WiNG 5.2 How-To Guide

3G WWAN

September 2011

Revision 1.0

Table of Contents:

1. Introduction:

3G or 3rd Generation is a family of standards for mobile telecommunications defined by the International Telecommunication Union which includes GSM, UMTS, CDMA as well as DECT and WiMAX. Compared with 2G or 2.5G, 3G offers simultaneous speech and data services and improved data rates allowing network operators to offer a wider range of advanced services to subscribers while achieving greater network capacity through improved spectral efficiency.

1.1 3G Applications:

3G WAN support is available in WiNG 5 on the RFS4000/RFS6000 WLAN Switch Controllers and the AP7131 tri-radio AP in which the 3rd radio is a 3G card, running WiNG 5.2.0.0 and above and can be deployed to provide primary Internet access at a remote site or Internet failover in the event of a primary wireline Internet service failure.

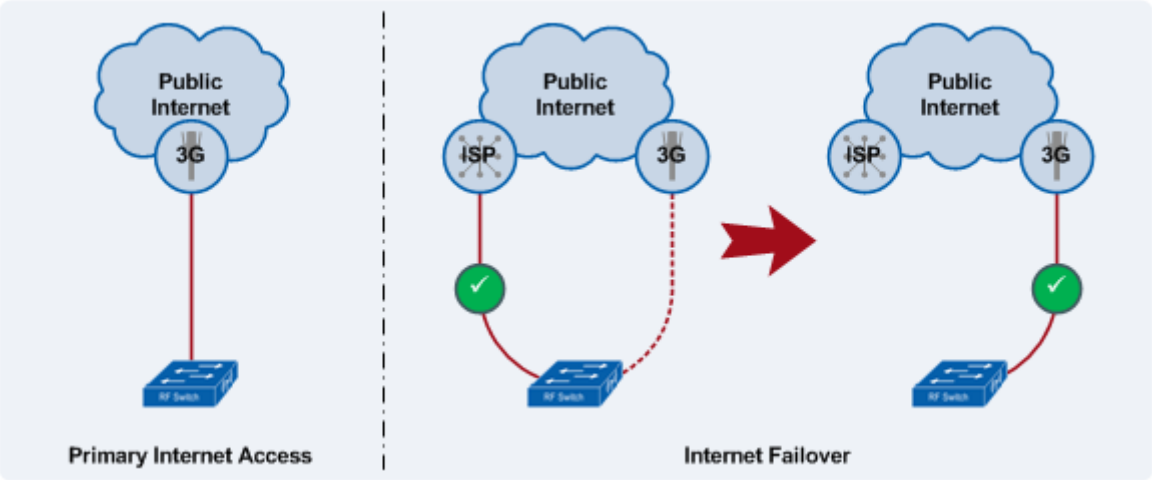


Figure 1 - 3G WWAN Applications

1.1.1 Primary Internet Access:

For primary Internet access the 3G WAN card provides the primary outbound path for the site to the public Internet. Once connected the 3G card interface will receive network addressing and DNS servers from the service providers DHCP server and the WiNG 5.2 device will utilize its own WWAN interface as the default gateway.

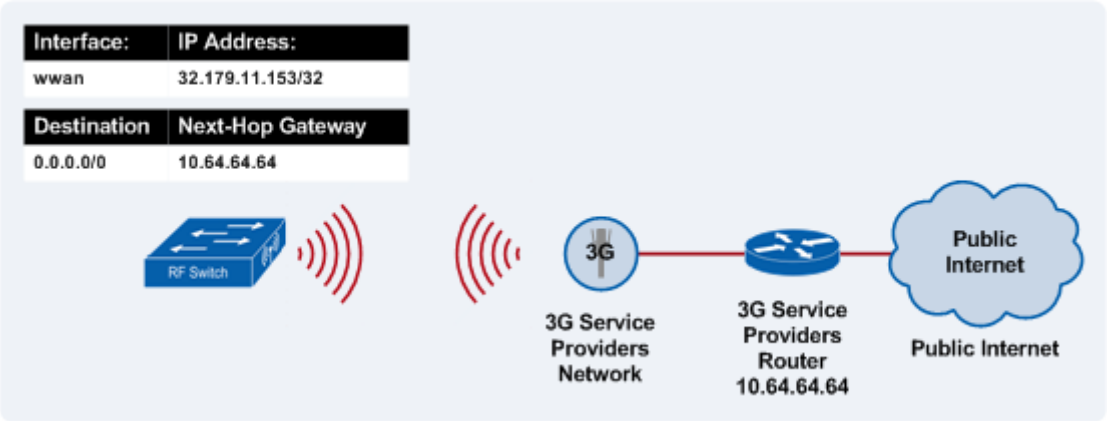


Figure 2 - Primary Internet Access

For primary Internet access a NAT rule must be defined that translates internal private addresses to the Public IP address assigned to the 3G interface. Note that unlike virtual IP interfaces, the 3G interface is automatically designated as a NAT outside interface.

