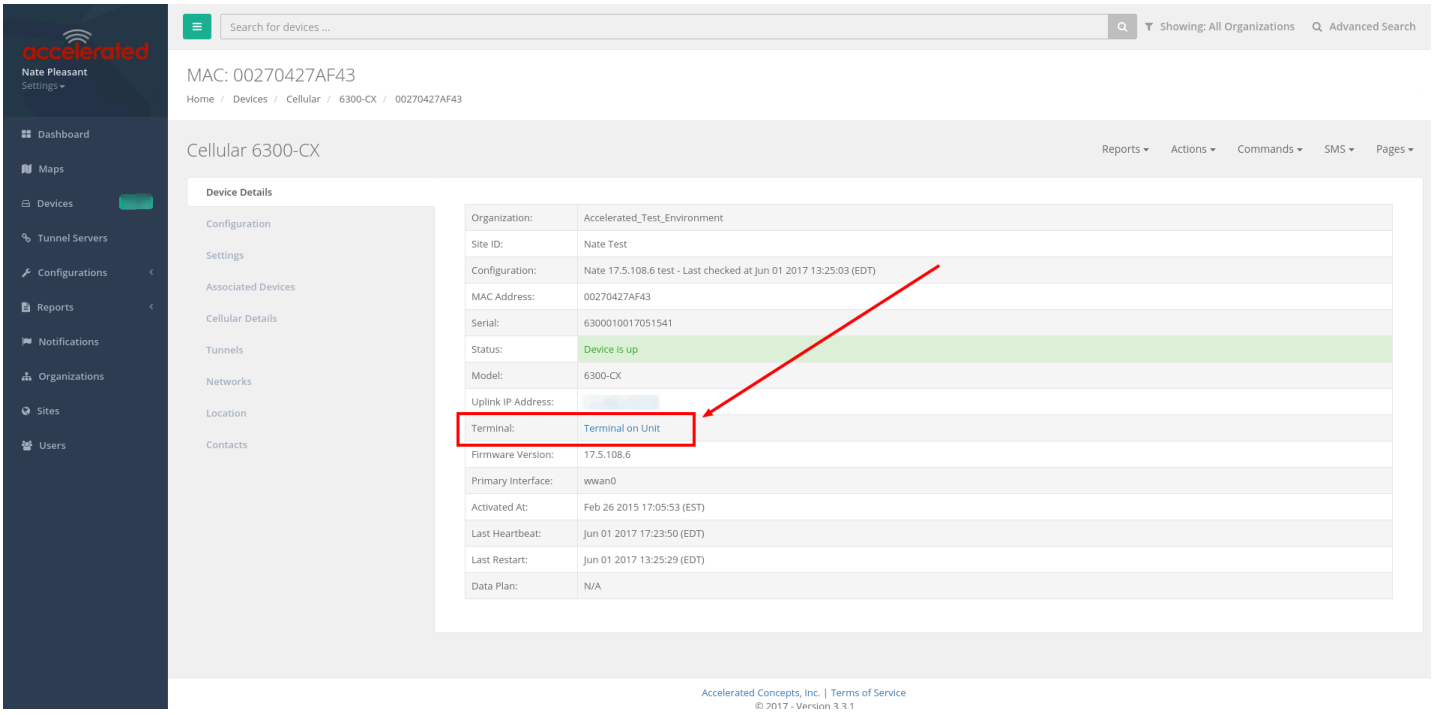
Terminal on Unit

Skill level: ***Intermediate***

Goal

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

> The ***Terminal on Unit*** access leverages the management tunnel established between the 63xx-series router and the management portal. 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 the management portal, and a 63xx-series router online and syncing with the management portal. If you see the 63xx-series router listed as up (green status) in the management portal, you are good to go.

Details

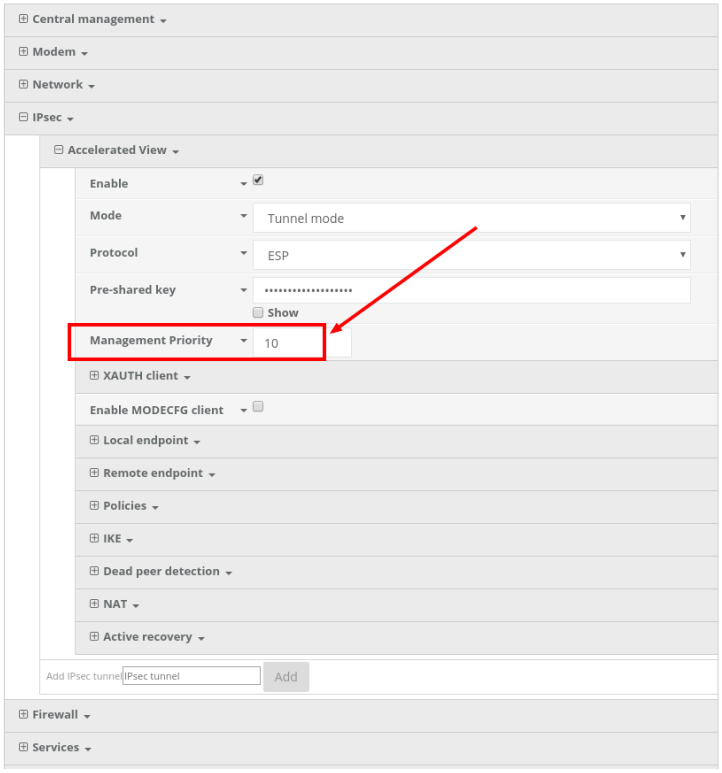
The management portal utilizes the IPSec tunnel the 63xx-series router establishes to remote.accns.com to provide terminal access to the console of the router.

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

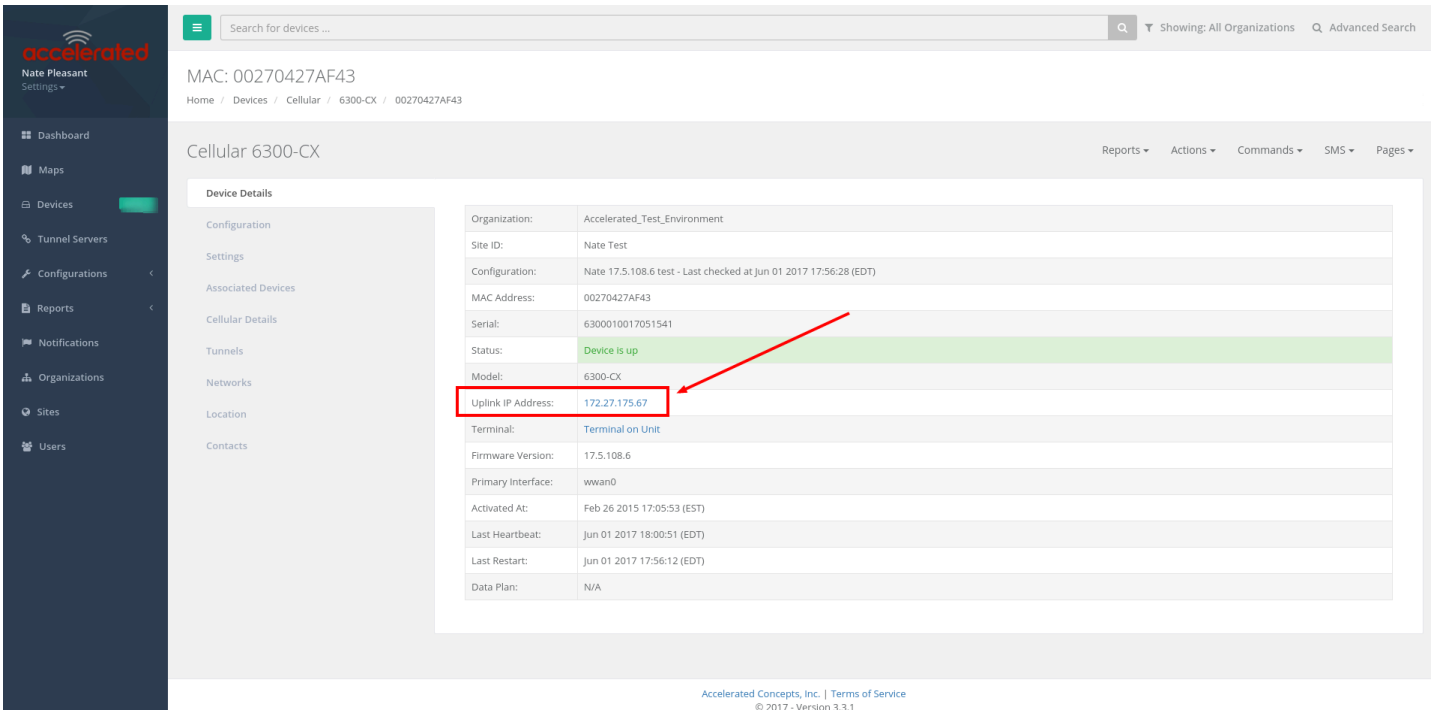
Data Usage Estimates

The following configuration settings will setup the 6300-CX to report its IPSec tunnel local IP address as the management IP that the management portal 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 this IPSec tunnel as the highest priority management interface, which it then reports to the management portal as the IP that can be used to access its console.



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 the management portal. You can verify that the management portal 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.



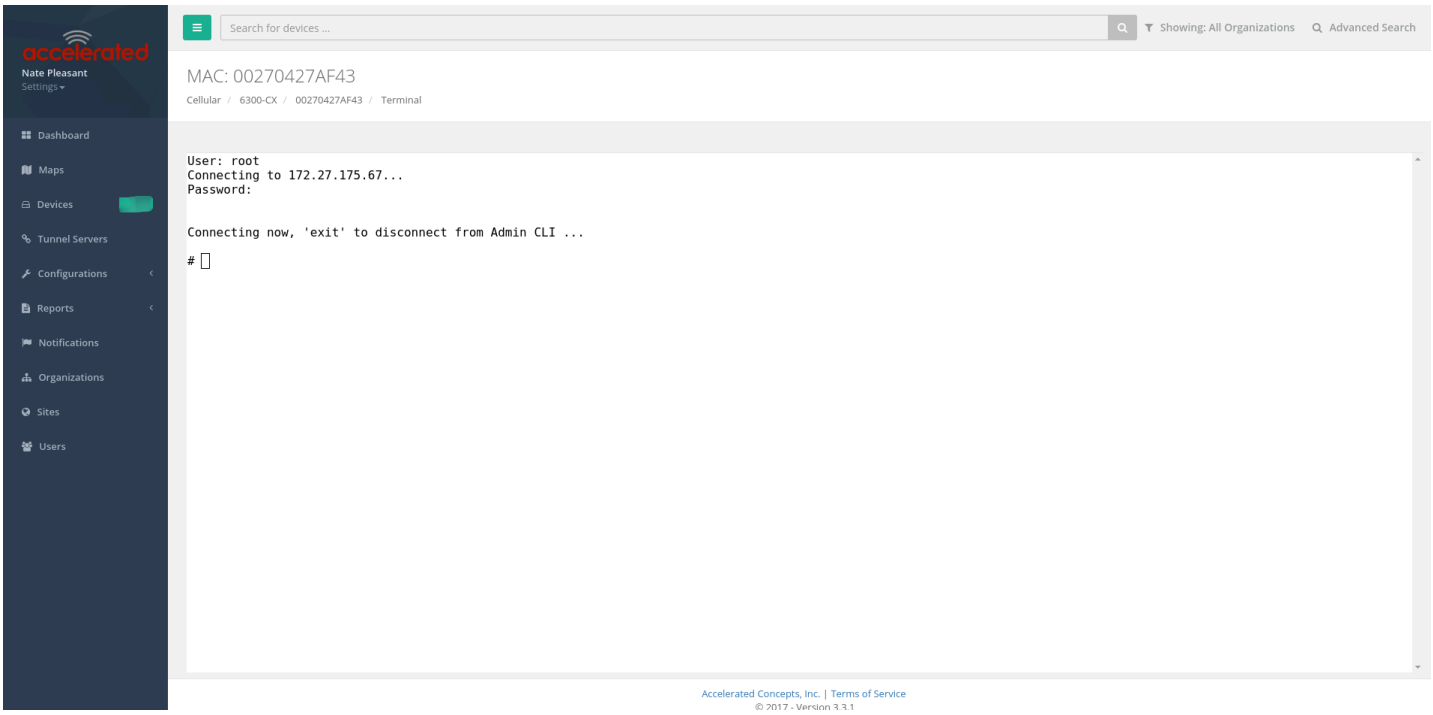
Using the Terminal on Unit link

Once the correct management IP is reported from the 63xx-series router to the management portal, clicking the ***Terminal on Unit*** will open a page on the management portal to provide the user access to the console of the 63xx-series router. Default login credentials are below.

User: root

Password: default

To create a different user or change the root user's password, refer to this article.



There is a known issue where the predictive/auto-correct feature of the Google keyboard renders it incompatible with the Terminal page. If you are access the above Terminal with an Android phone or tablet, you will need to use a different keyboard other than the native Google keyboard.

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
```

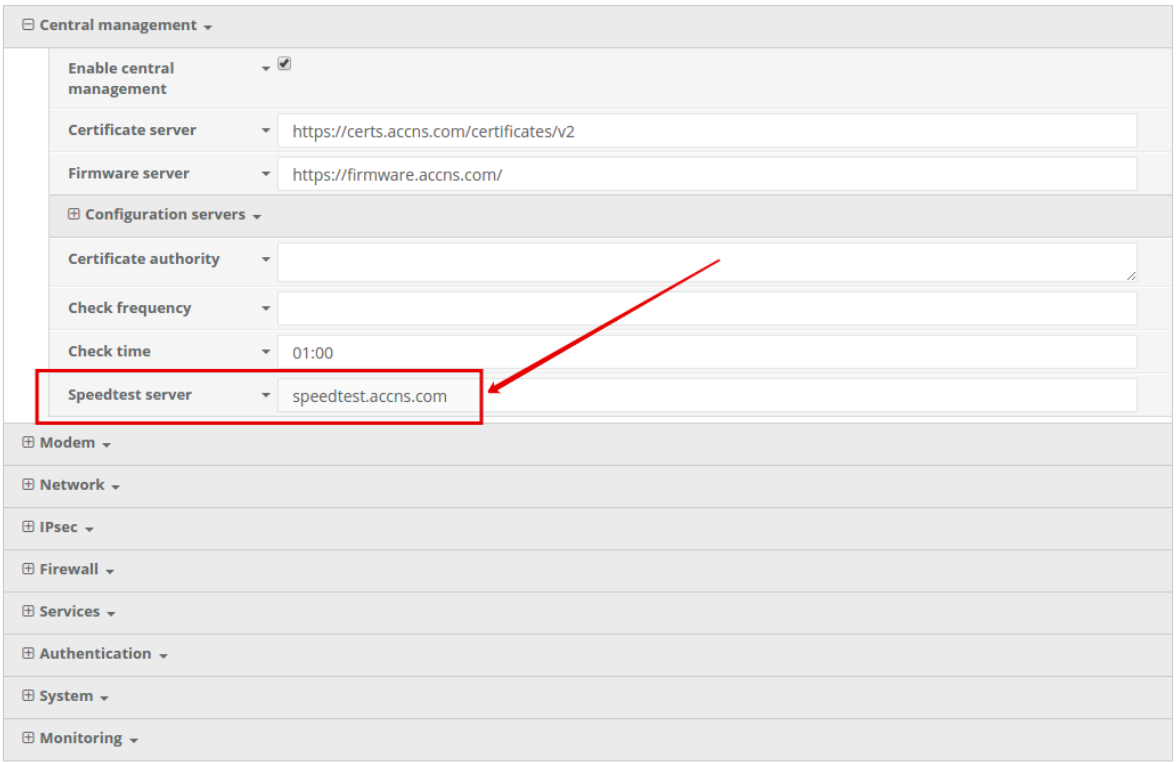
Then start the nuttcp speed test server with the following command:

```
nuttcp -S
```

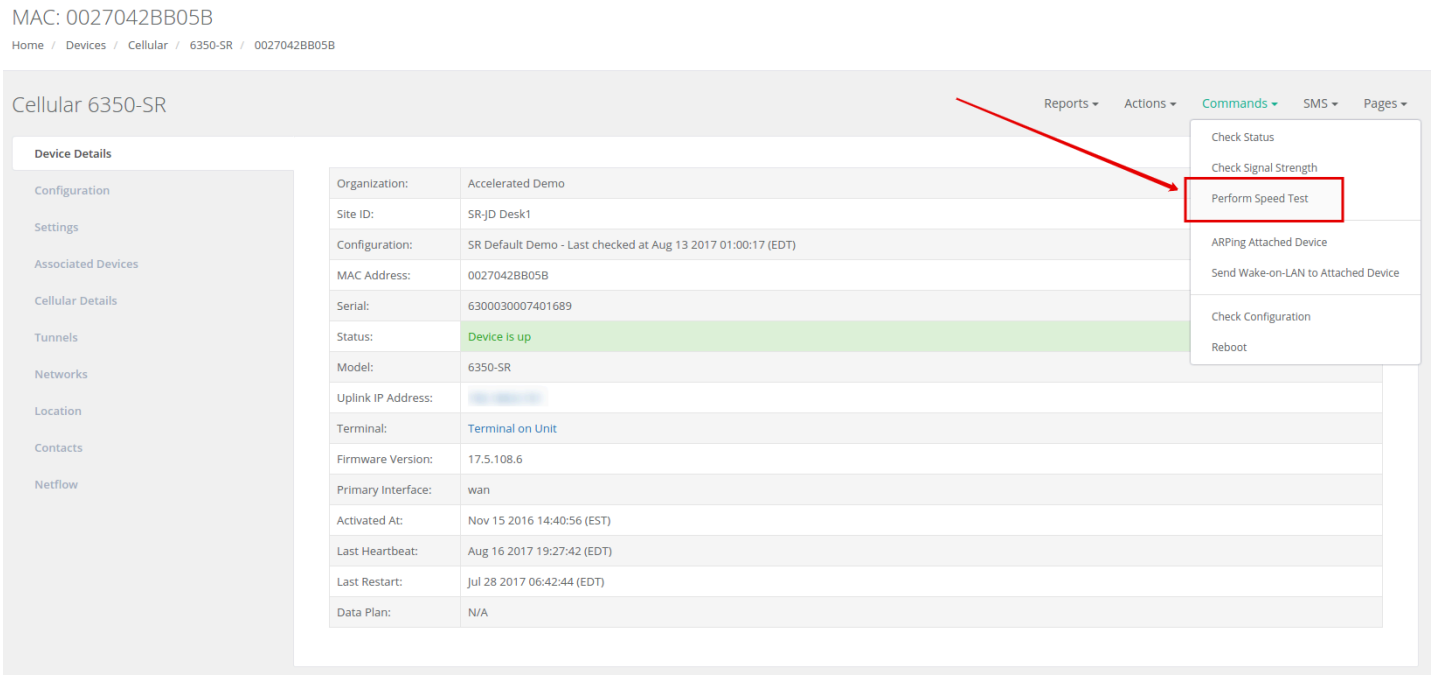
The 63xx-series router will need access to this server on UDP ports 5000 and 5001. Please ensure proper firewalls are opened to allow access to the IP address of the speed test server and its respective ports.

Using the new speed test server

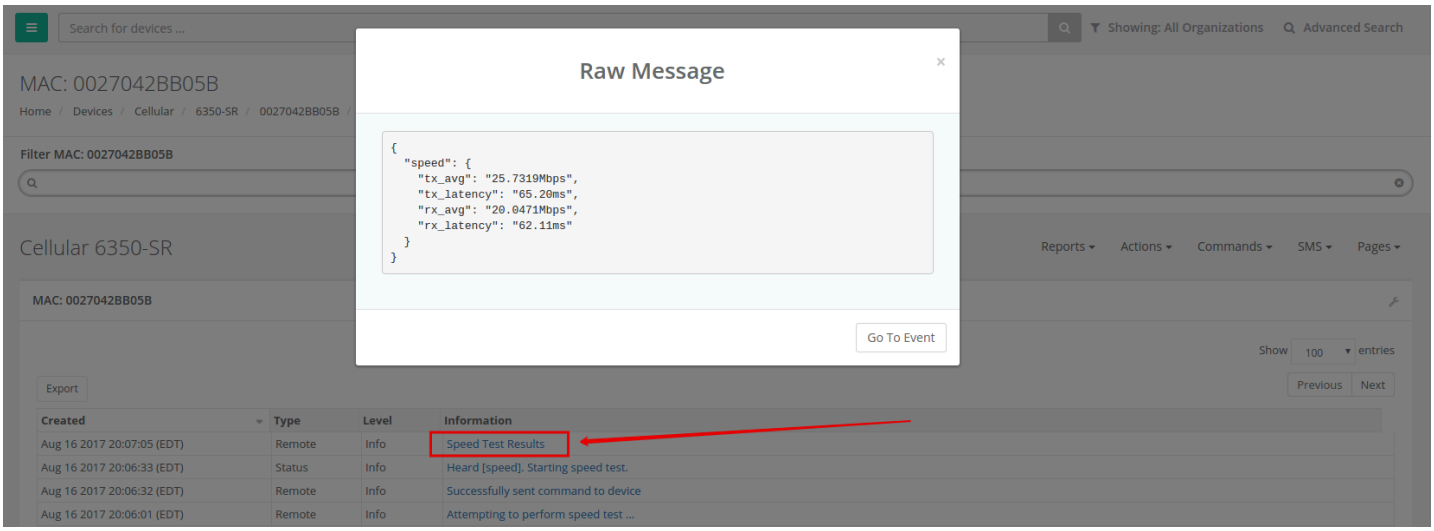
Once the new speed test server is running, add the IP address to the 63xx-series router's configuration profile under ***Central management -> speedtest server*** and apply the configuration to the device.



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.



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.



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*

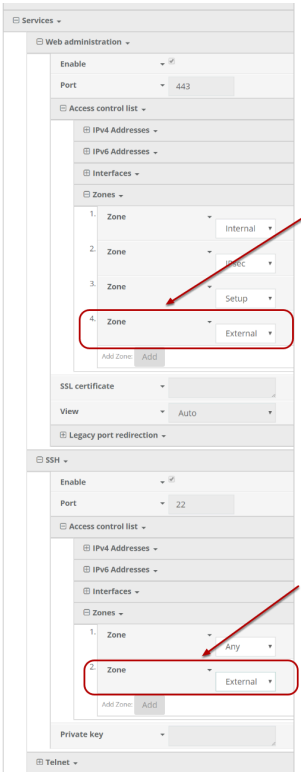
Password: *default*

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.

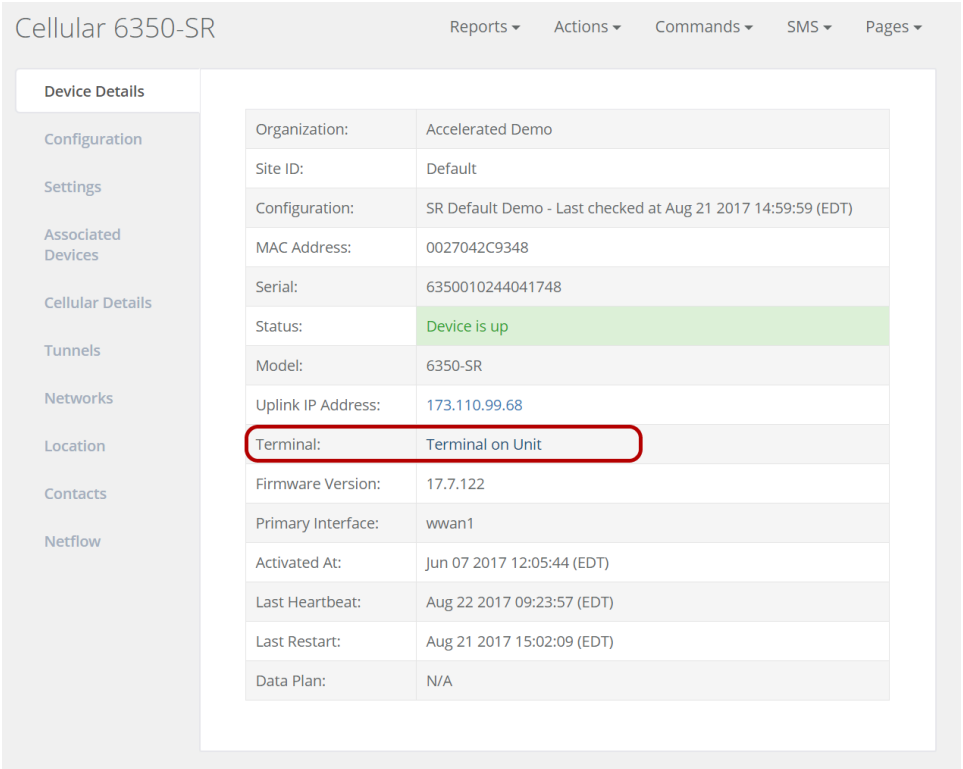
Sample Configuration

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."



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



USB-to-Serial Access

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

Goal

To enable serial out-of-band (OOB) access over SSH using the USB port.

Setup

A USB-to-Serial adapter will be required. Configuration varies depending upon the type of adapter -- single serial or a serial splitter.

USB-to-Serial Access

Serial out-of-band (OOB) access can be leveraged over SSH using the USB port. There are two types of USB-to-serial cables that can be utilized: single USB-to-Serial or a USB-to-Serial splitter. Purchasing options are available through Accelerated.

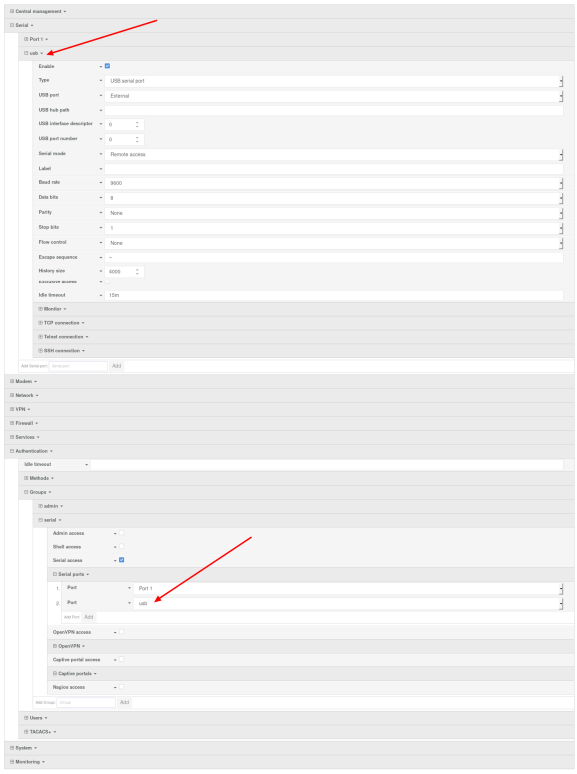
For assistance with enabling SSH, please refer to the following documentation:

- **Enabling Shell Access:** to enable full shell access to the device (as opposed to the admin CLI)
- **Remote Access:** to enable *external* SSH access
- **Terminal on Unit:** to enable SSH using the terminal available in aView.

Setup on firmware 18.8.14.122 or higher

This feature is now listed as an entry in the ***Serial*** section of the ACL router's configuration profile. Open the configuration profile for the ACL router and make the following changes:

1. Under ***Serial***, type in a name in the ***Add Serial port*** entry, then click ***Add***.
2. Set ***Type*** to ***USB serial port***
3. Set ***USB port*** to ***External***
4. Adjust the baud rage, data bits, and other serial parameters as needed to match those of the console being connected to the serial port.
5. Under ***Authentication -> Groups -> serial -> Serial ports***, click ***Add*** and select the newly created serial entry.
6. Click ***Save***



After the configuration is applied to the ACL router, an option will be added to the selection menu when a user establishes an SSH session to the device, or accesses the Terminal of the ACL router. Below is an example SSH session showing the newly created serial entry to access the USB-to-serial adapter.

```
$ ssh root@192.168.2.1
Password:
X11 forwarding request failed on channel 0


Access selection menu:

    a: Admin CLI
    1: Serial: port1         (9600,8,1,none,none)
    2: Serial: usb           (9600,8,1,none,none)
    s: Shell
    q: Quit

Select access or quit [admin] : 2


Connecting to usb:
Settings: 9600, 8, 1, none, none
Type '~.' to disconnect from port
Type '~?' to list commands
```

```
```

Setup on firmware 18.4.54.41 or lower

This feature is currently supported by shell interactions in an SSH session. With shell access enabled, press 's' after authenticating to the device.

```
$ ssh root@192.168.2.1
$ password
Access selection menu:

    a: Admin CLI
    s: Shell
    q: Quit

Select access or quit [admin] : s
Connecting now, 'exit' to disconnect from shell ...
#
```

The relevant command(s) for USB-to-Serial access will depend on the type of adapter being used.

Single USB-to-Serial Cable

Refer to the following command to bring up a single serial connection over USB.

```
tip -l "$(dmesg | grep "FTDI USB Serial Device converter now attached" | grep -m 1 -o
"ttyUSB[0-9]")" -c -s 9600
```

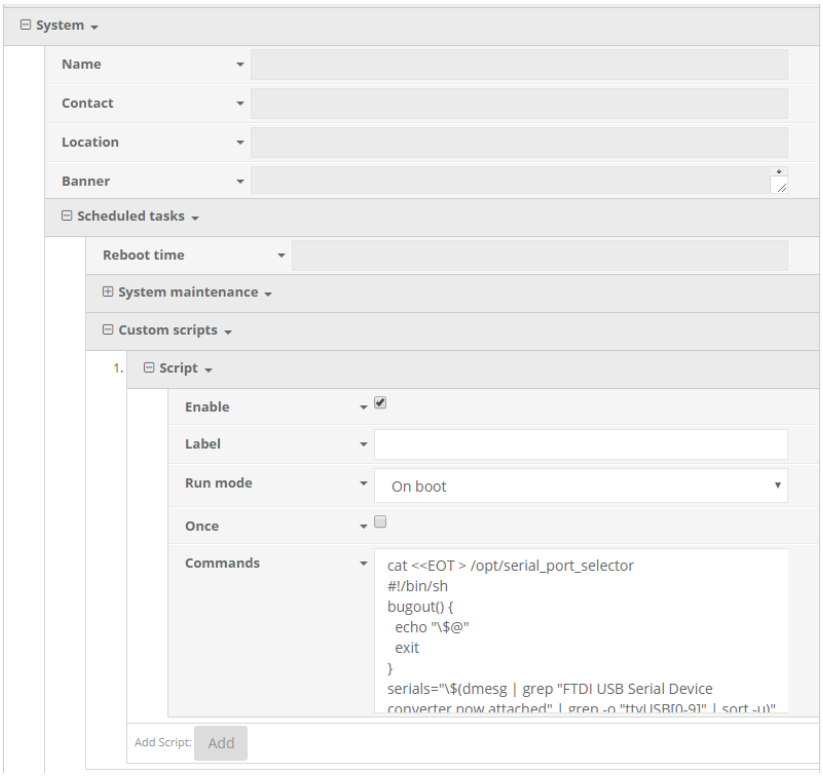
Pressing '~.' followed by ENTER will close the serial connection; note that this does not end the console session on the device being accessed over serial.

USB-to-Serial Splitter

To conveniently access multiple serial connections over SSH using this adapter, enter the following script into router's ***Custom Script*** field, setting its ***Run mode*** to "On boot." This field is nested under ***System > Scheduled Tasks > Custom Script***.

