6310-DX

Table of Contents

Supplemental Information

Inbound IP Passthrough Activity Not Acting as Intended on Device Firmware 18.4.54.22

Problem

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

Background

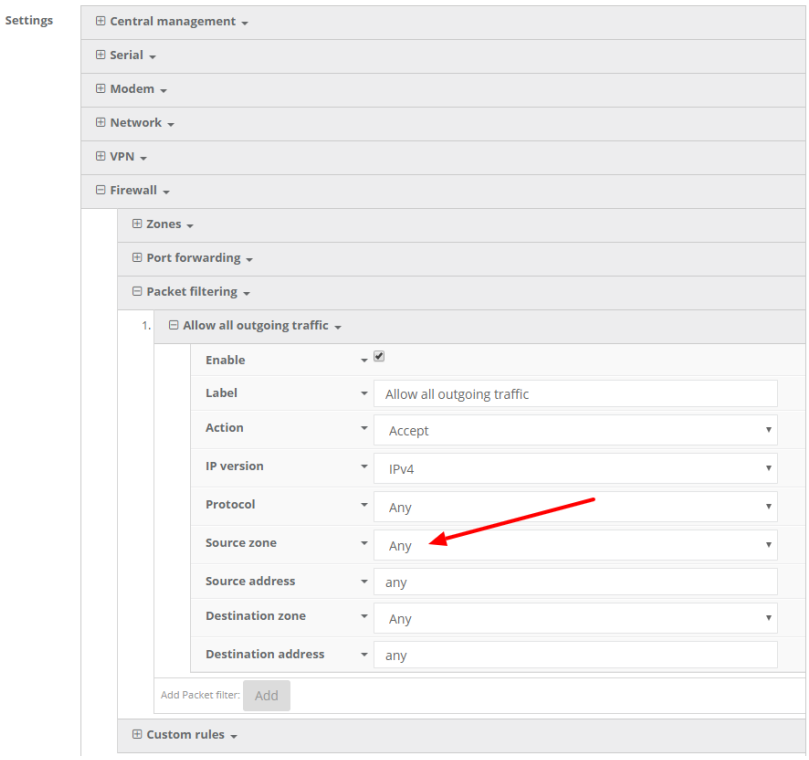
We've been seeing an issue where the latest firmware has unintentionally engaged the firewall for passthrough connections. This results in failed pings from an external source of the cellular IP of an Accelerated cellular router on firmware 18.4.54.22 configured with IP Passthrough.

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 18.4.54.22

Problem

A newly activated Verizon SIM with a static APN (e.g. ne01.vzwstatic) is inserted into a 63xx-series router on 18.4.54.22 device firmware using the CM04. 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

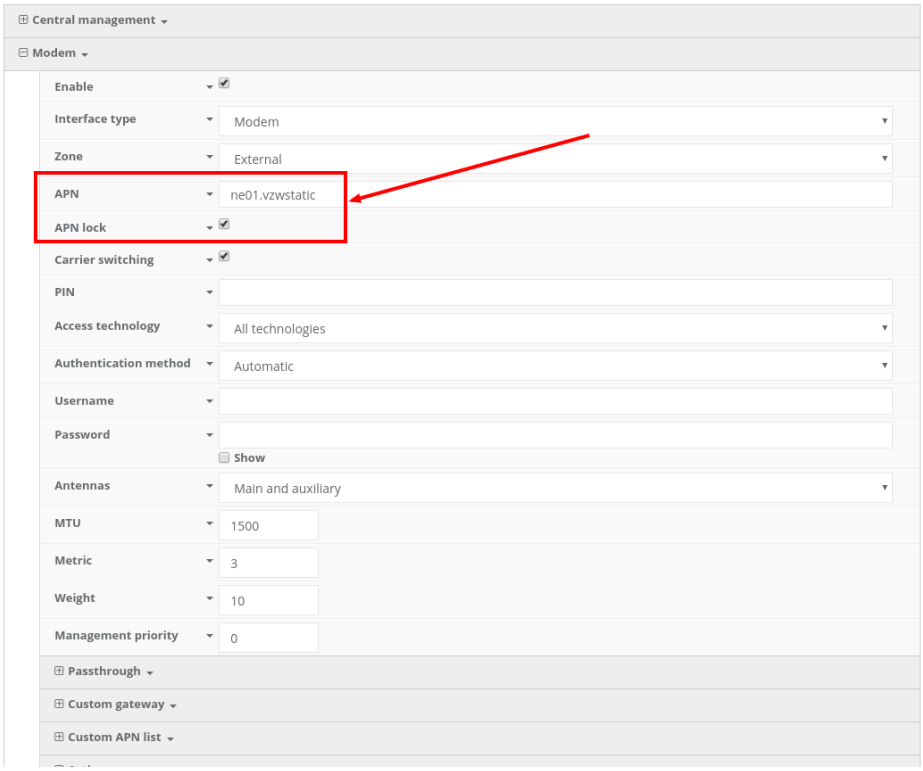
It can sometimes take longer than the 63xx-series router anticipates for the Verizon SIM to finish its registration process on the Verizon network. As a result, the 63xx-seris router tries establishing a cellular connection before this SIM finishes registering, which results in a failed connection. The 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.

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.



Package Contents

6310-DX Unit

Cellular Antennas (2x)

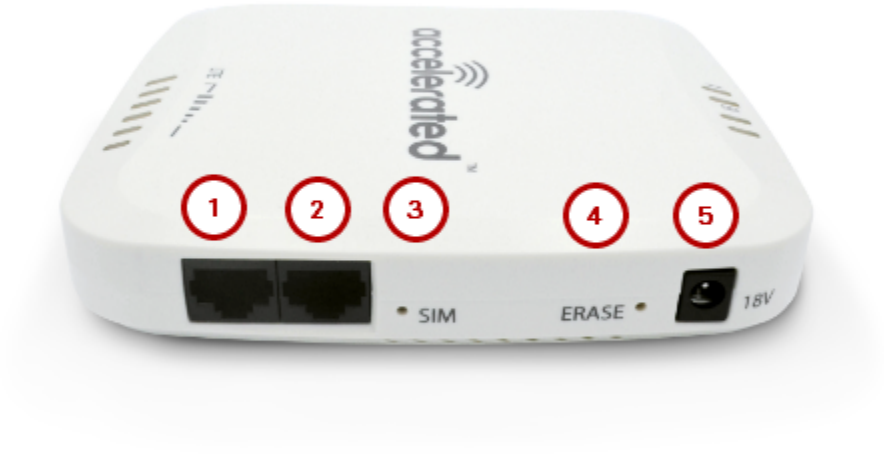
Ethernet Cable

Power Supply Unit

Mounting Bracket

Hardware Features

Right Side of 6310-DX



1. LAN/PoE Port
2. WAN Port
3. SIM Select Button
4. Factory Reset Button
5. Power Socket

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.

Front of the 6310-DX

6. Connection Indicator
7. Signal Bar Indicators

Back of the 6310-DX

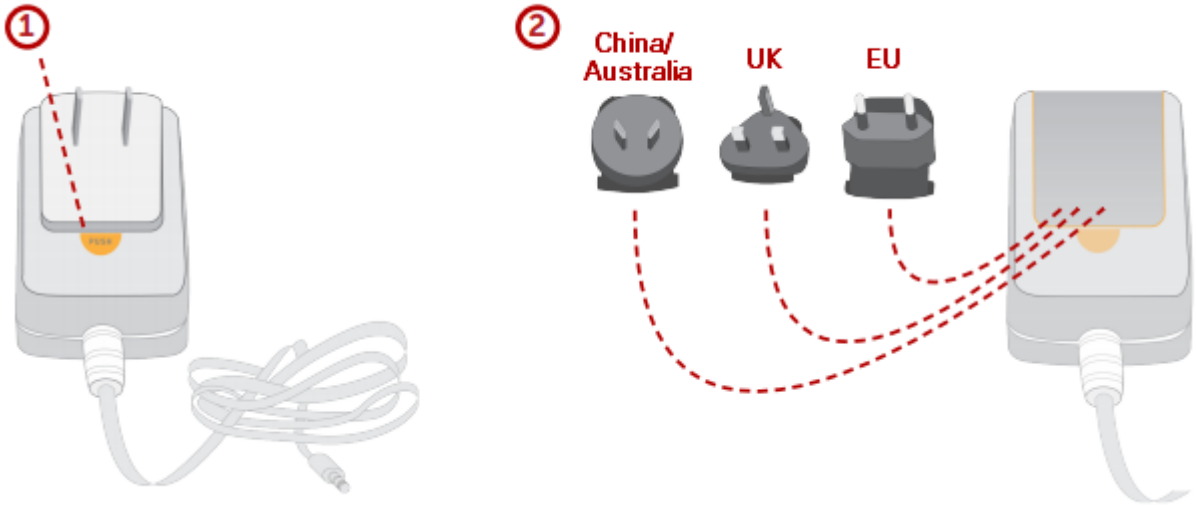
8. LAN/WAN Indicator
9. SIM1/2 Indicator

Exchanging Power Tips

The 6310-DX 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.

Plug-In LTE Modem

There is a label on the bottom of the DX-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 DX-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.

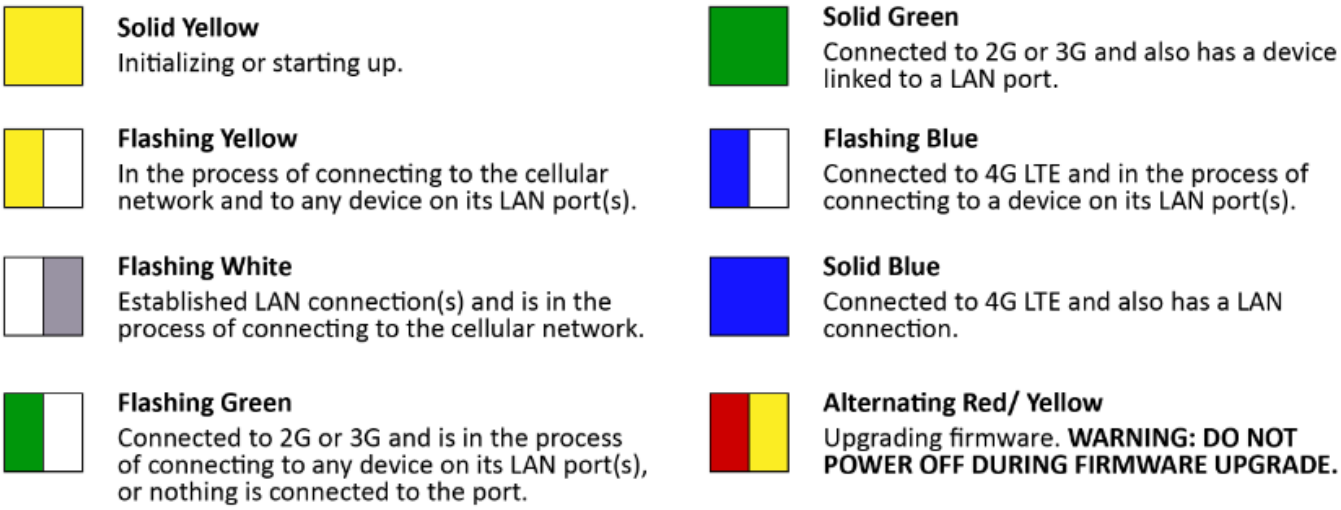
Device Status LEDs

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 6310-DX will attempt to use DHCP to establish an Internet connection either through its cellular modem or the ethernet port .

1. Indicator lights on the Wireless Strength Indicator show you the cellular network signal strength.
2. Cellular connectivity status is indicated by the color-coded LTE light.
3. Ethernet connections are confirmed via the light corresponding to the DX's port number.

LTE Status Indicators

Network Status LED



Solid Yellow
Initializing or starting up.

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

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

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

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

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

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.

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 6310-DX 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 6310-DX. 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 6310-DX 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 6310-DX with either the power supply unit or the PoE injector cable.

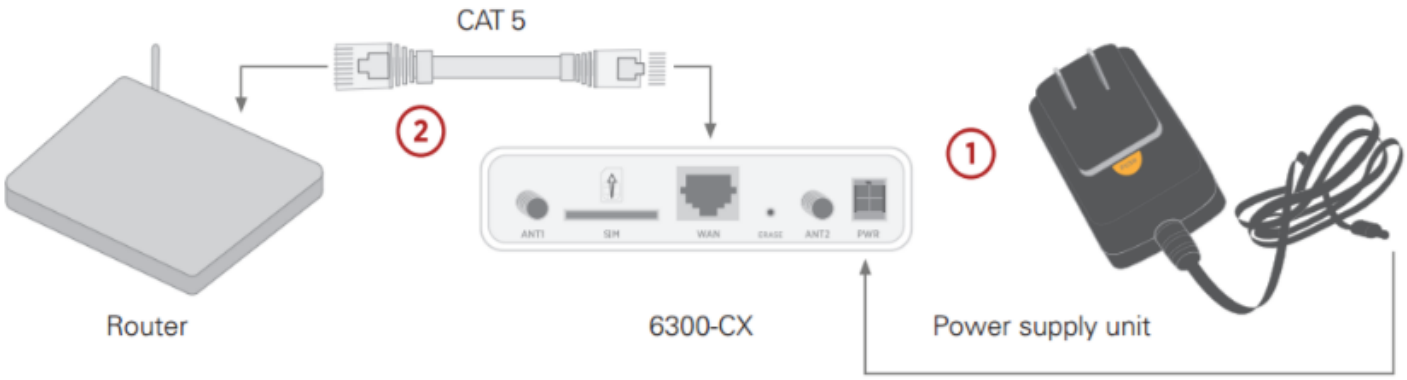
Site Survey Troubleshooting

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 6310-DX 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 6310-DX indicator lights to aid in diagnosis.

Physical Installation

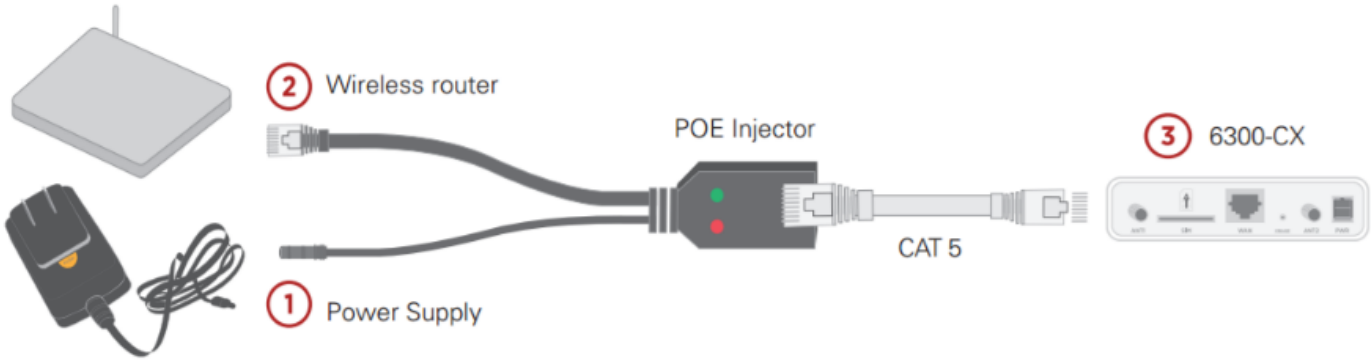
Connecting to the Site Network with Local Power



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

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 6310-DX via the Ethernet connection only.



1. Plug the power supply unit into an AC power outlet and connect to the PoE injector.
2. Connect the male RJ45 connector plug of the POE injector cable to the site network equipment/router.
3. Connect a standard Ethernet cable from the RJ45 socket/jack on the POE injector cable, (marked 'DC OUT'), to the LAN/PoE Ethernet port of the DX.

Remote Power Trouble Shooting

On the end of the POE injector cable (see diagram) there are two LEDs. The Red LED marked DC IN will be illuminated if the DX Power Supply Unit (PSU) in plugged into an AC power outlet and plugged into the POE Injector Cable. If the red LED is not illuminated check the following:

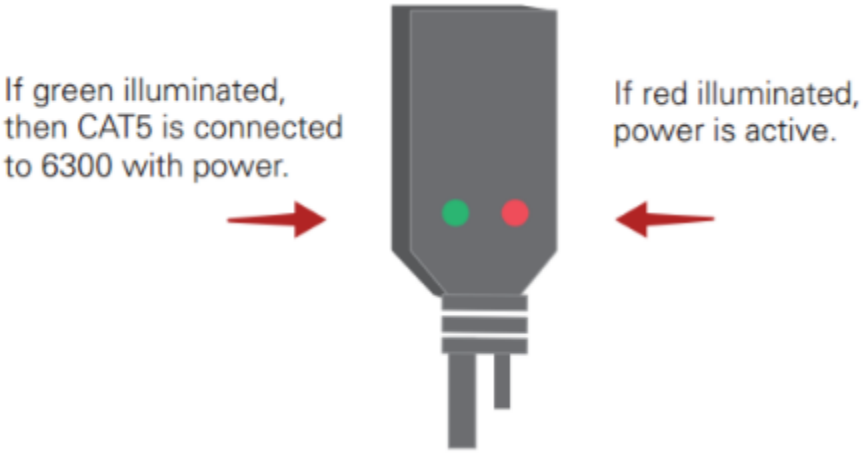
- Ensure that the PSU is plugged into an AC power outlet and is receiving power.
- Ensure that the PSU's power plug is correctly connected to the POE injector cable power input socket.

If the green LED marked **DC OUT** is not illuminated after connecting to the 6310-DX, verify the integrity of the Ethernet cable.

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

The Red LED marked DC IN and the Green LED marked DC OUT will both be illuminated on the POE injector cable (see diagram) if you have properly connected the PSU and you have connect a length of CAT5 cable properly to the POE injector cable and the 6310-DX. If the red LED is illuminated and the Green LED not illuminated check the following:

- Ensure that you have a good connection at both the ends of you CAT5 cable.
- Check your CAT5 cable.