1.1.2 Internet Failover:

For Internet failover the 3G WAN card provides a backup Internet path to a wireline Internet service directly connected to the WLAN Switch Controller. During normal operation the WLAN Switch Controller will use the wireline Internet service and all outbound Internet traffic will be forwarded to the wireline service provider's router. The wireline service provider's router is dynamically or statically defined as the WLAN Switch Controller's default router.
To detect a wireline Internet service failure the WLAN Switch Controller monitors the state of the default router will failover to the 3G interface if the default router becomes unreachable.
Outbound Internet will failover to the 3G interface if:
1) The physical port that the default router is connected through goes down.

2) The default router is no longer reachable by the WLAN Switch Controller.

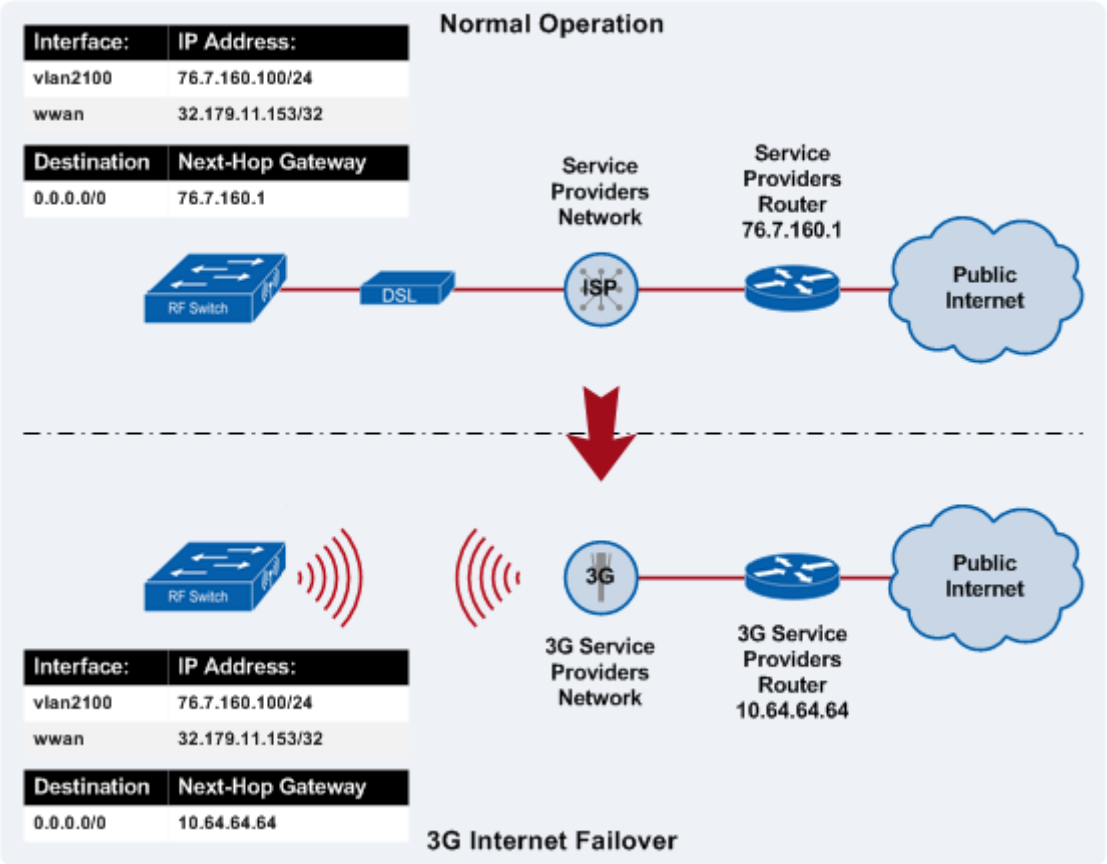


Figure 3 - Failover Internet Access

If the wireline service provider's router becomes unreachable, the WLAN Switch Controller will dynamically update the NAT rule to use the 3G interface as well as dynamically update the routing table so that the 3G WAN service provider's upstream router becomes the default gateway for the WLAN Switch Controller. All outbound traffic destined to the public Internet will then be forwarded via the 3G interface.

2. 3G Support:

WiNG 5.2 provides support for two new additional express cards, listed in the table below. 3G WAN Express cards are available from a number of service providers in each region and each card will require a data service plan from a service provider. The available data service plans vary by region and service provider and can ether permit unlimited data transfer or limited data transfer over the service providers 3G network. Service provides may also apply overage fees when a specific amount of traffic has been exceed.

The following table provides a list of supported 3G WAN Express cards supported by the RFS4000/RFS6000 WLAN Switch Controllers as well as the AP7131 tri-radio AP with 3G support, available by region and service provider. Before selecting a 3G Express card it is recommended that you reference the latest release notes for the latest list of supported cards as new models are being continuously introduced into the market.