```
cat <<EOT > /opt/serial_port_selector
#!/bin/sh
```

```
bugout() {
  echo "\$@"
  exit
}
serials="\$(dmesg | grep "FTDI USB Serial Device converter now attached" | grep -o
"ttyUSB[0-9]" | sort -u)"
[ "\$serials" ] || bugout 'no serial-to-USB converters found'
serial_count=\$(echo "\$serials" | wc -l)
echo "Found \$serial_count USB-to-serial converters."
for i in \$serials; do
  echo "\$i"
done
echo "Type the number of the USB port you wish to open a console connection to"
echo "(e.g. for ttyUSB2, type '2'), followed by ENTER:"
read port_num
serial_port=\$(echo "\$serials" | grep "\$port_num")
[ "\$serial_port" ] || bugout "Port number \$port_num is not available, please re-run
and specify a differnt port."
echo "Opening connection to USB-to-serial port \$serial_port."
echo "Press '~.' followed by ENTER to close connection."
tip -l "\$serial_port" -c -s 9600
EOT
chmod +x /opt/serial_port_selector
```



With the script enabled, SSH onto the device and enter the following command from the shell to bring up the available serial connections:

```
/opt/serial_port_selector
```

This will list all available connections. Enter the number of the USB port to proceed. For example:

```
Access selection menu:
    a: Admin CLI
    s: Shell
    q: Quit
Select access or quit [admin] : s
Connecting now, 'exit' to disconnect from shell ...
# /opt/serial_port_selector
Found 4 USB-to-serial converters.
ttyUSB0
ttyUSB1
ttyUSB2
ttyUSB3
Type the number of the USB port you wish to open a console connection to
(e.g. for ttyUSB2, type '2'), followed by ENTER:
3
Opening connection to USB-to-serial port ttyUSB3.
Press '~.' followed by ENTER to close connection.
Connected.
```

MAC address-based Policy Routing with Dual WAN

Difficulty: ***Expert***

Minimum firmware version: ***18.1.29***

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.

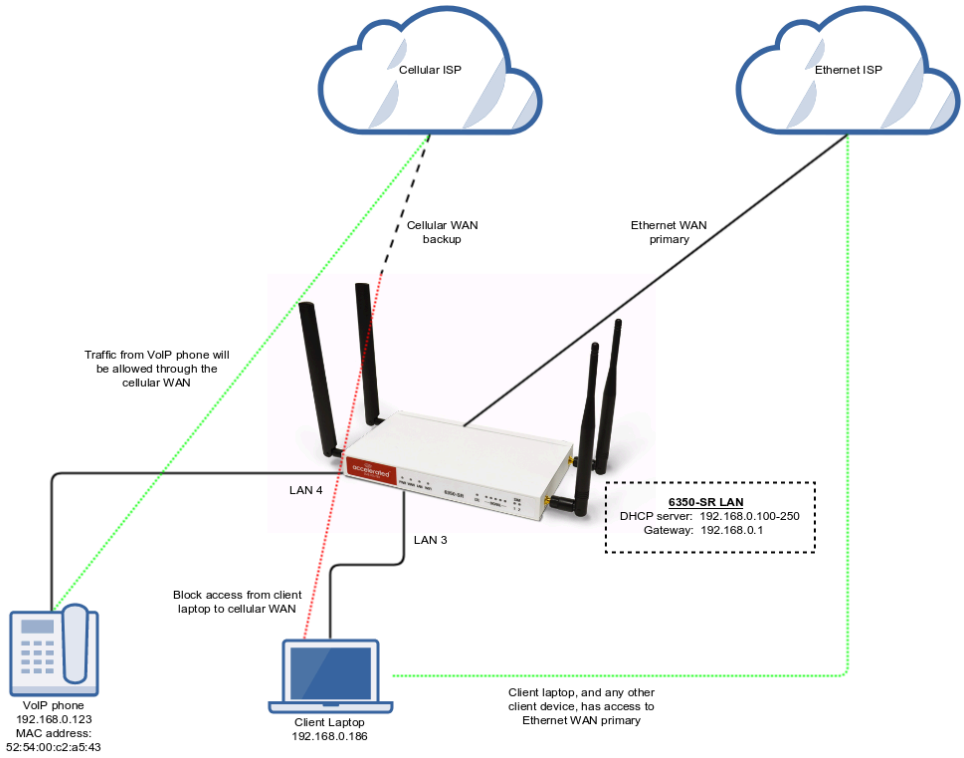
Sample

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.

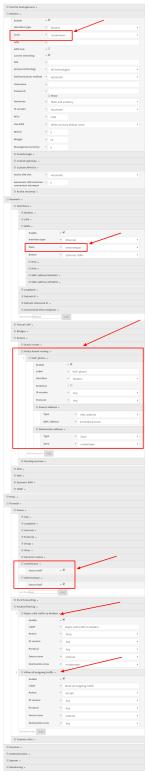


Sample Configuration

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 ***Network -> Routes -> Policy-based routing***, setup a new policy with the following settings:
    1. ***Interface:*** Modem
    2. ***Source address -> Type:*** MAC address
    3. ***Source address -> MAC address:*** 52:54:00:c2:a5:43
    4. ***Destination address -> Type:*** Zone
    5. ***Destination address -> Zone:*** modemwan

5. 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



Configuring an OpenVPN Server for iOS & Android OS Clients

Goal

Difficulty: Medium

Configuring a simple (username/password authentication only) OpenVPN server instance on an OpenVPN-enabled Accelerated device. Examples of client connection from an Apple iOS device is included. The steps to connect a Android OS device client to the server are similar.

This enables a *road-warrior* set up to allow roaming devices (iOS/Android OS devices) to connect into a device serving an OpenVPN TUN-style tunnel connection. For example on how to configure and connect an OpenVPN client on another Accelerated device, visit the article Configuring an OpenVPN Client on an Accelerated Device.

Relevant Files

The files used to create this article are attached below.

ca.crt

server.crt

server.key

dh2048.pem

root_default_tun.ovpn

Setup

This article assumes you have basic understanding of server-authentication, certificates, keys, and the fundamentals of OpenVPN. It also assumes the appropriate private and public certificate (*.crt), key (.*key), and Diffie-Hellman (dh2048.pem) files, as well as the OpenVPN configuration file (*.ovpn) are correctly generated. For more details on generating these files, visit https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-16-04

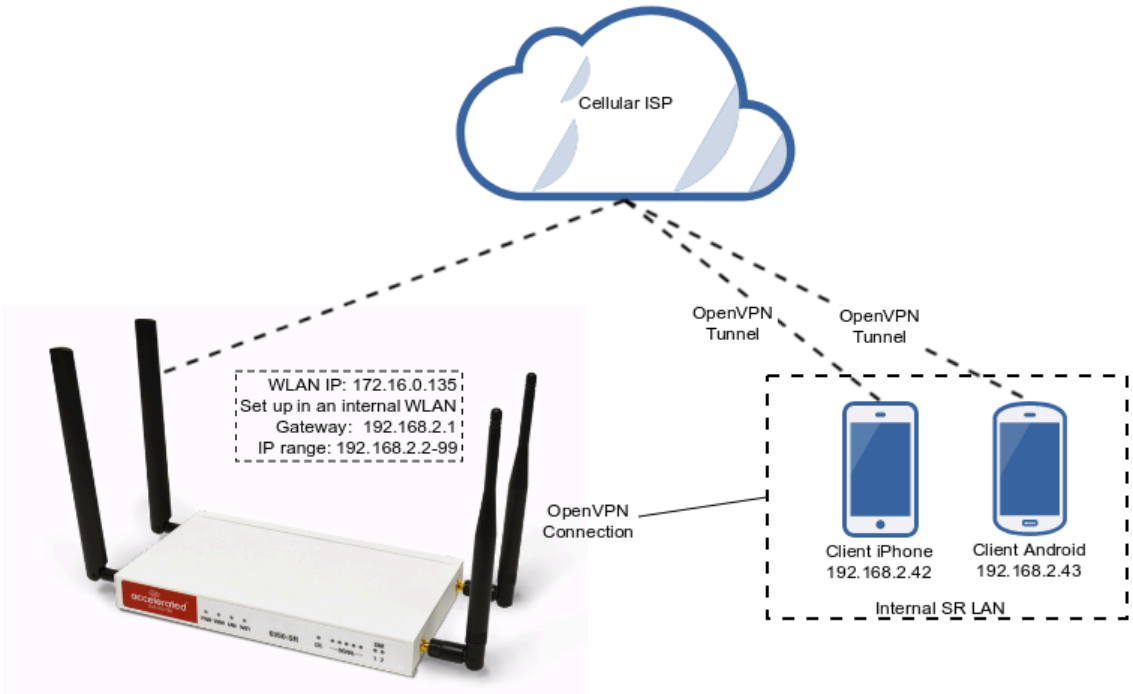
The client devices (iOS/Android OS devices) require the OpenVPN Connect app from their respective app libraries:

- App Store: https://itunes.apple.com/au/app/openvpn-connect/id590379981?mt=8
- Google Play: https://play.google.com/store/apps/details?id=net.openvpn.openvpn&hl=en

The *.ovpn file will need to be imported into the devices for OpenVPN Connect to use.

Sample

The sample configuration below shows an example network with an iOS device connected via the TUN-style tunnel. References to the Android OS are made.

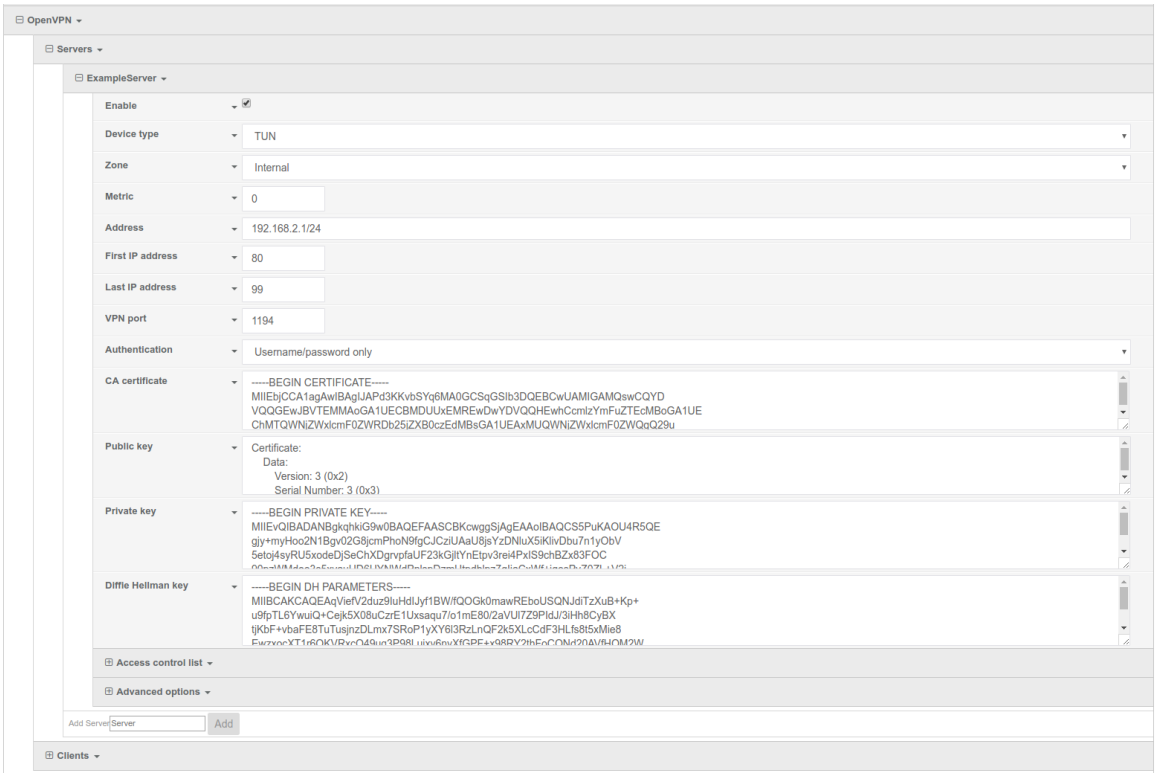


Sample Configuration

Open the configuration page and set the following configurations.

OpenVPN Section Configuration

1. In the ***VPN > OpenVPN > Servers*** section, specify a name for the new "OpenVPN" server (e.g. *ExampleServer*) and click ***Add***.
2. Ensure ***Enable*** is selected.
3. Ensure the ***Device type*** pull-down menu is selected to be *TUN.* This is necessary as iOS and Android OS only supports TUN-style OpenVPN tunnels.
4. Ensure the ***Zone*** pull-down menu is selected to be *Internal, as the clients are treated as a LAN devices.*
5. Set ***Address*** to *192.168.2.1/24*, this must be a valid gateway in the network of the IP address range.
6. Specify the ***First IP address*** and the ***Last IP address*** of the address range if different from the default values.
7. From the ***Authentication*** pull-down menu, select option *Username/password only*.
8. Insert the contents of the generated CA certificate (usually in ca.crt file), Public key (e.g. server.crt), Private key (e.g. server.key), and the Diffie Hellman key (usually in dh2048.pem) in their respective fields. The contents will be hidden when the configuration is saved.



Full files used in this example are attached in the Relevant Files section above.

Authentication Section Configuration

The following configurations add a new user/group to handle OpenVPN access:

1. In the ***Authentication > Groups*** section, specify a name for the OpenVPN group (e.g. *egGroup*).
2. Select ***OpenVPN access***.
3. Expand ***OpenVPN*** tab, using the pull-down menu next to ***Tunnel***, select appropriate OpenVPN instance, e.g. ***Server: ExampleServer***.
4. In the ***Authentication > Users*** section, specify a name for a new OpenVPN user (e.g. *egUser*).
5. In the new ***egUser*** user section, ensure ***Enable*** is checked, and specify a password for this user (e.g. *egPassword*).
6. In the ***egUser > Groups*** section, click ***Add*** and from the pull-down, select the OpenVPN group you wish to affiliate with this user (e.g. *egGroup*).
7. Press ***Save*** at the bottom of the configuration page to save changes.

The OpenVPN server should now be operational. The next step is to connect a roaming device to the server by loading a *.ovpn file in OpenVPN Connect. Below is an example *root_default_tun.ovpn* file (attached):

```
client
dev tun
proto udp
remote 172.16.0.135 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-CBC
verb 3
auth-user-pass
<ca>
-----BEGIN CERTIFICATE-----
MIIEbjCCA1agAwIBAgIJAPd3KKvbSYq6MA0GCSqGSIb3DQEBCwUAMIGAMQswCQYD
VQQGEwJBVTEMMAoGA1UECBMDUUxEMREwDwYDVQQHEwhCcmlzYmFuZTEcMBoGA1UE
ChMTQWNjZWxlcmF0ZWRDb25jZXB0czEdMBsGA1UEAxMUQWNjZWxlcmF0ZWQgQ29u
Y2VwdHMxEzARBgNVBCkTCnRlc3RzZXJ2ZXIwHhcNMTcxMTAxMDE1MzQxWhcNMjcx
MDMwMDE1MzQxWjCBgDELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA1FMRDERMA8GA1UE
BxMIQnJpc2JhbmUxHDAaBgNVBAoTE0FjY2VsZXJhdGVkQ29uY2VwdHMxHTAbBgNV
BAMTFEFjY2VsZXJhdGVkIENvbmNlcHRzMRMwEQYDVQQpEwp0ZXN0c2VydmVyMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyVTfVOJNPTTPYDFC0GtGnpky
q9rQthQ/CX+u9wUpsJ8yBenmENqi5Yq3L/DWJXwTmXd4z2PaQFjszHQlDDwoN9pW
W/aPt4ZkC/6ms9Ny3WbEM/XQwgri2LRXra3qpGmjGtUIgCpl2nC8nFtvfqsca8u8
1qAZZtuT3YXAM5FYpsLKEc4TZfgquyJW4I1JwNTIIobVq7Oiqvs8JbpMAFtmBxVv
NYU9LJsAFzwvO1OZkfoXefqz9/uxKK/MzTCNvu7Z64z6Q52EQVJciHYHE2jEMKdy
yyvpFJYii6Hocu3ocHpvGa6ki3Cw/ObeenbqLKTCK8zsIL99JJYXaUKyFq4zsQID
AQABo4HoMIHlMB0GA1UdDgQWBBQIeJbSenktJDlHp6a9lHIbzagE4zCBtQYDVR0j
BIGtMIGqgBQIeJbSenktJDlHp6a9lHIbzagE46GBhqSBgzCBgDELMAkGA1UEBhMC
```

```
QVUxDDAKBgNVBAgTA1FMRDERMA8GA1UEBxMIQnJpc2JhbmUxHDAaBgNVBAoTE0Fj
Y2VsZXJhdGVkQ29uY2VwdHMxHTAbBgNVBAMTFEFjY2VsZXJhdGVkIENvbmNlcHRz
MRMwEQYDVQQpEwp0ZXN0c2VydmVyggkA93coq9tJirowDAYDVR0TBAUwAwEB/zAN
BgkqhkiG9w0BAQsFAAOCAQEACjuztAUUOhpw4GUVKDMbw8IrMAVXkDEAxdwpfL+X
bT6mQc9sbZAFCXWxh9q425F5Xll9+TKOjrulZdHzaoominFclsoqwdpu0I+K4I3e
Qap0B+Ns7DGmcwu68I1LsQq6hJAaM03DvEGPFSbbZi/60zJRgQdVWjtGhAbW46by
6litNY64j0vN/UW41IfMjvRXeg8Zgyb7gICRTWUAvaV9CXlhHK0GWzCKCrIl225x
zfvsmuPERPYKFopPhfqV+xE/62Q/TcAcuJgaGfMipY3IXkRhqikj5pZS3g4gAVjZ
Z65upCz8o5CEngtwOQ/fSPUxo73ycpkLPxJF/QwXUJA/kw==
-----END CERTIFICATE-----
</ca>
```

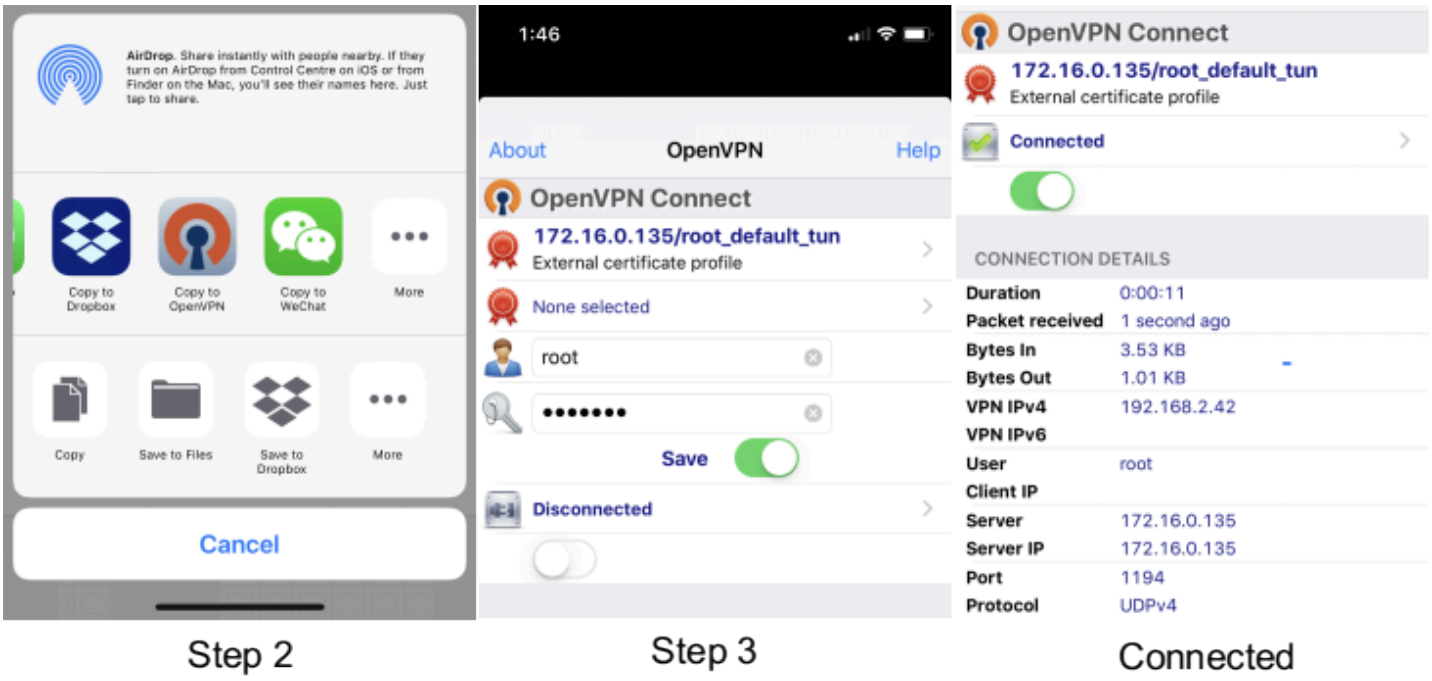
OpenVPN Connect on a mobile device may not require the *auth-user-pass* option. If the option is used, make sure there is no argument passed (i.e. pass.txt) as the application will try to search for the file locally.

Also ensure the correct static IP address and port is inserted in the "remote" line.

Example Client Device Set Up

The following example is taken from an iOS device. The steps are similar for an Android OS device:

1. Download and install **OpenVPN Connect** from App Store.
2. Transfer the *.ovpn file to the iOS device. One way is to send it via an email attachment, open it in the Mail app and select **Copy to OpenVPN**.
3. In the OpenVPN app, insert the appropriate credential for the server as it was set up during the certificate/key file creation phase. Save the credential as desired.
4. Select the switch beneath **Disconnected** to initiate the connection.



Step 2 Step 3 Connected

If the configuration is set up correctly, the OpenVPN Connect app will show all the active connection details.

Note for Android OS users: Step 2 - locating and opening the *.ovpn file can be quite different from an iOS device. You will need to apply the correct steps to load the ovpn file into OpenVPN Connect on Android.

Enabling intelliFlow

Difficulty level: ***Beginner***

Goal

To enable Accelerated intelliFlow feature in compatible devices to allow the monitoring of system resource information and network traffic flow in the local management interface (WebUI)'s Dashboard page.

Note: enabling Intelliflow will add an estimated 50MB of data usage on the 63xx-series router's Internet connection, as these Intelliflow metrics are reported to the Accelerated View portal.

Setup

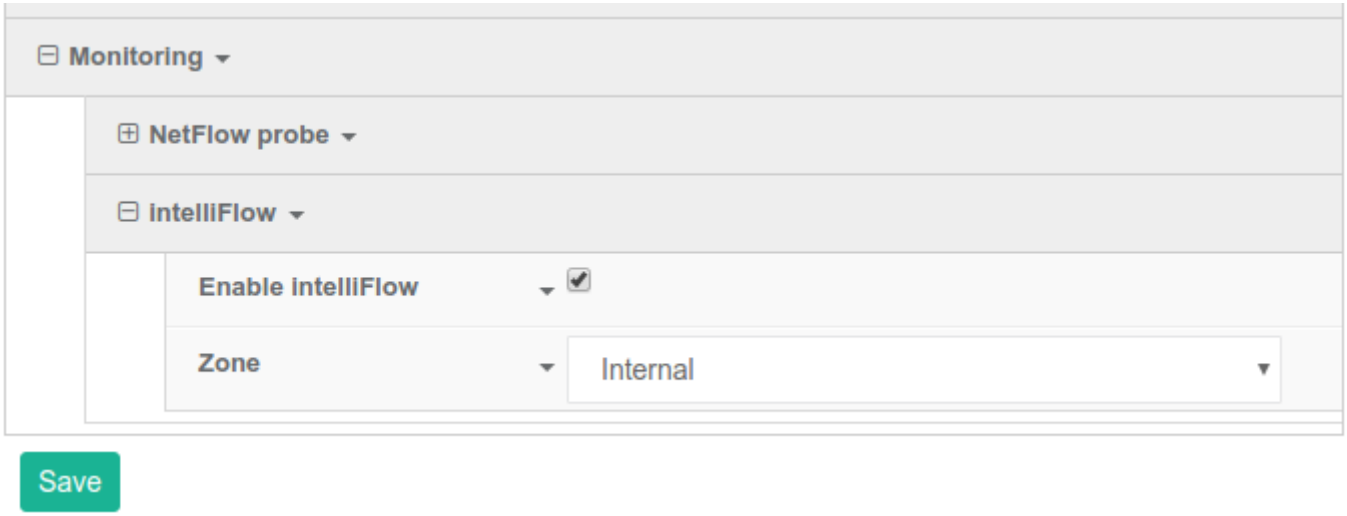
The purpose of intelliFlow is to keep track of the network data usage and traffic information, therefore the only requirement is that the device is powered on, and the local WebUI is accessible.

The comprehensive explanation of the Dashboard can be found in the User manual.

Sample Configuration

Open the configuration profile for the router device and make the following changes.

1. Under ***Monitoring*** > ***intelliFlow,*** check ***Enable intelliFlow***.
2. Click ***Save***.
3. To view intelliFlow data, select ***Dashboard***. Once intelliFlow data is collected, relevant information will display in the Dashboard.


Monitoring
NetFlow probe
IntelliFlow
Enable IntelliFlow
Zone
Internal
Save

Customizing WebUI Logo

Difficulty level: ***intermediate***

Goal

To customise the logo in the WebUI which persists across factory resets. There will be other parts of the WebUI to offer full customisation in the future.

Setup

Customizing the WebUI requires supporting files to be created and transferred onto the Accelerated device. This article assumes you have the knowledge and the resources to create these files. Tools such as scp, WinSCP, or PuTTY can be used to transfer files securely from the host PC to the device.

This configuration example also requires you to have the knowledge to enable shell access on the Accelerated device. For more information, visit Enabling Shell Access.

Sample Files

The files used in this guide are attached.

logo_custom.png

custom.css

Preparing the Files

Two files are required to be created and transferred onto the Accelerated device:

- **Logo file (*.png):** The file must be a transparent png file.
- **custom.css:** This file includes the CSS required to extend the 'logo_skin' class, which is read by WebUI.

The logo file are required to be approximately 180 pixels wide. There are no inbuilt facilities to automatically scale logo images. If the logo image is too large, it may not correctly fit into the WebUI's logo area. The suggested dimension is 180px wide and 60px high. If files are larger than the specified dimensions, downsizing will be required:

```
# convert -resize 95% logo_original.png logo_custom.png # assume ImageMagick is installed
```

To create the 'custom.css' file, open a new text file and rename it to 'custom.css'. In this file, specify the logo file, the width and the height of the drawable logo canvas. The 'custom.css' file should include the following:

```
.logo_skin { background-image: url("/assets/custom/logo_custom.png"); width:179px; height:107px; }
```

- **Logo path:** The path '/assets/custom/' is fixed. It is where the device's WebUI will look for the logo file.
- **logo_custom.png:** This filename can be customised as necessary, as long as it is the logo file's filename.
- **Logo canvas width/height:** This is the dimension of the drawable canvas. The logo may not be correctly formatted if it is more than 180px wide.

Updating the WebUI

Once the two files are created in the previous step, they are to be transferred onto the Accelerated device's device directory `/opt/custom/`. This directory cannot be altered as the software is hardcoded to search for customised resources in that directory.

To transfer the files onto the device, first, ensure the shell access to the device is enabled. An active connection to the machine where the newly created files are stored is also established.

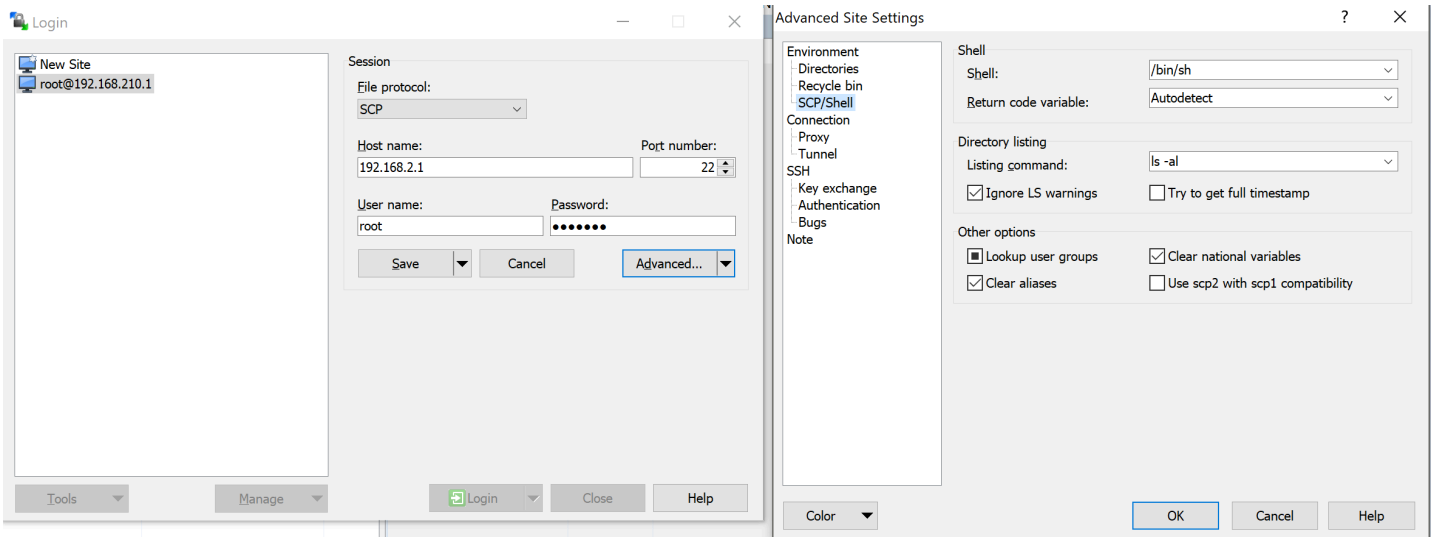
For Windows

Windows 10 or above has native support to run a Linux distribution inside the Operating System (OS) which enables the use of *SCP*. For details, visit this article and then follow the instructions under ***"For Mac OS/Linux"*** below.

Alternatively, WinSCP is a widely used program to transfer files via the SCP file transfer protocol. The following steps outline the file transfer process using WinSCP.

1. Install and open WinSCP
2. In the Login dialog box, input the appropriate credentials, for example:
   - File protocol: SCP
   - Host name: 192.168.2.1 (or 192.168.210.1 for the device's default IP)
   - Port number: 22
   - User name: root
   - Password: <your user or root password>
3. Click *Advanced...* button to reach the advanced settings dialog box
4. In *Advanced Site Settings* dialog box, identify and navigate to *Environment* > *SCP/Shell* to make the following adjustments as shown in the screenshot below:
   - Change "Shell:" to */bin/sh*
   - In *Directory listing*, uncheck *Try to get full timestamp*

5. Click OK to exit Advanced Site Settings and click Save in the Login dialog box to save the login profile
6. When saved, click *Login* to log into the device
7. Navigate to `opt/custom` and transfer the necessary resources into this directory



For Mac OS/Linux

Mac OS and Linux-based/emulated systems normally has the "SCP" utility built in by default. The following the steps outline the process to transfer the resource files.

1. Copy the two files into the device's `/opt/custom/` directory, e.g.:
   `scp /path/to/files/* root@192.168.210.1:/opt/custom/`
2. Once the files are transferred, reload the WebUI to see the updated logo

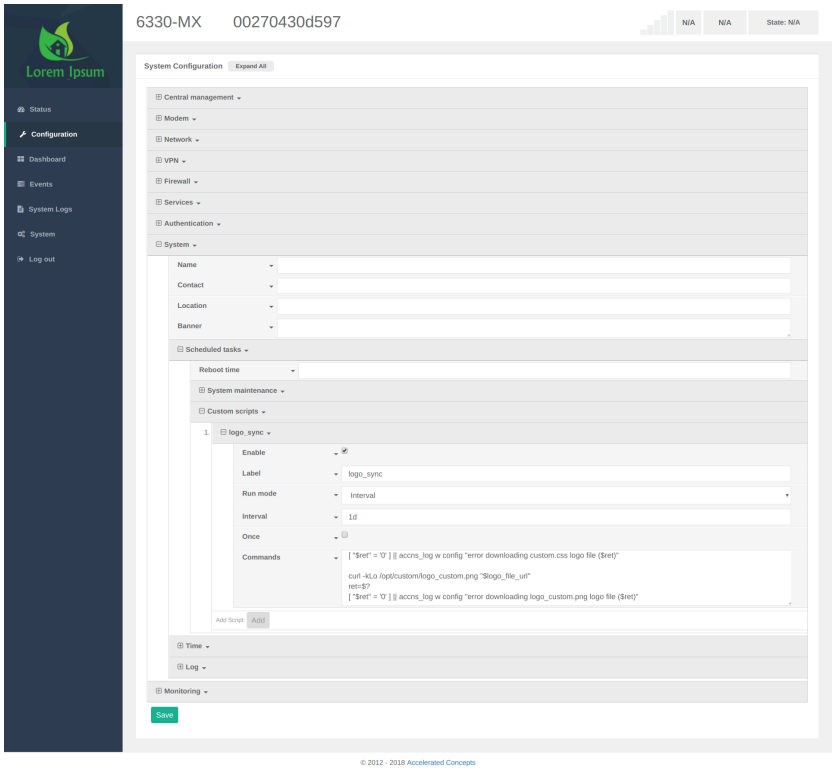
Automated download

If you have a fileserver, you can create a custom script to download files from that server onto the device.

1. Copy the two files onto the file server
2. Setup the following custom script on the device, replacing the urls for the two files with the appropriate domain and path based on your file server settings.