Default Settings

Ethernet ports

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

Interface Priorities

- WAN set at a metric of 1

> This metric sets the WAN port as the DX'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)

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 6310-DX 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 6310-DX.

- 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 6310-DX 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 6310-DX not provisioned in Accelerated View refer to Managing Device Locally section.

Local Device Management

NOTE: It is recommended that Accelerated View centrally manages the DX-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**"

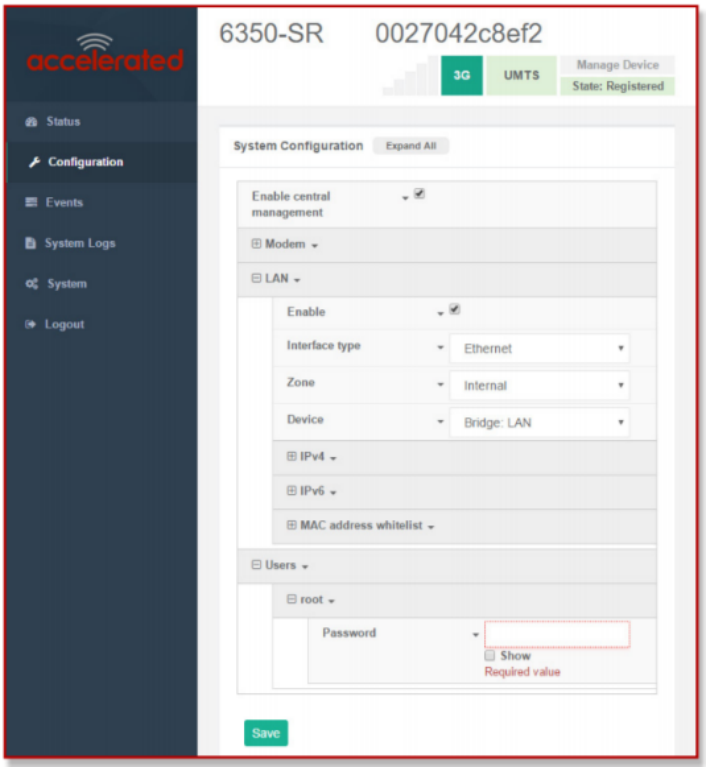
2. (optional) If this is the first time the device has been configured, you will also need to update the root user's password, under *Users -> Root -> Password*

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.)

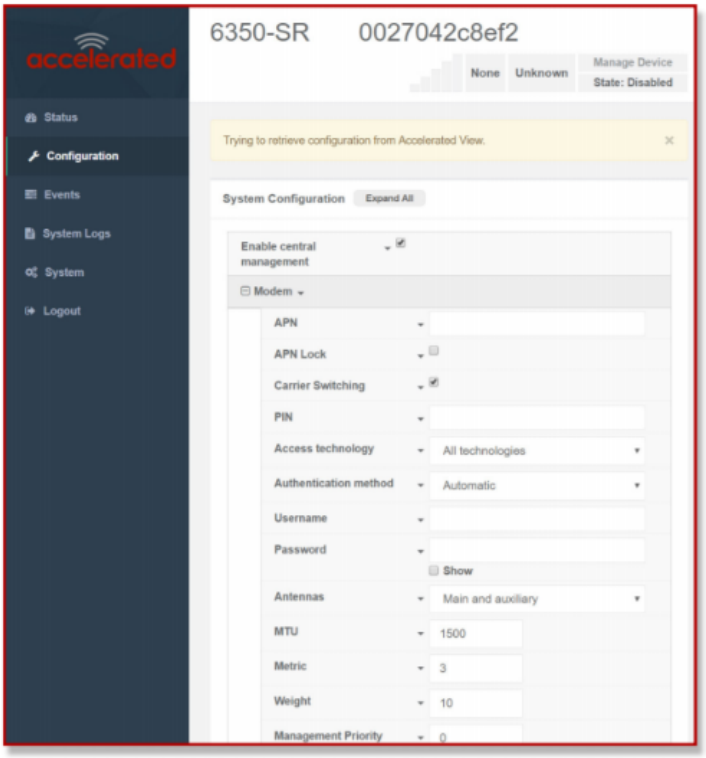


Defining a Custom APN

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.


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 DX'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 6310-DX 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.

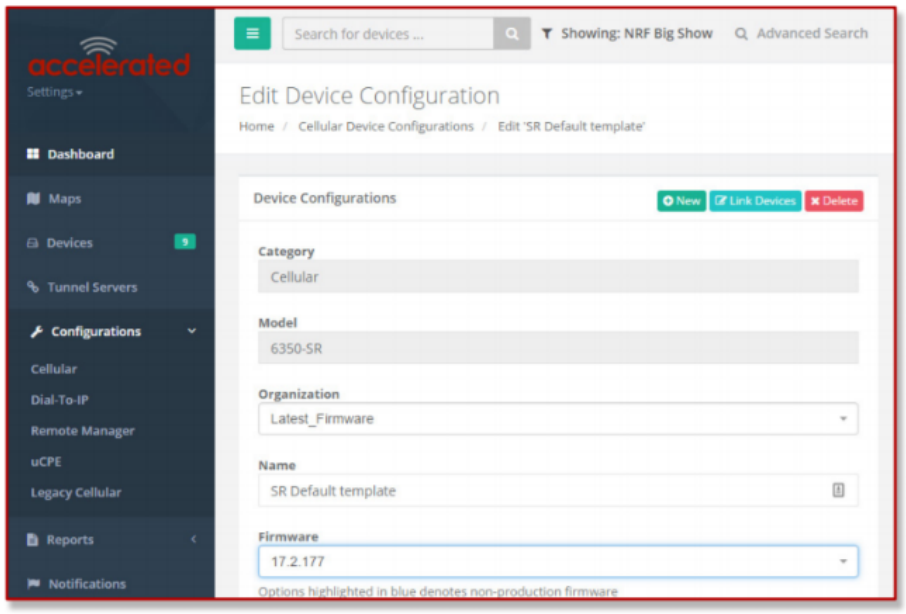
Devices will automatically apply configuration updates after the next daily sync (1am UTC by default). Refer to the Remote Commands sections for details on how to apply changes sooner.

Upgrading Firmware

> When the DX-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.



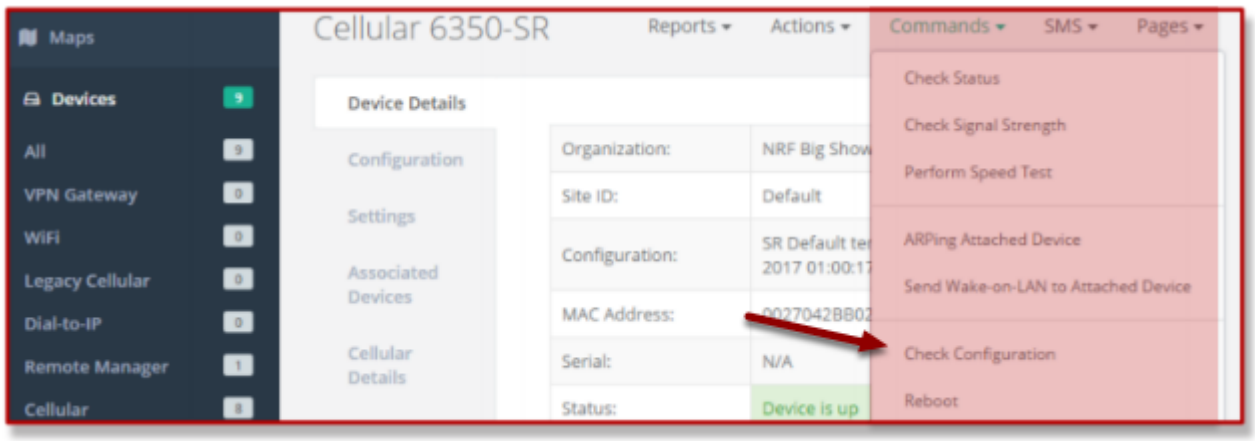
Using Remote Commands

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.

Custom Settings

Network-Managed Configuration

DX-series routers, like all Accelerated hardware, will automatically synchronize with the Accelerated View™ cloud management platform so long as it is able to establish a network connection. This web-based configuration and monitoring portal provides:

- Remote control and configuration updates
- Email notifications for user-defined parameters (connection quality, data usage, etc.)
- Out-of-Band SMS recovery
- Real-time monitoring for:
  1. Signal strength and quality
  2. Network connectivity details
  3. Location-based services
  4. Device performance

Changes made within Accelerated View will be applied to the intended recipient(s) as soon as those devices check in with the web service for synchronization. This occurs once every 24 hours by default (though it can be rescheduled as necessary).

This assumes the DX-series router being configured has been registered with Accelerated View.

To apply all pending changes immediately, reboot the DX or refer to the step-by-step guidance for issuing remote commands.

Local Configuration

If your Accelerated 6310-DX is not provisioned in Accelerated View, it will use a default local configuration profile.

Please refer to the Local Management section of this manual to change settings for an Accelerated DX-series without accessing Accelerated View.

Changes applied locally will be overridden should the device then sync with its config from Accelerated View.

Dual-WAN Configurations

The DX-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").

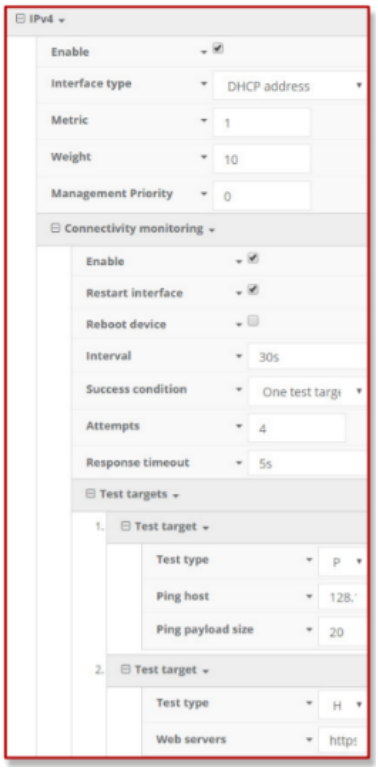
Connectivity Monitoring

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 DX'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 DX-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 DX 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

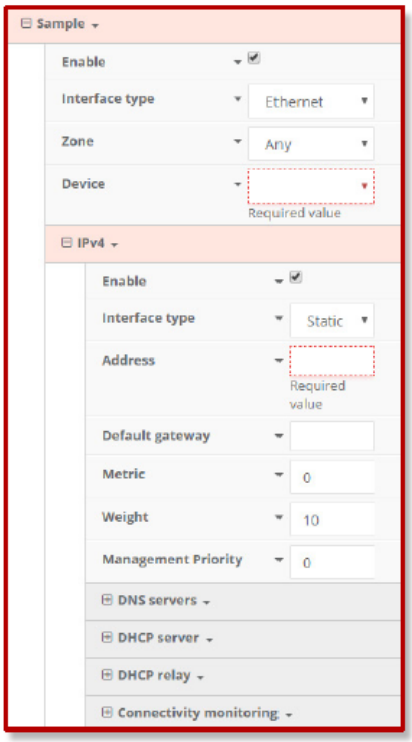
Changing the LAN Subnet

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

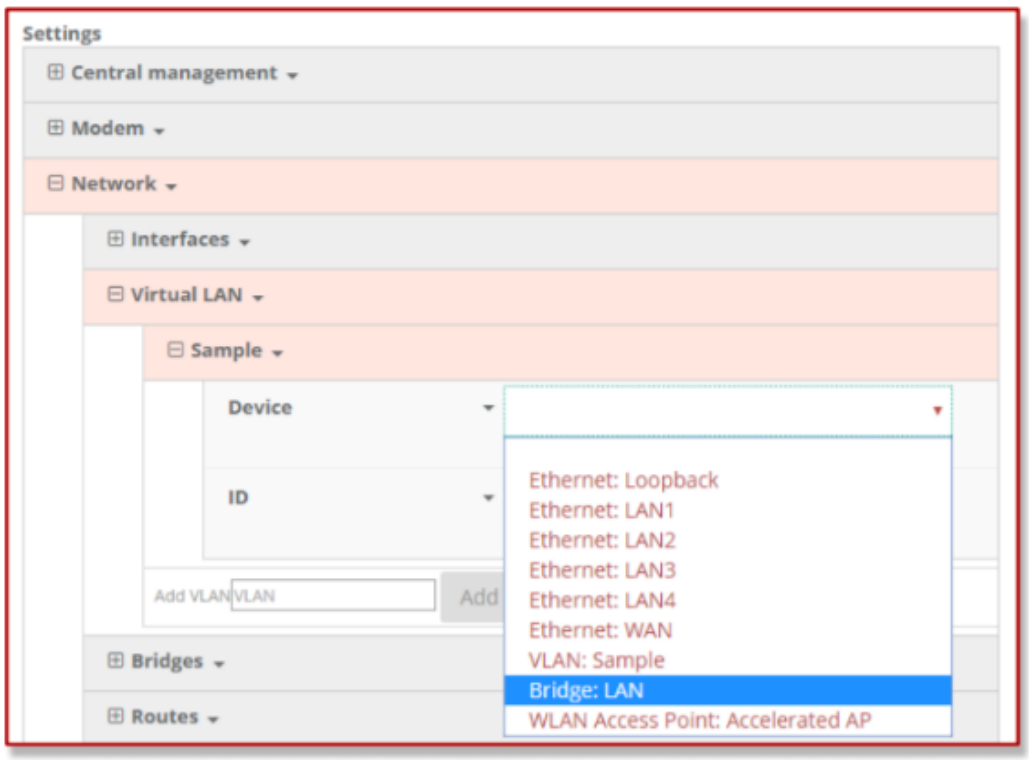
Before creating a Virtual LAN route for the DX-series router, be sure that its corresponding LAN interface has been configured (per the steps on the previous page).

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

Firewall Settings

The 6310-DX can function as a stateful firewall. Options for the 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

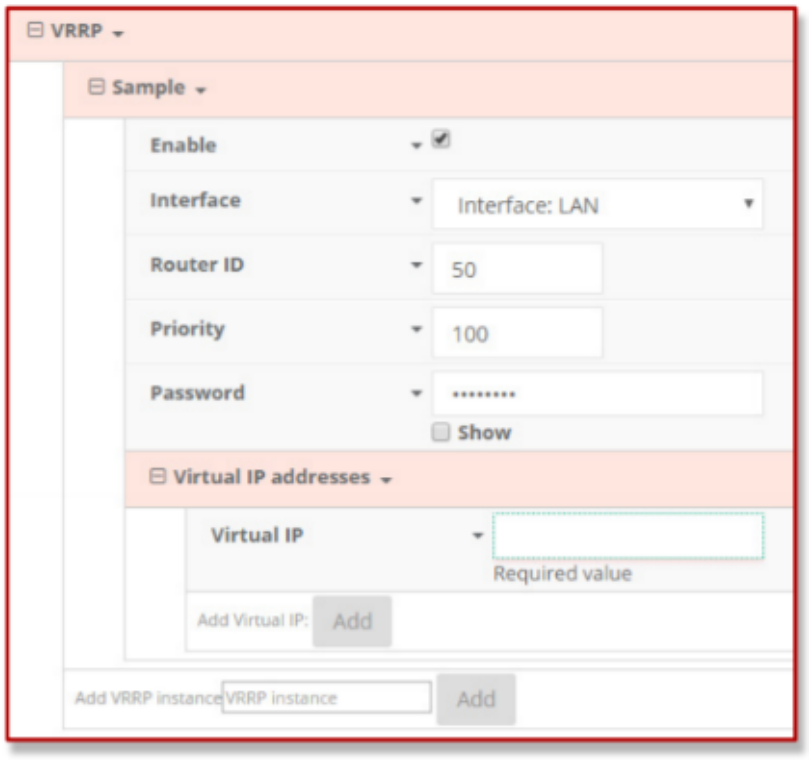
VRRP is a networking protocol used to configure devices as a "hot standby" for a primary router, where a backup device will only start routing traffic after the network detects that the primary device is offline (using parameters set by VRRP).

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.