```
css_file_url='https://downloads.accns.com/webui_logo/custom.css'
logo_file_url='https://downloads.accns.com/webui_logo/logo_custom.png'


curl -kLo /opt/custom/custom.css "$css_file_url"
ret=$?
[ "$ret" = '0' ] || accns_log w config "error downloading custom.css logo file ($ret)"


curl -kLo /opt/custom/logo_custom.png "$logo_file_url"
```

```
ret=$?
[ "$ret" = '0' ] || accns_log w config "error downloading logo_custom.png logo file
($ret)"
```



Enabling Shell Access

Difficulty: ***Beginner***

Goal

To enable shell access to an Accelerated User Equipment (UE) via the SSH protocol.

Setup

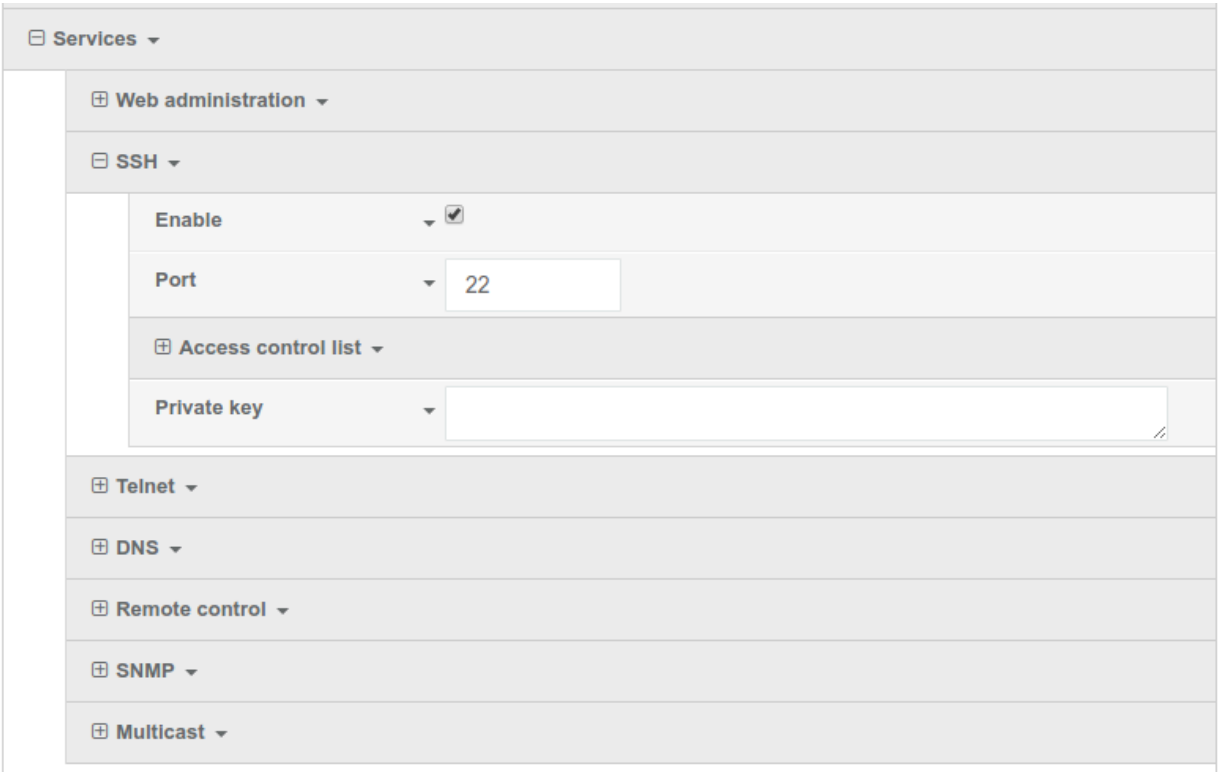
This article assumes the UE is running default configuration with the root password assignment, and central management disabled. Similar procedures apply if shell access is to be enabled in central management.

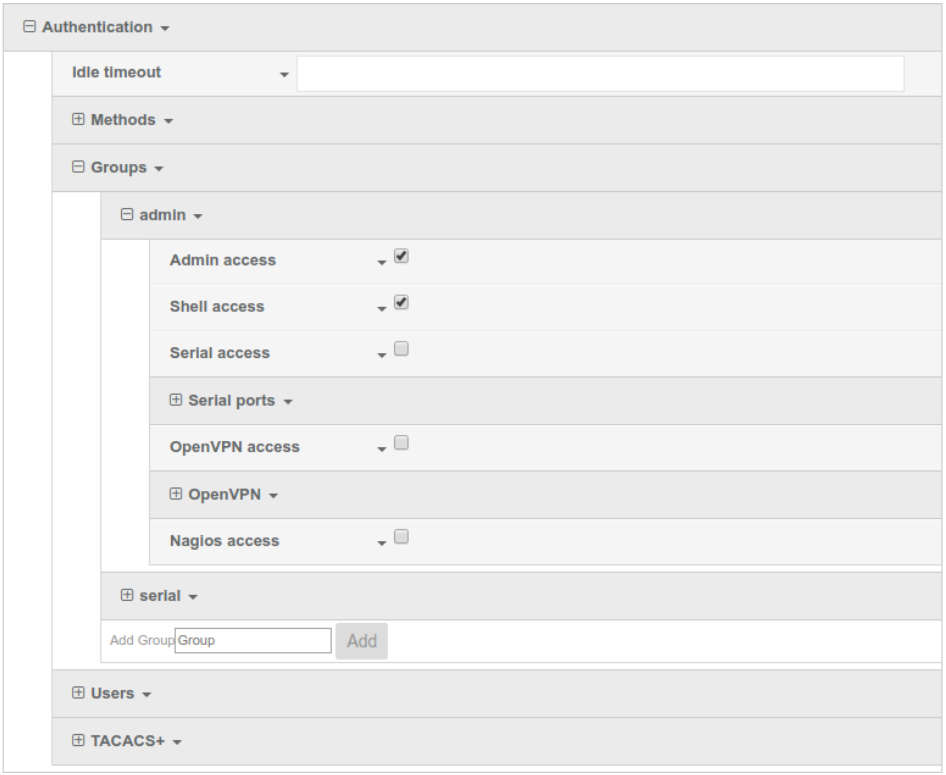
Configuration Steps

This configuration enables the local shell access for an existing root user. This procedure is applicable to any other users on the UE just the same.

Open the configuration page for the UE and make the following changes.

1. Ensure ***Service -> SSH -> Enable*** is checked.
2. Check the box under ***Authentication -> Groups -> admin -> Shell access***.
3. Click ***Save*** to update configurations.





Once the configurations have been successfully saved, the UE's shell can be accessed via SSH. Below is an example shell login process:

```
$ ssh root@192.168.2.1
$ password
```

```
Access selection menu:

    a: Admin CLI
    s: Shell
    q: Quit

Select access or quit [admin] : s

Connecting now, 'exit' to disconnect from shell ...

#
```

Local User Management

Skill level: ***Beginner***

Goal

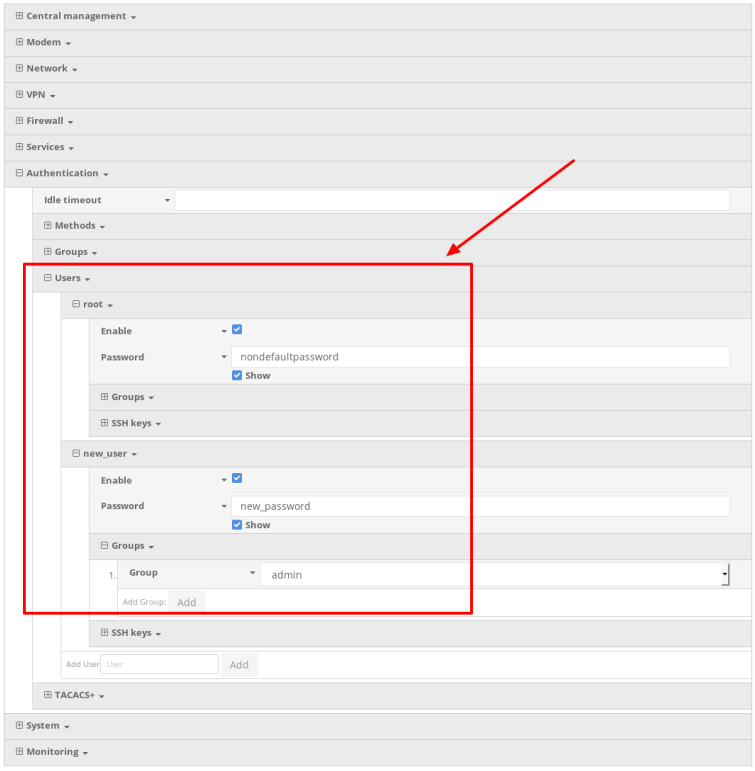
To create a new user and/or change the password of the default root user.

Details

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

1. To update the root user password, enter in the new password in the in the ***Authentication -> Users -> root -> Password*** option.
2. To create a new local admin user:
    1. Under ***Authentication -> Users -> Add User***, enter in the new username and click ***Add***.
    2. Enter in the password for the new user
    3. Under ***Groups*** for the new user, select the default ***admin*** group. You can create a new group, or edit the admin group's priviledges through the ***Authentication -> Groups*** section of the configuration profile.
3. Click ***Save*** or ***Update*** to apply the changes.

NOTE: *After saving a user's password, it is stored as a salted hash for security purposes. Clicking **show** prior to committing the password will reveal the true value; clicking show after that password has been saved reveals the salted hash.*


Central management
Modem
Network
VPN
Firewall
Services
Authentication
Idle timeout
Methods
Groups
Users
root
Enable
Password
nondefaultpassword
Show
Groups
SSH keys
new_user
Enable
Password
new_password
Show
Groups
1.
Group
admin
Add Group:
Add
SSH keys
Add User
User
Add
TACACS+
System
Monitoring

Dual Modem Setup

Goal

To configure an additional cellular WAN interface on an Accelerated device using an external USB modem.

NOTE: *Accelerated's SR- and MX-series devices have USB ports. The device must be running firmware versions 18.4.54.41 or 18.8.14.124*

Setup

This article assumes the USB-driven connection will serve as the primary WAN, and that the Accelerated device will fail over to the cellular connection provided by the 1002-CM module if the primary means of Internet access goes out. To learn more about configuring failover between WAN interfaces, click here.

For this setup, you will need an active Internet connection on both the Accelerated device and a supported USB modem. Ethernet WAN interfaces may be added to, or swapped in place of, failover prioritization between cellular WAN interfaces, if available.

NOTE: *Accelerated devices only support the following USB modems:*

Officially Supported:

- Sierra Wireless 340u (AT&T Beam)
- Sierra Wireless 313u (AT&T Momentum)
- Sierra Wireless 313u (T-mobile Unlocked Momentum)
- Aircard 320u (Telstra 4G)
- Novatel U620L (Verizon)
- Pantech UML290 (Verizon)
- Pantech UML295 (Verizon)

Sierra Wireless 340u note: The Beam is officially supported but under certain signal strength conditions we recommend they use the included USB extension cable that comes with the Beam Air Card

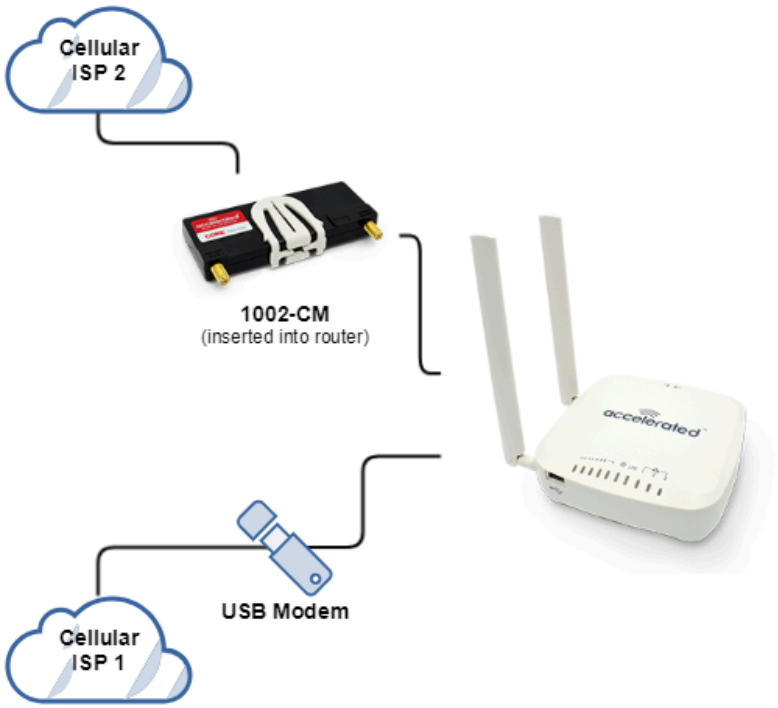
Supported, Modem Configuration Required*:

Netgear 341u (Sprint)

*Refer to our FAQ for More Information

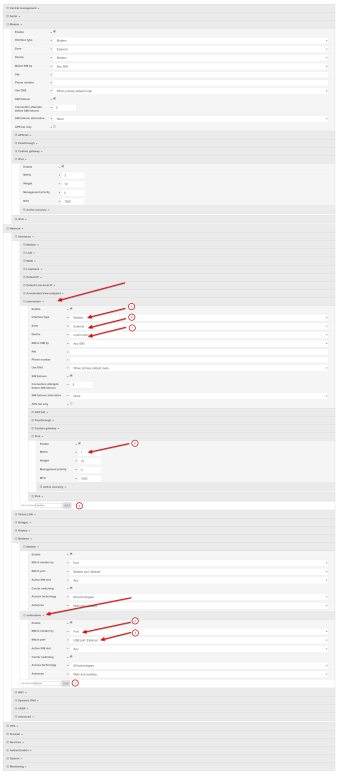
Sample

The sample configuration below shows an Accelerated device with two cellular Internet connections: one using the 1002-CM module and the other using a supported USB modem. Failover is set to assume the USB modem (ISP 1) is the primary connection, with the 1002-CM (ISP 2) serving as the backup that will step in should the primary line fail, though this can be adjusted as needed by altering the ***Metric*** value for each interface. Accelerated devices support both failover and load balancing between available Internet connections.

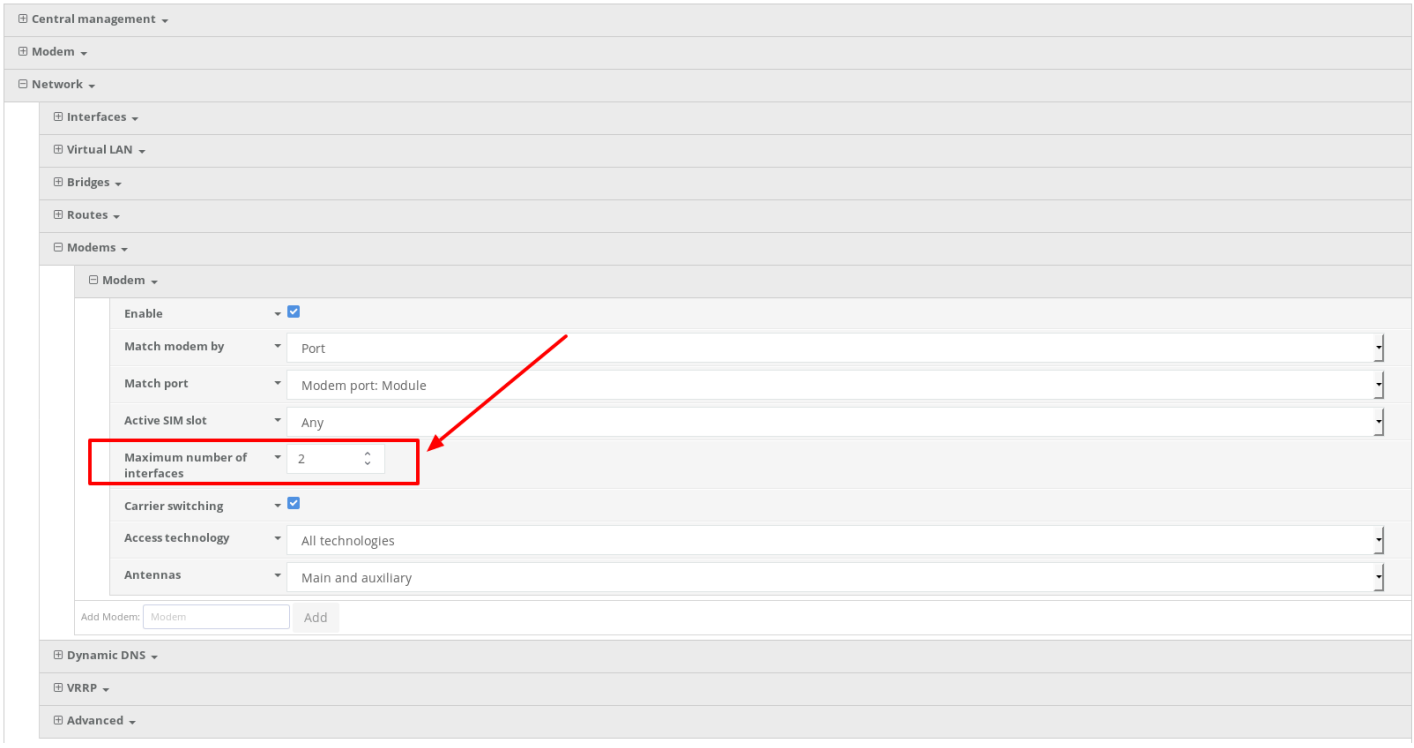


Sample Dual Modem aView Configuration

1. Under **Network > Modems > Add Modem**, create a new entry named "usbmodem." The name can be different if desired.
2. Change the **Match modem by** to "Port."
3. Change the **Match port** to "USB port: External."
4. Under **Network > Interfaces**, create a new entry named "usbmodem." The name **must match** the modem name from step 1 above for tracking and logging accuracy.
5. Change the **Interface type** to "Modem."
6. Change the **Zone** to "External."
7. Change the **Device** to "usbmodem" (the modem entry we created in Step 1 above).
8. Under **Network > Interfaces > usbmodem > IPv4,** change the **Metric** to "1" (this sets the external USB modem as the primary modem).
9. Click **Save.**



NOTE: on firmware versions 18.8 or higher, you will also need to increase the ***Maximum number of interfaces*** from 1 to 2 under the ***Network -> Modems -> Modem*** section of the configuration. This enables the device to allow more than one active cellular connection at a time.



Single USB Modem Setup

Goal

To configure a cellular WAN interface on an Accelerated device using an external USB modem.

NOTE: *Accelerated's SR- and MX-series devices have USB ports.*

Setup

This article assumes the USB-driven connection will serve as the only WAN.

For this setup, you will need an active Internet connection on the supported USB modem.

NOTE: *Accelerated devices only support the following USB modems:*

Officially Supported:

- Sierra Wireless 340u (AT&T Beam)
- Sierra Wireless 313u (AT&T Momentum)
- Sierra Wireless 313u (T-mobile Unlocked Momentum)
- Aircard 320u (Telstra 4G)
- Novatel U620L (Verizon)
- Pantech UML290 (Verizon)
- Pantech UML295 (Verizon)

Sierra Wireless 340u note: The Beam is officially supported but under certain signal strength conditions we recommend they use the included USB extension cable that comes with the Beam Air Card

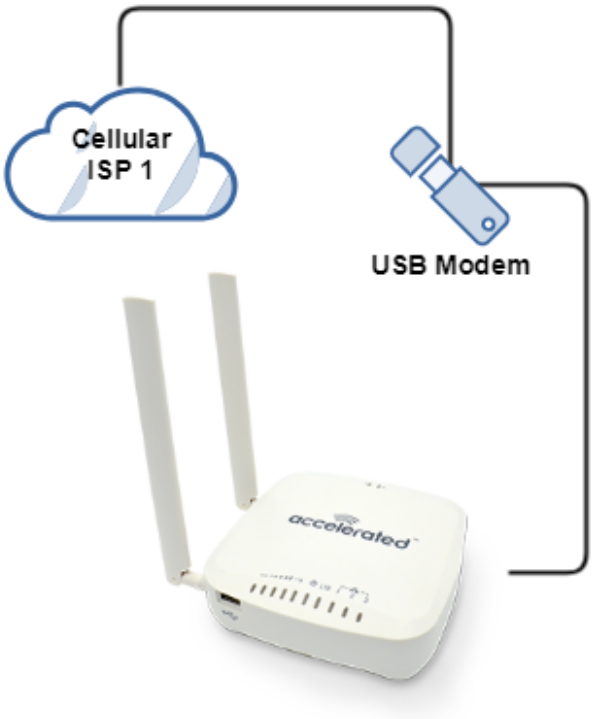
Supported, Modem Configuration Required*:

Netgear 341u (Sprint)

*Refer to our FAQ for More Information

Sample

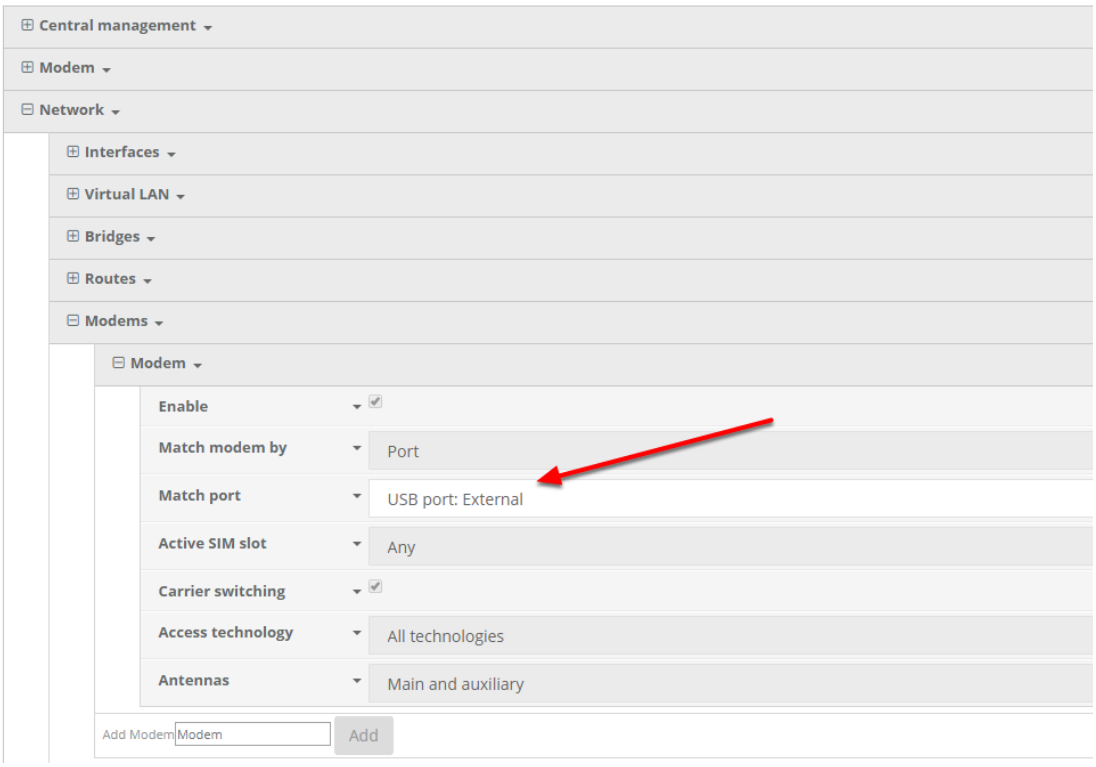
The sample configuration below shows an Accelerated device with a single cellular Internet connection using a supported USB modem.



Sample Single USB Modem aView Configuration

This sample single USB modem aView configuration sets the external USB as the primary modem. The internal 1002-CM modem will not be utilized.

1. Under **Network > Modems > Modem > Match port >** Choose "USB port: External."
2. Click **Save.**


Central management
Modem
Network
Interfaces
Virtual LAN
Bridges
Routes
Modems
Modem
Enable
Match modem by
Port
Match port
USB port: External
Active SIM slot
Any
Carrier switching
Access technology
All technologies
Antennas
Main and auxiliary
Add Modem
Modem
Add

Carrier-Specific APN List (firmware 18.4 and later)

Goal

To configure a customized APN list that will connect an Accelerated device to non-standard APNs based off of the cellular carrier associated with the SIM card.

NOTE: For a list of APNs automatically programmed into Accelerated's firmware settings, click here. The APNs on that list don't typically need to be programmed manually.

Setup

This article assumes that the the APN(s) being programmed in have been validated as the correct APN associated with an active SIM card. To create carrier-specific APN lists for multiple carriers, a new modem interface must be added and associated with the particular carrier.

The configuration steps described below covers how to assign a custom APN list to a configuration template in Accelerated View. It is important to keep in mind that the device connecting over a custom APN may require an alternative Internet connection (via its Ethernet WAN port) or a local configuration change before coming online to sync with its cloud template. Click here for more information about staging a device for initial connectivity.

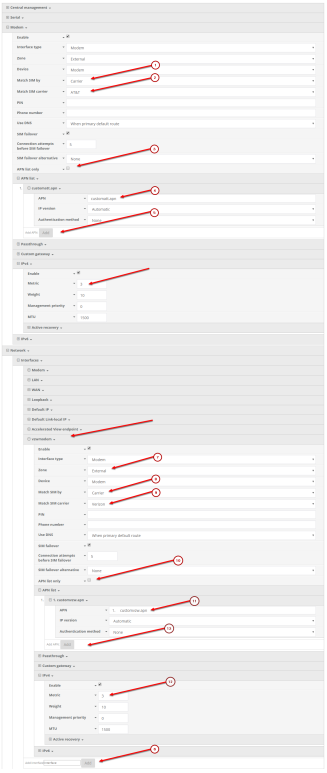
Sample

The sample configuration outlined below shows how to associate the default modem entry with one carrier (AT&T), and how to then create an additional modem interface associated with another carrier (Verizon). The custom APNs for each carrier are to be nested under the corresponding modem entry. While this example uses carrier detection to delineate between different APN lists, modem interfaces (and their associated APN lists) can instead be configured to specific SIM slots as needed.

Sample Configuration

NOTE: *You will need to know the custom APN for each SIM and/or Carrier. This is a sample configuration specifically utilizing AT&T and Verizon SIMs. Any other carrier SIM cards will not match this connection and will need to be configured with the corresponding Carriers and APNs.*

1. Under **Modem > Match SIM by,** choose "Carrier."
2. Under **Modem > Match SIM carrier,** choose the carrier matching the SIM card being inserted into the 1002-CM. In this example, it's "AT&T."
3. (Optional) Under **Modem > APN list only** can be checked to force the device to only try the APNs included in the list.
4. Under **Modem > APN list > APN**, type the APN. In this example, it's "customatt.apn." This will need to match the custom APN for the carrier specific SIM.
5. If an additional APN needs to be added, under **Modem > APN list >** add the additional APN by clicking **add** and type the additonal APN.
6. If multiple SIMs utilizing different carriers will be utilized, a second modem interface will need to be created under **Network > Interfaces > Add Interface**. In this example, it is "vzwmodem."
7. Under **Network > Interfaces > vzwmodem > Zone,** choose "External."
8. Under **Network > Interfaces > vzwmodem > Match SIM by,** choose "Carrier."
9. Under **Network > Interfaces > vzwmodem > Match SIM carrier,** choose the carrier matching the SIM card being inserted into the 1002-CM. In this example, it's "Verizon."
10. (Optional) Under **Network > Interfaces > vzwmodem > APN list only** can be checked to force the device to only try the APNs listed in the "APN list."
11. Under **Network > Interfaces > vzwmodem > APN list > APN**, type the APN. In this example, it's "customvzw.apn." This will need to match the custom APN for the carrier specific SIM.
12. Under **Network > Interfaces > vzwmodem > IPv4 > Metric,** change the **Metric** to match the metric from **Modem > IPv4.** In this case, it is "3." (Repeat this for **IPv6** if **IPv6** is being utilized)
13. If an additional APN needs to be added, under **Network > Interfaces > vzwmodem > APN list >** add the additional APN by clicking **add** and type the additional APN.



Carrier-Specific APN List (firmware 18.1 and prior)

Goal

To configure a customized APN list that will connect an Accelerated device to non-standard APNs based off of the cellular carrier associated with the SIM card.

NOTE: For a list of APNs automatically programmed into Accelerated's firmware settings, click here. The APNs on that list don't typically need to be programmed manually.

Setup

This article assumes that the the APN(s) being programmed in have been validated as the correct APN associated with an active SIM card.

The configuration steps described below covers how to assign a custom APN list to a configuration template in Accelerated View. It is important to keep in mind that the device connecting over a custom APN may require an alternative Internet connection (via its Ethernet WAN port) or a local configuration change before coming online to sync with its cloud template. Click here for more information about staging a device for initial connectivity.

Sample

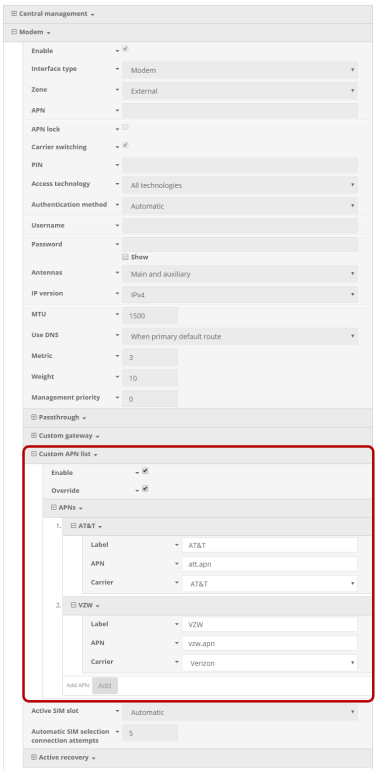
The sample configuration outlined below shows how to associate the default modem entry with one carrier (AT&T), and how to then create an additional modem interface associated with another carrier (Verizon). The custom APNs for each carrier are to be nested under the corresponding modem entry.

Sample Configuration

NOTE: *You will need to know the custom APN for each SIM and/or Carrier. This is a sample configuration specifically utilizing AT&T and Verizon SIMs. Any other carrier SIM cards will not match this connection and will need to be configured with the corresponding Carriers and APNs.*

1. Under ***Modem > Custom APN list***, select the checkbox next to ***Enable***.

2. (Optional) Selecting ***Override***, also nested under **Modem > APN list**, sets the device to *exclusively* attempt to connect using the APNs specified per the custom list. If left unselected, the custom APNs will be added to the start of the standard list of APNs referenced previously in this document (under the "Goals" section above).
3. Click the ***Add*** button to create a new APN entry for the list.
4. Enter a designation for the entry using the ***Label*** field. This does not have to match the APN
5. Specify the intended ***APN***.
6. Select the ***Carrier*** from the corresponding pull-down menu.
7. Create additional APN/ Carrier associations as necessary.
8. Click ***Save*** to finalize the changes.



Captive Portal Setup with open WiFi SSID

Difficulty level: *intermediate*

Minimum firmware: 18.8.14.37

Goal

To setup a captive portal authorization page that users must accept before gaining Internet access through an open WiFi SSID of the 63xx-series router.

Background

63xx-series routers provide a captive portal feature that can be applied to one or more SSIDs or LAN ports. Users can customize the logo and text presented on the captive portal, as well as setting up different types of authentication. The full list of available configuration options for a Captive Portal are:

- ***Interface***: the network interface to associate with the captive portal
- ***Session timeout:*** how long a user is authenticated before they must re-authorize through the captive portal
- ***Portal HTTP access***: Controls whether the captive portal authorization page can be accessed over HTTP, HTTPS, both, or redirected from HTTP to HTTPS
- ***Authorization***
  - simple click-to-accept and continue
  - username/password authentication - users are managed locally on the ACL router
    - Local User Management
  - required text info collection, and then click-to-accept
- ***Title:*** title shown at the top of the captive portal authentication page
- ***Message***: message shown under the title on the captive portal authentication page
- ***Terms and conditions***: the terms and conditions shown on the authentication page. The user must accept these terms in order to authenticate with the captive portal.
- ***Redirect to URL***: The website the user is redirected to after they authenticate with the Captive Portal

Setup

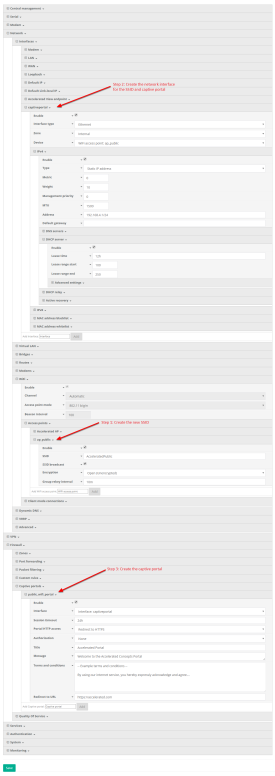
You will need to determine the SSID(s) or LAN networks you want to add the captive portal to before configuring the captive portal in 63xx-series router. For help with configuring a SSID, see the following article:

Add a New SSID

If you wish to apply the captive portal to multiple SSIDs and/or LAN ports, you will need to create a bridge and add those SSIDs/ports to the bridge, then assign that bridge to the network interface created for the captive portal.

Sample Configuration

The following configuration setting show a sample setup of an open SSID, a separate interface/ network for that SSID, and adding a captive portal to that SSID.



Demo WiFi connection and Captive Portal Auth

Two demos are listed below. The first shows a demo connection from a phone, the second from a Chromebook.

https://www.dropbox.com/s/jm7zrlshmg09yru/VID_20180809_142438748.mp4?dl=0

captive_portal_demo.webm

Change Port 2 from LAN to WAN for dual-wired-WAN

Difficulty level: ***intermediate***

Goal

To change the functionality of the 633x-MX router's port #2 from part of the LAN to be a WAN internet connection.

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).

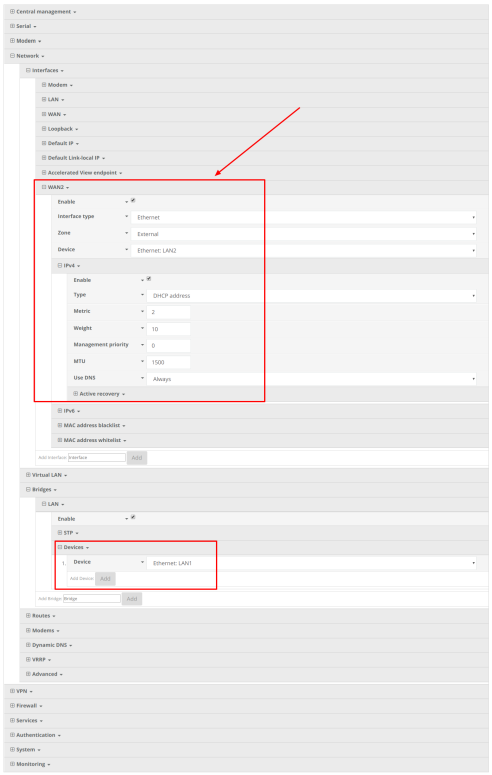
Configuration Steps

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

1. Under ***Network -> Interfaces*** , create a new interface called ***WAN2***
2. Set ***Network -> Interfaces -> WAN2 -> Zone*** to ***External***
3. ***Set Network -> Interfaces -> WAN2 -> Device*** to ***Ethernet: LAN2***
4. Under the new ***Network -> Interfaces -> WAN2 -> IPv4*** section, make the following changes:
    1. If a static IP address is needed for Internet connectivity on this port, enter in the static address and subnet in the ***Address*** field, and enter in the gateway for the static IP in the ***Default gateway*** field. If a static IP address is not necessary, which it typically is not, change ***Type*** to ***DHCP address***
    2. *Change **Metric** to **2**. This will setup port #2 of the 6330-MX to act as the backup wired-WAN Internet connection. The **WAN** port of the 6330-MX will remain the primary Internet connection.*
    3. *Optional:* setup failover or load balancing on the new WAN2 interface. See failover article here and load-balancing article here for reference, substituting the cellular modem for the WAN2 interface.

5. Under ***Network -> Bridges -> LAN -> Devices***, click the down-arrow next to ***Device*** *Ethernet: LAN2* and select ***Delete*** to remove port #2 from the LAN of the 6330-MX.

6. Save the configuration.



T-Mobile SIM with non-standard APN does not connect on Telit Modem [RESOLVED]

Goal

To establish a cellular connection using a custom T-Mobile APN that doesn't connect after the APN has been manually set on the device.

Setup

APNs that are not included on the standard firmware list must be programmed in manually before a device can properly join the intended cellular network. It has been observed that non-standard T-Mobile APNs (e.g. b2b.static) require an additional configuration change to establish a connection, specifically its MBIM context.

By following the sample configuration below, the required MBIM context can be automatically set using a custom script, allowing for seamless connectivity and carrier switching.

NOTE: *It is critical that the SIM being used has been verified as active, and that its intended APN has been confirmed. For guidance with setting custom APNs, please refer to the staging for initial connectivity instructions.*

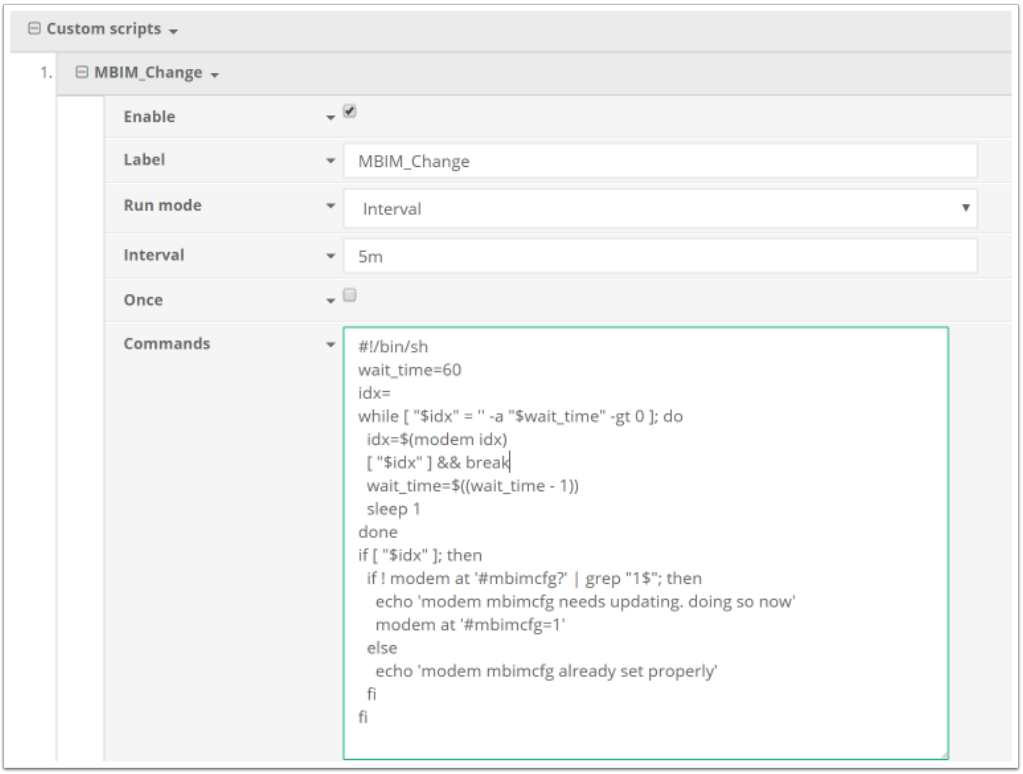
Sample Configuration

After programming in the custom APN, perform the following steps:

1. Under **System -> Scheduled Tasks -> Custom Scripts**, select ***add***.
2. Set a ***Label*** to identify the script (e.g. "MBIM_Change").
3. Change ***Run mode*** to "Interval."
4. Set ***Interval*** to "5m."
5. Paste the following script into the commands section:

```
#!/bin/sh
wait_time=60
idx=
while [ "$idx" = '' -a "$wait_time" -gt 0 ]; do
  idx=$(modem idx)
  [ "$idx" ] && break
  wait_time=$((wait_time - 1))
  sleep 1
```

```
done
if [ "$idx" ]; then
  if ! modem at '#mbimcfg?' | grep "1$"; then
    accns_log w 'modem mbimcfg needs updating. doing so now'
    modem at '#mbimcfg=1'
  fi
fi
```



Whitelisting Specific Domains

Goal

To configure network access such that only certain URLs are available to connected clients; domains not on the white list are blocked.

Setup

This article assumes that the only domains included on a user-defined white list are intended to be accessible.

For this setup, policy-based routes will be setup with two key rules:

1. Allow traffic out to the internet based on listed domains
2. Block all remaining outbound traffic

These two rules work together to restrict what destinations are reachable to client devices connected to the router.

NOTE: *It is critical that the rules are applied in the exact order outlined above (and described in the sample configuration below) -- the allow rule must precede the deny rule.*

This configuration requires firmware version 18.10.225.15 or higher.

Sample

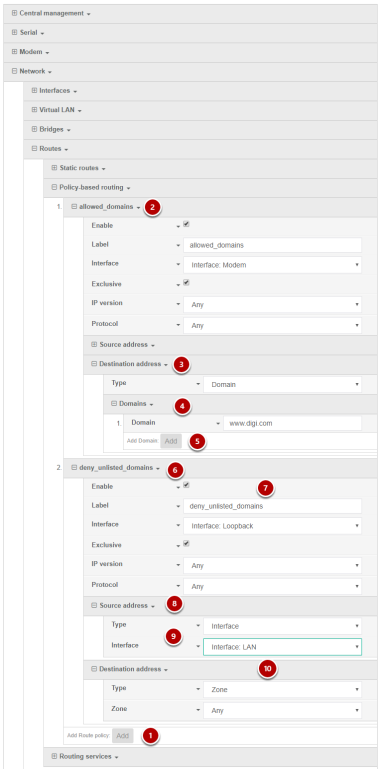
The sample configuration below shows an Accelerated device that can only browse to digi.com. Policy-based routing can also leverage firewall zones, IP addresses or device interfaces to create rules depending on what's selected as the source/ destination type.

Sample Domain Whitelist aView Configuration

1. Under ***Network > Routes > Policy-based routing*** click the ***Add*** button to create a new policy. This will house the list of allowed domains.
2. Enter/ confirm the following information for the new policy:
   - ***Label:*** a simple description of the rule.
   - ***Interface:*** the WAN interface being leveraged for the rule's intended scope (e.g. "modem" for the cellular connection versus "WAN" for the Ethernet ISP).

- ***Exclusive:*** leave checked to ensure that this policy must be enforced for traffic that falls within its scope; if unchecked, traffic is allowed to route out of alternative interfaces ***only*** if one is available in the event that the interface specified in the policy go down.
- ***IP version:*** leave as "any" unless otherwise required for network integration.
- ***Protocol:*** leave as "any" unless otherwise required for network integration.

3. Expand **Network > Routes > Policy-based routing > Destination address**.
4. Set the ***Type*** to "Domain" and then expand the ***Domains*** menu object.
5. Click the ***Add*** button and enter the URL intended to be white listed. Repeat as needed for additional domains.
6. Under ***Network >Routes > Policy-based routing*** click the ***Add*** button once again to create a second policy. This will establish the deny rule for all non-listed domains.
7. Enter/ confirm the following information for the new policy:
   - ***Label:*** a simple description of the rule.
   - ***Interface:*** select "Loopback" to prevent packets headed for any non-listed domain from reaching the internet.
   - ***Exclusive:*** leave checked to ensure that this policy must be enforced for traffic that falls within its scope; if unchecked, traffic is allowed to route out of alternative interfaces ***only*** if one is available in the event that the interface specified in the policy go down.
   - ***IP version:*** leave as "any" unless otherwise required for network integration.
   - ***Protocol:*** leave as "any" unless otherwise required for network integration.
8. Expand the ***Source address*** entry under the policy created in step #7 and set the ***Type*** to "Interface."
9. Select "LAN" from the ***Interface*** pulldown menu.
10. Expand the ***Destination address*** and confirm that ***Type*** is set to "Zone" and ***Zone*** is set to "Any."
11. Click ***Save*** to finalize the configuration changes.


Central management
Serial
Modem
Network
Interfaces
Virtual LAN
Bridges
Routes
Static routes
Policy-based routing
1.
allowed_domains
2
Enable
Label
allowed_domains
Interface
Interface: Modem
Exclusive
IP version
Any
Protocol
Any
Source address
Destination address
3
Type
Domain
Domains
4
1.
Domain
www.digi.com
Add Domain
Add
5
2.
deny_unlisted_domains
6
Enable
7
Label
deny_unlisted_domains
Interface
Interface: Loopback
Exclusive
IP version
Any
Protocol
Any
Source address
8
Type
Interface
9
Interface
Interface: LAN
Destination address
10
Type
Zone
Zone
Any
Add Route policy:
Add
1
Routing services

SIM Failover Script for Data Throttling

Design

This creates a rudimentary, but stable, data plan throttle that will force a failover to SIM2 if it detects SIM1 has gone over its monthly data usage limit. This is achieved by leveraging the data usage API available on aView. The main benefit is the API tracks data usage across reboots, so we can accurately measure the data usage over time.

This feature is implemented using two custom scripts. See example setup below. Note that the user must specify their API token in the data_throttle custom script. They can also adjust the data limit (default is 100MB) and the rollover day for the data plan (default is the first day of the month).

If the data plan limit is reached for the month, this script will force a failover to SIM2 by default. Similarly, when the device is within/under its data plan limit for the month, this script will failback to SIM1.

Config Setup

Create a new custom script under ***System -> Scheduled tasks -> custom scripts***, and enter in the following. The top three lines should be adjusted to put in the users API token from aView, the desired data plan limit in bytes, and the rollover day of the month (2-digits).

Keep in mind that each user in aView only gets 100 API requests every 15 minutes, so don't adjust this interval down so low to the point that the user runs out of API queries (e.g. running this script on 100 devices every 5 minutes equals 300 requests per 15-min, which is more than the API limit).

```
usage_limit='100000000'   # 100MB
rollover_day='01'  # pick day of month 01-31 to choose when data plan resets
api_token='xxxxxxxxxx'
SIM_to_monitor='1'
mac=$(runt get system.mac)
intf=$(runt dump network.modem | grep intf | tail -n 1 | cut -f2 -d'=') # 18.1 or older
firmware
[ -n "$intf" ] || intf=$(runt dump mm.bearer | grep intf | tail -n 1 | cut -f2 -d'=')
# 18.4 or higher firmware
[ -n "$intf" ] || intf='wwan0'  # default cellular interface

bugout() {
  accns_log w config "$@"
  exit
}
```

```
var_is_number(){
  [ -n "$1" ]  || return 1
  case $1 in
    ''|*[!0-9]*) return 1 ;;
    *) return 0 ;;
  esac
}

# Main
end_date=$(date "+%Y-%m-%d")
cur_year=$(date "+%Y")
cur_month=$(date "+%m")
if [ "$rollover_day" -lt "$(date +%d)" ]; then
  start_date="$cur_year-$cur_month-$rollover_day"
else
  case "$cur_month" in
    01)
      last_year=$((cur_year - 1))
      start_date="$last_year-12-$rollover_day"
      ;;
    02|03|04|05|06|07|08|09|10)
      last_month=$((cur_month - 1))
      start_date="$cur_year-0$last_month-$rollover_day"
      ;;
    *)
      last_month=$((cur_month - 1))
      start_date="$cur_year-$last_month-$rollover_day"
      ;;
  esac
fi

#We are monitoring SIM 1, as noted in the SIM_to_monitor variable above. If using
another SIM slot, don't monitor data usage.
[ "$(sim)" = "$SIM_to_monitor" ] || exit

url="https://aview.accns.com/api/v4/devices/usage.json?auth_token=${api_token}&
device_id=${mac}&start_date=${start_date}&end_date=${end_date}&interface=${intf}"

request_result=$(curl -kL -w %{http_code} -sfo /tmp/results.txt $url)

[ "$request_result" -eq '200' ] || bugout "error obtaining cellular usage from aView
API ($request_result)"

upload_usage=$(grep -o "upload\":[0-9]\{1,12\}"  /tmp/results.txt | cut -f2 -d':' | awk
'{s+=$1} END {print s}')
download_usage=$(grep -o "download\":[0-9]\{1,12\}" /tmp/results.txt | cut -f2 -d':' |
```

```
awk '{s+=$1} END {print s}')

usage=$((upload_usage + download_usage))
var_is_number "$usage" || bugout "Usage not available from aView API ($upload_usage,
$download_usage)"

if [ "$usage" -ge "$usage_limit" ]; then
  sim_slot=2
  [ "$(sim)" = 2 ] && sim_slot=1
  accns_log w config "Data usage limit exceeded ($usage out of $usage_limit bytes).
Switching to SIM slot $sim_slot."
  sim $sim_slot
fi
```

Create a new custom script under ***System -> Scheduled tasks -> custom scripts***, and enter in the following. The "rollover day" should be adjusted to put in the rollover day of the month (2-digits).

```
#!/bin/sh

# don't check for SIM preference if the modem is not connected, as we
# may be going through our normal connection/APN-selection process
modem cli 2> /dev/null | grep -q "'connected'" || exit

# Only run this script on a certain day of the month
rollover_day='01'
current_day="$(date +%d)"
```

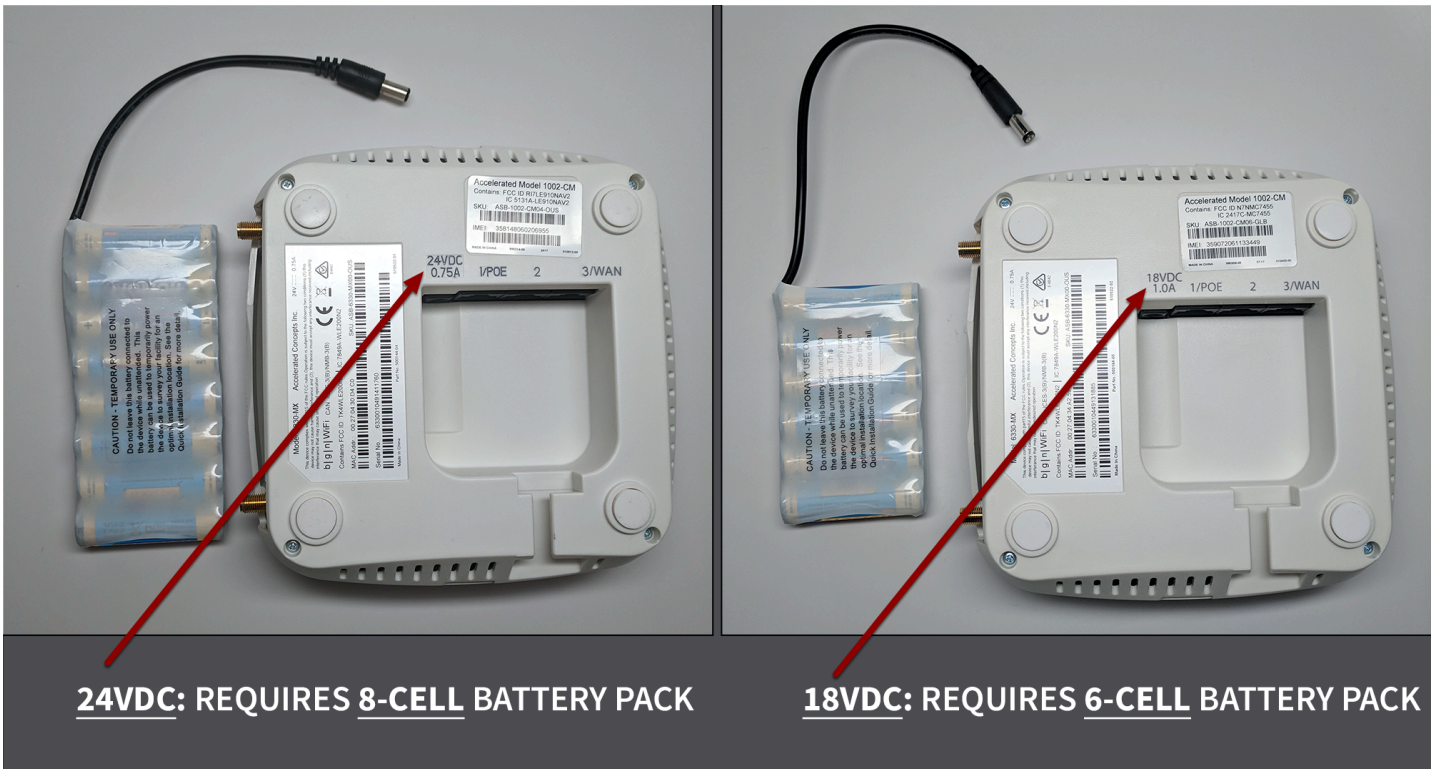
```
[ "$rollover_day" = "$current_day" ] || exit