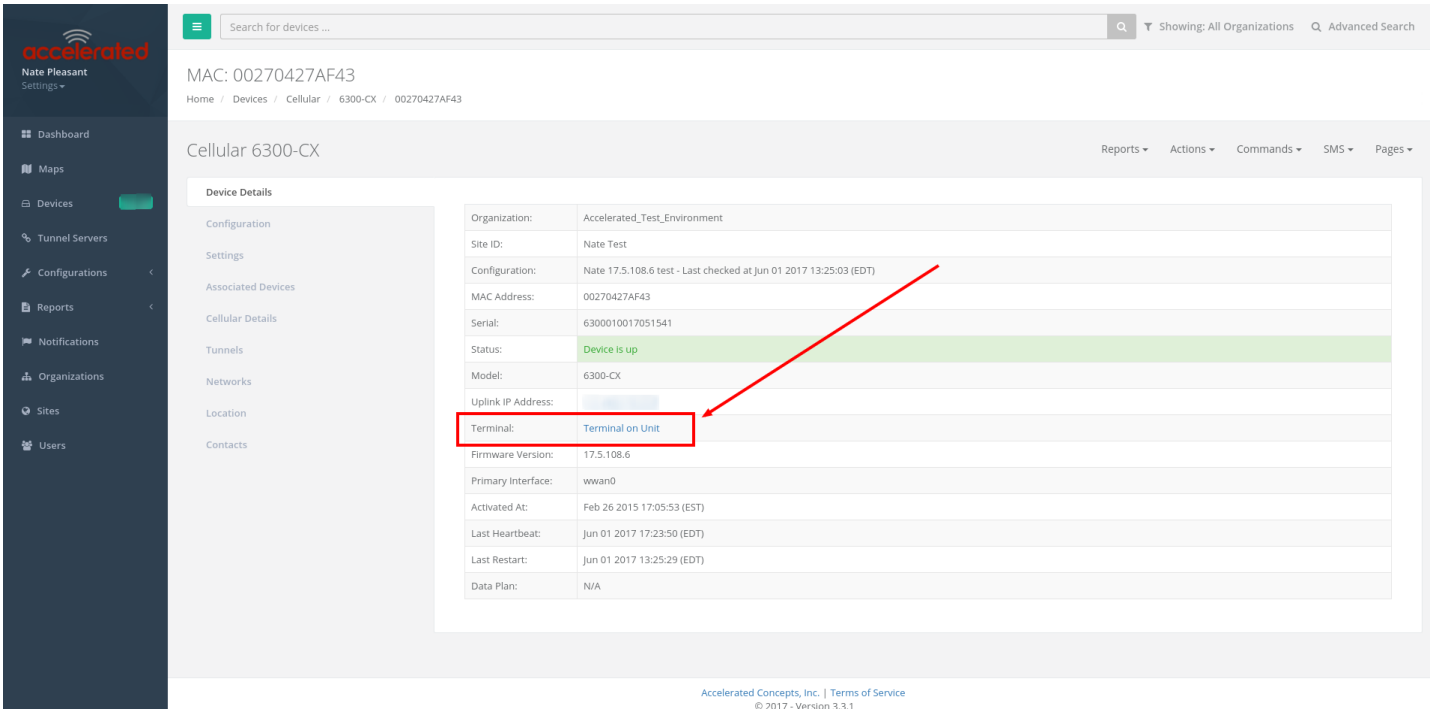
Terminal on Unit

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

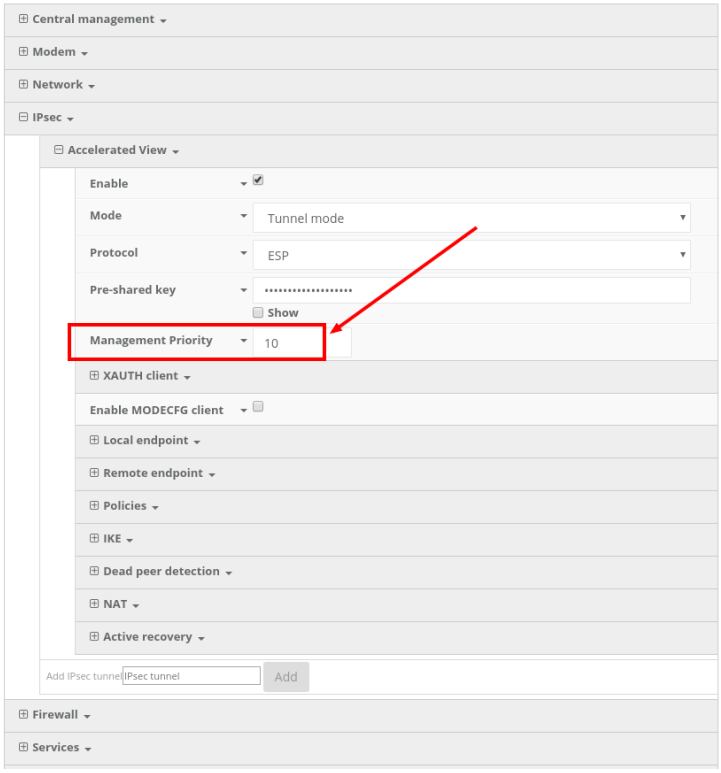
Accelerated View utilizes the IPSec tunnel the 63xx-series router establishes to remote.accns.com to provide terminal access to the console of the router.

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

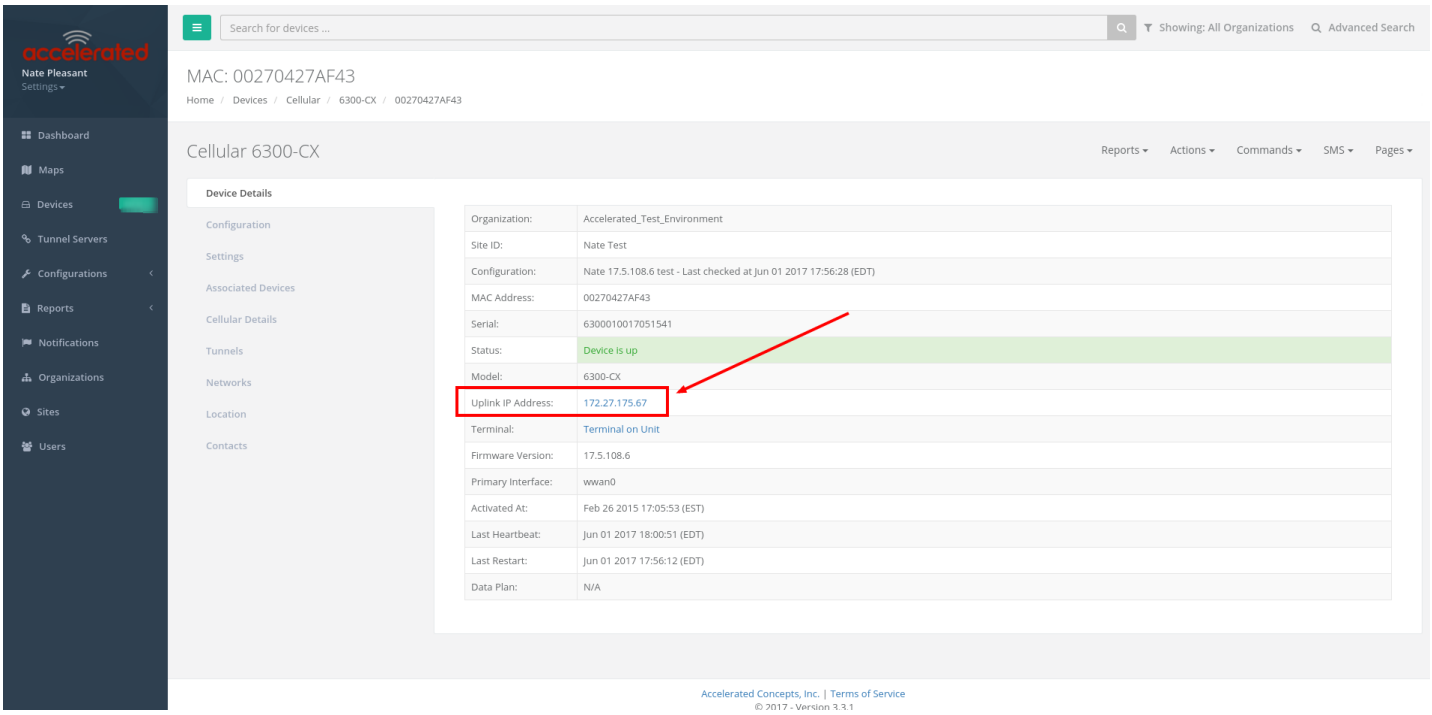
Data Usage Estimates

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.

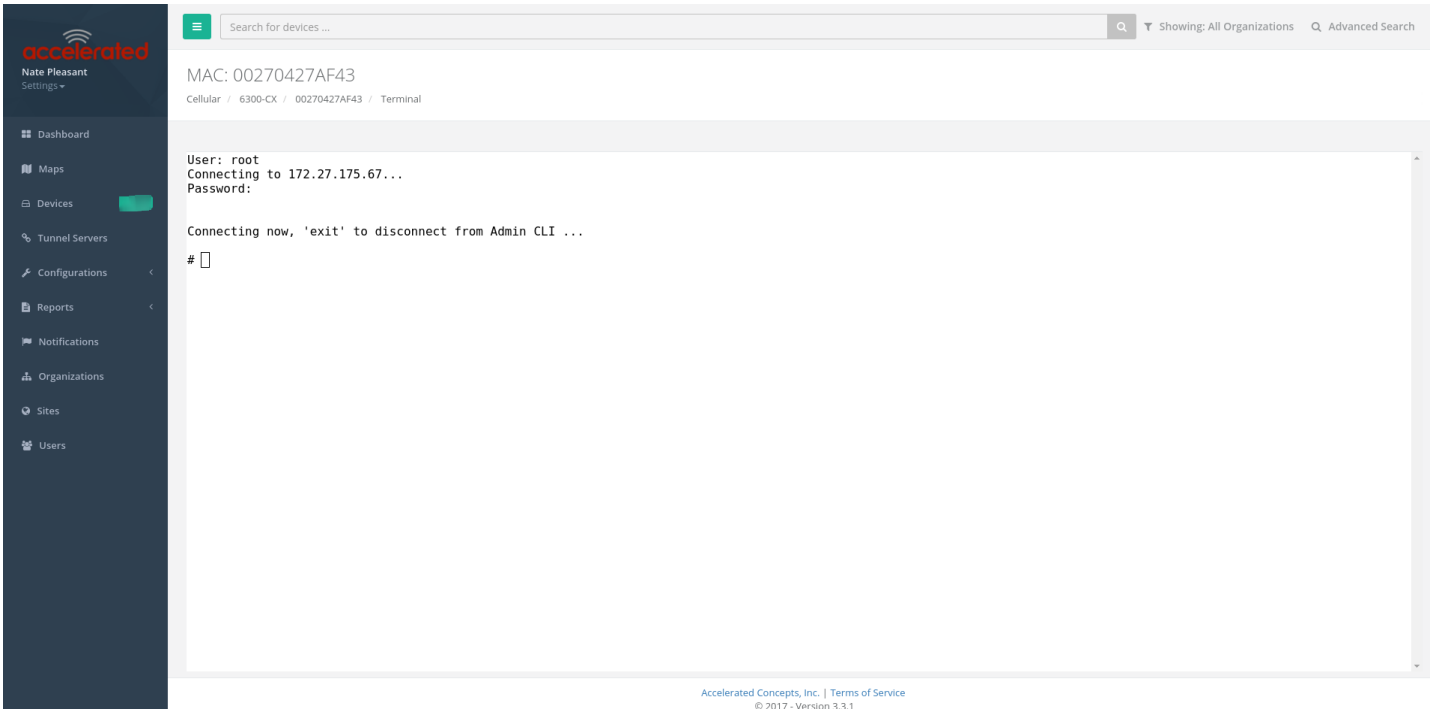


Once you apply the new configuration to the 63xx-series router, reboot the 63xx-series device so it rebuilds the IPSec tunnel and reports the new IPSec local IP address to Accelerated View. You can verify that Accelerated View is using the IPSec local IP as the management IP by looking at the *Uplink 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 6310-DX, 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 6310-DX at 192.168.210.1. Default login credentials are:
  - *username:* root
  - *password:* default
- Select **a** to access the Admin CLI. If the SSH session immediately gives you the # prompt, you are already in the Admin CLI.
- Type **atcmd** and press Enter. Type **n** when the SR prompts you if you want exclusive access. This allows you to send AT commands to the device while still allowing the device to connect, disconnect, and/or reconnect to the Sprint network.
- Example AT command access below:

```
$ ssh root@192.168.210.1
Password:

Access selection menu:

a: Admin CLI
s: Shell
q: Quit

Select access or quit [admin] : a

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

# atcmd

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

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

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

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

Troubleshooting

Resetting Your Device

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

To reset the device to factory default settings, press and release the ERASE switch once on the rear of the device when the device is switched on. This will erase all device-specific settings to their original state (excluding any automatically generated keys/certificates), 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.

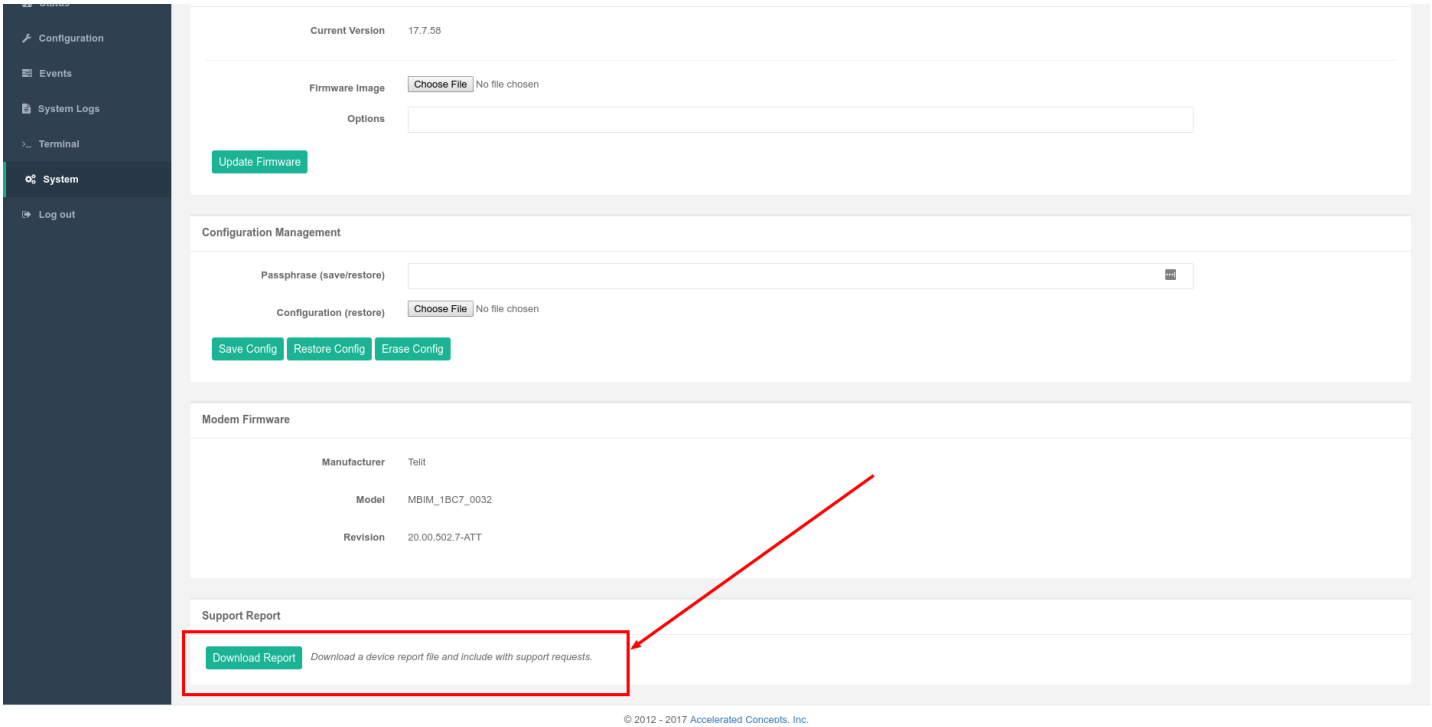
Support Report

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 6310-DX. They should receive an IP address via DHCP from the DX 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.

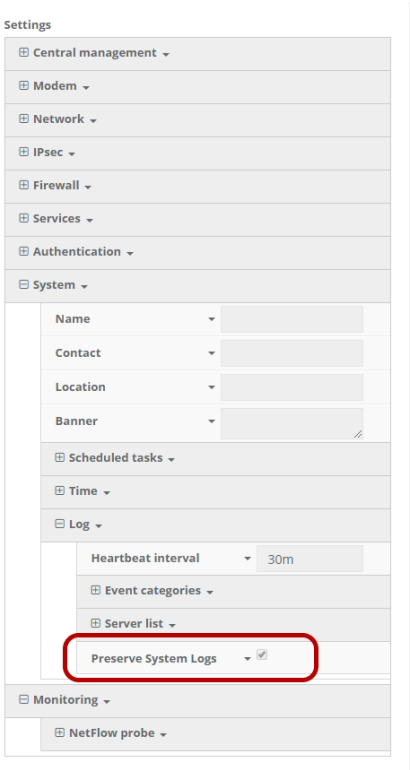


Persistent System Logs

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

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.**

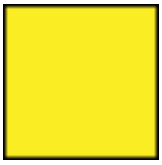
Signal Strength LEDs

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!

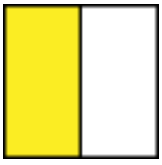
Solid Yellow



6310-DX is starting up.

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

Flashing Yellow



6310-DX 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 6310-DX 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?

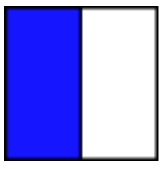
No

- 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

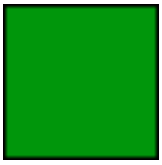
- Power off the 6300-CX, swap the antennas on the back of the 6300-CX, and power on the 6300-CX. If this resolves the connectivity and the 6300-CX displays two or more bars of signal strength, this may indicate that one of the antennas is faulty. You can continue to use the 6300-CX, but we suggest that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



6310-DX 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 6310-DX, 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.

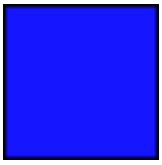
Online, but with VPN issues

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 6310-DX.

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 6310-DX?

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 6310-DX use?

By default, the Accelerated 6310-DX provisions IP addresses using DHCP over the LAN subnet of 192.168.2.1/24.

What size SIM card does the Accelerated 6310-DX use?

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

Does the Accelerated 6310-DX fail back to 3G?

Yes, if the Accelerated 6310-DX 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 6310-DX support IPv6?

Yes. In passthrough mode, when the 6310-DX 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 6310-DX will also pass the IPv6 DNS server using the SLAAC RDNSS option and stateless DHCPv6.

Regulatory Guide

FCC

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

European Union

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

Supported Countries

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

End User Agreement

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

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

LIMITED WARRANTY

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

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

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

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

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

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

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

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

LIMITED LIABILITY

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

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

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

SOFTWARE LICENSE

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

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

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

Change Port 2 from WAN to LAN

Difficulty level: *Intermediate*

Goal

To change the functionality of the 6310-DX router's port #2 from a WAN connection to be a part of LAN.

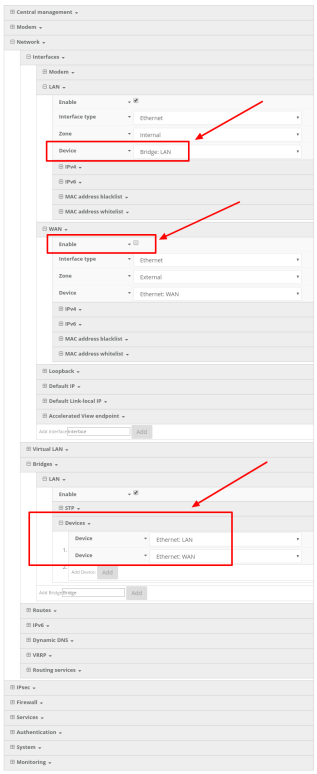
Setup

This article assumes the 6310-DX router is operating under default settings, which provides DHCP connectivity to device(s) connected on LAN port 1 of the 6310-DX. For more details on the default settings of the 6310-DX, see the Default Settings section of the 6310-DX User's Manual. Also, refer to the Getting started with Accelerated View for details on how to configure a 6310-DX (or the Local device management section, if you are managing the device without Accelerated View).

Configuration Steps

Open the configuration profile for the 6310-MX and make the following changes.

1. Under *Network -> Interfaces -> WAN*, de-select the *Enabled* checkbox.
2. Under *Network -> Bridges*, create a new entry called *LAN .*
3. Under *Network -> Bridges -> LAN -> Devices*, click *Add* twice. Select *Ethernet: LAN* from the drop-down for one entry, and *Ethernet: WAN* from the drop-down for the second entry.
4. Under *Network -> Interfaces -> LAN*, change *Device* to *Bridge: LAN*.


Central management
Modem
Network
Interfaces
Modem
LAN
Enable
Interface type
Ethernet
Zone
Internal
Device
Bridge: LAN
IPv4
IPv6
MAC address blacklist
MAC address whitelist
WAN
Enable
Interface type
Ethernet
Zone
External
Device
Ethernet: WAN
IPv4
IPv6
MAC address blacklist
MAC address whitelist
Loopback
Default IP
Default Link-local IP
Accelerated View endpoint
Add
Virtual LAN
Bridges
LAN
Enable
STP
Devices
Device
Ethernet: LAN
Device
Ethernet: WAN
Add Device
Add
Add Bridge
Add
Routes
IPv6
Dynamic DNS
VRRP
Routing services
IPsec
Firewall
Services
Authentication
System
Monitoring

LAN port with IP passthrough

Difficulty level: *Easy*

Goal

To setup a device attached to the LAN Ethernet port 1 to receive the passthrough IP address of the 6310-DX router's cellular modem connection.

Setup

This article assumes the 6310-DX router is operating under default settings, which provides DHCP connectivity to device(s) connected on LAN port 1 of the 6310-DX. For more details on the default settings of the 6310-DX router, see the Default Settings section of the User's Manual.

The 6310-DX router must be running firmware version 17.5.86 or higher.

Sample

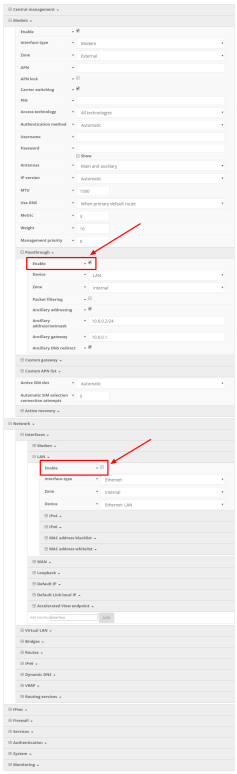
The following diagram shows a sample setup of a 6310-DX router with its LAN port 1 setup to provide the IP address of the cellular modem connection as a passthrough to the client device connected to port 1.

Important: The client device receiving the passthrough IP will only be able to use the 6310-DX's cellular WAN connection. Meaning, if the 6310-DX 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 6310-DX's WAN Ethernet interface.

Sample Configuration

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

1. Under *Modem -> Passthrough*, check the *Enabled* box and select the *LAN* interface under the *Device* drop-down.
2. De-select the *Network -> Interfaces -> LAN -> Enable* checkbox.
3. Save and apply the new configuration settings to the device.



Router Mode Setup

Difficulty level: *Easy*

Goal

To setup the 6310-DX as a standard DHCP router with dual WAN failover between the DX's WAN Ethernet port and its cellular modem.

Once router mode is enabled, the 6310-DX will use its WAN Ethernet port as the primary Internet connection for all client devices, and the cellular modem will be the backup connection.

Setup

This article assumes the 6310-DX router is operating under default settings, which provides passthrough connectivity to a device connected on port 1 of the 6310-DX. For more details on the default settings of the 6310-DX, see the Default Settings section of the 6310-DX User's Manual. Also, refer to the Getting started with Accelerated View for details on how to configure a 6310-DX (or the Local device management section, if you are managing the device without Accelerated View).

Configuration Steps

Open the configuration profile for the 6310-DX and make the following changes.

1. Under *Modem -> Passthrough*, de-select the *Enabled* checkbox.
2. Under *Network -> Interfaces -> LAN*, select the *Enabled* checkbox.

Configure DHCP Server for PXE Booting

Difficulty level: *advanced*

Goal

To set up the 6310-DX 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

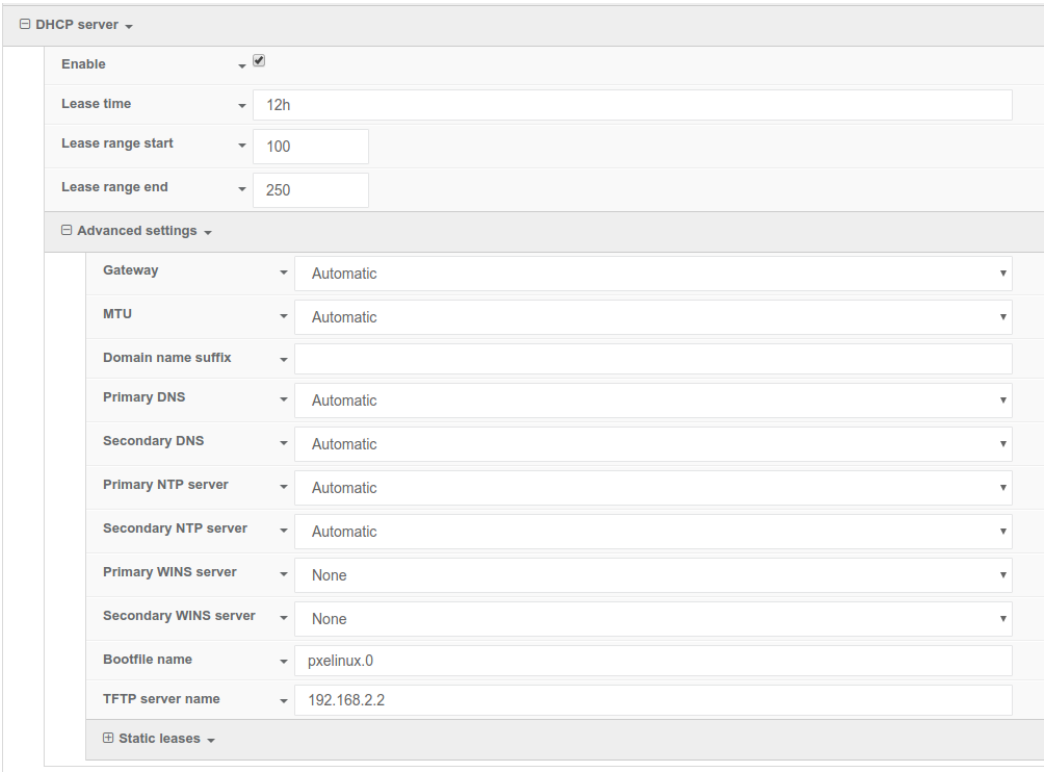
This article assumes the 6310-DX router is operating under default settings, all relevant PXE boot files and TFTP server processes are in place ready to be connected, and the client device is in a state ready for PXE boot.

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 6310-DX 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

Port Forwarding

Goal

To access a client device on the LAN port of a 6310-DX using a specific port and the external IP address of the 6310-DX.

Setup

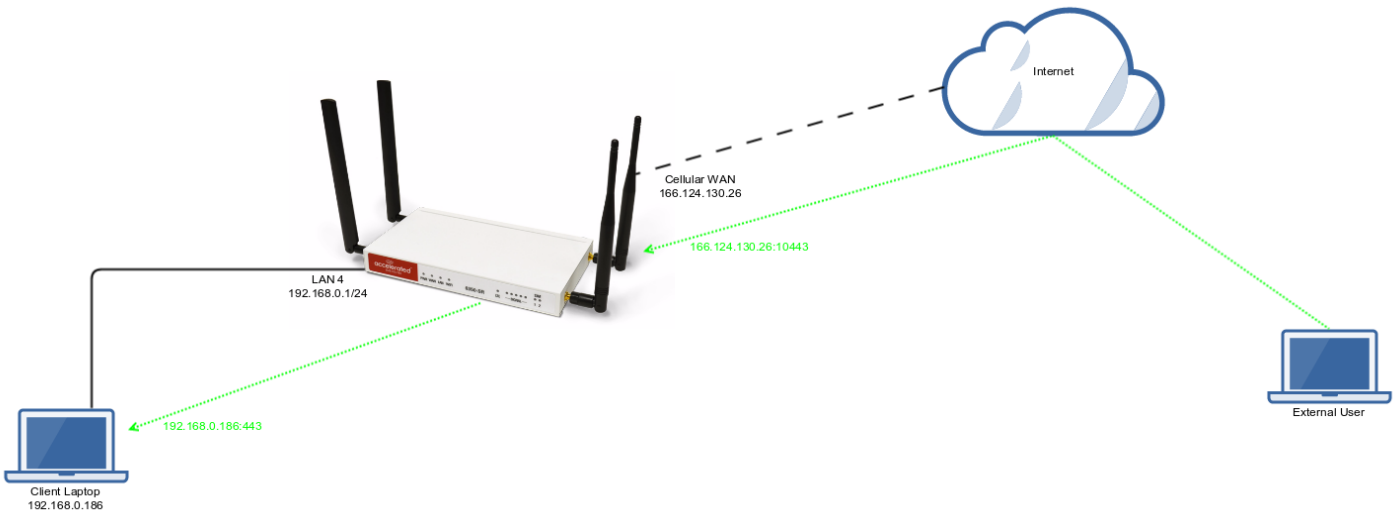
This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 6310-DX's LAN ports. For more details on the default settings of the 6310-DX, see the *Default Settings* section of the 6310-DX User's Manual.

You will need to establish the following details before configuring the 6310-DX.

- 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

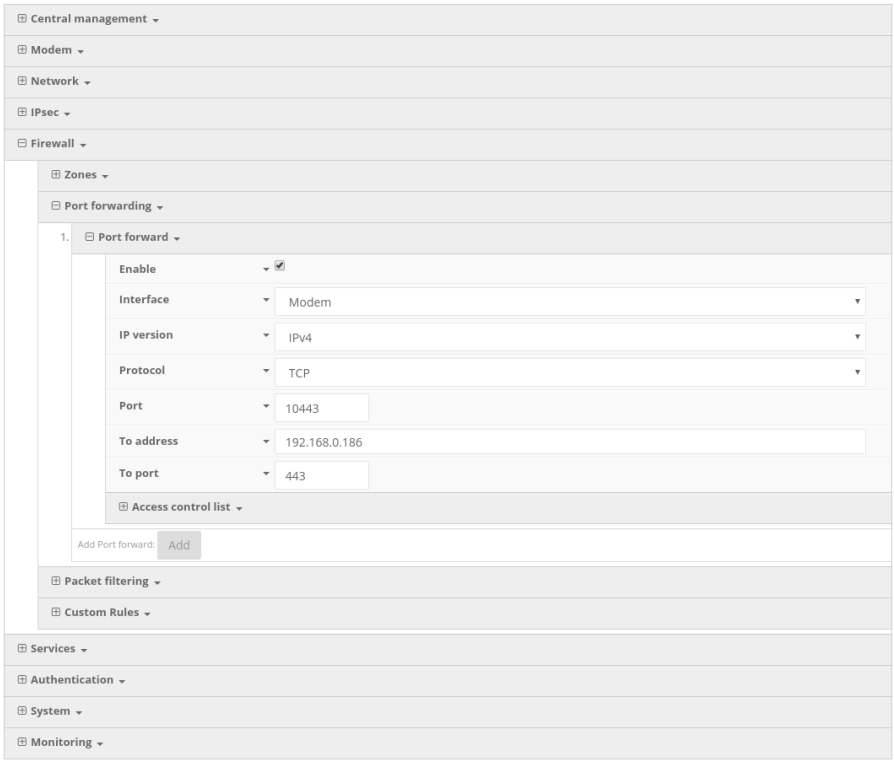
The following diagram shows a sample setup of a 6310-DX with a cellular WAN connection and a client's laptop connected to LAN port 4. In this setup, we want to access TCP port 443 of the client laptop from the external IP address of the 6310-DXs cellular WAN connection. We will be configuring the 6310-DX 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 6310-DX 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

Goal

To use the 6310-DX'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 6310-DX'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 6310-DXs configuration, under the *Modem -> APN* option.

Sample

By default, the 6310-DX is setup for automatic SIM selection. Meaning, if the 6310-DX is unable to connect with the SIM in slot 1, after a specified number of failures the 6310-DX 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 6310-DX to failover between SIM cards if either SIM is unable to establish a cellular connection.

In the sample configuration below, the 6310-DX is setup to test the cellular network connection once every two minutes. If three sequential tests fail, then the 6310-DX 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 6310-DX will switch to the secondary SIM slot.

Summed up, if a SIM's cellular connection fails, with the below configuration the 6310-DX will failover to the secondary SIM in under 10 minutes.

Sample Configuration

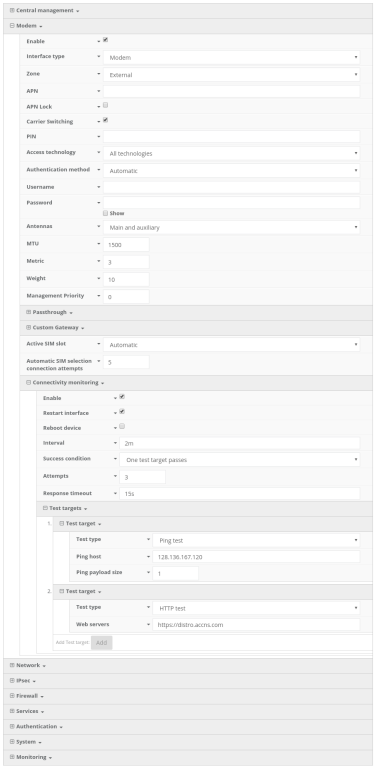
Open the configuration profile for the 6310-DX and make the following changes. Under *Modem*, set the following options.

- 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

Goal

To use the 6310-DX's cellular modem as a backup WAN connection for the primary WAN Ethernet port. The 6310-DX 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 6310-DX's LAN ports. For more details on the default settings of the 6310-DX, see the *Default Settings* section of the 6310-DX User's Manual.

For this setup, you will need the 6310-DX with both a primary WAN Ethernet connection, and a cellular modem connection.

Sample

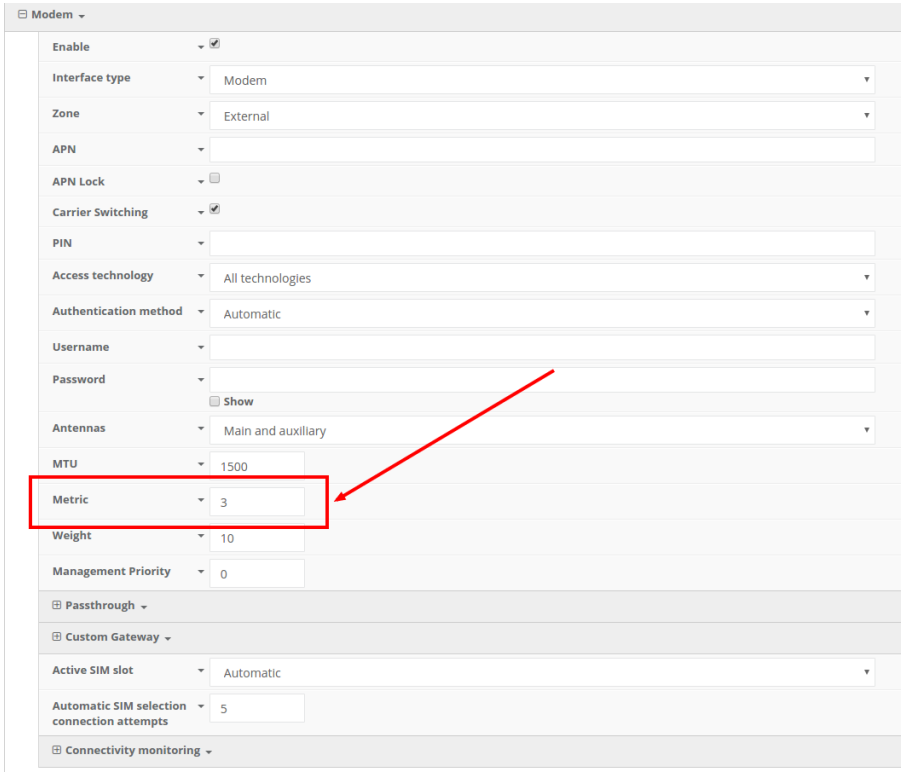
The sample configuration below shows a 6310-DX with two internet connections. The WAN Ethernet interface will be used as the primary Internet connection. The 6310-DX is setup to test the WAN Ethernet connection twice every minute. If three sequential tests fail, then the 6310-DX will restart the WAN Ethernet connection, and failover to the cellular modem's Internet connection until the WAN Ethernet connection is re-established.

Summed up, if a 6310-DX's primary WAN connection fails, with the below configuration the 6310-DX will failover to the cellular modem in under 2 minutes.

Sample Configuration

Open the configuration profile for the 6310-DX and make the following changes.

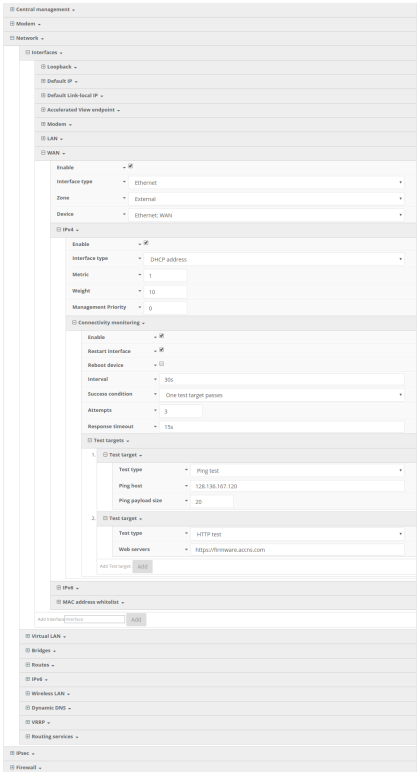
In the *Modem -> Metric entry*, ensure the value is set to a number higher than the the value in *Network -> Interfaces -> WAN -> IPv4 -> Metric*. The interface with the lower metric takes higher precedence. By default, the cellular modem metric should be 3 and the WAN Ethernet's metric should be 1, 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
Add
Virtual LAN
Bridges
Routes
IPv6
Wireless LAN
Dynamic DNS
VRRP
Routing services
IPsec
Firewall

Load Balancing

Goal

To configure additional WAN interfaces on the 6310-DX 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*.

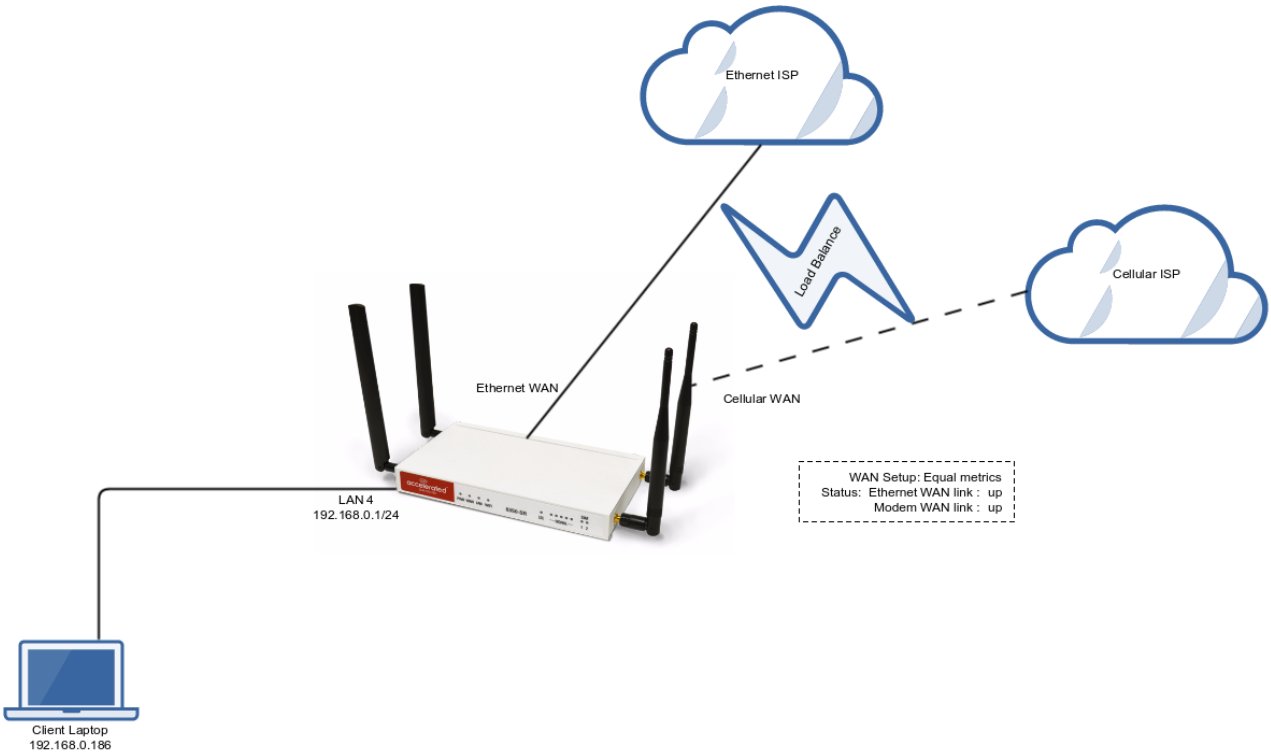
Setup

This article assumes the LAN ports are operating under default settings, which provide DHCP connectivity to devices connected to the 6310-DX's LAN ports. For more details on the default settings of the 6310-DX, see the *Default Settings* section of the DX-Series User Manual.

For this setup, you will need the 6310-DX with both a primary WAN Ethernet connection and a secondary means of WAN access.

Sample

The sample configuration below shows a 6310-DX with two Internet connections: a cellular-based WAN connection through the 6310-DX's modem, and a broadband-based WAN connection through the 6310-DX's WAN Ethernet port. Both WAN interfaces will be utilized equally, sharing 50% of the WAN network traffic.

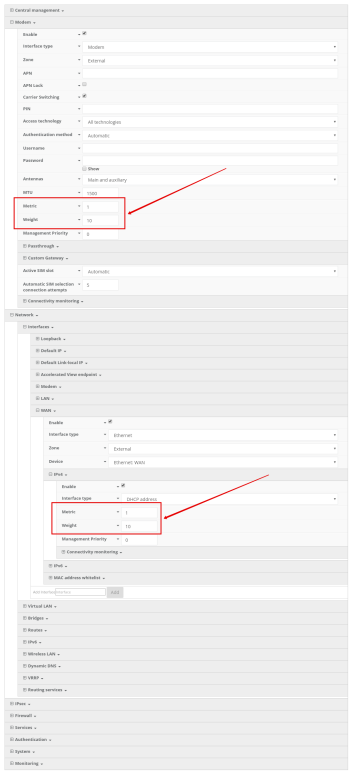


Sample Configuration

Open the configuration profile for the 6310-DX 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*).



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

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

Goal

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

Setup

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

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

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

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

Sample

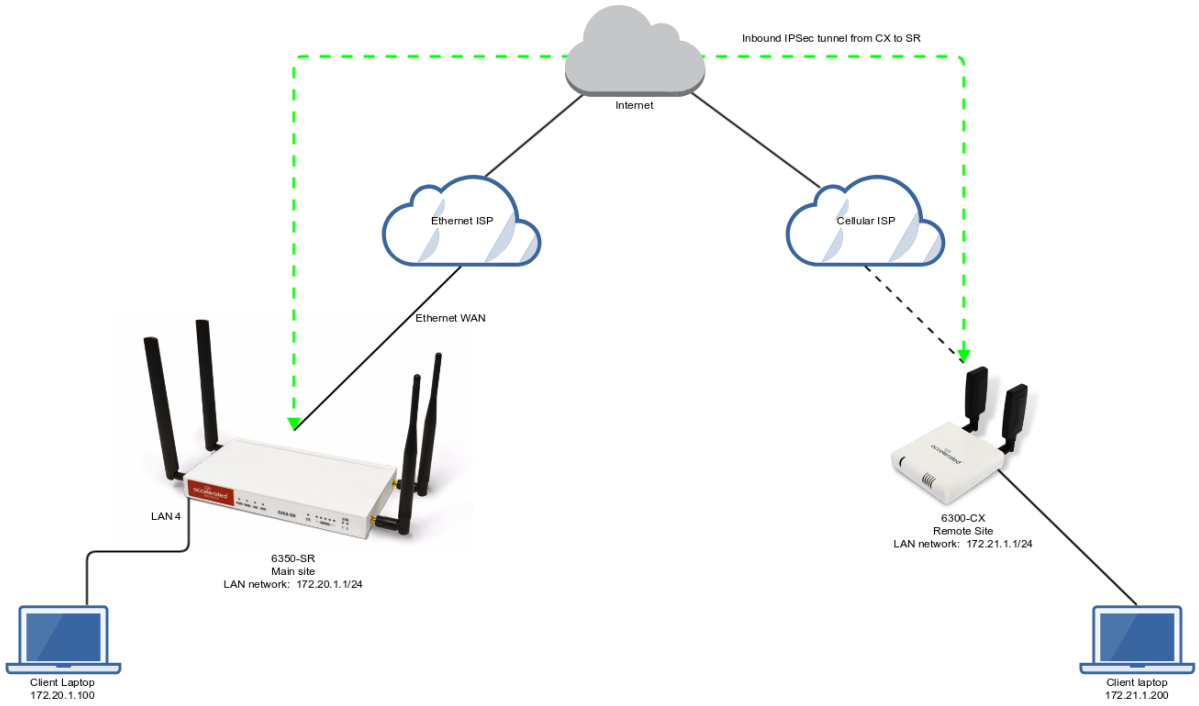
The sample configuration below shows a 6300-CX building a tunnel to a 6350-SR through its cellular modem. The client laptop connected to the LAN Ethernet port of the 6300-CX can then use that IPSec tunnel to access any IP address in the 172.20.1.1/24 range behind the 6350-SR. Any traffic not destined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

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

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

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

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



6350-SR Sample Configuration

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

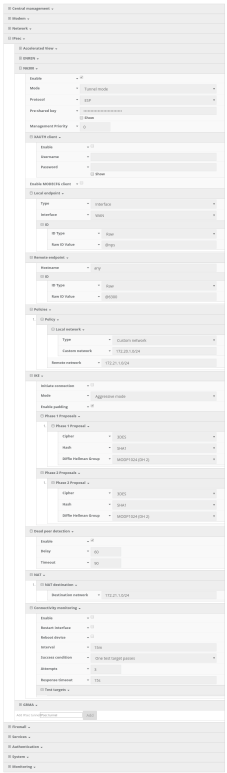
1. Enter in the PSK into the ***Pre-shared key***.
2. Change ***Local endpoint -> ID -> ID type*** to ***Raw***
3. Set the local ID in ***Local endpoint -> ID -> Raw ID Value***, e.g. *@nps*
4. Set ***Local endpoint -> type*** to ***Interface***,and set ***Local endpoint -> Interface*** to ***WAN***,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

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

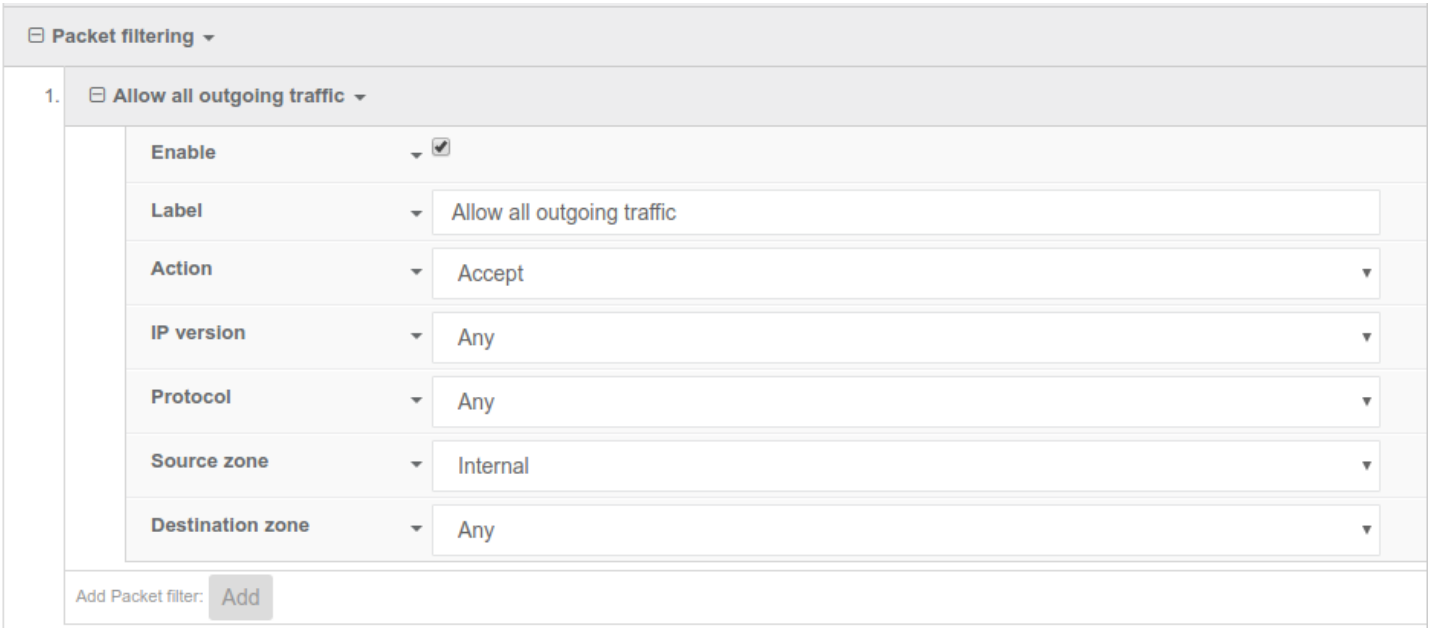
8. Set *IKE -> Mode* to *Aggressive mode*.
9. Uncheck the *IKE -> Initiate connection* option.
10. Set *IKE -> Phase 1 Proposals* and *IKE -> Phase 2 Proposals*. In this example, both proposals are set to 3DES, SHA1, MODP1024.
11. Under NAT, add a destination that corresponds to the local address range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

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

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



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



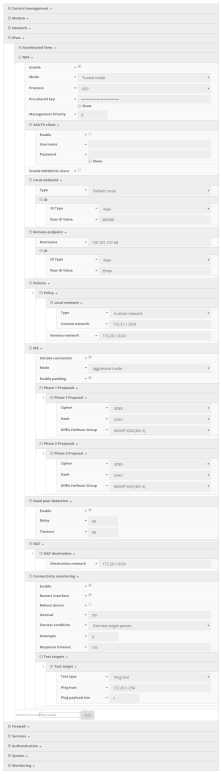
6300-CX Sample Configuration

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

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

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

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



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
```