# Prefer SIM slot 1.  If we're connected with SIM slot 2, switch back to slot 1
if [ "$(sim)" = 2 ]; then
  accns_log w config "Preferred SIM not detected. Switching to SIM slot 1."
  sim 1
fi
```

MX-Series Battery Pack Variations

Initial production runs of the MX-series cellular routers (6330s and 6335s) have a different power requirement than the standard 18V DC that is officially listed. The first wave of MXs are labeled accordingly, showing a 24VDC label above its power port.

The battery pack included with the MX Remote Mounting Kit (RMK) will differ slightly to reflect the increased power draw of units from the initial builds. As depicted below, the 24V MXs require an 8-cell battery pack compared to the 6-cell standard that's included for subsequent, 18V MXs.

This battery is intended to serve as a temporary power source for "site surveys" performed during the installation of the MX cellular router. They cannot be recharged, nor will they serve as a battery backup for power failures; the cells are disposable after depletion.



NOTE: *The smaller, 6-cell battery pack will* ***NOT*** *power the 24V version of the MX.*

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.

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
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 per status/interval	Notes	Protocol/port used
Syslog check-in	Every 30 minutes	1KB	Used for reporting and alerts	UDP 514 (syslog)
Configuration check-in	Once nightly -- 1am (UTC)	12KB	Recommended for remote management	TCP 443 (HTTPS)
Boot-up sequence	Each device reboot	24KB	Used for reporting and remote management	UDP 123 (NTP) UDP 514 (syslog)
Device firmware upgrade	As needed (~8 releases per year)	10MB	Updates device firmware upon new release	TCP 443 (HTTPS)
Modem firmware upgrade	As needed (less frequent than device firmware updates)	60MB	Updates firmware on the embedded cellular modem	TCP 443 (HTTPS)
Remote control tunnel	Always-on, if enabled	25MB per month	Minimum keep-alive traffic	UDP 500 and 4500 (IPSec)

Accelerated View Ports and URL Access

IP Address

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

18.213.16.77 with Ports (UDP: 500/4500 IPSec)

URLs

time.accns.com; logs.accns.com; syslog.accns.com; certs.accns.com; configuration.accns.com; remote.accns.com;ipsec.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 Cellular Extender** 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

x.ispsn

Cellular Support Info by Country

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

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:

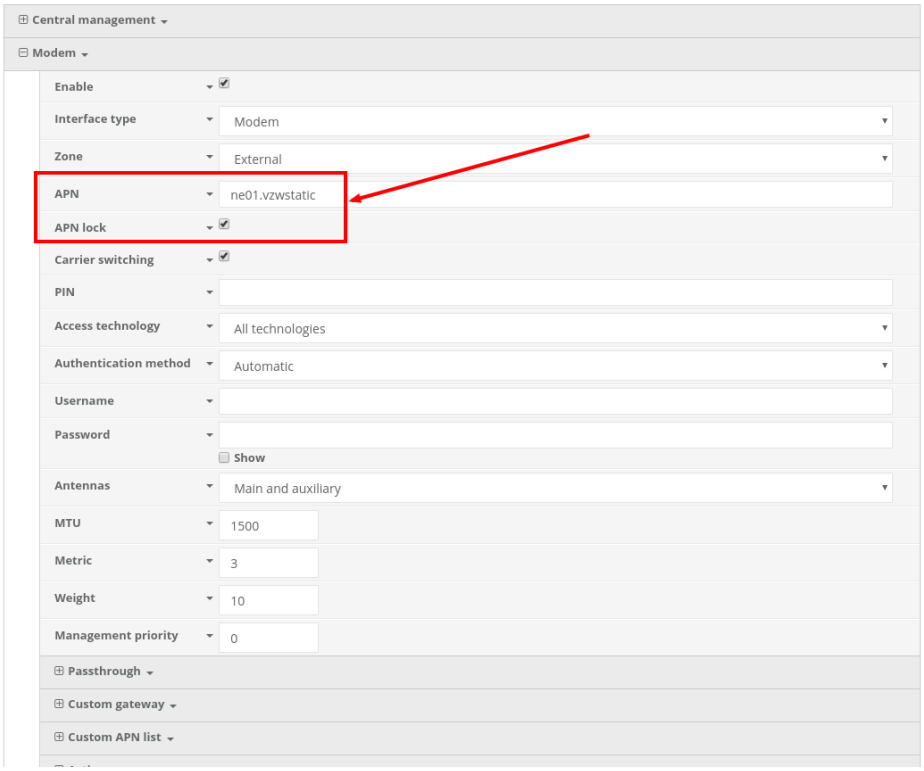
http://kb.accelerated.com/m/67105/l/729960-getting-started-with-accelerated-view#UpgradingFirmware

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

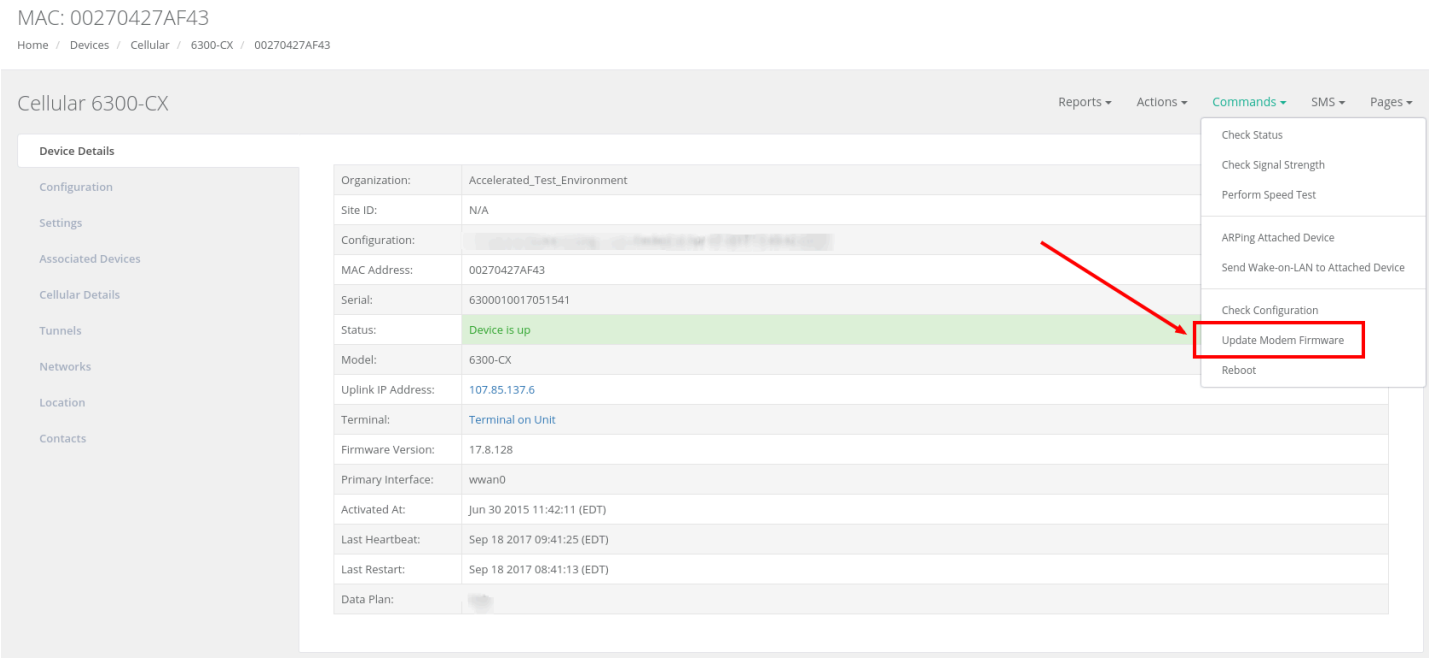
There are several options for upgrading the firmware on the modem inside your 63xx-series router. Users can upgrade the firmware on this modem either through the Accelerated View portal or the local web UI of the 63xx-series router, depending on the level of access and network connectivity the LTE router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

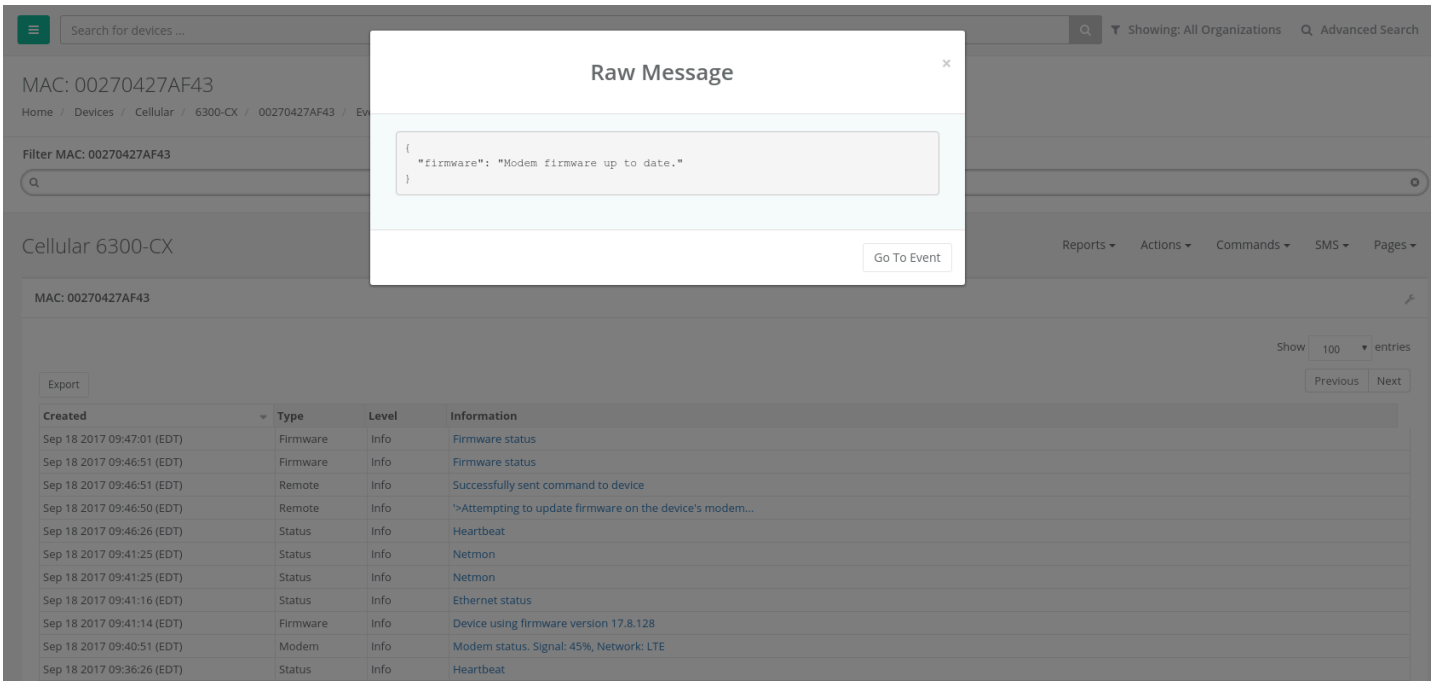
Option 1 - OTA command

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.



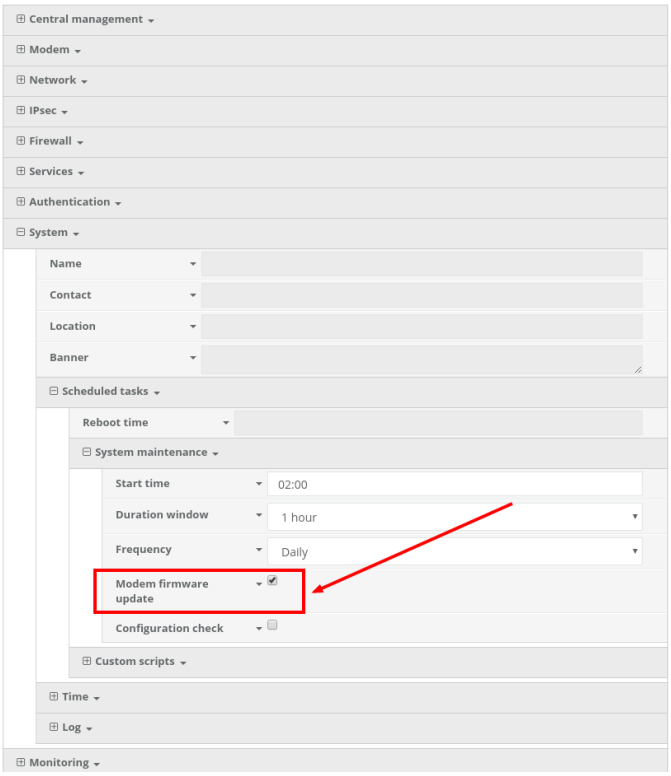
This command will trigger the 63xx-series router to query the Accelerated firmware server. If a newer modem firmware version is found for the current carrier-specific firmware used on the modem in the 63xx-series router, the 63xx-series router will automatically download the new firmware and flash it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



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

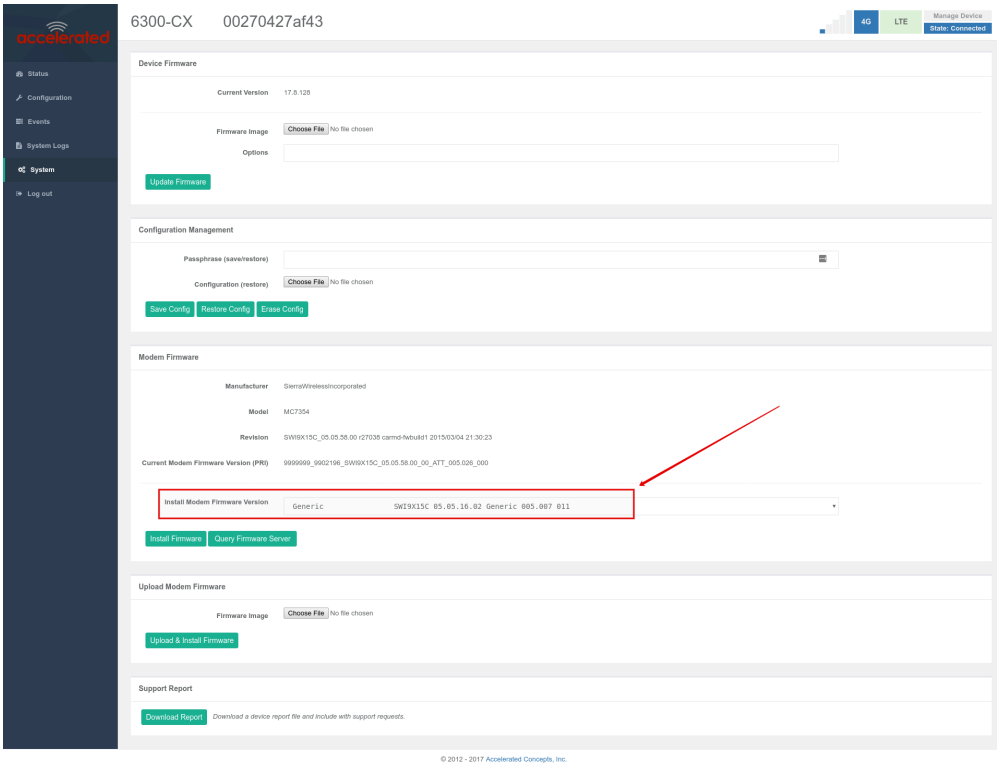
Upgrading the modem firmware using any of the following options requires the user to directly access the web UI of the 63xx-series router.

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.



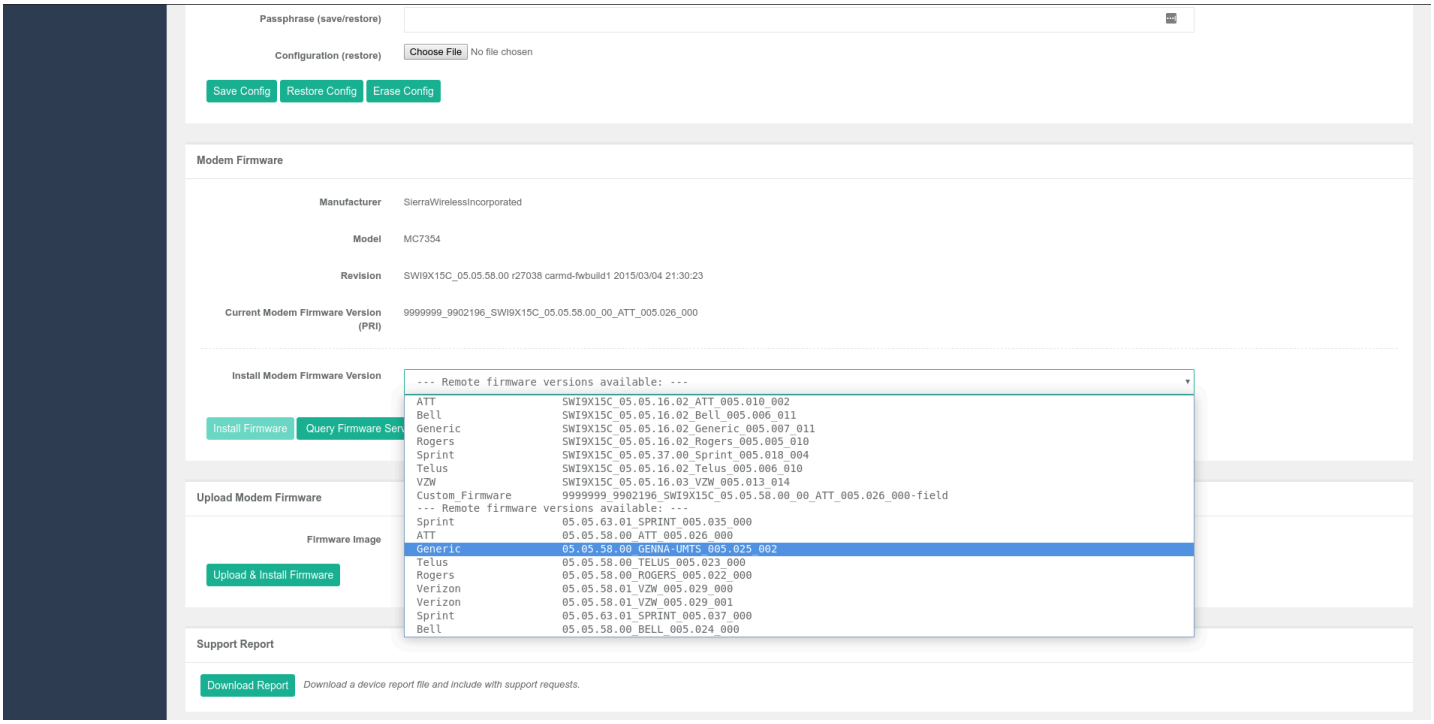
Option 2 - Query Firmware Server

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:

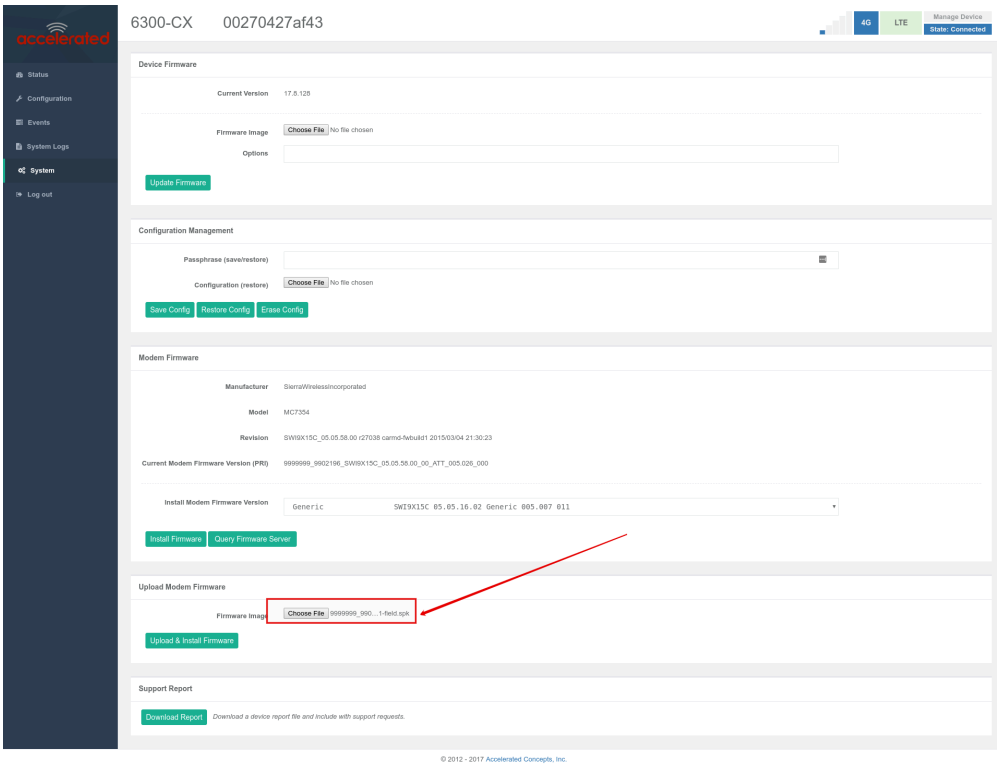
1. Click on the ***Query Firmware Server*** button.
2. Once the query completes, the drop-down will list the available remote firmware versions.
3. Select the desired firmware version from the list
4. Click the ***Install Firmware*** button. A progress bar will appear indicating the status of the modem's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



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
4G LTE
Manage Device
State: Connected
Status
Configuration
Events
System Logs
System
Log out
Device Firmware
Current Version 17.8.128
Firmware Image Choose File No file chosen
Options
Update Firmware
Configuration Management
Passphrase (save/restore)
Configuration (restore) Choose File No file chosen
Save Config
Restore Config
Erase Config
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
Install Firmware
Query Firmware Server
Upload Modem Firmware
Firmware Image Choose File 9999999_990...1-field.spk
Upload & Install Firmware
Support Report
Download Report
Download a device report file and include with support requests.
© 2012 - 2017 Accelerated Concepts, Inc.

Internet connection over Huawei E8372 (T-Mobile) USB modem

Difficulty level: ***Intermediate***

Goal

Configure an Accelerated 63xx-series router to use the Huawei E8372 modem for Internet connectivity.

This setup requires a WiFi-enabled 63xx-series router from Accelerated with a USB port. The current available models that provide these features are listed below:

- 6350-SR
- 6330-MX

Setup

Before configuring the 63xx-series router, perform the following setup:

1. Note the WiFi SSID and passphrase printed on the E8372 modem.
2. Connect the E8372 to the USB port of the 63xx-series router.
3. Power on the 63xx-series router.

Next, make the following configuration changes on the 63xx-series router to provision the device to connect to the E8372's WiFi network and use it as a WiFi-as-WAN internet connection.

1. Deselect ***Enable central management*** and click ***Save***. This is required in order to locally display the full range of configuration options. This can be re-enabled later once the 63xx-series router is online, be please ensure you make the same config changes mentioned below on the devices configuration profile in aView. Here is a link detailing how users configure a device in aView.
2. Under ***Network -> WiFi -> Channel***, select the channel used by the E8372 modem'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 -> WiFi -> Access points*** config options, you do not need to specify a specific wireless channel, and can instead leave this ***Channel*** option set to ***Automatic.***
3. Under ***Network -> WiFi -> Client mode connections***, create a new entry named ***huawei***. The name can be different if desired.
4. Under the new client mode connection entry, enter in the SSID and authentication credentials for the SSID of the E8372 modem.

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

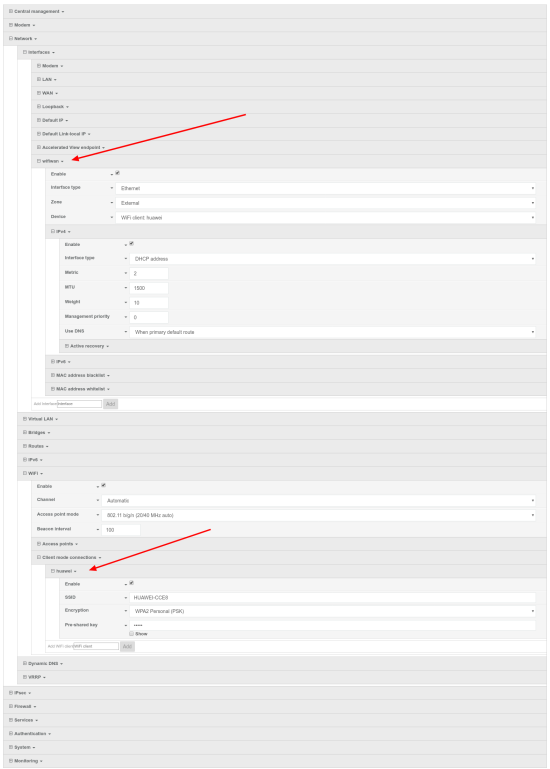
1. Set the ***Zone*** for the new interface to ***External***.
2. Set the ***Device*** for the new interface to ***WLAN Client: huawei***
3. Under ***IPv4***, set the ***Interface type*** to ***DHCP address***.
    1. *NOTE:* This will trigger the 63xx-series router to obtain a DHCP connection to the E8372 modem'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***.

After applying these changes to the 63xx-series router, it will authenticate to the E8372's SSID and use the WiFi connection for Internet access.

If you need to make any configuration changes to the Huawei E8372 modem, the suggested method is to connect to the E8372 modem's SSID with a laptop, and access the web UI of the modem. Resources for accessing and configuring the E8372 modem can be found in the links below.

http://consumer.huawei.com/en/mobile-broadband/e8372/

https://images.wirelessdealer.ca/images/phones/userguide3967.pdf



Please note that with the above setup, the 63xx-series router is treating this E8372 connection as a WiFi-as-WAN connection, and not a direct cellular connection. This means that the 63xx-series router will not

display any cellular-related details about the E8372 (e.g. signal strength, network type, etc.). To find this information, a user would have to access the web UI of the E8372 modem itself.

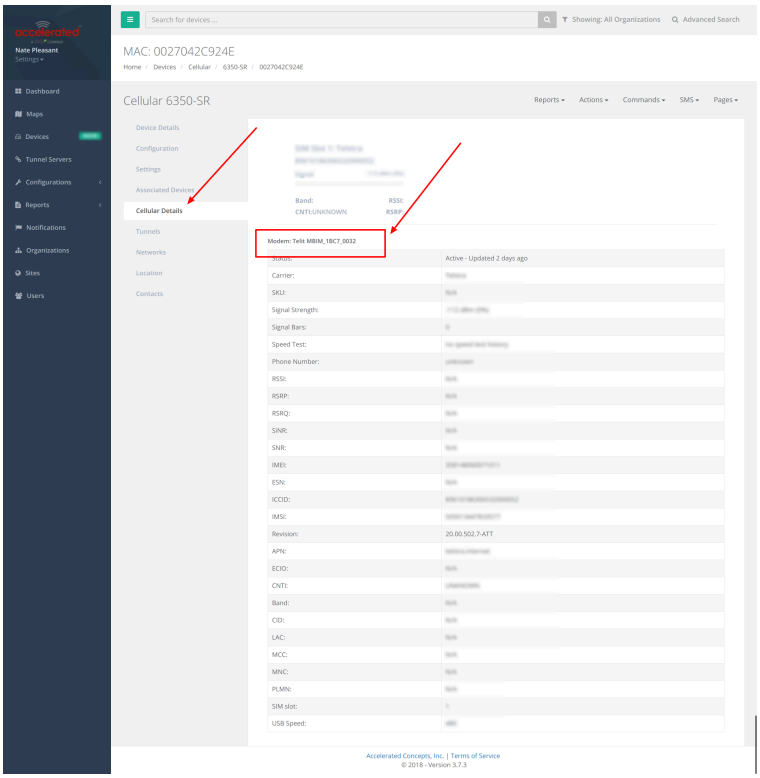
AT&T/T-Mobile SIM unable to connect with 1002-CM04 plug-in modem

Problem

An Accelerated 63xx-series router is unable to establish a 4G LTE cellular connection when using an AT&T or T-Mobile SIM card and 1002-CM04 plug-in modem.

This issue only affects 63xx-series devices utilizing the 1002-CM04 plug-in modem variant. The 1002-CM03 and 1002-CM06 modules do not experience this issue, and can connect reliably on LTE with AT&T/T-Mobile SIM cards. To check if your 63xx-series router is using a 1002-CM04 modem, navigate to the ***Cellular Details*** tab for the device in Accelerated View, or to the ***System*** tab of the 63xx-series router's local web UI. Look for the modem model. The 1002-CM04 modem is listed with the following model name:

Telit MBIM_1BC7_0032



Background

The 1002-CM04 performs additional pre-registration steps when connecting to AT&T or T-Mobile's LTE network, which can interfere with the 63xx-series router's timing on establishing a cellular connection. The result is intermittent or no connectivity on AT&T's LTE network.

Solution

Firmware versions 18.4.54.22 or higher resolves the connectivity issues on the 1002-CM04 module with AT&T/T-Mobile SIMs. You can use the following instructions to upgrade a 63xx-seris router to the new 18.4.54.22 firmware:

https://kb.accelerated.com/m/67492/l/815080-updating-firmware#managing-the-device-locally

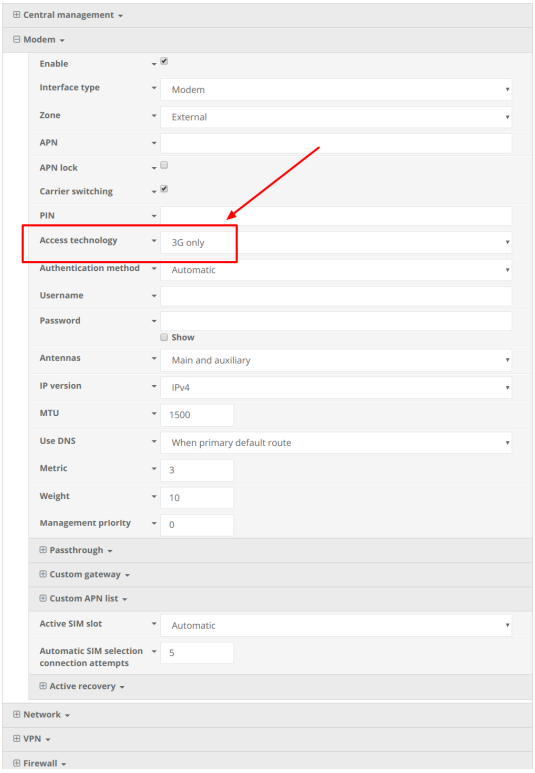
Manual Solution

Before implementing this manual solution, please ensure your 63xx-series router is running firmware version 17.8.128.64 or higher.

Users can lock the 63xx-series router to 3G only. This allows the 63xx-series router to reliably establish a cellular connection with an AT&T/T-Mobile SIM and 1002-CM04 module, albeit on a possibly slower 3G connection.

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

1. In ***Modem -> Access technology***, set the value to ***3G***.


Central management
Modem
Enable
Interface type
Modem
Zone
External
APN
APN lock
Carrier switching
PIN
Access technology
3G only
Authentication method
Automatic
Username
Password
Show
Antennas
Main and auxiliary
IP version
IPv4
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
VPN
Firewall

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

Support Report Overview

Generating a Support Report

Support reports provide a snapshot of a device's current settings and connection status at the time of the report's generation. The relevant log files are packaged into a .bin file that can be downloaded from the ***local*** (Web) UI of all Accelerated devices. For more information about generating support reports, please click here.

NOTE: *Information logged on the device will be erased when the device is powered off/ rebooted to avoid unnecessary wear to the flash memory. Click here for more information on how to enable persistent system logs.*

Use 7-Zip or any other file-archiving utility to extract a support report. Its contents are organized into the following directories:

/etc

This folder most notably contains a running list of the cellular connections that have been registered by the device's radio.

Directory	File Name		Notes
/etc			
	version		Active firmware version
	config/ mm.json		Cellular connections logged as having been engaged by the radio; establishes previous APN associations

/opt

Information stored here persists between reboots and system resets.

Directory	File Name		Notes
/opt			
	log_last/ messages		With persistent system logs enabled, syslog info will be stored in the /opt directory which isn't erased after reboots or system resets

/tmp

Output from a series of diagnostic queries is stored in a randomly generated sub-directory within /tmp. When combing through these logs, pay particular attention to ***config_dump-public*** (to verify local device settings) and ***mmcli-dump*** (to validate the cellular connection status).

Directory	File Name		Notes
/tmp/#*			*# is generated at random
	arp_-nv		The table of IP-address to MAC-address translations used by the address resolution protocol (ARP)
	arptables_-nvv_-L		The tables of ARP packet filter rules in the Linux kernel
	cat_procmeminfo		A breakdown of memory utilization at the time when the support report was generated
	cat_procslabinfo		Frequently used objects in the Linux kernel (buffer heads, inodes, dentries, etc.) have their own cache, contained in this output
	config_dump-public		The device's current settings, scrubbed of passwords and preshared keys
	conntrack_-L		A list of all currently tracked connections through the system
	conntrack_-S		A summary of currently tracked connections
	date		Local system time. If the device isn't online when the support report is generated, the date will be based on the date/month/year that the firmware running on the device was created (e.g. 18.4.54.41 was created 2018-07-05)
	df_-h		A report of the file system disk space usage
	event_list		A list of events leveraged for syslog messages
	fw_printenv		The entire environment for the bootloader U-Boot
	ip_addr_list		IP addresses listed per interface
	ip_route_list		Default routing information per interface
	ip6tables_-nv_-L		A list of IPv6 routing tables

Directory	File Name		Notes
	ip6tables_-nv_-L_-t_mangle		Firewall table used when handling mangled/fragmented IPv6 packets
	ip6tables_-nv_-L_-t_nat		Firewall table used to direct NAT'd traffic
	iptables_-nv_-L		A list of IPv4 firewall tables
	iptables_-nv_-L_-t_mangle		Firewall table used when handling mangled/fragmented IPv4 packets
	iptables_-nv_-L_-t_nat		Firewall table used to direct NAT'd traffic
	ls_-RlhA_etcconfig		An index of items in /etc/config (and its sub-directories)
	ls_-RlhA_opt		An index of items in /opt (and its sub-directories)
	ls_-RlhA_tmp		An index of items in /tmp (and its sub-directories)
	ls_-RlhA_var		An index of items in /var (and its sub-directories)
	lsusb		A list of USB ports and any connected peripherals
	mmcli-dump		A repository of critical information about the cellular radio based off of the cited modem-manager output and defined set of AT commands
	netstat_-i		Interface statistics for transmitted/ received packets
	netstat_-na		List of both listening and non-listening network sockets on the device
	netstat_-s		A statistical summary of network traffic broken down by protocol
	ps_l		A snapshot of the current processes running at the time of generating the report
	runt_json		Storage for active/ engaged system variables
	sprite_config_dump		Not used for cellular devices
	ubus-dump		A log of ubus calls for network devices and interfaces
	uptime		The device's uptime at the time of generating the report, along with CPU load averages for the past 1, 5, and 15

Directory	File Name		Notes
			minutes

/var/log

The running system log is stored in "messages" until reaching a set line count (1,000 lines by default). Once this limit is exceeded, that file is renamed to "messages.0" and a new running log is written to the now-empty "messages" log.

Directory	File Name		Notes
/var/log			
	messages		Current syslog information
	messages.0		Rollover syslog information

/var/run

This directory can be disregarded for most troubleshooting/ diagnostic purposes.

Directory	File Name		Notes
/var/run			
	All files		Runtime settings for the device -- referenced in the syslog data gathered in /tmp (see above)

Standard APNs

Accelerated's APN List

Each carrier has a set of default Access Point Names (APNs) for their network. Accelerated automatically attempts to establish a connection using the below default APNs. If your carrier has provided you with a custom APN, it will need to be programmed into the device's configuration before connecting to the cellular network as intended.

NOTE: *For assistance with initial cellular connectivity using non-standard APNs, please click here.*

AT&T

- 10008
- i2gold
- 11226.mcs
- MNS-OOB-APN01.com.attz
- altaworx02.com.attz
- m2m.com.attz
- 11904.mcs
- broadband

Verizon

- mw01.vzwstatic
- ne01.vzwstatic
- so01.vzwstatic
- we01.vzwstatic
- vzwinternet

T-Mobile

- fast.t-mobile.com
- epc.tmobile.com
- internet.t-mobile

Sprint

- r.ispsn
- n.ispsn

Rogers

- ltemobile.apn
- lteinternet.apn
- ltestaticip.apn
- ltepublicip.apn
- ltemobile.com

Bell Canada

- crmstatic.bell.ca

Telstra Australia

- telstra.internet
- telstra.m2m

Vodafone

- live.vodafone.com (Australia)
- wbb.attbusiness.net (Netherlands)

Other

- blank
- 10008
- i2gold
- 11226.mcs
- MNS-OOB-APN01.com.attz
- altaworx02.com.attz
- 11904.mcs
- m2m.com.attz
- broadband
- mw01.vzwstatic
- ne01.vzwstatic
- so01.vzwstatic
- we01.vzwstatic
- vzwinternet
- telstra.internet
- fast.t-mobile.com
- epc.tmobile.com
- mobinilweb
- web.vodafone.de

- everywhere
- internet.com
- inet.bell.ca
- isp.telus.com
- internet.telecom.co.nz
- inetgsm.vzw3g.com
- isp.cingular
- internet
- everywhere
- ltemobile.apn

Default Service Provider List

Accelerated devices leverage ModemManager to control the device's cellular radio. This software includes a list of APNs associated with "default service providers" that the device will attempt to connect with should it fail to join a cellular network using Accelerated's APN list.

NOTE: *If both the Accelerated and Default Provider list fail to yield a successful connection, the device will continue cycling through these APNs until joining a cellular network. Devices can be locked to specific APNs as necessary to prevent this behavior.*

Default APNs by Service Provider

country code	carrier	plmnid	iccid prefix	apn	connection type	d
ad	Andorra Telecom (Mobiland)	21303	8937603	internetand	internet	dr
ad	Andorra Telecom (Mobiland)	21303	8937603	internetclic	internet	dr
ae	Etisalat	42402	8997102	mnet	internet	dr 19
ae	Etisalat	42402	8997102	etisalat.ae	internet	dr
ae	Etisalat	42402	8997102	etisalat	mms	dr
ae	Etisalat	42402	8997102	etisalat	mms	dr

ae	du	42403	8997103	du	internet	dr
ae	du	42403	8997103	du	mms	dr
af	AWCC	41201	899301	internet	internet	dr
al	Vodafone	27602	8935502	Twa	internet	dr
al	Vodafone	27602	8935502	vodafoneweb	internet	dr
al	Vodafone	27602	8935502	mms	mms	dr
al	Vodafone	27602	8935502	portalnmms	mms	dr
am	Beeline	28301	8937401	internet.beeline.am	internet	dr
am	Beeline	28301	8937401	mms.beeline.ua	mms	dr
am	Beeline	28301	8937401	mms	mms	dr
am	Orange	28310	8937410	internet.orange	internet	dr
am	Orange	28310	8937410	internet	internet	dr
am	Orange	28310	8937410	mms	mms	dr
am	Orange	28310	8937410	orangemms	mms	dr
am	Orange	28310	8937410	mms	mms	dr
am	Orange	28310	8937410	orange.mms	mms	dr
am	Orange	28310	8937410	orangemms	mms	dr
am	Orange	28310	8937410	mms.orange.dk	mms	dr
am	Orange	28310	8937410	mms.orange.md	mms	dr
am	Orange	28310	8937410	mms.orange.jo	mms	dr
am	Orange	28310	8937410	orangerun.acte	mms	dr
am	VivaCell/MTS	28305	8937405	connect.vivacell.am	internet	dr
am	VivaCell/MTS	28305	8937405	inet.vivacell.am	internet	dr
am	Karabakh Telecom	28304	8937404	connect.kt.am	internet	dr
ao	Unitel	63102	8924402	internet.unitel.co.ao	internet	dr

ao	Unitel	63102	8924402	unitel	mms	dr
ar	Personal	722341 72234	8954341 895434	gprs.personal.com	internet	dr 17
ar	Personal	722341 72234	8954341 895434	datos.personal.com	internet	dr
ar	Arnet	722340	8954340	arnet.personal.com	internet	dr 17
ar	Arnet	722340	8954340	mms	mms	dr
ar	Arnet	722340	8954340	mms	mms	dr
ar	Claro	722310 722320 722330	8954310 8954320 8954330	gprs.claro.com.ar	internet	dr 17
ar	Claro	722310 722320 722330	8954310 8954320 8954330	internet.ctimovil.com.ar	internet	dr
ar	Claro	722310 722320 722330	8954310 8954320 8954330	mms.claro.com.br	mms	dr
ar	Movistar	722010 722070	8954010 8954070	internet.gprs.unifon.com.ar	internet	dr
ar	Movistar	722010 722070	8954010 8954070	internet.gprs.unifon.com.ar	internet	dr
at	A1/Telekom Austria	23201	894301	a1.net	internet	dr 19
at	A1/Telekom Austria	23201	894301	aon.data	internet	dr
at	A1/Telekom Austria	23201	894301	aon.at	internet	dr
at	A1/Telekom Austria	23201	894301	free.A1.net	mms	dr
at	ABroadband	23201	894301	mdata.com	internet	dr
at	Bob	23211	894311	bob.at	internet	dr

at	Bob	23211	894311	bob.at	internet	dr 19
at	Bob	23211	894311	mms.bob.at	internet	dr
at	Bob	23211	894311	mms.bob.at	mms	dr
at	HoT	23207	894307	webaut	internet	dr
at	HoT	23207	894307	mmsaut	mms	dr
at	Lycamobile	23208	894308	data.lycamobile.at	internet	dr
at	T-Mobile	23203	894303	gprswap	wap	dr
at	T-Mobile	23203	894303	gprsinternet	internet	dr 21
at	T-Mobile	23203	894303	business.gprsinternet	internet	dr
at	T-Mobile	23203	894303	general.t-mobile.uk	mms	dr
at	T-Mobile	23203	894303	wap.voicestream.com	mms	dr
at	tele.ring	23207	894307	web	internet	dr 21
at	tele.ring	23207	894307	mms	mms	dr
at	Orange	23205	894305	web.one.at	internet	dr 19
at	Orange	23205	894305	wap.one.at	wap	dr
at	Orange	23205	894305	mms.one.at	mms	dr
at	Orange	23205	894305	fullspeed	internet	dr
at	Orange	23205	894305	orange.web	internet	dr 19
at	Orange	23205	894305	orange.mms	mms	dr
at	Drei (3)	23210	894310	drei.at	internet	dr 21
at	Drei (3)	23210	894310	drei.at	mms	dr
at	Drei (3)	23210	894310	three.co.uk	mms	dr

at	Drei (3)	23210	894310	mobile.three.com.hk	mms	dr
at	Drei (3)	23210	894310	3services	mms	dr
at	Drei (3)	23210	894310	3mms	mms	dr
at	Yesss	23212	894312	web.yesss.at	internet	dr
at	VOLmobil	23203	894303	volmobil	internet	dr
at	VOLmobil	23203	894303	gprsmms	mms	dr
au	Amaysim	50502	896102	internet		dr
au	Amaysim	50502	896102	mms	mms	dr
au	Apex Telecom	50502	896102	splns357		dr
au	Beagle	50502	896102	splns357		dr
au	BLiNK	50502	896102	splns888a1		dr
au	BLiNK	50502	896102	connect		dr
au	Crazy John's	50503 50538	896103 896138	purtona.net	internet	dr 20
au	Crazy John's	50503 50538	896103 896138	purtona.wap	wap	dr
au	Crazy John's	50503 50538	896103 896138	purtona.wap	mms	dr
au	Dodo	50502	896102	WirelessBroadband		dr
au	Dodo	50502	896102	DODOLNS1		dr
au	Escape Net	50502	896102	splns357		dr
au	Exetel	50502	896102	exetel1		dr
au	Exetel	50502	896102	INTERNET		dr
au	Exetel	50502	896102	OPTUSWAP		dr
au	Exetel	50502	896102	YesINTERNET		dr
au	Exetel (Vodafone based)	50503	896103	vfinternet.au		dr

au	Highway1	50502	896102	splns357		dr
au	iiNet	50502	896102	iinet	internet	dr
au	Internode	50502	896102	internode	internet	dr
au	Internode	50502	896102	splns333a1	internet	dr
au	iPrimus	50502	896102	primuslns1		dr
au	Lycamobile	50519	896119	data.lycamobile.com.au	internet	dr
au	Optus	50502	896102	internet	internet	dr 19
au	Optus	50502	896102	yesinternet	internet	dr 19
au	Optus	50502	896102	connect	internet	dr 19
au	Optus	50502	896102	connectcap	internet	dr 19
au	Optus	50502	896102	preconnect	internet	dr 19
au	Optus	50502	896102	mms	mms	dr
au	TPG Mobile	50502	896102	yesinternet		dr
au	TPG Mobile	50502	896102	internet	internet	dr
au	TPG Mobile	50502	896102	mms	mms	dr
au	Pennytel	50503	896103	live.vodafone.com		dr
au	Pennytel	50503	896103	vfinternet.au		dr
au	Smelly Black Dog	50502	896102	splns357		dr
au	Telstra	50501	896101	telstra.wap	internet	dr 20
au	Telstra	50501	896101	telstra.datapack	internet	dr 20
au	Telstra	50501	896101	telstra.internet	internet	dr

au	Telstra	50501	896101	telstra.pcpack	internet	dr 20
au	Telstra	50501	896101	telstra.iph	wap	dr
au	Telstra	50501	896101	telstra.mms	mms	dr
au	Telstra	50501	896101	telstra.bigpond	internet	dr
au	Telstra	50501	896101	telstra.mms	mms	dr
au	Three	50506	896106	3netaccess	internet	dr 20
au	Three	50506	896106	3services	internet	dr 20
au	Virgin Mobile	50502	896102	VirginInternet	internet	dr
au	Virgin Mobile	50502	896102	VirginBroadband	internet	dr