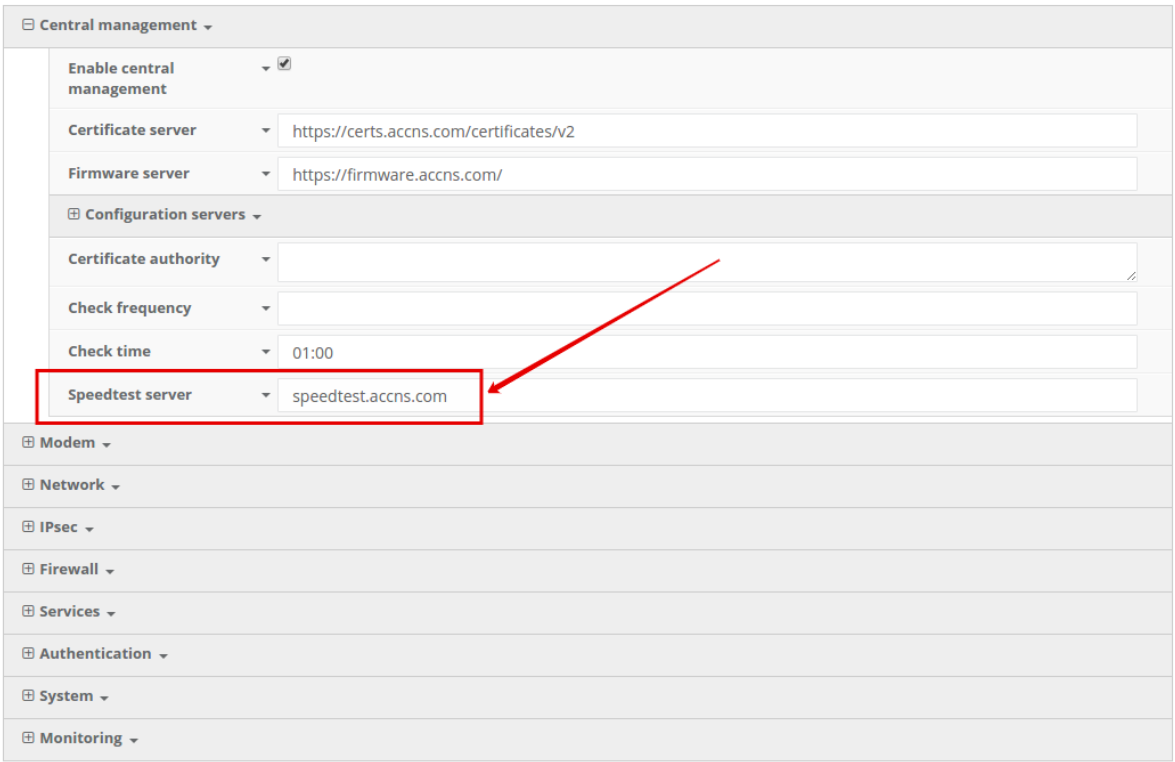
Then start the nuttcp speed test server with the following command:

```
nuttcp -S
```