au	Vodafone	50503	896103	vfinternet.au	internet	dr
au	Vodafone	50503	896103	vfprepaymbb	internet	dr 20
au	Vodafone	50503	896103	live.vodafone.com	internet	dr
au	Westnet	50502	896102	yesinternet		dr
au	Westnet	50502	896102	internet		dr
az	Azercell	40001	8999401	internet	internet	dr
az	Azercell	40001	8999401	mms	mms	dr
az	Bakcell	40002	8999402	mms	internet	dr
az	Azerfon	40004	8999404	azerfon	internet	dr
ba	BH GSM	21890	8938790	mms.bhmobile.ba	mms	dr
ba	BH GSM	21890	8938790	mms.bhmobile.ba	mms	dr
ba	m:tel	21805	8938705	mtelgprs1	internet	dr 81
ba	m:tel	21805	8938705	mtelgprs2	internet	dr

ba	m:tel	21805	8938705	mtelgprs3	internet	d 8
ba	m:tel	21805	8938705	mtelgprs4	internet	d 8
ba	m:tel	21805	8938705	mtelfun	internet	d 8
ba	m:tel	21805	8938705	mobismms	mms	d
ba	HT-ERONET	21803	8938703	gprs.eronet.ba	internet	d
ba	HT-ERONET	21803	8938703	mms.eronet.ba	mms	d
bb	Digicel	342750	891750	isp.digicelbarbados.com	internet	d
bd	Robi (AKTel)	47002	8988002	internet	internet	d
bd	Robi (AKTel)	47002	8988002	internet	internet	d
bd	Robi (AKTel)	47002	8988002	wap	mms	d
bd	Banglalink	47003	8988003	blweb	internet	d
bd	Banglalink	47003	8988003	blweb	internet	d
bd	Banglalink	47003	8988003	blmms	mms	d
bd	GrameenPhone	47001	8988001	gpinternet	internet	d 2
bd	GrameenPhone	47001	8988001	gpinternet	internet	d 2
bd	GrameenPhone	47001	8988001	gpmms	mms	d
bd	Airtel (Warid)	47007	8988007	internet	internet	d
bd	Airtel (Warid)	47007	8988007	internet	internet	d
bd	Airtel (Warid)	47007	8988007	mms	mms	d
bd	Teletalk	47004	8988004	wap	internet	d
bd	Teletalk	47004	8988004	mms	mms	d
be	Lycamobile	20606	893206	data.lycamobile.be	internet	d

be	Mobistar	20610	893210	web.pro.be	internet	dr 21
be	Mobistar	20610	893210	internet.be	internet	dr 21
be	Mobistar	20610	893210	iew.be	internet	dr 21
be	Mobistar	20610	893210	mworld.be	internet	dr 21
be	Mobistar	20610	893210	mms.be	mms	dr
be	Telenet Mobile	20610	893210	mobile.internet.be	internet	dr
be	Telenet Mobile	20610	893210	telenetwap.be	internet	dr
be	Telenet Mobile	20610	893210	telenetwap.be	internet	dr
be	Orange	20610	893210	orangeinternet	internet	dr
be	Proximus	20601	893201	internet.proximus.be	internet	dr 81
be	Proximus	20601	893201	intraprox.be	internet	dr 19
be	Proximus	20601	893201	event.proximus.be	mms	dr
be	Base	20620	893220	gprs.base.be	internet	dr 21
be	Base	20620	893220	mms.base.be	mms	dr
be	Mobile Vikings	20620	893220	web.be	internet	dr
bf	Airtel 3G	61302	8922602	internet	internet	dr
bg	GloBul	28405	8935905	internet.globul.bg	internet	dr
bg	GloBul	28405	8935905	mms.globul.bg	mms	dr
bg	M-Tel	28401	8935901	inet-gprs.mtel.bg	internet	dr 21
bg	M-Tel	28401	8935901	mms-gprs.mtel.bg	mms	dr
bg	Vivacom	28403	8935903	internet.vivacom.bg	internet	dr

bg	Vivacom	28403	8935903	internet.vivatel.bg	internet	dr '
bg	Vivacom	28403	8935903	mms.vivacom.bg	mms	dr
bh	Batelco	42601	8997301	internet.batelco.com	internet	dr
bh	Batelco	42601	8997301	mms.batelco.com	mms	dr
bh	Zain BH	42602	8997302	internet	internet	dr
bh	Zain BH	42602	8997302	hsdpa	internet	dr
bh	Zain BH	42602	8997302	http://172.18.83.129	mms	dr
bh	STC	42604	8997304	viva.bh	internet	dr
br	Brasil Telecom	72416	895516	brt.br	internet	dr
br	Brasil Telecom	72416	895516	mms.brt.br	mms	dr
br	Claro	72405	895505	claro.com.br	internet	dr
br	Claro	72405	895505	bandalarga.claro.com.br	internet	dr
br	CTBC	72407 72432 72433 72434	895507 895532 895533 895534	ctbc.br	internet	dr
br	CTBC	72407 72432 72433 72434	895507 895532 895533 895534	mms.ctbc.br	mms	dr
br	Oi	72416 72431 72424	895516 895531 895524	gprs.oi.com.br	internet	dr
br	Oi	72416 72431 72424	895516 895531 895524	wapgprs.oi.com.br	wap	dr
br	Oi	72416 72431 72424	895516 895531 895524	mmsgprs.oi.com.br	mms	dr
br	TIM	72402 72403	895502 895503	tim.br	internet	dr 10

		72404 72408	895504 895508			
br	TIM	72402 72403 72404 72408	895502 895503 895504 895508	unico.tim.it	mms	dr
br	TIM	72402 72403 72404 72408	895502 895503 895504 895508	timbrasil.br	mms	dr
br	Velox			wap.telcel.com	internet	dr
br	Vivo	72406 72410 72411 72423	895506 895510 895511 895523	zap.vivo.com.br	internet	dr
br	Vivo	72406 72410 72411 72423	895506 895510 895511 895523	mms.vivo.com.br	mms	dr
bs	Batelco	364390	891390	internet.btcbahamas.com	internet	dr
bm	CellOne	35000	89100	web.c1.bm	internet	dr
bn	B-Mobile	52802	8967302	bmobilewap	internet	dr
bn	B-Mobile	52802	8967302	bmobilemms	mms	dr
bn	DSTCOM	52811	8967311	dst.wap	internet	dr
bn	DSTCOM	52811	8967311	mms.movistar.es	mms	dr
by	velcom	25701	8937501	wap.velcom.by	wap	dr
by	velcom	25701	8937501	web.velcom.by	internet	dr
by	velcom	25701	8937501	plus.velcom.by	internet	dr
by	velcom	25701	8937501	privet.velcom.by	internet	dr
by	velcom	25701	8937501	web1.velcom.by	internet	dr
by	velcom	25701	8937501	web2.velcom.by	internet	dr

by	velcom	25701	8937501	web3.velcom.by	internet	dr
by	velcom	25701	8937501	vmi.velcom.by	internet	dr
by	velcom	25701	8937501	mms.velcom.by	mms	dr
by	MTS	25702	8937502	internet.mts.by	internet	dr
by	MTS	25702	8937502	mms	mms	dr
by	MTS	25702	8937502	mms.mts.ru	mms	dr
by	MTS	25702	8937502	mms.umc.ua	mms	dr
by	MTS	25702	8937502	sp.mts	mms	dr
by	life:)	25703	8937503	internet.life.com.by	internet	dr
bw	Mascom Wireless	65201	8926701	internet.mascom	internet	dr
bw	Mascom Wireless	65201	8926701	mms	mms	dr
bw	Orange	65202	8926702	internet.orange.co.bw	internet	dr
bi	Leo/UCom	64203	8925703	ucnet	internet	dr
bi	Tempo/Africell	64202	8925702	internet	internet	dr
bi	Tempo/Africell	64202	8925702	mms.mascom	mms	dr
ca	Fido	302370	891370	internet.fido.ca	internet	dr 20
ca	Fido	302370	891370	mms.fido.ca	mms	dr
ca	Rogers	302720	891720	internet.com	internet	dr 20
ca	Rogers	302720	891720	media.com	mms	dr
ca	Bell Mobility	302610 302640 302651 302880	891610 891640 891651 891880	inet.bell.ca	internet	dr
ca	Bell Mobility	302610 302640	891610 891640	pda.bell.ca	internet	dr

		302651 302880	891651 891880			
ca	Bell Mobility	302610 302640 302651 302880	891610 891640 891651 891880	pda2.bell.ca	internet	dr
ca	Bell Mobility	302610 302640 302651 302880	891610 891640 891651 891880	pda.bell.ca	mms	dr
ca	Telus Mobility	302220 302860 302880	891220 891860 891880	isp.telus.com	internet	dr
ca	Telus Mobility	302220 302860 302880	891220 891860 891880	vpn.telus.com	internet	dr
ca	Telus Mobility	302220 302860 302880	891220 891860 891880	bb.telus.com	internet	dr
ca	Telus Mobility	302220 302860 302880	891220 891860 891880	sp.telus.com	internet	dr
ca	Telus Mobility	302220 302860 302880	891220 891860 891880	sp.telus.com	mms	dr
ca	SaskTel Mobility	302680 302750 302780 302880	891680 891750 891780 891880	inet.stm.sk.ca	internet	dr
ca	Vidéotron	302500 302510	891500 891510	media.videotron	internet	dr
ca	Vidéotron	302500 302510	891500 891510	ihvm.videotron	internet	dr
ca	Vidéotron	302500 302510	891500 891510	media.videotron	mms	dr
ca	WIND Mobile	302490	891490	broadband.windmobile.ca	internet	dr

ca	WIND Mobile	302490	891490	internet.windmobile.ca	internet	dr
ca	WIND Mobile	302490	891490	mnet.b-online.gr	mms	dr
ca	WIND Mobile	302490	891490	mms.windmobile.ca	mms	dr
ca	Mobilicity	302320	891320	wap.davewireless.com	internet	dr
ca	Mobilicity	302320	891320	internet.davewireless.com	internet	dr
ca	Mobilicity	302320	891320	mms.davewireless.com	mms	dr
cd	Vodacom	63001	8924301	vodanet	internet	dr
cd	Vodacom	63001	8924301	vodalive	mms	dr
ch	Lycamobile	22854	894154	data.lycamobile.ch	internet	dr
ch	Orange	22803	894103	mobileoffice3g	internet	dr 21
ch	Orange	22803	894103	click	internet	dr 21
ch	Orange	22803	894103	intranetaccess	internet	dr
ch	Orange	22803	894103	internet		dr
ch	Sunrise	22802	894102	internet	internet	dr 19
ch	Sunrise	22802	894102	wap.sunrise.ch		dr
ch	Sunrise	22802	894102	mms.sunrise.ch		dr
ch	Sunrise	22802	894102	mms.sunrise.ch	mms	dr
ch	Swisscom	22801	894101	gprs.swisscom.ch	internet	dr 13
ch	Swisscom	22801	894101	corporate.swisscom.ch	internet	dr
ch	Swisscom	22801	894101	event.swisscom.ch	internet	dr
ch	Swisscom	22801	894101	event.swisscom.ch	mms	dr
ch	M-Budget	22801	894101	gprs.swisscom.ch	internet	dr
ci	MTN	61205	8922505	internet	internet	dr

ci	MTN	61205	8922505	fast-mms	mms	dr
ci	MTN	61205	8922505	myMTN	mms	dr
cl	Claro Chile	73003	895603	bam.clarochile.cl	internet	dr
cl	Claro Chile	73003	895603	bap.clarochile.cl	internet	dr
cl	Claro Chile	73003	895603	wap.clarochile.cl	wap	dr
cl	Claro Chile	73003	895603	mms.clarochile.cl	mms	dr
cl	Entel PCS	73001	895601	imovil.entelpcs.cl	internet	dr
cl	Entel PCS	73001	895601	bam.entelpcs.cl	internet	dr
cl	Entel PCS	73001	895601	mms.entelpcs.cl	mms	dr
cl	Movistar	73002 73010	895602 895610	web.tmovil.cl	internet	dr
cl	Movistar	73002 73010	895602 895610	wap.tmovil.cl	wap	dr
cl	Movistar	73002 73010	895602 895610	dst.mms	mms	dr
cl	Movistar	73002 73010	895602 895610	dst.mms	mms	dr
cl	Virgin Mobile	73007	895607	imovil.virginmobile.cl	internet	dr
cl	VTR Movil	73008	895608	movil.vtr.com	internet	dr
cl	Nextel	73009	895609	wap.nextelmovil.cl	internet	dr
cm	Orange	62402	8923702	orangecmgprs	internet	dr
cm	MTN	62401	8923701	INTERNET	internet	dr
cn	China Mobile	46000 46002	898600 898602	cmwap	wap	dr
cn	China Mobile	46000 46002	898600 898602	cmnet	internet	dr '
cn	China Mobile	46000 46002	898600 898602	cmwap	mms	dr

cn	China Unicom	46001	898601	3gnet	internet	dr
cn	China Unicom	46001	898601	3gwap	mms	dr
cr	IceCelular	71201 71202	8950601 8950602	icecelular	internet	dr '
cr	Kolbi	71203	8950603	kolbi3g	internet	dr
cr	Kolbi	71203	8950603	mms.ideasclaro	mms	dr
co	Claro	732101	8957101	internet.comcel.com.co	internet	dr
co	eTb			moviletb.net.co	internet	dr
co	Movistar	732102 732123	8957102 8957123	internet.movistar.com.co	internet	dr
co	Tigo	732103 732111	8957103 8957111	web.colombiamovil.com.co	internet	dr
co	Tigo	732103 732111	8957103 8957111	mms.sentelgsm.com	mms	dr
co	Uff			web.uffmovil.com.co	internet	dr
co	UNE	732103 732111	8957103 8957111	www.une.net.co	internet	dr
co	UNE	732103 732111	8957103 8957111	une4glte.net.co	internet	dr
co	UNE	732103 732111	8957103 8957111	mms.colombiamovil.com.co	mms	dr
co	Virgin Mobile	732123	8957123	web.vmc.net.co	internet	dr
co	Virgin Mobile	732123	8957123	mms.movistar.com.co	mms	dr
cy	Cytamobile-Vodafone	28001	8935701	internet	internet	dr
cy	Cytamobile-Vodafone	28001	8935701	pp.internet	internet	dr
cy	Cytamobile-Vodafone	28001	8935701	cytamobile	mms	dr
cy	MTN	28010	8935710	internet	internet	dr

cz	Vodafone	23003	8942003	internet	internet	dr 21
cz	O2	23002	8942002	internet	internet	dr 16
cz	O2	23002	8942002	internet.open	internet	dr 16
cz	O2	23002	8942002	internet	internet	dr
cz	O2	23002	8942002	mms	mms	dr
cz	T-Mobile	23001	8942001	internet.t-mobile.cz	internet	dr 21
cz	MOBIL.CZ	23001	8942001	internet.t-mobile.cz	internet	dr
de	AldiTalk/ MedionMobile	26203 26205 26277	894903 894905 894977	internet.eplus.de	internet	dr 21
de	AldiTalk/ MedionMobile	26203 26205 26277	894903 894905 894977	mms.eplus.de	mms	dr
de	blau.de	26203 26205 26277	894903 894905 894977	internet.eplus.de	internet	dr
de	blau.de	26203 26205 26277	894903 894905 894977	tagesflat.eplus.de	internet	dr
de	Bild Mobil	26202	894902	access.vodafone.de	internet	dr
de	Bild Mobil	26202	894902	web.vodafone.de	internet	dr 13
de	Bild Mobil	26202	894902	event.vodafone.de	internet	dr
de	Bild Mobil	26202	894902	event.vodafone.de	mms	dr
de	E-Plus	26203 26205 26277	894903 894905 894977	internet.eplus.de	internet	dr 21
de	Lycamobile	26243	894943	data.lycamobile.de	internet	dr

de	O2	26207 26208 26211	894907 894908 894911	pinternet.interkom.de	internet	dr 19
de	O2	26207 26208 26211	894907 894908 894911	internet	internet	dr 62
de	O2	26207 26208 26211	894907 894908 894911	surfo2	internet	dr 62
de	O2	26207 26208 26211	894907 894908 894911	internet	mms	dr
de	Tchibo-Mobil	26207 26208 26211	894907 894908 894911	webmobil1	internet	dr
de	T-Mobile(Telekom)	26201 26206	894901 894906	internet.t-d1.de	internet	dr 19
de	T-Mobile(Telekom)	26201 26206	894901 894906	internet.t-mobile	internet	dr 19
de	T-Mobile(Telekom)	26201 26206	894901 894906	internet.t-mobile	mms	dr
de	Congstar	26201	894901	internet.t-mobile	internet	dr 10
de	Vodafone	26202 26204 26209	894902 894904 894909	web.vodafone.de	internet	dr 13
de	Vodafone	26202 26204 26209	894902 894904 894909	event.vodafone.de	internet	dr 13
de	FONIC	26207 26208 26211	894907 894908 894911	pinternet.interkom.de	internet	dr
de	simyo Internet	26203 26205 26277	894903 894905 894977	internet.eplus.de	internet	dr 21

de	Alice	26207	894907	internet.partner1	internet	dr 19
de	1&1	26202 26204 26209	894902 894904 894909	web.vodafone.de	internet	dr
de	1&1	26202 26204 26209	894902 894904 894909	mail.partner.de	internet	dr
de	Netzclub	26207 26208 26211	894907 894908 894911	pinternet.interkom.de	internet	dr
dk	3	23806	894506	bredband.tre.dk	internet	dr
dk	3	23806	894506	net.tre.dk	internet	dr
dk	3	23806	894506	data.tre.dk	internet	dr
dk	3	23806	894506	static.tre.dk	internet	dr
dk	OiSTER	23806	894506	bredband.oister.dk	internet	dr
dk	OiSTER	23806	894506	data.dk	internet	dr
dk	OiSTER	23806	894506	data.tre.dk	mms	dr
dk	Lycamobile	23812	894512	data.lycamobile.dk	internet	dr
dk	Telenor	23802 23877	894502 894577	internet	internet	dr 21
dk	Telenor	23802 23877	894502 894577	telenor	mms	dr
dk	CBB Mobil	23802 23877	894502 894577	internet	internet	dr
dk	TDC	23801	894501	internet	internet	dr 19
dk	TDC	23801	894501	internet.no	internet	dr
dk	TDC	23801	894501	internet.se	internet	dr
dk	TDC	23801	894501	mms.tdc.fi	mms	dr

dk	Fullrate			internet	internet	dr
dk	Telia	23830	894530	www.internet.mtelia.dk	internet	dr
dk	Telia	23830	894530	www.mms.mtelia.dk	mms	dr
dk	BiBoB	23802	894502	internet.bibob.dk	internet	dr
dk	Telmore	23801	894501	internet	internet	dr 19
dk	Telmore	23801	894501	mms	mms	dr
dk	Unotel	23801	894501	internet	internet	dr
dk	happiimobil	23801	894501	internet	internet	dr
dk	Onfone Internet DK	23801	894501	internet	internet	dr
do	Orange	37001	89101	orangenet.com.do	internet	dr
do	Claro	37002	89102	internet.ideasclaro.com.do	internet	dr 19
do	Viva	37004	89104	edge.viva.net.do	internet	dr
dz	Djezzy	60302	8921302	djezzy.internet	internet	dr
dz	Djezzy	60302	8921302	djezzy.mms	mms	dr
dz	Mobilis	60301	8921301	internet	internet	dr
dz	Mobilis	60301	8921301	mms	mms	dr
dz	Nedjma	60303	8921303	internet	internet	dr
dz	Nedjma	60303	8921303	nedjmaMMS	mms	dr
ec	Movistar UMTS	74000	8959300	navega.movistar.ec	internet	dr
ec	Movistar UMTS	74000	8959300	mms.movistar.com.ec	mms	dr
ec	Porta 3G	74001	8959301	internet.porta.com.ec	internet	dr
ec	Porta 3G	74001	8959301	mms.porta.com.ec	mms	dr
ee	EMT	24801	8937201	internet.emt.ee	internet	dr 21

ee	EMT	24801	8937201	mms.emt.ee	mms	dr
ee	Nordea	24801	8937201	internet.emt.ee	internet	dr
ee	Elisa	24802	8937202	internet	internet	dr
ee	Elisa	24802	8937202	mms	mms	dr
ee	Elisa	24802	8937202	mms	mms	dr
ee	Tele2	24803	8937203	internet.tele2.ee	internet	dr
ee	Tele2	24803	8937203	internet.tele2.fi	mms	dr
eg	Vodafone	60202	892002	internet.vodafone.net	internet	dr 2
eg	Etisalat	60203	892003	etisalat	internet	dr
eg	Etisalat	60203	892003	Etisalat	mms	dr
eg	MobiNil	60201	892001	mobinilweb	internet	dr 1
eg	MobiNil	60201	892001	mobinilmms	mms	dr
es	Euskaltel	21408	893408	internet.euskaltel.mobi	internet	dr
es	Lebara			gprsmov.lebaramobile.es	internet	dr
es	Lowi			lowi.private.omv.es	internet	dr
es	Lycamobile	21425	893425	data.lycamobile.es	internet	dr
es	Másmovil	21403	893403	internetmas	internet	dr
es	móbil R (Mundo-R)	21417	893417	internet.mundo-r.com	internet	dr
es	Happy Móvil/ moviData	21403	893403	INTERNETTPH	internet	dr 6
es	ONO	21418	893418	internet.ono.com	internet	dr 6
es	Pepephone	21406	893406	gprs.pepephone.com	internet	dr
es	Pepephone	21406	893406	gprsmov.pepephone.com	internet	dr
es	Orange	21403	893403	internet	internet	dr

		21409	893409			85
es	Simyo	21419	893419	gprs-service.com	internet	dr 19
es	Telecable	21416	893416	internet.telecable.es	internet	dr
es	Movistar (Telefónica)	21405 21407	893405 893407	telefonica.es	internet	dr 19
es	Movistar (Telefónica)	21405 21407	893405 893407	movistar.es	internet	dr
es	Vodafone	21401 21406 21456	893401 893406 893456	ac.vodafone.es	internet	dr 21
es	Vodafone	21401 21406 21456	893401 893406 893456	airtelnet.es	internet	dr 21
es	Vodafone	21401 21406 21456	893401 893406 893456	mms.vodafone.net	mms	dr
es	Yoigo	21404	893404	internet	internet	dr 21
es	Yoigo	21404	893404	mms	mms	dr
es	Jazztel	21421	893421	jazzinternet	internet	dr 87
es	Carrefour Móvil			CARREFOURINTERNET	internet	dr
es	Tuenti Móvil	21405	893405	tuenti.com	internet	dr
es	Eroski Móvil	21424	893424	gprs.eroskimovil.es		dr
es	LlamaYa móvil	21403	893403	moreinternet	internet	dr
es	Amena	21403	893403	orangeworld	internet	dr
et	Ethio Telecom	63601	8925101	etc.com	internet	dr 21
fo	Vodafone FO	28802	8929802	vmc.vodafone.fo	internet	dr
fi	Kuiri	24431	8935831	kuirinet	internet	dr

fi	DNA	24412	8935812	data.dna.fi	internet	dr
fi	DNA	24412	8935812	internet	internet	dr
fi	Elisa	24405	8935805	internet	internet	dr
fi	Saunalahti	24421	8935821	internet.saunalahti	internet	dr 19
fi	Saunalahti	24421	8935821	internet4	internet	dr 19
fi	Saunalahti	24421	8935821	internet	internet	dr 19
fi	Saunalahti	24421	8935821	mms.saunalahti.fi	mms	dr
fi	Sonera	24491	8935891	internet	internet	dr 19
fi	Sonera	24491	8935891	prointernet	internet	dr 19
fi	Sonera	24491	8935891	telefinland	mms	dr
fi	Welho			internet.welho.fi	internet	dr
fj	Vodafone / Kidanet	54201	8967901	vfinternet.fj	internet	dr
fj	Vodafone / Kidanet	54201	8967901	kidanet.fj	internet	dr
fj	Vodafone / Kidanet	54201	8967901	prepay.vfinternet.fj	internet	dr
fr	A Mobile (Auchan Telecom)			wap65	internet	dr
fr	Bouygues Telecom	20820 20821	893320 893321	a2bouygtel.com	internet	dr
fr	Bouygues Telecom	20820 20821	893320 893321	b2bouygtel.com	internet	dr
fr	Bouygues Telecom	20820 20821	893320 893321	ebouygtel.com	internet	dr

fr	Bouygues Telecom	20820 20821	893320 893321	mmsbouygtel.com	internet	dr
fr	Bouygues Telecom	20820 20821	893320 893321	pcebouygtel.com	internet	dr
fr	Bouygues Telecom	20820 20821	893320 893321	mmsbouygtel.com	mms	dr
fr	Free Mobile	20815	893315	free	internet	dr
fr	Free Mobile	20815	893315	mmsfree	mms	dr
fr	Free Mobile	20815	893315	mmsfree	mms	dr
fr	Lycamobile	20825	893325	data.lycamobile.fr	internet	dr
fr	Orange	20801 20800	893301 893300	orange.fr	internet	dr 19
fr	Orange	20801 20800	893301 893300	internet-entreprise	internet	dr 19
fr	Orange	20801 20800	893301 893300	orange	internet	dr 19
fr	Orange	20801 20800	893301 893300	orange-mib	internet	dr 17
fr	Orange	20801 20800	893301 893300	orange-acte	mms	dr
fr	Orange	20801 20800	893301 893300	orange.ie	internet	dr
fr	Prixtel	20801 20810	893301 893310	Orange	internet	dr
fr	Prixtel	20801 20810	893301 893310	orange.acte	mms	dr
fr	Prixtel	20801 20810	893301 893310	sl2sfr	internet	dr
fr	Prixtel	20801 20810	893301 893310	sl2sfr	mms	dr
fr	SFR	20810 20811	893310 893311	websfr	internet	dr 17

fr	SFR	20810 20811	893310 893311	wapsfr	wap	dr
fr	SFR	20810 20811	893310 893311	internetpro	internet	dr
fr	SFR	20810 20811	893310 893311	ipnet	internet	dr
fr	SFR	20810 20811	893310 893311	slsfr	internet	dr 17
fr	SFR	20810 20811	893310 893311	sl2sfr	internet	dr
fr	SFR	20810 20811	893310 893311	internetneuf	internet	dr
fr	SFR	20810 20811	893310 893311	mms65	mms	dr
fr	Transatel Telecom	20822	893322	netgprs.com	internet	dr
fr	TEN	20801	893301	ao.fr	internet	dr
fr	TEN	20801	893301	ofnew.fr	internet	dr
fr	TEN	20801	893301	orange.acte	mms	dr
gb	BT Mobile	23400	894400	btmobile.bt.com	internet	dr
gb	Lycamobile	23426	894426	data.lycamobile.co.uk	internet	dr
gb	O2	23402 23410 23411	894402 894410 894411	mobile.o2.co.uk	internet	dr 19
gb	O2	23402 23410 23411	894402 894410 894411	mobile.o2.co.uk	internet	dr 19
gb	O2	23402 23410 23411	894402 894410 894411	payandgo.o2.co.uk	internet	dr
gb	O2	23402 23410 23411	894402 894410 894411	idata.o2.co.uk	internet	dr

gb	O2	23402 23410 23411	894402 894410 894411	m-bb.o2.co.uk	internet	dr 82
gb	O2	23402 23410 23411	894402 894410 894411	wap.o2.co.uk	wap	dr
gb	giffgaff	23402 23410 23411	894402 894410 894411	giffgaff.com	internet	dr
gb	giffgaff	23402 23410 23411	894402 894410 894411	wap.o2.co.uk	mms	dr
gb	TalkTalk			mobile.talktalk.co.uk		dr
gb	T-Mobile	23430	894430	general.t-mobile.uk	internet	dr 14
gb	T-Mobile	23430	894430	general.t-mobile.uk	internet	dr 14
gb	Tesco Mobile	23402 23410 23411	894402 894410 894411	prepay.tesco-mobile.com	internet	dr '
gb	Virgin Mobile	23431 23432	894431 894432	vdata	internet	dr 19
gb	Virgin Mobile	23431 23432	894431 894432	goto.virginmobile.uk	internet	dr
gb	Virgin Mobile	23431 23432	894431 894432	orange.acte	mms	dr
gb	Virgin Mobile	23431 23432	894431 894432	vmms	mms	dr
gb	Vodafone	23415	894415	internet	internet	dr 10
gb	Vodafone	23415	894415	pp.vodafone.co.uk	internet	dr 17
gb	Vodafone	23415	894415	ppbundle.internet	internet	dr 10

gb	Vodafone	23415	894415	pp.internet	internet	dr
gb	Asda Mobile	23415	894415	asdamobiles.co.uk	internet	dr
gb	Asda Mobile	23415	894415	asdamobiles.co.uk	mms	dr
gb	3	23420	894420	3internet	internet	dr
gb	3	23420	894420	three.co.uk	internet	dr 17
gb	Orange	23433 23434	894433 894434	orangeinternet	internet	dr 19
gb	Orange	23433 23434	894433 894434	internetvpn	internet	dr 19
gb	Orange	23433 23434	894433 894434	orangewap	wap	dr 15
ge	Geocell	28201	8999501	Internet	internet	dr 21
ge	Geocell	28201	8999501	mms	mms	dr
gg	Airtel-Vodaphone	23403	894403	airtel-ci-gprs.com	internet	dr
gg	Sure (Cable & Wireless)	23455	894455	wap	wap	dr
gg	Sure (Cable & Wireless)	23455	894455	internet	internet	dr
gg	Sure (Cable & Wireless)	23455	894455	mms	mms	dr
gg	Wave Telecom	23450	894450	pepper	internet	dr 21
gg	Wave Telecom	23450	894450	mms	mms	dr
gh	MTN	62001	8923301	internet	internet	dr
gh	Vodafone	62002	8923302	browse	internet	dr
gh	Tigo	62003	8923303	web.tigo.com.gh	internet	dr
gh	Airtel	62006	8923306	internet	internet	dr

gh	GloGhana	62007	8923307	internet	internet	dr
gh	GloGhana	62007	8923307	mms	mms	dr
gl	Tele Greenland A/S			internet	internet	dr
gr	Cosmote	20201	893001	internet	internet	dr
gr	Vodafone	20205	893005	internet	internet	dr
gr	Vodafone	20205	893005	web.session	internet	dr 2
gr	Wind	20209 20210	893009 893010	gint.b-online.gr	internet	dr
gr	Wind	20209 20210	893009 893010	q-mms.myq.gr	mms	dr
gt	Claro	70401	8950201	internet.ideasclaro	internet	dr
gt	Comcel / Tigo	70402	8950202	Wap.tigo.gt	internet	dr
gt	Comcel / Tigo	70402	8950202	mms.tigo.gt	mms	dr
gt	Movistar	70403	8950203	internet.movistar.gt	internet	dr
gn	Orange	61101	8922401	internetogn	internet	dr
gn	Cellcom	61105	8922405	internet.cellcom.com	internet	dr
gy	GT&T Cellink Plus	73802	8959202	wap.cellinkgy.com	internet	dr
gy	DigiCel	73801	8959201	internet	internet	dr
gy	DigiCel	73801	8959201	wap.digicelgy.com	mms	dr
hk	CSL	45400 45402	8985200 8985202	internet	internet	dr 20
hk	CSL	45400 45402	8985200 8985202	hkcsl	mms	dr
hk	New World	45410	8985210	internet	internet	dr
hk	New World	45410	8985210	peoples.mms	mms	dr

hk	China Mobile	45412	8985212	peoples.net	internet	dr
hk	China Mobile	45412	8985212	SmarTone-Vodafone	mms	dr
hk	SmarTone	45406	8985206	internet	internet	dr
hk	PCCW (Sunday)	45416 45419	8985216 8985219	internet	internet	dr
hk	PCCW (Sunday)	45416 45419	8985216 8985219	pccwdata	internet	dr
hk	PCCW (Sunday)	45416 45419	8985216 8985219	pccw	internet	dr
hk	PCCW (Sunday)	45416 45419	8985216 8985219	pccwmms	mms	dr
hk	PCCW (Sunday)	45416 45419	8985216 8985219	pccw	mms	dr
hk	Sunday	45416	8985216	internet	internet	dr
hk	Orange	45404	8985204	web.orangehk.com	internet	dr
hk	3	45403 45404	8985203 8985204	mobile.three.com.hk	internet	dr
hk	3	45403 45404	8985203 8985204	mobile.lte.three.com.hk	internet	dr
hk	Lycamobile	45423	8985223	data.lycamobile.hk	internet	dr
hn	Tigo	70802	8950402	internet.tigo.hn	internet	dr
hr	T-Mobile	21901	8938501	web.htgprs	internet	dr
hr	VIPNET	21910	8938510	data.vip.hr	internet	dr
hr	VIPNET	21910	8938510	gprs5.vipnet.hr	internet	dr
hr	VIPNET	21910	8938510	gprs0.vipnet.hr	internet	dr
hr	VIPNET	21910	8938510	3g.vip.hr	internet	dr 2
hr	VIPNET	21910	8938510	mms.vipnet.hr	mms	dr
hr	CARNet VIPNET	21910	8938510	carnet.vip.hr	internet	dr

hr	CARNet Tele2	21902	8938502	carnet.tele2.hr	internet	d
hr	CARNet Tele2	21902	8938502	internet.tele2.hr	mms	d
hr	Tele2	21902	8938502	mobileinternet.tele2.hr	internet	d