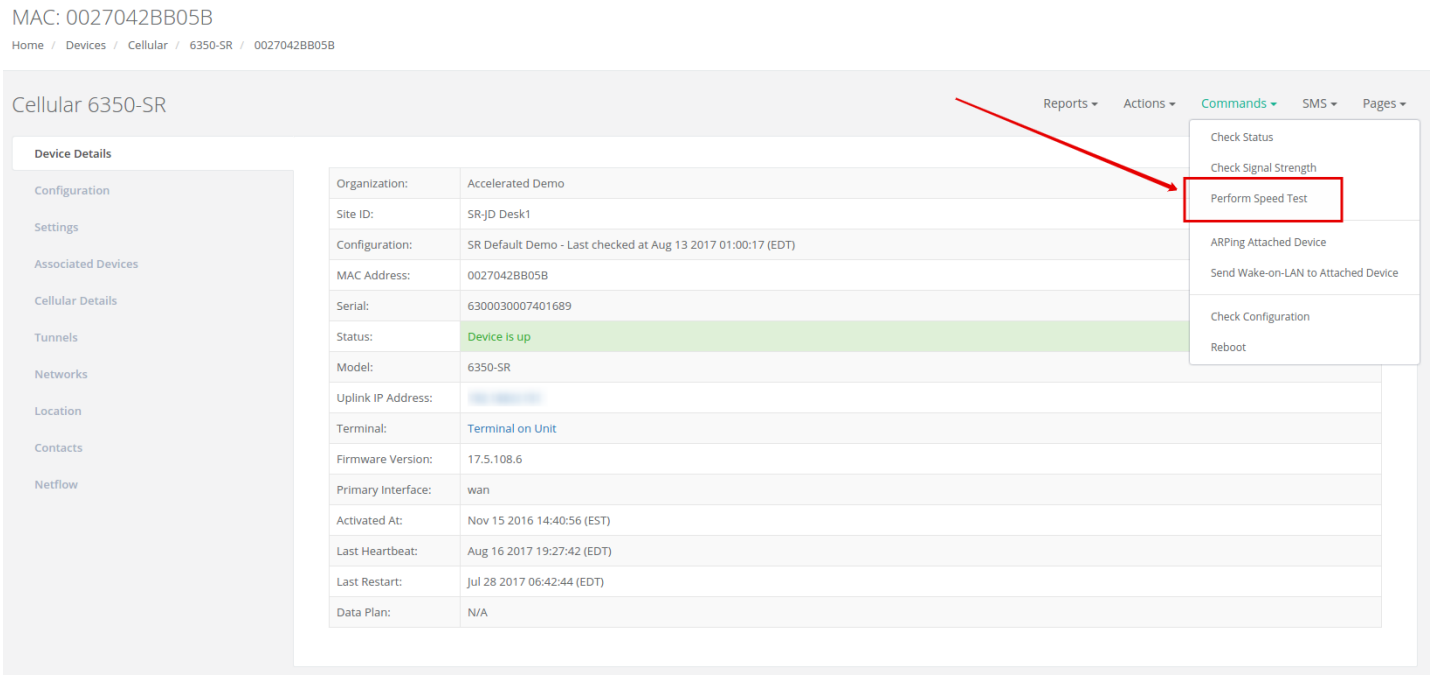
The 63xx-series router will need access to this server on UDP ports 5000 and 5001. Please ensure proper firewalls are opened to allow access to the IP address of the speed test server and its respective ports.

Using the new speed test server

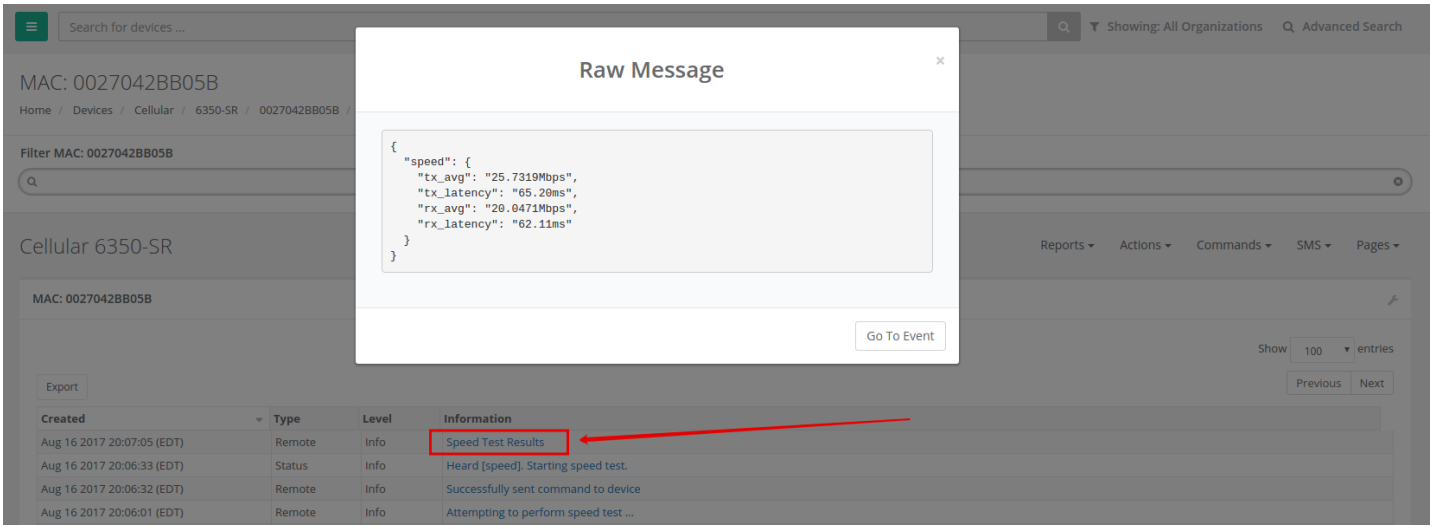
Once the new speed test server is running, add the IP address to the 63xx-series router's configuration profile under *Central management -> speedtest server* and apply the configuration to the device.



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*

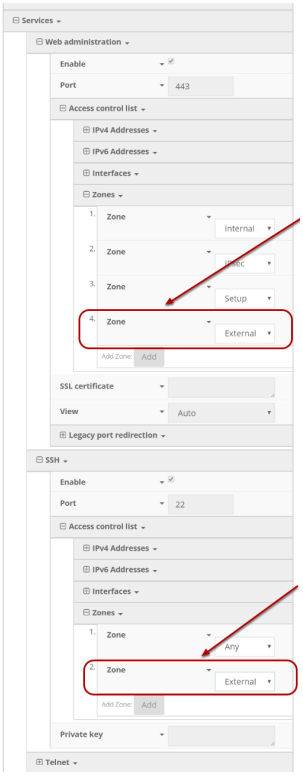
Password: *default*

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.

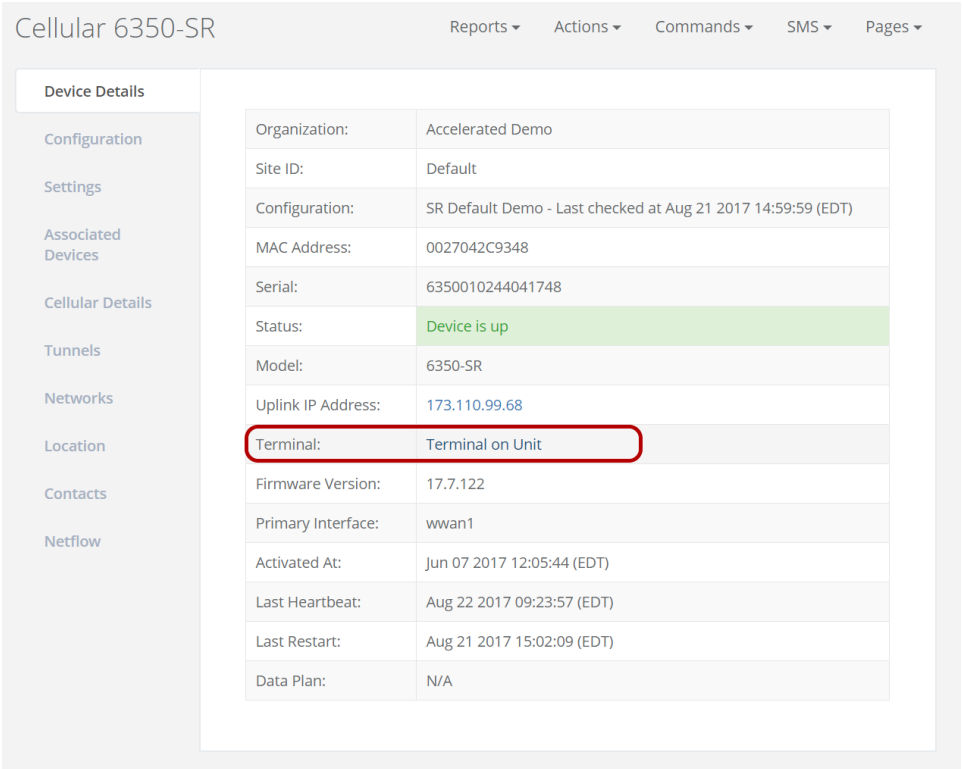
Sample Configuration

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.



MAC address-based Policy Routing with Dual WAN

Difficulty: *Expert*

Minimum firmware version: *17.11.125*

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.

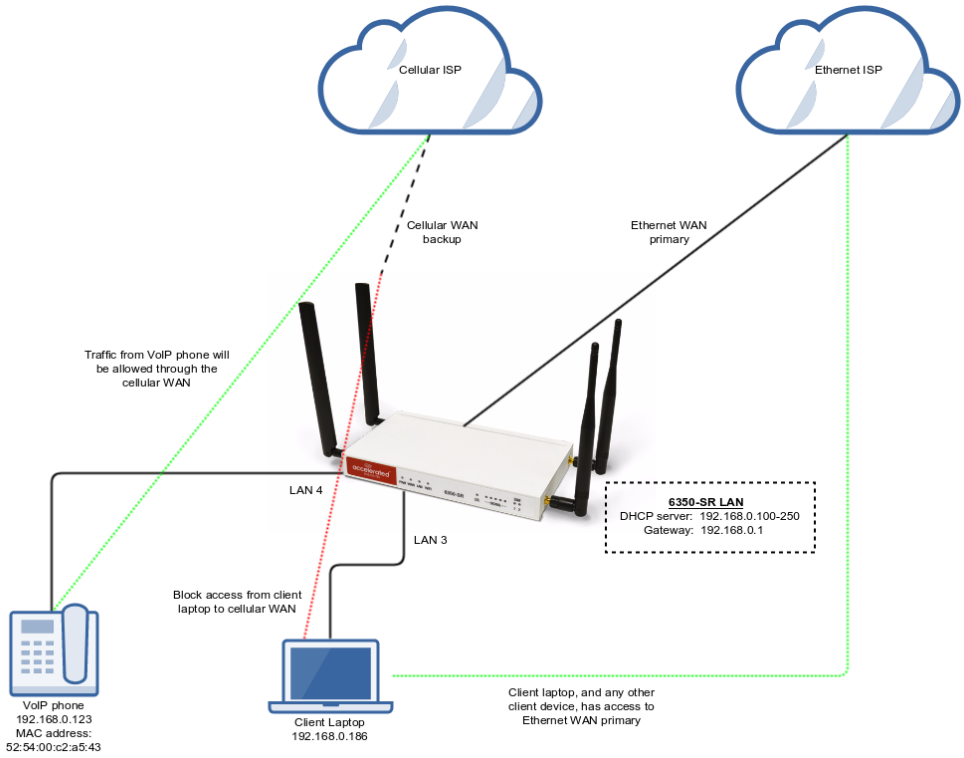
Sample

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

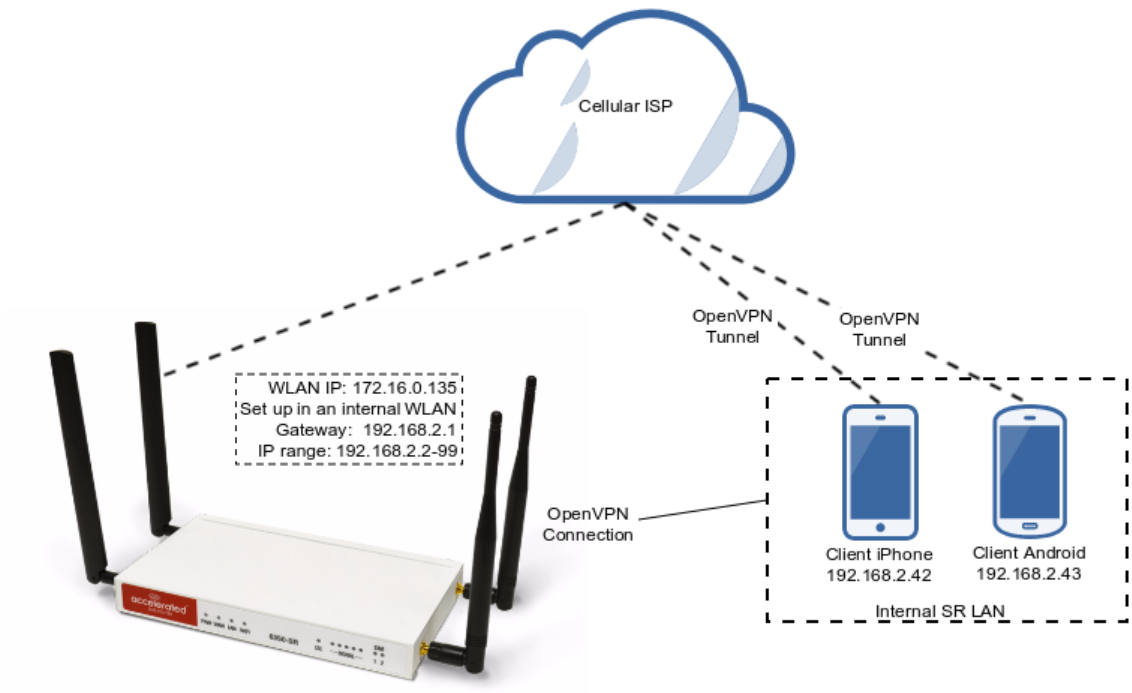
The client devices (iOS/Android OS devices) require the OpenVPN Connect app from their respective app libraries:

- 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.

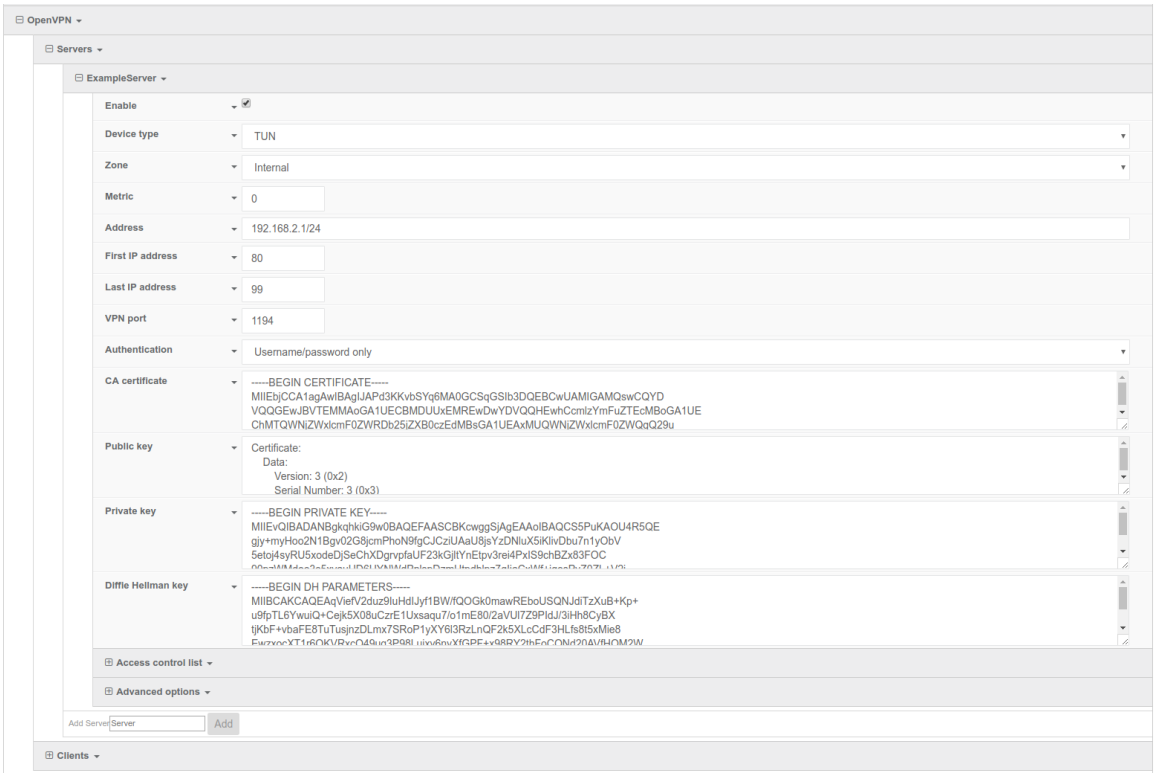


Sample Configuration

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>
```

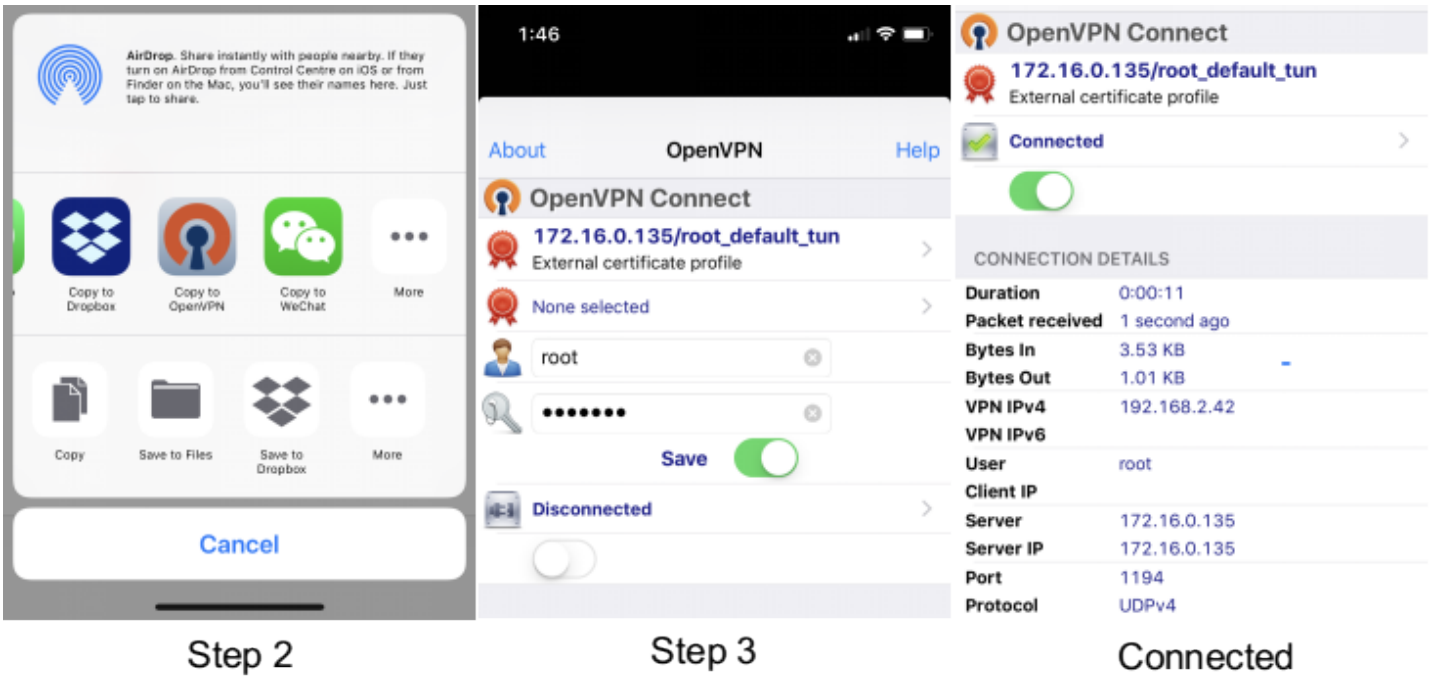
OpenVPN Connect on a mobile device may not require the *auth-user-pass* option. If the option is used, make sure there is no argument passed (i.e. pass.txt) as the application will try to search for the file locally.

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.

Setup

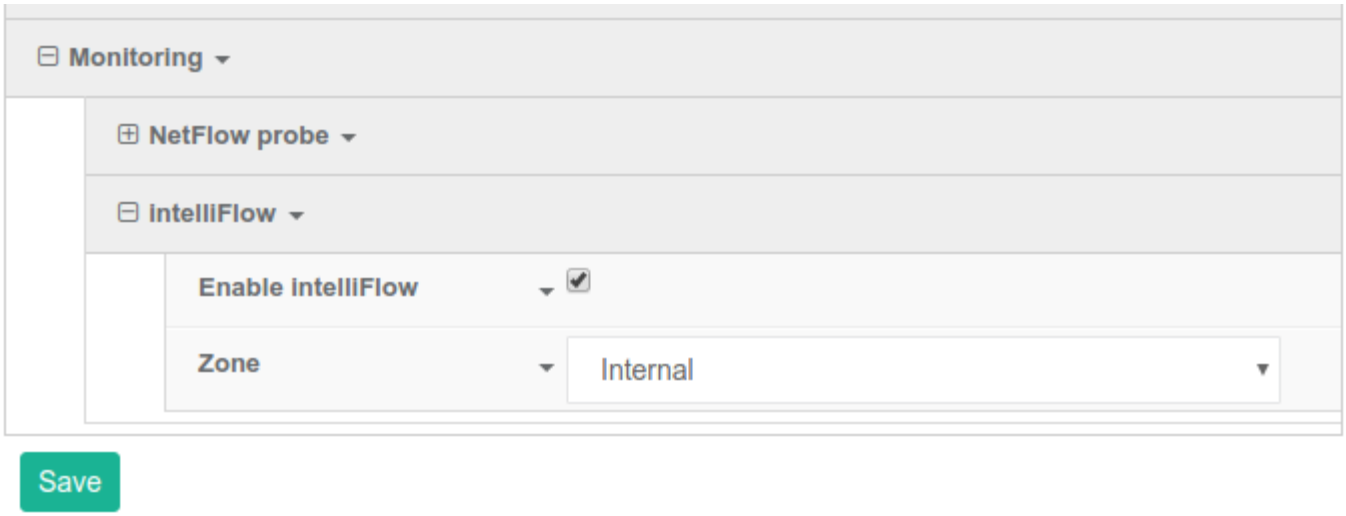
The purpose of intelliFlow is to keep track of the network data usage and traffic information, therefore the only requirement is that the device is powered on, and the local WebUI is accessible.

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.



Enabling Shell Access

Difficulty: *Beginner*

Goal

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

Setup

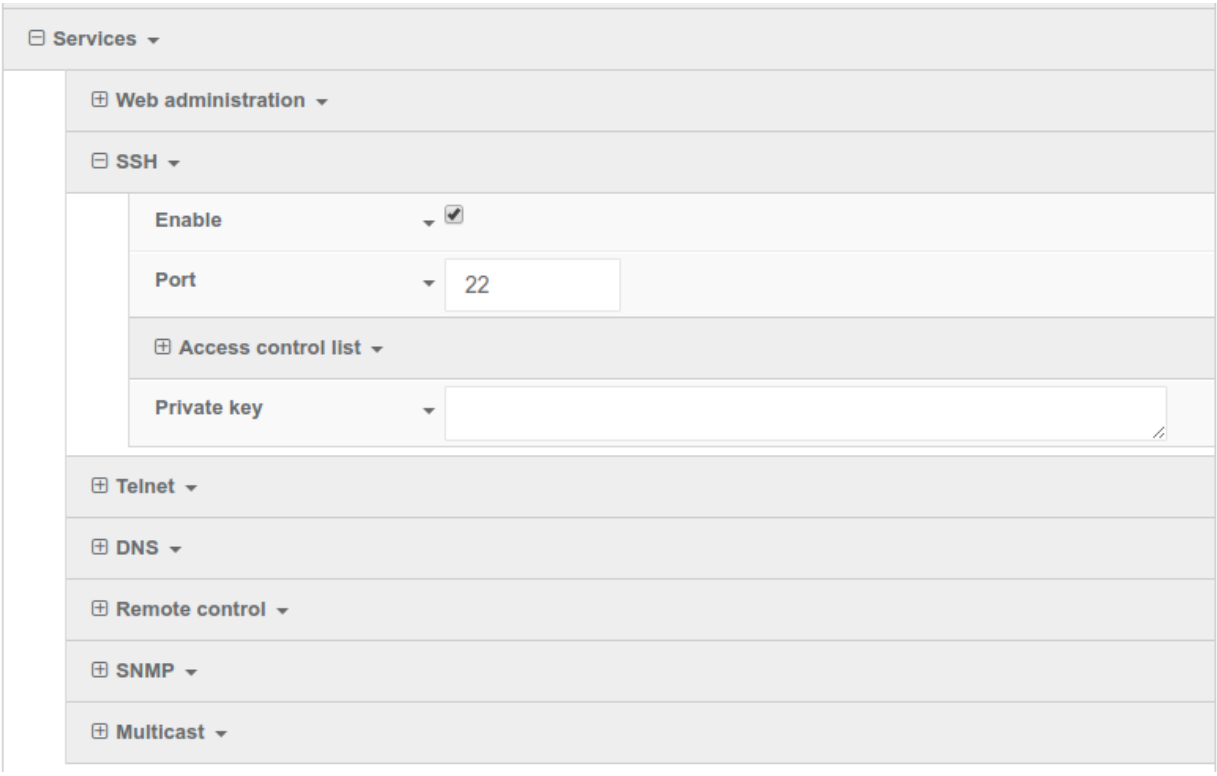
This article assumes the UE is running default configuration with the root password assignment, and central management disabled. Similar procedures apply if shell access is to be enabled in central management.

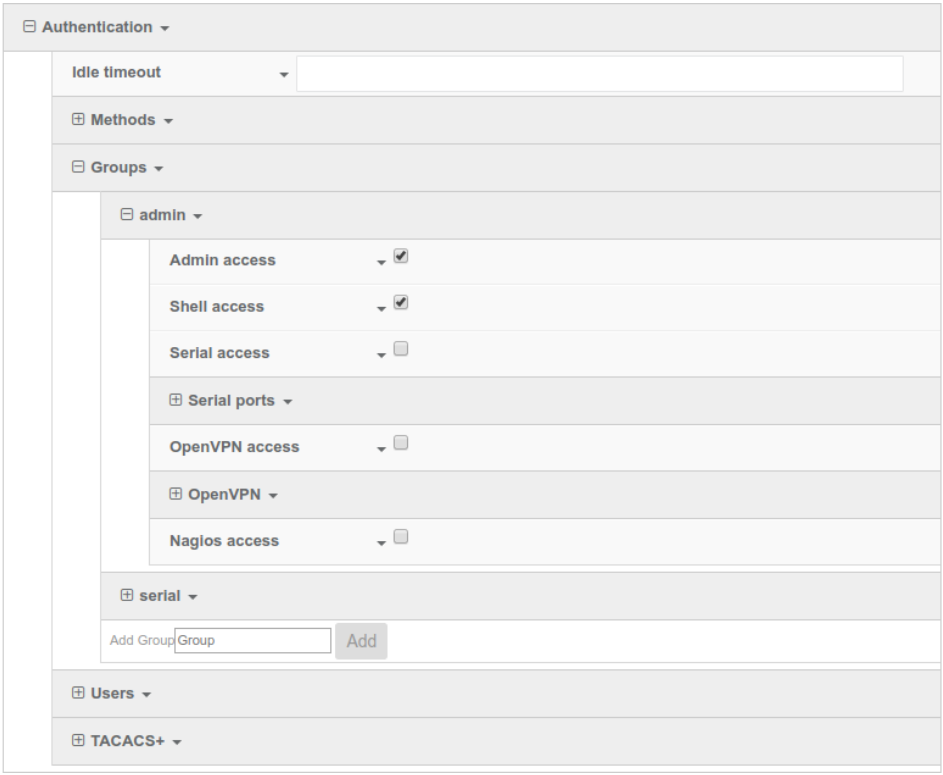
Configuration Steps

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

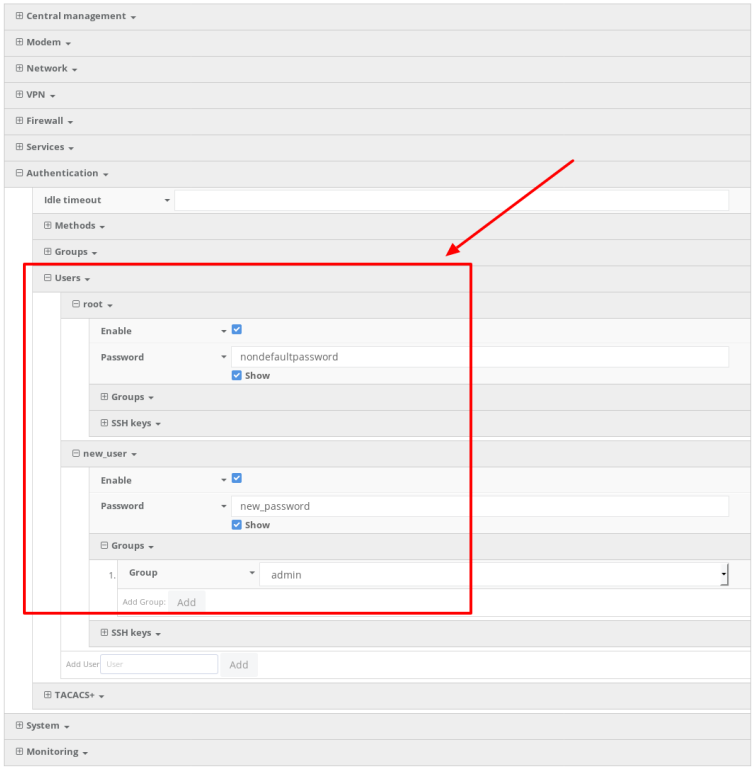
To create a new user and/or change the password of the default root user.

Details

Open the configuration profile for the 63xx-series router 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 in Accelerated View, 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

Data Plan Throttling

Design

This creates a rudimentary, but stable, data plan throttle that will disable any/all LAN traffic on a device if it detects that it 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 a custom script. See example setup below. Note that the user must specify their API token in the 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 disable the LAN interface by default (you can change script to disable passthrough mode instead). Similarly, when the device is within/under its data plan limit for the month, this script will ensure the LAN (or passthrough, if specified) interface is disabled.

Config Setup

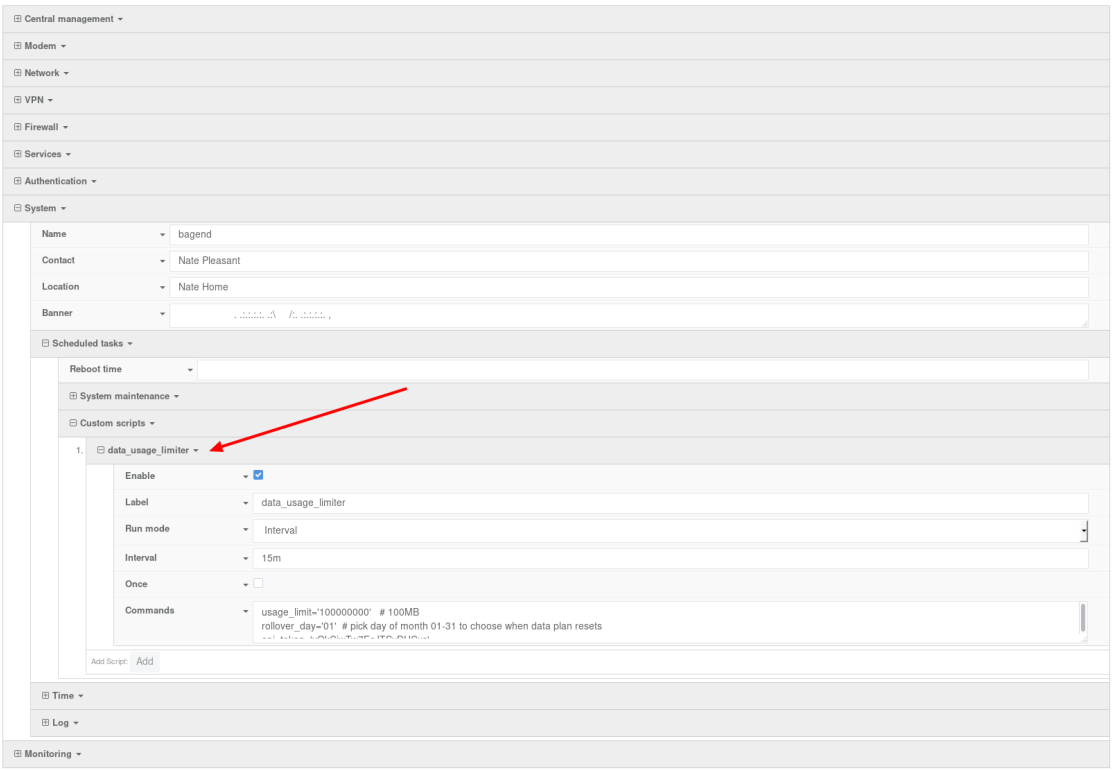
Create a new custom script under *System -> Scheduled tasks -> custom scripts*, and enter in the following. The top three lines should be adjusted to put in the users API token from aView, the desired data plan limit in bytes, and the rollover day of the month.

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).

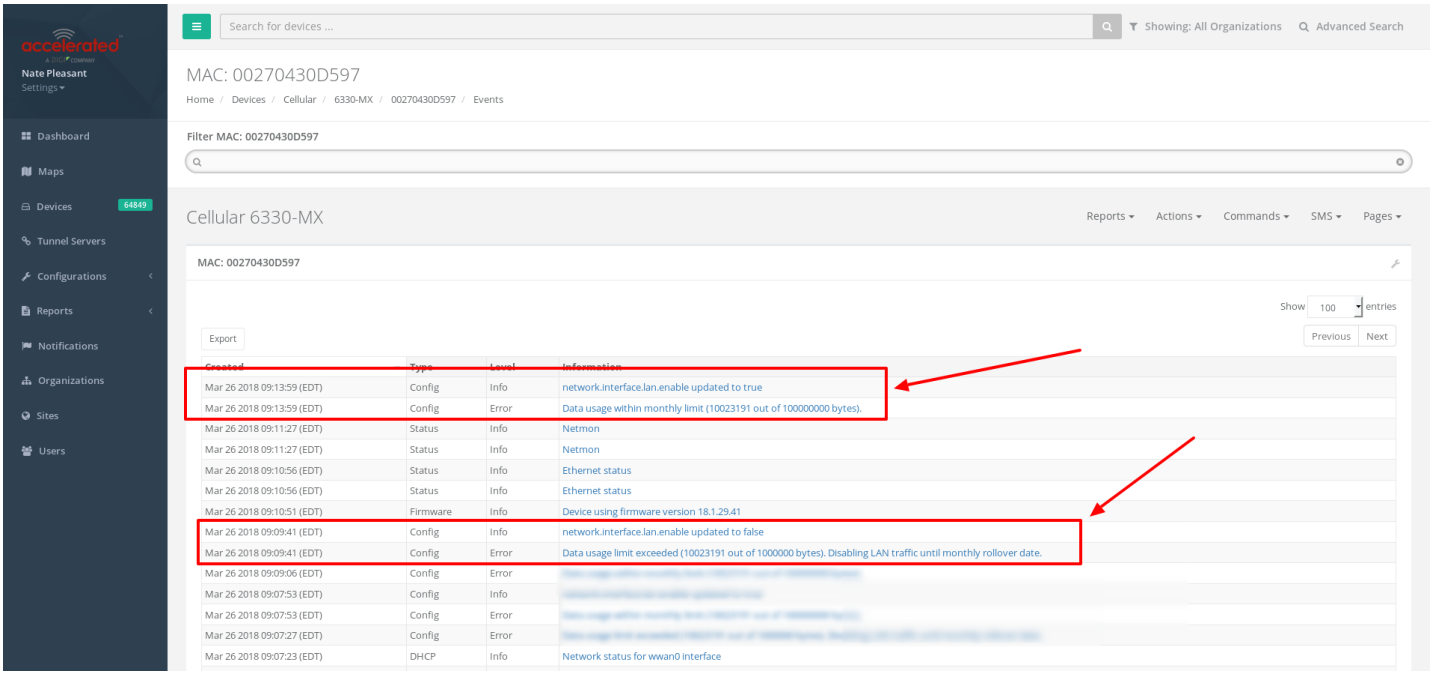
```
usage_limit='100000000'   # 100MB
rollover_day='01'  # pick day of month 01-31 to choose when data plan resets
api_token='xxxxxxxxxx'
mac=$(runt get system.mac)
intf=$(runt dump network.modem | grep intf | tail -n 1 | cut -f2 -d'=')
network_to_enable_disable='network.interface.lan'  # set to modem.passthrough if device
in passthrough mode
network_enabled="$(config get $network_to_enable_disable.enable)"