hu	Telenor	21601	893601	net	internet	d
hu	Telenor	21601	893601	mms	mms	d
hu	DIGI	21601	893601	digi	internet	d
hu	T-Mobile	21630	893630	internet	internet	d
hu	T-Mobile	21630	893630	mms-westel	mms	d
hu	Vodafone	21670	893670	standardnet.vodafone.net	internet	d
hu	Vodafone	21670	893670	internet.vodafone.net	internet	d
hu	Vodafone	21670	893670	vitamax.snet.vodafone.net	internet	d
hu	Vodafone	21670	893670	vitamax.internet.vodafone.net	internet	d
hu	Invitel			invitel.mobilnet	internet	d
id	3	51089	896289	3gprs	internet	d
id	3	51089	896289	3data	internet	d
id	AXIS	51008	896208	AXIS	internet	d
id	AXIS	51008	896208	AXISmms	mms	d
id	Indosat	51021 51001	896221 896201	indosatgprs	internet	d
id	Indosat	51021 51001	896221 896201	indosatgprs	internet	d
id	Indosat	51021	896221	indosatgprs	internet	d

		51001	896201			
id	Indosat	51021 51001	896221 896201	indosatmms	mms	dr
id	Telkomsel	51010 51020	896210 896220	telkomsel	internet	dr 20
id	Telkomsel	51010 51020	896210 896220	flash	internet	dr
id	Telkomsel	51010 51020	896210 896220	internet	internet	dr
id	Telkomsel	51010 51020	896210 896220	mms	mms	dr
id	Excelcomindo (XL)	51011	896211	www.xlgprs.net	internet	dr 20
id	Excelcomindo (XL)	51011	896211	www.xlmms.net	mms	dr
ie	Lycamobile	27213	8935313	data.lycamobile.ie	internet	dr
ie	O2	27202	8935302	open.internet	internet	dr 62
ie	O2	27202	8935302	pp.internet	internet	dr 62
ie	O2	27202	8935302	internet	internet	dr
ie	O2	27202	8935302	internet	mms	dr
ie	Vodafone	27201	8935301	hs.vodafone.ie	internet	dr 89
ie	Vodafone	27201	8935301	isp.vodafone.ie	internet	dr
ie	Vodafone	27201	8935301	live.vodafone.com	internet	dr
ie	E-Mobile	27203	8935303	broadband.eircommbb.ie	internet	dr 21
ie	E-Mobile	27203	8935303	mms.mymeteor.ie	mms	dr
ie	Meteor	27203	8935303	data.mymeteor.ie	internet	dr

ie	Meteor	27203	8935303	broadband.mymeteor.ie	internet	dr 2
ie	Meteor	27203	8935303	isp.mymeteor.ie	internet	dr
ie	Three Ireland	27205	8935305	3ireland.ie	internet	dr 1
ie	Three Ireland	27205	8935305	3ireland.ie	mms	dr
il	CellCom	42502	8997202	internetg	internet	dr
il	CellCom	42502	8997202	mms	mms	dr
il	GolanTelecom	42508	8997208	internet.golantelecom.net.il	internet	dr
il	Home Cellular	42515	8997215	hcminternet	internet	dr
il	Hot Mobile	42507	8997207	net.hotm	internet	dr
il	Orange	42501	8997201	uinternet	internet	dr 1
il	Pelephone	42503	8997203	internet.pelephone.net.il	internet	dr
il	Pelephone	42503	8997203	mms.pelephone.net.il	mms	dr
il	Rami Levi	42516	8997216	internet.rl	internet	dr
il	YouPhone 3G	42514	8997214	data.youphone.co.il	internet	dr
im	Manx Telecom	23458	894458	3gpronto	internet	dr
im	Manx Telecom	23458	894458	mms.manxpronto.net	mms	dr
im	Sure (Cable & Wireless)	23436 23455	894436 894455	wap	wap	dr
im	Sure (Cable & Wireless)	23436 23455	894436 894455	internet	internet	dr
in	AIRCEL	40417 40428 40429 40437 40441 40442 40491 405800	899117 899128 899129 899137 899141 899142 899191 8991800	aircelweb	internet	dr

		405801 405802 405803 405804 405805 405806 405807 405808 405809 405810 405811 405812	8991801 8991802 8991803 8991804 8991805 8991806 8991807 8991808 8991809 8991810 8991811 8991812			
in	AIRCEL	40417 40428 40429 40437 40441 40442 40491 405800 405801 405802 405803 405804 405805 405806 405807 405808 405809 405810 405811 405812	899117 899128 899129 899137 899141 899142 899191 8991800 8991801 8991802 8991803 8991804 8991805 8991806 8991807 8991808 8991809 8991810 8991811 8991812	aircelgprs	internet	dr
in	AIRCEL	40417 40428 40429 40437 40441 40442 40491 405800 405801 405802 405803 405804 405805	899117 899128 899129 899137 899141 899142 899191 8991800 8991801 8991802 8991803 8991804 8991805	aircelgprs.po	internet	dr

		405806 405807 405808 405809 405810 405811 405812	8991806 8991807 8991808 8991809 8991810 8991811 8991812			
in	AIRCEL	40417 40428 40429 40437 40441 40442 40491 405800 405801 405802 405803 405804 405805 405806 405807 405808 405809 405810 405811 405812	899117 899128 899129 899137 899141 899142 899191 8991800 8991801 8991802 8991803 8991804 8991805 8991806 8991807 8991808 8991809 8991810 8991811 8991812	aircelgprs.pr	internet	dr
in	AIRCEL	40417 40428 40429 40437 40441 40442 40491 405800 405801 405802 405803 405804 405805 405806 405807 405808 405809 405810	899117 899128 899129 899137 899141 899142 899191 8991800 8991801 8991802 8991803 8991804 8991805 8991806 8991807 8991808 8991809 8991810	aircelmms	mms	dr

		405811 405812	8991811 8991812			
in	AIRCEL	40417 40428 40429 40437 40441 40442 40491 405800 405801 405802 405803 405804 405805 405806 405807 405808 405809 405810 405811 405812	899117 899128 899129 899137 899141 899142 899191 8991800 8991801 8991802 8991803 8991804 8991805 8991806 8991807 8991808 8991809 8991810 8991811 8991812	aircelmms.po	mms	dr
in	AIRCEL	40417 40428 40429 40437 40441 40442 40491 405800 405801 405802 405803 405804 405805 405806 405807 405808 405809 405810 405811 405812	899117 899128 899129 899137 899141 899142 899191 8991800 8991801 8991802 8991803 8991804 8991805 8991806 8991807 8991808 8991809 8991810 8991811 8991812	aircelmms	mms	dr
in	Airtel	40402 40403	899102 899103	airtelgprs.com	internet	dr 20

		40406 40410 40428 40431 40437 40440 40441 40442 40445 40449 40470 40490 40492 40493 40496 40497 40498 40551 40552 40554 40556	899106 899110 899128 899131 899137 899140 899141 899142 899145 899149 899170 899190 899192 899193 899196 899197 899198 899151 899152 899154 899156			
in	Vodafone	40401 40405 40411 40413 40415 40420 40427 40430 40443 40446 40460 40484 40486 40488 40566 405750 405751 405752 405753 405754 405755 405756	899101 899105 899111 899113 899115 899120 899127 899130 899143 899146 899160 899184 899186 899188 899166 8991750 8991751 8991752 8991753 8991754 8991755 8991756	www	internet	dr
in	Vodafone	40401 40405	899101 899105	portalnmms	mms	dr

		40411 40413 40415 40420 40427 40430 40443 40446 40460 40484 40486 40488 40566 405750 405751 405752 405753 405754 405755 405756	899111 899113 899115 899120 899127 899130 899143 899146 899160 899184 899186 899188 899166 8991750 8991751 8991752 8991753 8991754 8991755 8991756			
in	BSNL/CellOne	40434 40438 40451 40453 40454 40455 40457 40458 40459 40462 40464 40466 40471 40472 40473 40474 40475 40476 40477 40480 40481	899134 899138 899151 899153 899154 899155 899157 899158 899159 899162 899164 899166 899171 899172 899173 899174 899175 899176 899177 899180 899181	bsnlnet	internet	dr
in	BSNL/CellOne	40434 40438 40451 40453	899134 899138 899151 899153	bsnlwap	wap	dr

		40454 40455 40457 40458 40459 40462 40464 40466 40471 40472 40473 40474 40475 40476 40477 40480 40481	899154 899155 899157 899158 899159 899162 899164 899166 899171 899172 899173 899174 899175 899176 899177 899180 899181			
in	BSNL/CellOne	40434 40438 40451 40453 40454 40455 40457 40458 40459 40462 40464 40466 40471 40472 40473 40474 40475 40476 40477 40480 40481	899134 899138 899151 899153 899154 899155 899157 899158 899159 899162 899164 899166 899171 899172 899173 899174 899175 899176 899177 899180 899181	bsnlsouth	internet	dr
in	BSNL/CellOne	40434 40438 40451 40453 40454 40455 40457	899134 899138 899151 899153 899154 899155 899157	gprssouth.cellone.in	internet	dr

		40458 40459 40462 40464 40466 40471 40472 40473 40474 40475 40476 40477 40480 40481	899158 899159 899162 899164 899166 899171 899172 899173 899174 899175 899176 899177 899180 899181			
in	BSNL/CellOne	40434 40438 40451 40453 40454 40455 40457 40458 40459 40462 40464 40466 40471 40472 40473 40474 40475 40476 40477 40480 40481	899134 899138 899151 899153 899154 899155 899157 899158 899159 899162 899164 899166 899171 899172 899173 899174 899175 899176 899177 899180 899181	gprsnorth.cellone.in	internet	dr
in	BSNL/CellOne	40434 40438 40451 40453 40454 40455 40457 40458 40459 40462	899134 899138 899151 899153 899154 899155 899157 899158 899159 899162	gprswest.cellone.in	internet	dr

		40464 40466 40471 40472 40473 40474 40475 40476 40477 40480 40481	899164 899166 899171 899172 899173 899174 899175 899176 899177 899180 899181			
in	BSNL/CellOne	40434 40438 40451 40453 40454 40455 40457 40458 40459 40462 40464 40466 40471 40472 40473 40474 40475 40476 40477 40480 40481	899134 899138 899151 899153 899154 899155 899157 899158 899159 899162 899164 899166 899171 899172 899173 899174 899175 899176 899177 899180 899181	www.e.pr	internet	dr 21
in	BSNL/CellOne	40434 40438 40451 40453 40454 40455 40457 40458 40459 40462 40464 40466 40471	899134 899138 899151 899153 899154 899155 899157 899158 899159 899162 899164 899166 899171	www.e.po	internet	dr 21

		40472 40473 40474 40475 40476 40477 40480 40481	899172 899173 899174 899175 899176 899177 899180 899181			
in	BSNL/CellOne	40434 40438 40451 40453 40454 40455 40457 40458 40459 40462 40464 40466 40471 40472 40473 40474 40475 40476 40477 40480 40481	899134 899138 899151 899153 899154 899155 899157 899158 899159 899162 899164 899166 899171 899172 899173 899174 899175 899176 899177 899180 899181	bsnlmms	mms	dr
in	Idea Cellular	40404 40407 40412 40414 40419 40422 40424 40444 40456 40482 40570 405799 405845 405848 405850	899104 899107 899112 899114 899119 899122 899124 899144 899156 899182 899170 8991799 8991845 8991848 8991850	internet	internet	dr

in	Idea Cellular	40404 40407 40412 40414 40419 40422 40424 40444 40456 40482 40570 405799 405845 405848 405850	899104 899107 899112 899114 899119 899122 899124 899144 899156 899182 899170 8991799 8991845 8991848 8991850	mms	mms	dr
in	Idea Cellular	40404 40407 40412 40414 40419 40422 40424 40444 40456 40482 40570 405799 405845 405848 405850	899104 899107 899112 899114 899119 899122 899124 899144 899156 899182 899170 8991799 8991845 8991848 8991850	mmsc	mms	dr
in	MTNL	40468 40469	899168 899169	mtnl.net	internet	dr
in	MTNL	40468 40469	899168 899169	mtnl.net	internet	dr
in	MTNL	40468 40469	899168 899169	gprsmtnldel	internet	dr
in	MTNL	40468 40469	899168 899169	gprsppsmum	internet	dr
in	MTNL	40468 40469	899168 899169	gprsmtnlmum	internet	dr

in	MTNL	40468 40469	899168 899169	mmsmtnldel	mms	dr
in	Reliance	40409 40436 40452 40483 40485 40505 40510 40513	899109 899136 899152 899183 899185 899105 899110 899113	smartnet	internet	dr
in	Reliance	40409 40436 40452 40483 40485 40505 40510 40513	899109 899136 899152 899183 899185 899105 899110 899113	smartwap	wap	dr
in	Reliance	40409 40436 40452 40483 40485 40505 40510 40513	899109 899136 899152 899183 899185 899105 899110 899113	rcomnet	internet	dr
in	Reliance	40409 40436 40452 40483 40485 40505 40510 40513	899109 899136 899152 899183 899185 899105 899110 899113	mms	mms	dr
in	Reliance	40409 40436 40452 40483 40485 40505 40510 40513	899109 899136 899152 899183 899185 899105 899110 899113	rcommms	mms	dr

in	Spice telecom	40414 40444	899114 899144	Simplyenjoy	internet	dr
in	Spice telecom	40414 40444	899114 899144	simplydownload	internet	dr
in	Spice telecom	40414 40444	899114 899144	mmsc	mms	dr
in	Tata Docomo	405025 405026 405027 405029 405030 405031 405032 405034 405035 405036 405037 405038 405039 405041 405042 405043 405044 405045 405046 405047	8991025 8991026 8991027 8991029 8991030 8991031 8991032 8991034 8991035 8991036 8991037 8991038 8991039 8991041 8991042 8991043 8991044 8991045 8991046 8991047	TATA.DOCOMO.INTERNET	internet	dr
in	Tata Docomo	405025 405026 405027 405029 405030 405031 405032 405034 405035 405036 405037 405038 405039 405041 405042 405043 405044	8991025 8991026 8991027 8991029 8991030 8991031 8991032 8991034 8991035 8991036 8991037 8991038 8991039 8991041 8991042 8991043 8991044	TATADOCOMO3G	internet	dr

		405045 405046 405047	8991045 8991046 8991047			
in	Tata Docomo	405025 405026 405027 405029 405030 405031 405032 405034 405035 405036 405037 405038 405039 405041 405042 405043 405044 405045 405046 405047	8991025 8991026 8991027 8991029 8991030 8991031 8991032 8991034 8991035 8991036 8991037 8991038 8991039 8991041 8991042 8991043 8991044 8991045 8991046 8991047	TATA.DOCOMO.MMS	mms	dr
iq	Korek	41840	8996440	net.korek.com	internet	dr
iq	Asia Cell	41850	8996450	net.asiacell.com	internet	dr
iq	Asia Cell	41850	8996450	mtnirancell	mms	dr
ir	همراه اول	43211	899811	mcinet	internet	dr
ir	ایرانسل	43235	899835	mtnirancell	internet	dr
is	Vodafone	27402 27403	8935402 8935403	vmc.gprs.is	internet	dr 21
is	Nova	27411	8935411	internet.nova.is	internet	dr 19
is	Nova	27411	8935411	mms.nova.is	mms	dr
is	Síminn	27401	8935401	internet	internet	dr 21
is	Síminn	27401	8935401	mms.simi.is	mms	dr

it	Vodafone	22210	893910	mobile.vodafone.it	internet	d
it	Vodafone	22210	893910	web.omnitel.it	internet	d
it	Vodafone	22210	893910	web.omnitel.it	internet	d 8
it	TIM	22201	893901	ibox.tim.it	internet	d 2
it	TIM	22201	893901	wap.tim.it	wap	d 2
it	Wind	22288	893988	internet.wind	internet	d 1
it	Wind	22288	893988	internet.wind.biz	internet	d 1
it	Wind	22288	893988	mms.wind	mms	d
it	3	22299	893999	tre.it	internet	d 6
it	3	22299	893999	datacard.tre.it	internet	d
it	Fastweb	22299	893999	apn.fastweb.it	internet	d
it	Fastweb	22299	893999	datacard.fastweb.it	internet	d 2
it	Fastweb	22299	893999	tre.it	mms	d
it	PosteMobile	22210	893910	internet.postemobile.it	internet	d
it	PosteMobile	22210	893910	mms.postemobile.it	mms	d
it	CoopVoce	22201	893901	web.coopvoce.it	internet	d
it	Bip	22299	893999	internet.vistream.it	internet	d
it	Nòverca	22207	893907	web.noverca.it	internet	d
it	Nòverca	22207	893907	mms.noverca.it	mms	d
it	Nòverca	22207	893907	wap.noverca.it	wap	d
it	Tiscali	22201	893901	tiscalimobileinternet	internet	d

it	Lycamobile	22235	893935	data.lycamobile.it	internet	dr
je	Airtel-Vodaphone	23403	894403	airtel-ci-gprs.com	internet	dr
je	Sure (Cable & Wireless)	23455	894455	wap	wap	dr
je	Sure (Cable & Wireless)	23455	894455	internet	internet	dr
je	Jersey Telecom	23450	894450	pepper	internet	dr 21
jm	Cable & Wireless	338020	891020	wap	internet	dr
jm	Digicel	338050	891050	web.digiceljamaica.com	internet	dr 20
jo	Orange	41677	8996277	net.orange.jo	internet	dr
jo	Zain	41601	8996201	zain	internet	dr
jo	Zain	41601	8996201	Zain	mms	dr
jp	Softbank Mobile	44004 44006 44020 44040 44041 44042 44043 44044 44045 44046 44047 44048 44090 44092 44093 44094 44095 44096 44097 44098	898104 898106 898120 898140 898141 898142 898143 898144 898145 898146 898147 898148 898190 898192 898193 898194 898195 898196 898197 898198	softbank	internet	dr
jp	b-mobile	44010	898110	dm.jplat.net	internet	dr

jp	e-mobile	44000	898100	emb.ne.jp	internet	d
jp	NTTdocomo	44001 44002 44003 44009 44010 44011 44012 44013 44014 44015 44016 44017 44018 44019 44021 44022 44023 44024 44025 44026 44027 44028 44029 44030 44031 44032 44033 44034 44035 44036 44037 44038 44039 44049 44058 44060 44061 44062 44063 44064 44065 44066 44067 44068	898101 898102 898103 898109 898110 898111 898112 898113 898114 898115 898116 898117 898118 898119 898121 898122 898123 898124 898125 898126 898127 898128 898129 898130 898131 898132 898133 898134 898135 898136 898137 898138 898139 898149 898158 898160 898161 898162 898163 898164 898165 898166 898167 898168	mopera.ne.jp	internet	d

		44069 44087 44099	898169 898187 898199			
jp	NTTdocomo	44001 44002 44003 44009 44010 44011 44012 44013 44014 44015 44016 44017 44018 44019 44021 44022 44023 44024 44025 44026 44027 44028 44029 44030 44031 44032 44033 44034 44035 44036 44037 44038 44039 44049 44058 44060 44061 44062 44063 44064 44065 44066	898101 898102 898103 898109 898110 898111 898112 898113 898114 898115 898116 898117 898118 898119 898121 898122 898123 898124 898125 898126 898127 898128 898129 898130 898131 898132 898133 898134 898135 898136 898137 898138 898139 898149 898158 898160 898161 898162 898163 898164 898165 898166	mopera.net	internet	dr

		44067 44068 44069 44087 44099	898167 898168 898169 898187 898199			
ke	Airtel	63903	8925403	ke.celtel.com	internet	dr
ke	Airtel	63903	8925403	mms.yu.co.ke	mms	dr
ke	Safaricom	63902	8925402	safaricom	internet	dr
ke	Safaricom	63902	8925402	safaricom	internet	dr
ke	Safaricom	63902	8925402	mms.safaricom.com	mms	dr
ke	yu (Econet)	63905	8925405	internet.econet.co.ke	internet	dr
ke	Orange	63907	8925407	bew.orange.co.ke	internet	dr
kg	Beeline	43701	8999601	internet.beeline.kg	internet	dr
kg	MegaCom	43705	8999605	internet	internet	dr
kg	O!	43709	8999609	internet	internet	dr
kh	Cellcard	45601	8985501	cellcard	internet	dr
kh	Cellcard	45601	8985501	internet	mms	dr
kh	Cellcard	45601	8985501	mms	mms	dr
kh	Hello	45602	8985502	hellowww	internet	dr
kh	Hello	45602	8985502	hellomms	mms	dr
kh	qb	45604	8985504	WAP	internet	dr
kh	Smart Mobile	45606	8985506	smart	internet	dr
kh	Metfone	45608	8985508	metfone	internet	dr
kh	Beeline	45609	8985509	gprs.beeline.com.kh	internet	dr
kh	Mfone	45618	8985518	Mfone	internet	dr
kr	KT	45008	898208	alwayson.ktfwing.com	internet	dr
kr	KT	45008	898208	lte.ktfwing.com	internet	dr

kr	KT	45008	898208	lte.ktfwing.com	mms	dr
kr	LG U+	45006	898206	internet.lguplus.co.kr	internet	dr
kr	LG U+	45006	898206	internet.lguplus.co.kr	mms	dr
kr	SK Telecom	45005	898205	web.sktelecom.com	internet	dr
kr	SK Telecom	45005	898205	lte.sktelecom.com	internet	dr
kr	SK Telecom	45005	898205	lte.sktelecom.com	mms	dr
kw	Zain	41902	8996502	pps	internet	dr
kw	Zain	41902	8996502	apn01	internet	dr
kw	Wataniya	41903	8996503	action.wataniya.com	internet	dr
kw	Wataniya	41903	8996503	mms.wataniya.com	mms	dr
kw	Viva	41904	8996504	viva	internet	dr
kw	Viva	41904	8996504	viva	mms	dr
kz	Beeline	40101	89701	internet.beeline.kz	internet	dr 19
kz	K'CELL	40102	89702	internet	internet	dr
kz	K'CELL	40102	89702	mms	mms	dr
kz	Activ	40102	89702	internet	internet	dr
kz	Tele2	40177	89777	internet	internet	dr
kz	Altel 4G	40177	89777	internet	internet	dr
la	ETL	45702	8985602	etlnet	internet	dr
la	Lao Telecom	45701	8985601	ltcnet	internet	dr
la	Unitel	45703	8985603	startelecom	internet	dr
la	Unitel	45703	8985603	unitel3g	internet	dr
la	Beeline (Tigo)	45708	8985608	beelinenet	internet	dr
lb	MTC Touch	41503	8996103	gprs.mtctouch.com.lb	internet	dr
lb	MTC Touch	41503	8996103	mms.mtctouch.com.lb	mms	dr

li	Datamobile	29505	8942305	datamobile.ag	internet	dr
lc	Cable & Wireless	358110	891110	internet	internet	dr
lc	Cable & Wireless	358110	891110	multimedia	mms	dr
lk	Airtel	41305	899405	www.wap.airtel.lk	internet	dr
lk	Dialog GSM	41302	899402	www.dialogsl.com	internet	dr
lk	Dialog GSM	41302	899402	ppinternet	internet	dr
lk	Dialog GSM	41302	899402	dialogbb	internet	dr
lk	Dialog GSM	41302	899402	kitbb.com	internet	dr
lk	Dialog GSM	41302	899402	www.dialogsl.com	mms	dr
lk	Dialog GSM	41302	899402	ppwap	mms	dr
lk	Hutch	41308	899408	htwap	internet	dr
lk	Mobitel	41301	899401	isp	internet	dr
lk	Tigo	41303	899403	wap	internet	dr
ls	Vodacom Lesotho	65101	8926601	internet	internet	dr
lt	Bite	24602	8937002	banga	internet	dr 19
lt	Bite	24602	8937002	mms	mms	dr
lt	TELE2 GPRS	24603	8937003	internet.tele2.lt	internet	dr
lt	TELE2 GPRS	24603	8937003	mms.tele2.lt	mms	dr
lt	TELE2 GPRS	24603	8937003	mms.tele2.lv	mms	dr
lt	Omnitel (contract)	24601	8937001	gprs.omnitel.net	internet	dr 19
lt	Omnitel (contract)	24601	8937001	gprs.startas.lt	internet	dr 19
lt	Omnitel	24601	8937001	gprs.mms.lt	mms	dr

	(contract)					
lu	LUXGSM	27001	8935201	web.pt.lu	internet	dr 19
lu	LUXGSM	27001	8935201	mms.pt.lu	mms	dr
lu	Tango	27077	8935277	hspa	internet	dr
lu	Tango	27077	8935277	internet	internet	dr 21
lu	Tango	27077	8935277	mms	mms	dr
lu	Tango	27077	8935277	mms.li	mms	dr
lu	Orange	27099	8935299	orange.lu	internet	dr 85
lu	VOXmobile	27099	8935299	vox.lu	internet	dr
lu	VOXmobile	27099	8935299	vox.lu	mms	dr
lv	LMT	24701	8937101	internet.lmt.lv	internet	dr 21
lv	LMT	24701	8937101	open.lmt.lv	internet	dr
lv	LMT	24701	8937101	okarte.lmt.lv	internet	dr
lv	LMT	24701	8937101	mms.lmt.lv	mms	dr
lv	Tele2	24702	8937102	internet.tele2.lv	internet	dr
lv	Tele2	24702	8937102	mobileinternet.tele2.lv	internet	dr
lv	Tele2	24702	8937102	data.tele2.lv	internet	dr
lv	Bite	24705	8937105	wap	internet	dr
lv	Bite	24705	8937105	internet	internet	dr
ma	Ittissalat Al Maghrib (IAM)	60401	8921201	www.iamgprs1.ma	internet	dr
ma	Ittissalat Al Maghrib (IAM)	60401	8921201	www.iamgprs2.ma	internet	dr
ma	Ittissalat Al	60401	8921201	Mmsiam	mms	dr

	Maghrib (IAM)					
ma	Medi Telecom	60400	8921200	internet1.meditel.ma	internet	dr
ma	Medi Telecom	60400	8921200	internet2.meditel.ma	internet	dr
ma	Medi Telecom	60400	8921200	mms.meditel.ma	mms	dr
ma	WANA	60402	8921202	www.wana.ma	internet	dr
ma	WANA	60402	8921202	mms.wana.ma	mms	dr
md	Moldcell	25902	8937302	internet	internet	dr
md	Moldcell	25902	8937302	mms	mms	dr
md	Unité	25905	8937305	internet.unite.md	internet	dr
md	Unité	25905	8937305	internet3g.unite.md	internet	dr
md	Orange	25901	8937301	internet	internet	dr
me	ProMonte GSM	29701	8938201	gprs.promonte.com	internet	dr
me	ProMonte GSM	29701	8938201	mms.promonte.com	mms	dr
me	T-Mobile	29702	8938202	tmcg-data	internet	dr
me	T-Mobile	29702	8938202	tmcg-nw	internet	dr
me	T-Mobile	29702	8938202	internet-postpaid	internet	dr
me	T-Mobile	29702	8938202	internet-prepaid	internet	dr
me	m:tel	29703	8938203	gprsinternet	internet	dr
me	m:tel	29703	8938203	mtelmms	mms	dr
mg	Airtel	64601	8926101	internet	internet	dr
mg	Orange	64602	8926102	orangeworld	internet	dr
mg	Telma	64604	8926104	internet	internet	dr
ml	Malitel	61001	8922301	web.malitel3.ml	internet	dr
ml	Orange	61002	8922302	iew	internet	dr
ml	Orange	61002	8922302	internet	internet	dr

mm	MPT	41401	899501	mptnet	internet	dr
mm	Telenor	41406	899506	internet	internet	dr
mm	Ooredoo	41405	899505	internet	internet	dr
mn	MobiCom	42899	8997699	internet	internet	dr
mn	MobiCom	42899	8997699	mms	mms	dr
mo	3 / Hutchison	45503 45505	8985303 8985305	web.hutchisonmacau.com	internet	dr
mo	3 / Hutchison	45503 45505	8985303 8985305	mms.hutchisonmacau.com	mms	dr
mo	CTM	45501 45504	8985301 8985304	ctm-mobile	internet	dr
mo	CTM	45501 45504	8985301 8985304	ctmmms	mms	dr
mk	T-Mobile	29401	8938901	internet	internet	dr
mk	One	29402	8938902	datacard	internet	dr
mk	One	29402	8938902	mms	mms	dr
mk	Vodafone	29403	8938903	vipoperator	internet	dr
mk	Lycamobile	29404	8938904	data.lycamobile.mk	internet	dr
mt	GO Mobile	27821	8935621	gosurfing	internet	dr
mt	GO Mobile	27821	8935621	rtgsurfing	internet	dr
mt	GO Mobile	27821	8935621	gomms	mms	dr
mt	Melita	27877	8935677	web.melita	internet	dr
mt	Vodafone	27801	8935601	Internet	internet	dr 80
mu	Emtel	61710	8923010	WEB	internet	dr
mv	Dhiraagu	47201	8996001	internet.dhimobile	internet	dr
mv	Dhiraagu	47201	8996001	mms.dhimobile	mms	dr
mv	Wataniya	47202	8996002	WataniyaNet	internet	dr

mw	TNM	65001	8926501	Internet	internet	dr
mx	Telcel	33402	895202	internet.itelcel.com	internet	dr
mx	Telcel	33402	895202	mms.itelcel.com	mms	dr
mx	Movistar	33403	895203	internet.movistar.mx	internet	dr
my	DiGi	50216	896016	diginet	internet	dr 20
my	DiGi	50216	896016	3gdgnet	internet	dr
my	DiGi	50216	896016	digimms	mms	dr
my	Maxis	50212 50217	896012 896017	maxisbb	internet	dr
my	Maxis	50212 50217	896012 896017	net	internet	dr
my	Maxis	50212 50217	896012 896017	unet	internet	dr 10
my	Maxis	50212 50217	896012 896017	unet	mms	dr
my	Celcom	50213 50219	896013 896019	celcom.net.my	internet	dr
my	Celcom	50213 50219	896013 896019	celcom3g	internet	dr
my	Celcom	50213 50219	896013 896019	celcom3g	mms	dr
mz	MCel	64301	8925801	isp.mcel.mz	internet	dr 2
mz	MCel	64301	8925801	mms.mcel.mz	mms	dr
mz	Vodacom	64304	8925804	internet	internet	dr
na	MTC	64901	8926401	ppsinternet	internet	dr
na	MTC	64901	8926401	internet	internet	dr
na	Leo	64903	8926403	internet	internet	dr

na	Leo	64903	8926403	mms	mms	dr
ng	Airtel NG	62120 62180	8923420 8923480	internet.ng.airtel.com.ng	internet	dr
ng	MTN	62130 62160	8923430 8923460	web.gprs.mtnnigeria.net	internet	dr
ng	Glo Mobile	62150 62170	8923450 8923470	glosecure	internet	dr
ng	Glo Mobile	62150 62170	8923450 8923470	gloflat	internet	dr
ng	Etisalat	62190	8923490	etisalat	internet	dr
ni	Claro	71021 71073	8950521 8950573	wap.emovil	wap	dr
ni	Claro	71021 71073	8950521 8950573	web.emovil	internet	dr
ni	Claro	71021 71073	8950521 8950573	internet.ideasalo.ni	internet	dr
ni	Claro	71021 71073	8950521 8950573	wap.ideasalo.ni	wap	dr
ni	Movistar	71030	8950530	internet.movistar.ni	internet	dr
nl	Hi	20408	893108	portalmmm.nl	internet	dr
nl	Hi	20408	893108	portalmmm.nl	mms	dr