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

var_is_number(){
  [ "$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

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
  accns_log w config "Data usage limit exceeded ($usage out of $usage_limit bytes).
 Disabling LAN traffic until monthly rollover date."
  [ "$network_enabled" = '0' ] || config set $network_to_enable_disable.enable false
else
  accns_log w config "Data usage within monthly limit ($usage out of $usage_limit
bytes)."
  [ "$network_enabled" = '0' ] && config set $network_to_enable_disable.enable true
fi
```



Example alert notifying data plan throttle enable and disable



VPN Access with IPSec tunnels

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

Goal

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

Setup

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

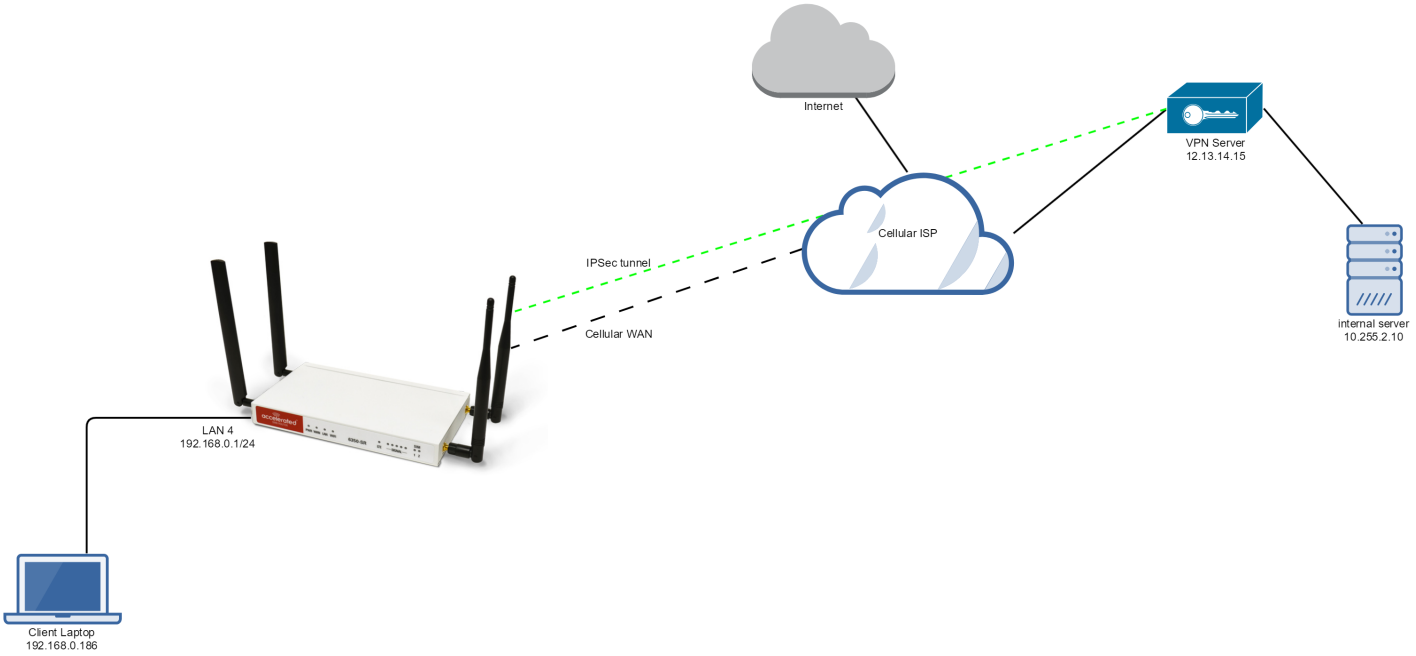
You will also need to know the IPSec credentials and settings needed to build a tunnel to the IPSec endpoint.

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

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

Sample

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

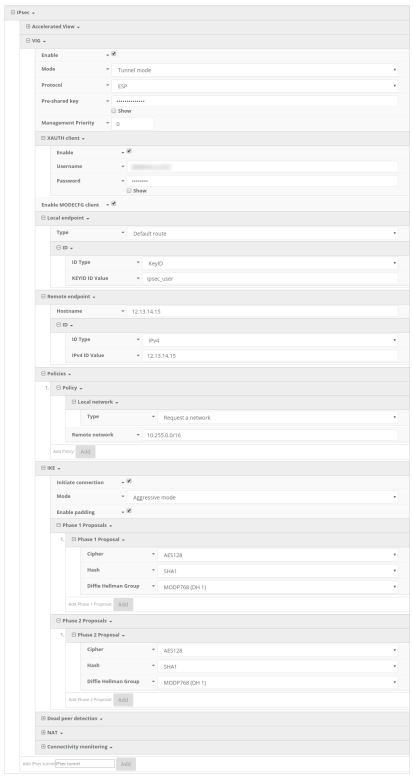
Open the configuration profile for the 6350-SR. Under *IPSec*, create a new entry titled *Tunnel*, and add your IPSec settings to the new entry. The following settings reflect the sample setup in the diagram above.

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

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

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

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



Dual Modem Setup

Goal

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

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

Setup

This article assumes the USB-driven connection will serve as the primary WAN, and that the Accelerated router 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 router 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 routers 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

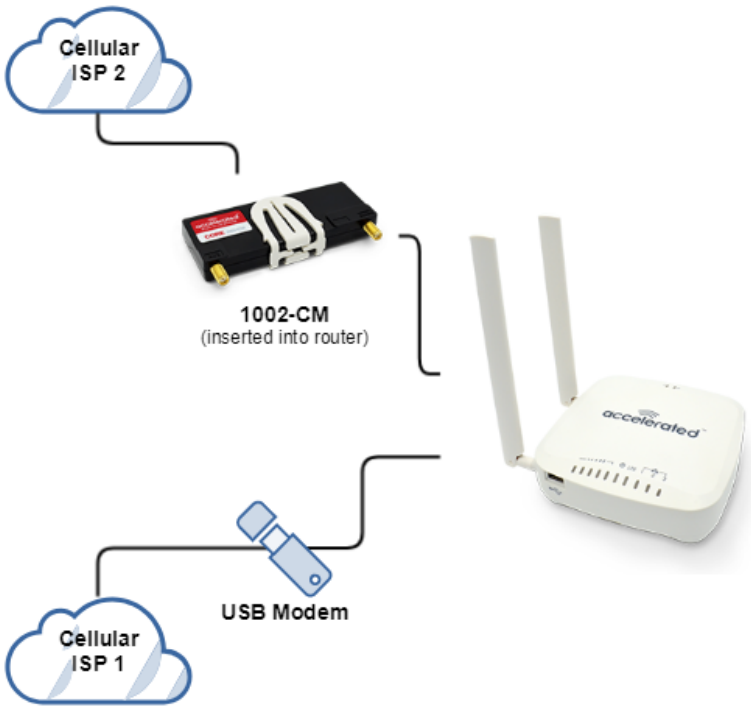
Supported, Modem Configuration Required*:

Netgear 341u (Sprint)

*Refer to our FAQ for More Information

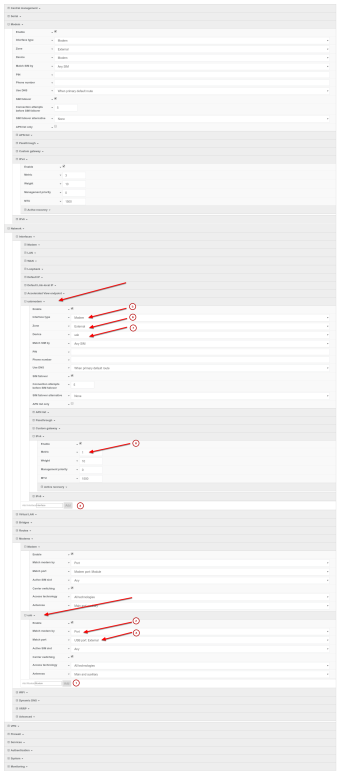
Sample

The sample configuration below shows an Accelerated router 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 routers 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 "usb." 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 can be different if desired.
5. Change the **Interface type** to "Modem."
6. Change the **Zone** to "External."
7. Change the **Device** to "usb" (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.**



Single USB Modem Setup

Goal

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

NOTE: *Accelerated's SR- and MX-series routers 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 routers 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

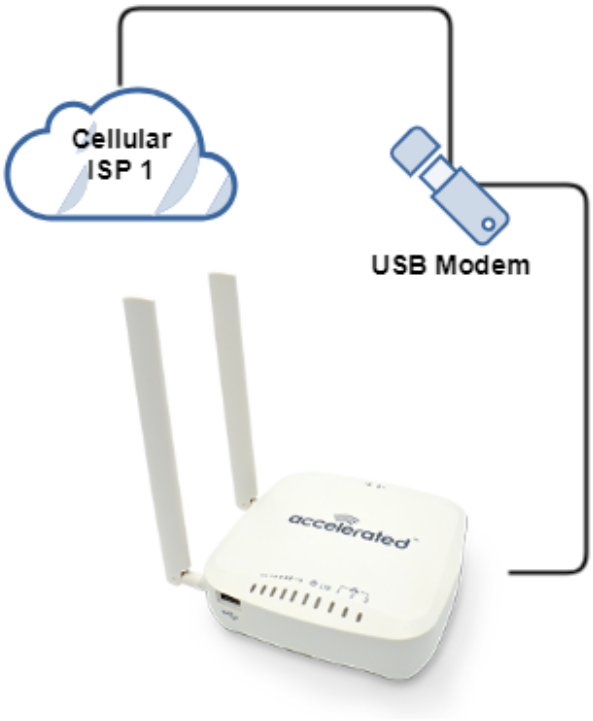
Supported, Modem Configuration Required*:

Netgear 341u (Sprint)

*Refer to our FAQ for More Information

Sample

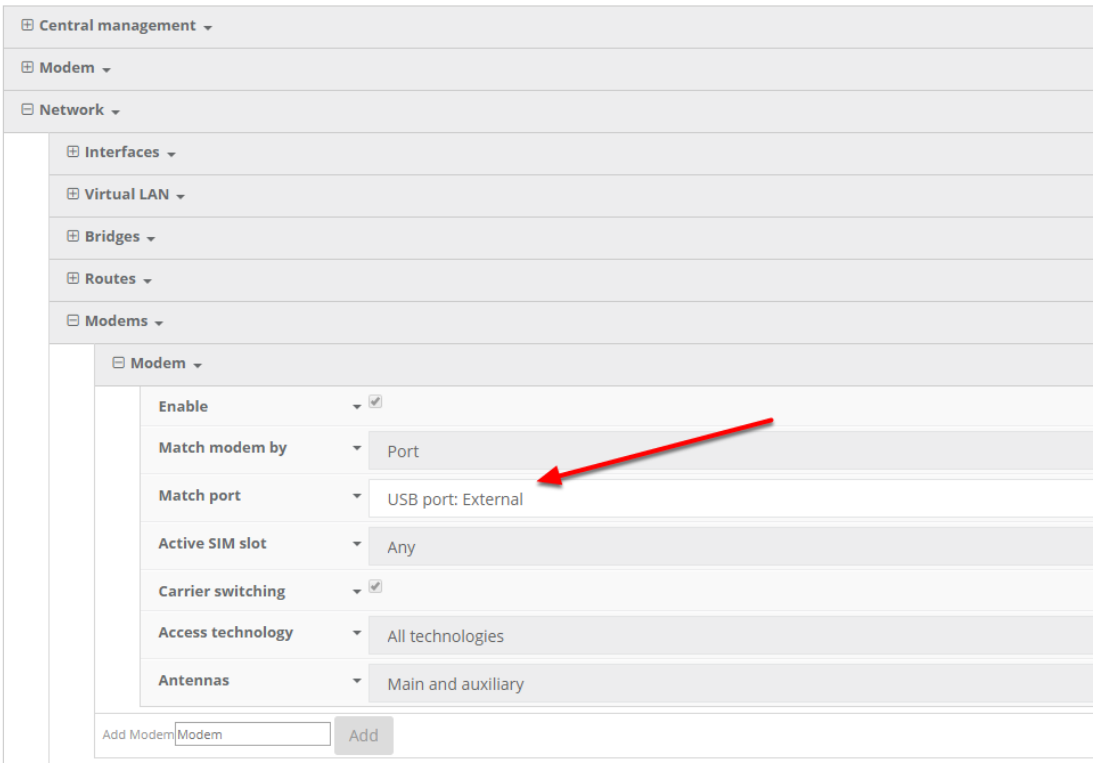
The sample configuration below shows an Accelerated router with a single cellular Internet connection using a supported USB modem.



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 router 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 router 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.

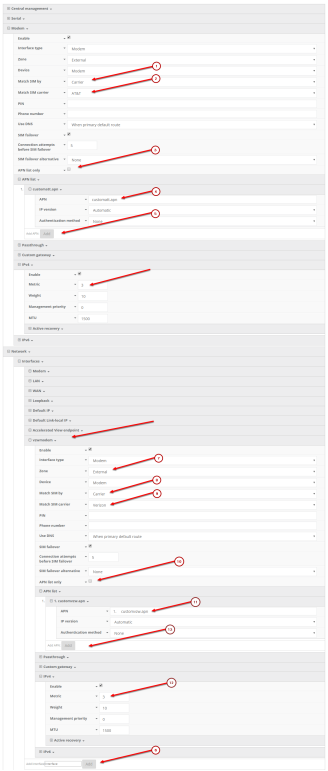
Sample

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 router 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 router 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.

IP Passthrough Not Acting as Intended on Device Firmware 18.4.54.22

Problem

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

Background

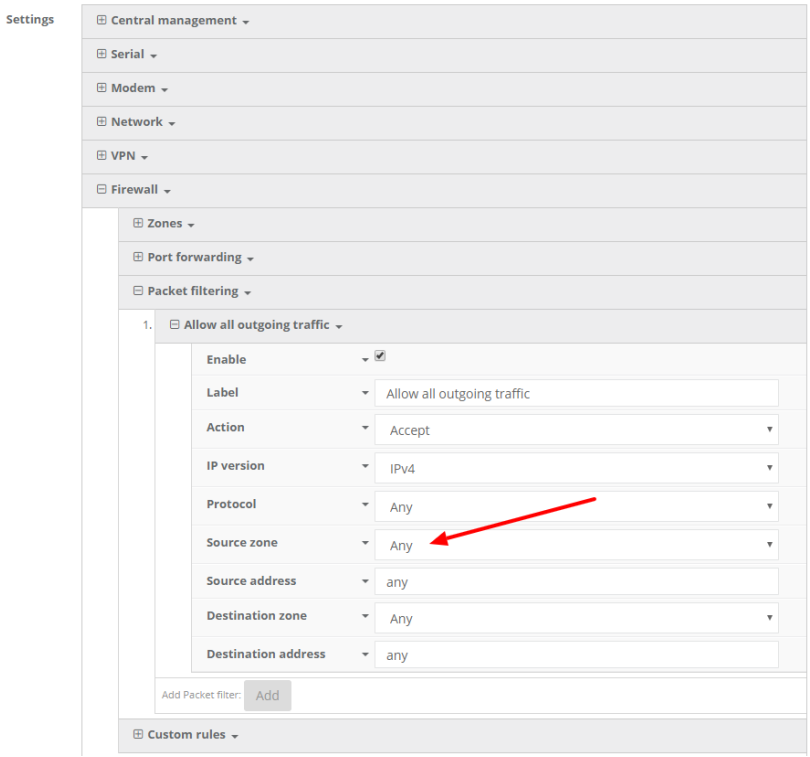
We've been seeing an issue where the latest firmware has unintentionally engaged the firewall for passthrough connections. This results in failed pings from an external source of the cellular IP of an Accelerated cellular router on firmware 18.4.54.22 configured with IP Passthrough.

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.



Support Report Overview

Generating a Support Report

Support reports provide a snapshot of a router'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 routers. For more information about generating support reports, please click here.

NOTE: *Information logged on the device will be erased when the router 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 router'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 router 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 routers
	ubus-dump		A log of ubus calls for network devices and interfaces

Directory	File Name		Notes
	uptime		The device's uptime at the time of generating the report, along with CPU load averages for the past 1, 5, and 15 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 router'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
- 11904.mcs
- MNS-OOB-APN01.com.attz
- altaworx02.com.attz
- m2m.com.attz
- 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

Other

- blank
- 11315
- managedvpn
- telstra.internet
- mobinilweb,internet
- web.vodafone.de
- everywhere
- internet.com
- inet.bell.ca
- isp.telus.com
- internet.telecom.co.nz
- inetgsm.vzw3g.com
- isp.cingular
- internet
- everywhere