nl	Lebara	20412	893112	multimedia.lebara.nl	internet	dr
nl	Lebara	20412	893112	internet	mms	dr
nl	Lycamobile	20409	893109	data.lycamobile.nl	internet	dr
nl	KPN NL	20408	893108	prepaidinternet	internet	dr
nl	KPN NL	20408	893108	fastinternet	internet	dr
nl	KPN NL	20408	893108	internet	internet	dr 62
nl	KPN NL	20408	893108	KPN4G.nl	internet	dr

nl	KPN NL	20408	893108	portalmmm.nl	internet	dr
nl	KPN NL	20408	893108	portalmmm.nl	mms	dr
nl	MEDIONmobile	20408 20410	893108 893110	portalmmm.nl	internet	dr
nl	Telfort	20412	893112	internet	internet	dr
nl	T-Mobile	20416	893116	internet	internet	dr
nl	T-Mobile	20416	893116	smartsites.t-mobile	internet	dr
nl	T-Mobile	20416	893116	mms	mms	dr
nl	Ben	20416	893116	basic.internet.ben.data	internet	dr 19
nl	Ben	20416	893116	internet.ben	internet	dr 19
nl	Ben	20416	893116	mms.ben	mms	dr
nl	Orange	20420	893120	internet	internet	dr
nl	Tele2	20402	893102	data.tele2.nl	internet	dr
nl	XS4ALL Mobiel Internet			umts.xs4all.nl	internet	dr
nl	Vodafone	20404 20444	893104 893144	live.vodafone.com	internet	dr 62
nl	Vodafone	20404 20444	893104 893144	office.vodafone.nl	internet	dr
nl	Vodafone	20404 20444	893104 893144	m2m.global.vodafone.nl	internet	dr
nl	Galaxy	20408	893108	internet	internet	dr
no	Netcom	24202	894702	internet.netcom.no	internet	dr 21
no	Netcom	24202	894702	mms.netcom.no	mms	dr
no	Chess	24202	894702	netcom	internet	dr
no	Chess	24202	894702	mms.netcom.no	mms	dr

no	Telenor	24201	894701	telenor.smart	internet	dr
no	Telenor	24201	894701	telenor.smart	mms	dr
no	Telenor	24201	894701	mms.ventelo.no	mms	dr
no	TDC	24208	894708	internet.no	internet	dr 80
no	Network Norway	24205	894705	internet	internet	dr
no	Network Norway	24205	894705	mms	mms	dr
no	OneCall	24205	894705	internet	internet	dr
no	MyCall	24205	894705	internet	internet	dr
no	Altibox			internet	internet	dr
no	Telipol	24205	894705	internet	internet	dr
no	Ventelo	24207	894707	internet.ventelo.no	internet	dr
no	Ludo Mobil	24207	894707	internet.ventelo.no	internet	dr
no	Tele2	24202 24204	894702 894704	internet.tele2.no	wap	dr
no	Tele2	24202 24204	894702 894704	mobileinternet.tele2.no	internet	dr
no	Phonero	24201	894701	internet.phonero.no	internet	dr
no	Lycamobile	24223	894723	data.lyca-mobile.no	internet	dr
np	Nepal Telecom	42901	8997701	ntnet	internet	dr
np	Mero Mobile	42902	8997702	mero	internet	dr
nz	Telecom New Zealand	53000 53005	896400 896405	wap.telecom.co.nz	wap	dr
nz	Telecom New Zealand	53000 53005	896400 896405	internet.telecom.co.nz	internet	dr 20
nz	Telecom New Zealand	53000 53005	896400 896405	direct.telecom.co.nz	internet	dr 20

nz	Telecom New Zealand	53000 53005	896400 896405	oa.telecom.co.nz	internet	dr
nz	Telecom New Zealand	53000 53005	896400 896405	wap.telecom.co.nz	mms	dr
nz	Vodafone	53001	896401	live.vodafone.com	internet	dr 20
nz	Vodafone	53001	896401	www.vodafone.net.nz	internet	dr
nz	Vodafone	53001	896401	internet	internet	dr 20
nz	2-Degrees	53024	896424	mms	mms	dr
nz	2-Degrees	53024	896424	internet	internet	dr 1
nz	2-Degrees	53024	896424	mms	mms	dr
nz	TelstraClear			www.telstraclear.net.nz	internet	dr
nz	Orcon			www.orcon.net.nz	internet	dr
om	Oman Mobile	42202	8996802	taif	internet	dr
om	Oman Mobile	42202	8996802	internet	internet	dr
om	Oman Mobile	42202	8996802	MMS	mms	dr
om	Nawras	42203	8996803	isp.nawras.com.om	internet	dr
om	Nawras	42203	8996803	mms.nawras.com.om	mms	dr
pa	Cable and Wireless	71401	8950701	apn01.cwpanama.com.pa	internet	dr
pa	Cable and Wireless	71401	8950701	apn02.cwpanama.com.pa	mms	dr
pa	Movistar	71402	8950702	internet.movistar.pa	internet	dr 20
pe	Claro	71610	895110	tim.pe	internet	dr
pe	Claro	71610	895110	ba.amx	internet	dr
pe	Movistar	71606	895106	movistar.pe	internet	dr

pe	Nextel	71607	895107	datacard.nextel.com.pe	internet	dr
pe	Nextel	71607	895107	mms	mms	dr
pf	Vini	54720	8968920	internet	internet	dr
pg	Digicel	53703	8967503	internet.digicelpng.com	internet	dr 8.
ph	Globe Telecom	51502	896302	internet.globe.com.ph	internet	dr 20
ph	Globe Telecom	51502	896302	http.globe.com.ph	internet	dr 20
ph	Globe Telecom	51502	896302	www.globe.com.ph	internet	dr 20
ph	Globe Telecom	51502	896302	mms.globe.com.ph	mms	dr
ph	Smart	51503	896303	internet	internet	dr 20
ph	Smart	51503	896303	mms	mms	dr
ph	Digitel (Sun Cellular)	51505	896305	minternet	internet	dr
ph	Digitel (Sun Cellular)	51505	896305	mms	mms	dr
pk	Djuice	51506	899206	internet	internet	dr
pk	Mobilink	51501	899201	connect.mobilinkworld.com	internet	dr
pk	Mobilink	51501	899201	jazzconnect.mobilinkworld.com	internet	dr
pk	Telenor	51506	899206	internet	internet	dr
pk	Ufone	41003	899203	ufone.internet	internet	dr
pk	Ufone	41003	899203	ufone.mms	mms	dr
pk	Warid	51507	899207	warid	internet	dr
pk	Warid	51507	899207	zongmms	mms	dr
pk	ZONG	51504	899204	zonginternet	internet	dr

pl	T-mobile	26002	894802	internet	internet	dr 2
pl	T-mobile	26002	894802	mms	mms	dr
pl	Play Online	26006	894806	internet	internet	dr
pl	Play Online	26006	894806	mms	mms	dr
pl	Orange	26003	894803	internet	internet	dr 19
pl	Orange	26003	894803	vpn	internet	dr 19
pl	Plus	26001	894801	www.plusgsm.pl	internet	dr 2
pl	Plus	26001	894801	pro.plusgsm.pl	internet	dr 2
pl	Plus	26001	894801	m2m.plusgsm.pl	internet	dr 2
pl	Plus	26001	894801	optimizer	internet	dr 2
pl	Plus	26001	894801	mms.plusgsm.pl	mms	dr
pl	Cyfrowy Polsat	26012	894812	multi.internet	internet	dr
pl	aero2	26017	894817	darmowy	internet	dr
pl	Multimo	26003	894803	internet	internet	dr
pl	Multimo	26003	894803	mni.internet	internet	dr
pl	Multimo	26003	894803	telogic.internet	internet	dr
pl	FreeM	26001	894801	freedata.pl	internet	dr
pl	Heyah	26002	894802	heyah.pl	internet	dr 2
pl	GaduAIR	26001	894801	internet.gadu-gadu.pl	internet	dr
pl	Aster	26003	894803	aster.internet	internet	dr
pl	Netia	26006	894806	internet	internet	dr

pl	Vectra	26006	894806	internet	internet	dr
pl	mBank mobile	26001	894801	www.mobile.pl	internet	dr
pl	INEA	26003	894803	telogic.internet	internet	dr
pl	Mobilking	26002	894802	wapMOBILKING	internet	dr
pl	SamiSwoi	26001	894801	www.plusgsm.pl	internet	dr
pl	Lycamobile	26009	894809	data.lycamobile.pl	internet	dr
pt	Kanguru	26803	8935103	kanguru-portatil	internet	dr 62
pt	Kanguru	26803	8935103	kanguru-tempo	internet	dr 62
pt	Kanguru	26803	8935103	kangurufixo	internet	dr 62
pt	Kanguru	26803	8935103	noapn		dr 62
pt	Kanguru	26803	8935103	umts	mms	dr
pt	Clix	26803	8935103	clixinternetmovel	internet	dr
pt	Optimus	26803	8935103	umts	internet	dr
pt	Optimus	26803	8935103	internet	internet	dr
pt	Lycamobile	26804	8935104	data.lycamobile.pt	internet	dr
pt	TMN	26806	8935106	internet	internet	dr 88
pt	TMN	26806	8935106	mmsc.tmn.pt	mms	dr 19
pt	TMN	26806	8935106	mmsc.tmn.pt	mms	dr
pt	Vodafone	26801	8935101	internet.vodafone.pt	internet	dr 21
pt	Vodafone	26801	8935101	net2.vodafone.pt	internet	dr
pt	Vodafone	26801	8935101	vas.vodafone.pt	mms	dr

pt	ZON	26801	8935101	internet.zon.pt	internet	dr
pt	ZON	26801	8935101	vas.zon.pt	mms	dr
pt	ZON	26801	8935101	vas.zon.pt	mms	dr
py	VOX	74401	8959501	vox.wap	internet	dr
py	VOX	74401	8959501	vox.mms	mms	dr
py	Personal	74405	8959505	internet	internet	dr
py	Tigo	74404	8959504	internet.tigo.py	internet	dr
py	Tigo	74404	8959504	broadband.tigo.py	internet	dr
py	Claro	74402	8959502	gprs.claro.com.py	internet	dr
qa	Vodafone	42702	8997402	web.vodafone.com.qa	internet	dr
qa	Vodafone	42702	8997402	vodafone.com.qa	internet	dr
qa	Q-Tel	42701	8997401	gprs.qtel	internet	dr
qa	Q-Tel	42701	8997401	mms.qtel	mms	dr
re	SFR Réunion	64710	8926210	websfr	internet	dr
re	SFR Réunion	64710	8926210	slsfr	internet	dr
re	SFR Réunion	64710	8926210	internetpro	internet	dr
re	SFR Réunion	64710	8926210	ipnet	internet	dr
re	SFR Réunion	64710	8926210	mmssfr	mms	dr
ro	Orange	22610	894010	internet	internet	dr 17
ro	Vodafone	22601	894001	tobe.vodafone.ro	internet	dr
ro	Vodafone	22601	894001	internet.vodafone.ro	internet	dr
ro	Vodafone	22601	894001	internet.pre.vodafone.ro	internet	dr
ro	Vodafone	22601	894001	live.vodafone.com	internet	dr
ro	Vodafone	22601	894001	live.pre.vodafone.ro	internet	dr
ro	Digi.Net Mobil	22605	894005	internet	internet	dr

ro	Digi.Net Mobil	22605	894005	static	internet	dr
ro	Lycamobile	22616	894016	data.lycamobile.ro	internet	dr
rs	Telenor	22001	8938101	internet	internet	dr
rs	Telenor	22001	8938101	mms	mms	dr
rs	Telekom Srbija	22003	8938103	gprsinternet	internet	dr
rs	Telekom Srbija	22003	8938103	mms	mms	dr
rs	VIP Mobile	22005	8938105	vipmobile	internet	dr
rs	VIP Mobile	22005	8938105	vipmobile.mms	mms	dr
rw	MTN	63510	8925010	internet.mtn	internet	dr
rw	Tigo	63513	8925013	web.tigo.rw	internet	dr
ru	BaikalWestCom	25012	89712	inet.bwc.ru	internet	dr 81
ru	BaikalWestCom	25012	89712	mms.bwc.ru	mms	dr
ru	Beeline	25028 25099	89728 89799	home.beeline.ru	internet	dr 21
ru	Beeline	25028 25099	89728 89799	internet.beeline.ru	internet	dr 21
ru	ETK	25005	89705	wap.etk.ru	internet	dr
ru	MTS	25001	89701	internet.mts.ru	internet	dr 21
ru	Megafon	25002	89702	internet	internet	dr
ru	Megafon	25002	89702	mms	mms	dr
ru	NCC	25003	89703	internet	internet	dr '
ru	NTC	25016	89716	internet.ntc	internet	dr 80
ru	NTC	25016	89716	mms.ntc	mms	dr
ru	Enisey TeleCom	25005	89705	internet.etk.ru	internet	dr

ru	Motiv	25035	89735	inet.ycc.ru	internet	dr 21
ru	Tatincom			internet.tatincom.ru	internet	dr 89
ru	Tele2	25020	89720	internet.tele2.ru	internet	dr 13
ru	U-tel	25039	89739	internet.usi.ru	internet	dr
ru	U-tel	25039	89739	mnc039.mcc250.gprs	mms	dr
sa	Mobily	42003	8996603	web1	internet	dr
sa	Mobily	42003	8996603	web2	internet	dr
sa	Mobily	42003	8996603	mms1	mms	dr
sa	STC	42001	8996601	jawalnet.com.sa	internet	dr 21
sa	STC	42001	8996601	mms.net.sa	mms	dr
sa	STC	42001	8996601	mms.net.sa	mms	dr
sa	Zain	42004	8996604	zain	internet	dr
se	3	24002 24004	894602 894604	data.tre.se	internet	dr
se	3	24002 24004	894602 894604	bredband.tre.se	internet	dr
se	3	24002 24004	894602 894604	net.tre.se	internet	dr
se	Glocalnet	24008	894608	bredband.glocalnet.se	internet	dr
se	Glocalnet	24008	894608	internet.glocalnet.se	internet	dr
se	Glocalnet	24008	894608	services.glocalnet.se	mms	dr
se	Halebop	24001	894601	halebop.telia.se	internet	dr
se	Halebop	24001	894601	mms.telia.se	mms	dr

se	Tele2	24007 24005	894607 894605	internet.tele2.se	internet	dr
se	Tele2	24007 24005	894607 894605	mobileinternet.tele2.se	internet	dr
se	Comviq	24007 24005	894607 894605	data.comviq.se	internet	dr
se	Comviq	24007 24005	894607 894605	internet.tele2.se	internet	dr
se	Comviq	24007 24005	894607 894605	mobileinternet.tele2.se	internet	dr
se	Comviq	24007 24005	894607 894605	internet.tele2.se	mms	dr
se	Multicom Security	24001 24005	894601 894605	mobiflex.telia.se	internet	dr
se	Multicom Security	24001 24005	894601 894605	mms.telia.se	mms	dr
se	Telenor	24004 24006 24008	894604 894606 894608	internet.telenor.se	internet	dr
se	Telenor	24004 24006 24008	894604 894606 894608	services.telenor.se	internet	dr
se	Telenor	24004 24006 24008	894604 894606 894608	bredband.telenor.se	internet	dr
se	Telenor	24004 24006 24008	894604 894606 894608	sp-services	mms	dr
se	Telia	24001 24005	894601 894605	online.telia.se	internet	dr
se	TDC	24014	894614	internet.se	internet	dr
se	TDC	24014	894614	data.tre.se	mms	dr
se	djuice	24009	894609	internet.djuice.se	internet	dr

se	Com Hem	24002 24004	894602 894604	bredband.comhem.se	internet	dr
se	Parlino	24007	894607	internet.parlino.se	internet	dr
se	Universal Telecom			sp-internet	internet	dr
se	Universal Telecom			internet.uvtc.com	internet	dr
se	Lycamobile	24012	894612	data.lycamobile.se	internet	dr
sg	M1	52503	896503	sunsurf	internet	dr 20
sg	M1	52503	896503	miworld	internet	dr
sg	M1	52503	896503	miworldcard	internet	dr
sg	M1	52503	896503	prepaidbb	internet	dr
sg	M1	52503	896503	sunsurfmcard	internet	dr
sg	M1	52503	896503	miworld	mms	dr
sg	SingTel	52501 52502	896501 896502	internet	internet	dr 16
sg	SingTel	52501 52502	896501 896502	e-ideas	mms	dr
sg	Starhub	52505	896505	shwap	wap	dr
sg	Starhub	52505	896505	shppd	internet	dr
sg	Starhub	52505	896505	shinternet	internet	dr
sg	Starhub	52505	896505	shmms	mms	dr
si	Mobitel	29341	8938641	internet	internet	dr 19
si	Mobitel	29341	8938641	internetpro	internet	dr 19
si	Vodafone / Simobil	29340	8938640	internet.simobil.si	internet	dr 19

si	Vodafone / Simobil	29340	8938640	mms.simobil.si	mms	dr
si	T-2	29364	8938664	internet.t-2.net	internet	dr
si	T-2	29364	8938664	mms.t-2.net	mms	dr
sk	Slovak Telekom	23102 23104	8942102 8942104	internet	internet	dr 19
sk	Slovak Telekom	23102 23104	8942102 8942104	mms	mms	dr
sk	Orange	23101	8942101	internet	internet	dr 21
sk	O2	23106	8942106	o2internet	internet	dr 19
sk	O2	23106	8942106	o2mms	mms	dr
sn	Tigo	60802	8922102	wap.sentelgsm.com	internet	dr 20
sv	Movistar	70604	8950304	internet.movistar.sv	internet	dr
sv	digicel	70602	8950302	wap.digicelsv.com	internet	dr
sv	digicel	70602	8950302	wap.digicelsv.com	mms	dr
sv	Tigo	70603	8950303	internet.tigo.sv	internet	dr
sv	Claro	70601	8950301	internet.ideasclaro	internet	dr
sd	Zain	63401	8924901	internet	internet	dr
sd	MTN	63402	8924902	internet	internet	dr
sd	Sudani	63407	8924907	sudaninet	internet	dr
th	AIS	52001	896601	internet	internet	dr 20
th	AIS	52001	896601	multimedia	mms	dr
th	DTAC	52018	896618	www.dtac.co.th	internet	dr 20
th	DTAC	52018	896618	mms	mms	dr

th	True Move	52099	896699	internet	internet	dr
th	True Move	52099	896699	mms	mms	dr
th	TOT 3G	52015	896615	internet	internet	dr
tn	Orange	60501	8921601	weborange	internet	dr
tn	Orange	60501	8921601	mms.otun	mms	dr
tn	Orange	60501	8921601	keygp	internet	dr
tn	Orange	60501	8921601	keypro	internet	dr
tn	Tunisie Télécom / TUNTEL	60502	8921602	mms.tn	mms	dr
tn	Tunisie Télécom / TUNTEL	60502	8921602	gprs.tn	internet	dr
tn	Tunisie Télécom / TUNTEL	60502	8921602	internet.tn	internet	dr
tn	Tunisie Télécom / TUNTEL	60502	8921602	mms.tn	mms	dr
tn	Lycamobile	60502	8921602	data.lycamobile.tn	internet	dr
tn	Tunisiana	60503	8921603	internet.tunisiana.com		dr
tn	Tunisiana	60503	8921603	mms.tunisiana.com	mms	dr
tr	Avea	28603 28604	899003 899004	internet	internet	dr 21
tr	Avea	28603 28604	899003 899004	aycell	internet	dr 21
tr	Avea	28603 28604	899003 899004	mms	mms	dr
tr	Turkcell	28601	899001	internet	internet	dr
tr	Turkcell	28601	899001	mgb	internet	dr
tr	Turkcell	28601	899001	mms	mms	dr
tr	Vodafone	28602	899002	internet	internet	dr

tr	Vodafone	28602	899002	edge.kktctelsim.com	internet	dr
tt	Digicel	37413	89113	wap.digiceltt.com	internet	dr
tt	Digicel	37413	89113	wap.digiceltt.com	mms	dr
tt	bmobile / TSTT	37412	89112	internet	internet	dr
tt	bmobile / TSTT	37412	89112	mms	mms	dr
tw	Chunghwa Telecom (emome)	46692	8992	emome	internet	dr
tw	Chunghwa Telecom (emome)	46692	8992	internet	internet	dr
tw	Chunghwa Telecom (emome)	46692	8992	emome	mms	dr
tw	Far EasTone / KGT	46601	8901	internet	internet	dr
tw	Far EasTone / KGT	46601	8901	fetnet01	mms	dr
tw	TW Mobile	46699	8999	internet	internet	dr
tw	TW Mobile	46699	8999	mms	mms	dr
tw	TransAsia	46697	8997	internet	internet	dr
tw	TransAsia	46697	8997	vibo	mms	dr
tw	Vibo Telecom / Aurora	46689	8989	vibo	internet	dr
tw	Vibo Telecom / Aurora	46689	8989	MMS	mms	dr
tz	Airtel Tanzania	64005	8925505	internet	internet	dr
tz	Vodacom	64004	8925504	internet	internet	dr
tz	Zantel	64003	8925503	znet	internet	dr
tz	tiGO	64002	8925502	internet	internet	dr

ua	kyivstar	25503	8938003	www.ab.kyivstar.net	internet	dr
ua	kyivstar	25503	8938003	www.kyivstar.net	internet	dr
ua	kyivstar	25503	8938003	3g.kyivstar.net	internet	dr
ua	kyivstar	25503	8938003	mms.kyivstar.net	mms	dr
ua	Djuice	25503	8938003	www.djuice.com.ua	internet	dr
ua	Djuice	25503	8938003	xl.kyivstar.net	internet	dr
ua	Djuice	25503	8938003	3g.kyivstar.net	internet	dr
ua	life:)	25506	8938006	internet	internet	dr 2
ua	life:)	25506	8938006	speed	internet	dr 2
ua	Beeline	25502	8938002	internet.beeline.ua	internet	dr
ua	Jeans	25501	8938001	www.jeans.ua	internet	dr 8
ua	Jeans	25501	8938001	hyper.net	internet	dr 2
ua	MTS	25501	8938001	internet	internet	dr 2
ua	MTS	25501	8938001	hyper.net	internet	dr
ua	MTS	25501	8938001	active	internet	dr
ua	MTS	25501	8938001	www.umc.ua	internet	dr 8
ua	Utel	25507	8938007	3g.utel.ua	internet	dr
ua	Utel	25507	8938007	3g.utel.ua	mms	dr
ug	MTN	64110	8925610	yellopix.mtn.co.ug	internet	dr 1
ug	Orange	64114	8925614	orange.ug	internet	dr
ug	Orange	64114	8925614	mms.warid.co.ug	mms	dr

ug	UTL	64111	8925611	utbroadband	internet	dr
ug	UTL	64111	8925611	utweb	internet	dr
ug	UTL	64111	8925611	utwap	mms	dr
ug	Warid	64122	8925622	web.waridtel.co.ug	internet	dr
ug	Zain	64101	8925601	web.ug.zain.com	internet	dr
us	AT&T	310038 310090 310150 310410 310560 310680	891038 891090 891150 891410 891560 891680	wap.cingular	internet	dr
us	AT&T	310038 310090 310150 310410 310560 310680	891038 891090 891150 891410 891560 891680	Broadband	internet	dr
us	AT&T	310038 310090 310150 310410 310560 310680	891038 891090 891150 891410 891560 891680	isp.cingular	internet	dr
us	AT&T	310038 310090 310150 310410 310560 310680	891038 891090 891150 891410 891560 891680	pta	internet	dr
us	AT&T	310038 310090 310150 310410 310560 310680	891038 891090 891150 891410 891560 891680	wap.cingular	mms	dr
us	T-Mobile	310026 310160 310200	891026 891160 891200	fast.t-mobile.com	internet	dr

		310210 310220 310230 310240 310250 310260 310270 310310 310490 310580 310660 310800	891210 891220 891230 891240 891250 891260 891270 891310 891490 891580 891660 891800			
us	T-Mobile	310026 310160 310200 310210 310220 310230 310240 310250 310260 310270 310310 310490 310580 310660 310800	891026 891160 891200 891210 891220 891230 891240 891250 891260 891270 891310 891490 891580 891660 891800	epc.tmobile.com	internet	dr 10
us	T-Mobile	310026 310160 310200 310210 310220 310230 310240 310250 310260 310270 310310 310490 310580 310660 310800	891026 891160 891200 891210 891220 891230 891240 891250 891260 891270 891310 891490 891580 891660 891800	wap.voicestream.com	internet	dr
us	T-Mobile	310026 310160	891026 891160	internet2.voicestream.com	internet	dr

		310200 310210 310220 310230 310240 310250 310260 310270 310310 310490 310580 310660 310800	891200 891210 891220 891230 891240 891250 891260 891270 891310 891490 891580 891660 891800			
us	T-Mobile	310026 310160 310200 310210 310220 310230 310240 310250 310260 310270 310310 310490 310580 310660 310800	891026 891160 891200 891210 891220 891230 891240 891250 891260 891270 891310 891490 891580 891660 891800	internet3.voicestream.com	internet	dr
us	Cincinnati Bell Wireless	310420	891420	wap.gocbw.com	internet	dr
us	Cincinnati Bell Wireless	310420	891420	wap.gocbw.com	mms	dr
us	Verizon	310995 311480	891995 891480	vzwims	ims	dr
us	Verizon	310995 311480	891995 891480	vzwinternet	internet	dr 69
us	Verizon	310995 311480	891995 891480	vzwapp	wap	dr
us	Alltel	310590	891590	MMS	mms	dr

us	Alltel	310590	891590	cellular1wap	mms	dr
us	BendBroadband	311570	891570	ISP	internet	dr
us	MTPCS (Cellular One)	310570	891570	wapgw.chinookwireless.net	internet	dr
us	Straight Talk	310410	891410	att.mvno	internet	dr
us	Straight Talk	310410	891410	tfdata	internet	dr
us	Lycamobile	311960	891960	data.lycamobile.com	internet	dr
uy	Ancel	74800 74801	8959800 8959801	adslmovil	internet	dr 20
uy	Ancel	74800 74801	8959800 8959801	prepago.ancel	internet	dr
uy	Ancel	74800 74801	8959800 8959801	gprs.ancel	internet	dr 20
uy	Ancel	74800 74801	8959800 8959801	mms	mms	dr
uy	Claro	74810	8959810	gprs.claro.com.uy	internet	dr
uy	Claro	74810	8959810	internet.ctimovil.com.uy	internet	dr
uy	Movistar	74807	8959807	apnumt.movistar.com.uy	internet	dr
uy	Movistar	74807	8959807	webapn.movistar.com.uy	internet	dr
uz	Beeline	43404	8999804	internet.beeline.uz	internet	dr
uz	Ucell	43405	8999805	internet		dr
uz	UMS	43407	8999807	net.ums.uz	internet	dr
vc	Digicel	360070	891070	wap.digiceloecs.com	internet	dr
ve	Digitel TIM	73401 73402 73403	895801 895802 895803	gprsweb.digitel.ve	internet	dr
ve	Digitel TIM	73401 73402 73403	895801 895802 895803	expresate.digitel.ve	mms	dr

ve	Movilnet	73406	895806	int.movilnet.com.ve	internet	dr 20
ve	Movilnet	73406	895806	mm.movilnet.com.ve	mms	dr
ve	Movistar	73404	895804	internet.movistar.ve	internet	dr 20
vn	MobiFone	45201	898401	m-wap	internet	dr
vn	MobiFone	45201	898401	m-i090	mms	dr
vn	Vinaphone	45202	898402	m3-world	internet	dr
vn	Vinaphone	45202	898402	m3-card	internet	dr
vn	Vinaphone	45202	898402	m3-mms	mms	dr
vn	Viettel Mobile	45204	898404	v-internet	internet	dr
vn	Viettel Mobile	45204	898404	e-connect	internet	dr
vn	Viettel Mobile	45204	898404	v-mms	mms	dr
vn	Vietnamobile	45205	898405	internet	internet	dr
vn	Vietnamobile	45205	898405	mms	mms	dr
vn	EVNTelecom/E-Mobile	45208	898408	e-internet	internet	dr
vn	Beeline VN	45207	898407	internet	internet	dr
za	Cell-c	65507	892707	internet	internet	dr 19
za	MTN	65510	892710	internet	internet	dr 20
za	Vodacom	65501	892701	internet	internet	dr 19
za	Vodacom	65501	892701	unrestricted	internet	dr 19
za	Vodacom	65501	892701	mms.vodacom.net	mms	dr
za	Virgin Mobile	65507	892707	vdata	internet	dr 19

za	8.ta	65502	892702	internet	internet	dr
za	8.ta	65502	892702	mms	mms	dr

Inbound IP Passthrough Activity Not Acting as Intended on Device Firmware [RESOLVED]

NOTE: *This issue is resolved as of the 18.4.54.41 release.*

Problem

Unable to send inbound traffic from an external source to the cellular IP (IE: ping) of an Accelerated cellular device on firmware 18.4.54.22 configured with IP Passthrough

Background

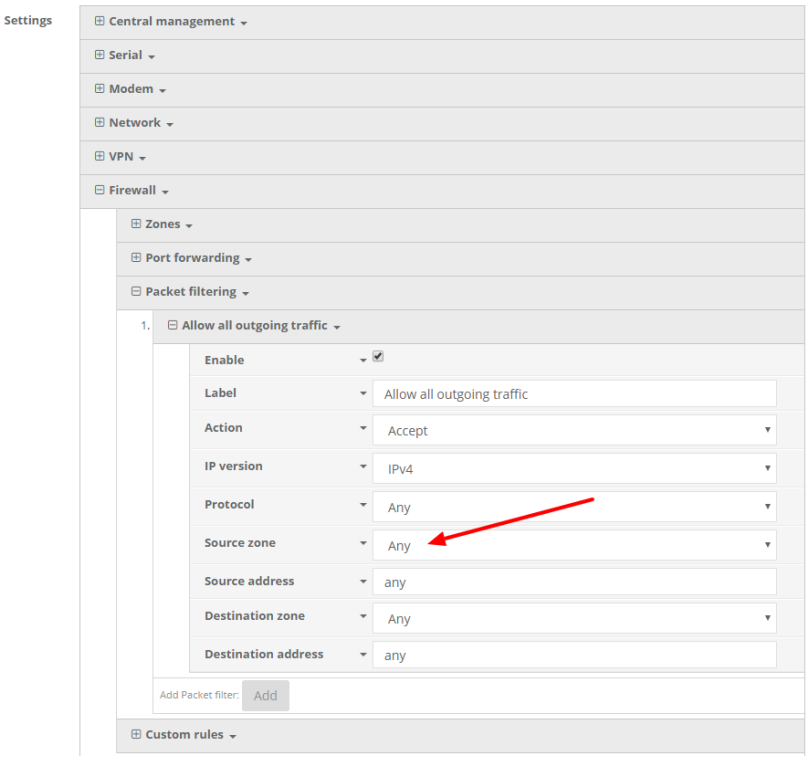
We've been seeing an issue where the latest firmware has unintentionally engaged the firewall for passthrough connections. This results in failed pings from an external source of the cellular IP of an Accelerated cellular device on firmware 18.4.54.22 configured with IP Passthrough.

IP Passthrough Knowledge Article: http://kb.accelerated.com/m/67105/l/745871-lan-port-with-ip-passthrough

Manual Solution

On firmware 18.4.54.22, a change can be made to the Packet Filter's config (Firewall > Packet filtering > Allow all outgoing traffic > Source Zone > Change to "Any" instead of "Internal"). This is the intended passthrough functionality and how it operates on firmware versions 18.1 and prior.

The unintentional engagement of the firewall for passthrough connections will be addressed in a subsequent firmware release.


Settings
Central management
Serial
Modem
Network
VPN
Firewall
Zones
Port forwarding
Packet filtering
1.
Allow all outgoing traffic
Enable
Label
Allow all outgoing traffic
Action
Accept
IP version
IPv4
Protocol
Any
Source zone
Any
Source address
any
Destination zone
Any
Destination address
any
Add Packet filter:
Add
Custom rules

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

NOTE: *This issue is resolved as of the 18.4.54.41 release.*

Problem

A newly activated Verizon SIM with a static APN (e.g. ne01.vzwstatic) is inserted into a 63xx-series device on 18.4.54.22 device firmware using the CM04. The 63xx-series cellular extender is able to detect the SIM and seeing an available Verizon network, but the 63xx-series device is unable to establish a cellular connection. The LED behavior on the front of the 63xx-series device will be a flashing white status/LTE LED, and intermittent 5 bars of signal strength.

Background

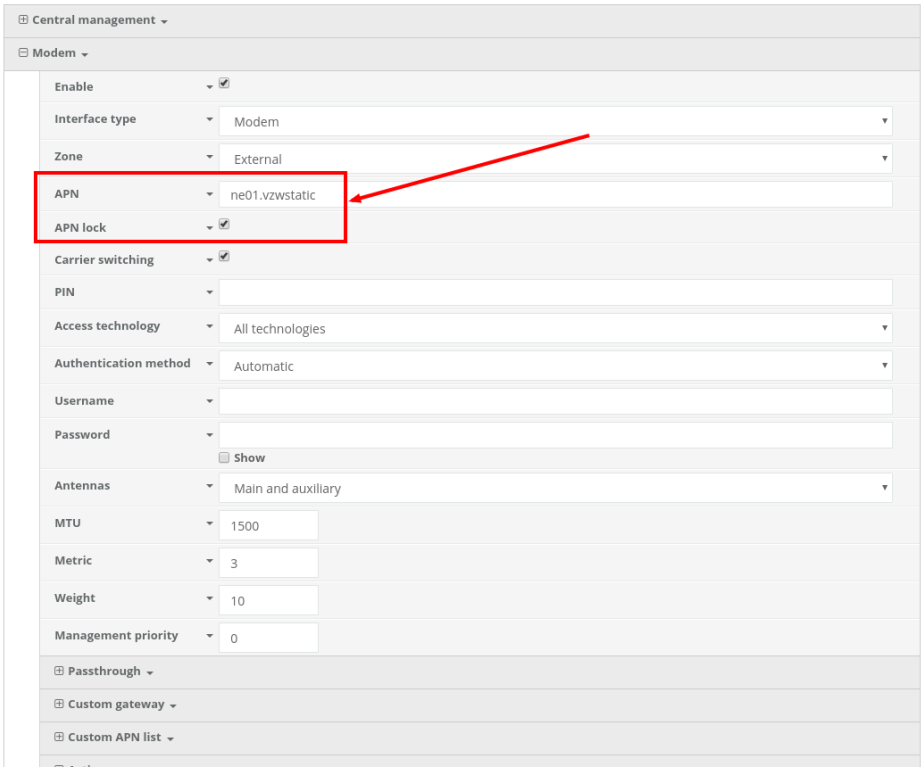
It can sometimes take longer than the 63xx-series device anticipates for the Verizon SIM to finish its registration process on the Verizon network. As a result, the 63xx-seris device tries establishing a cellular connection before this SIM finishes registering, which results in a failed connection. The 63xx-series device 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 device gets stuck trying a fallback list of APNs, of which none will work with the given SIM.

Manual Solution

Users can lock the 63xx-series device to keep trying the same APN. This allows the 63xx-series device to retry the same APN that the SIM card is provisioned with. Even if the 63xx-series device 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 device 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.



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 Cellular Extender and 6330-MX LTE Router, 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).