Region	Service Provider	Card	3G Technology
NA/LA	AT&T Wireless	Option GT Ultra Express	Tri-band HSDPA and quad-band EDGE
NA/LA	Verizon Wireless	V740 Express Card	CDMA 1xEV-DO
NA/LA	AT&T Wireless	AirCard 890	Tri-band HSDPA and quad-band EDGE
EMEA	Vodafone	Novatel Merlin XU870	Tri-band HSDPA/UMTS and quad-band EDGE/GPRS
EMEA	Vodafone	E3730 3G Express card	Tri-band HSDPA/UMTS and quad-band EDGE/GPRS
APAC	Telstra	Telstra Turbo 7 AirCard 880E	Tri-band HSPA/UMTS and Quad-band EDGE
APAC	Telstra	AirCard 503	Tri-band HSPA/UMTS and Quad-band EDGE

Table 1 - 3G WAN Express Card Support

New 3G PCI-Express Card Support

Figure 4 - Aircard 503

Figure 5 - Aircard 504 (AT&T 890)

3. Pre-Requisites:

3.1 Requirements:

The following requirements must be met prior to attempting this configuration:

- A wireline Internet service is connected to the WiNG 5 device and NAT and Firewall rules applied.
- A supported Express 3G WAN card is activated and installed in the WiNG 5 device.
- A Windows XP workstation is available with Microsoft Internet Explorer or Mozilla Firefox to perform Web UI or CLI configuration.
- The reader has read the Motorola RFS Series Wireless LAN Switches - WiNG System Reference Guide.

3.2 Components Used:

The information in this document is based on the following Motorola hardware and software versions:

- 1 x AP7131N running version 5.2.0.0-057R
- 1 x AT&T GT Ultra Express 3G Card
- 1 x Cable Wireless Internet Service
- 1 x US AT&T 3G Data Plan

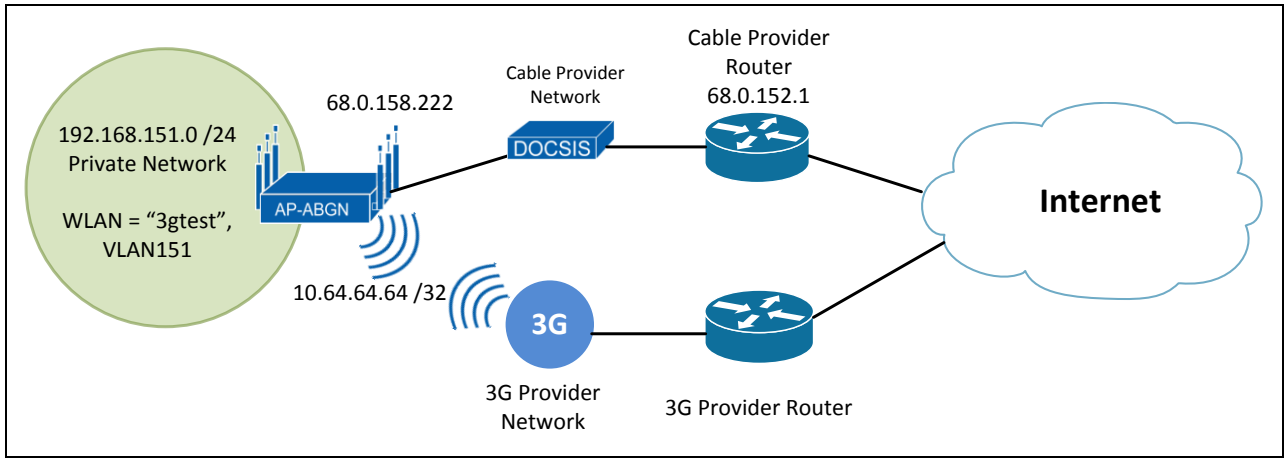
✔ Registered users may download the latest software and firmware from Motorola Technical Support site: http://support.symbol.com.

3.3 Network Diagram

The following diagram illustrates the topology of the example environment. The primary Internet service is provided by cable, while the 3G service is provided by AT&T. The AP7131 acts as the primary router (default-gateway) for the private network, having Ge1 interface on the private network and Ge2 on the cable network.

The AP7131 running-config will be included at the end of this document.

1)	Network Diagram



4. Configuration:

Currently, configuration of the 3G interface is very similar to that which was done in WiNG 4.x. The following sections outline the configuration steps required for this scenario:

1. Installation of AT&T 3G Card (Section 4.1)
2. Installation of Verizon 3G Card (Section 4.2)
3. Network Address Translation (Section 4.3)

Creating the IP firewall rules to protect the internal network will not be covered in this document. However, IP firewall rules need to be configured. Please see "WiNG5_Firewall_How-To.pdf" to understand creating the firewall rules.

4.1 AT&T 3G Card Installation

AT&T used to require the login credentials and APN configuration, however this is not the case any longer. So simply plugging the card into the router and activating it is all that is needed.

1)	Install the 3G card
2)	Activate the card

```
ap71xx(config)#self
ap71xx(config-device-ap71xx)#interface wwan1
ap71xx(config-device-ap71xx-if-wwan1)#no shutdown
ap71xx(config-device-ap71xx-if-wwan1)#commit write
ap71xx(config-device-ap71xx-if-wwan1)#end
```

3)	Verify

```
ap71xx#show wwan status
>>> WWAN Status:
```

```
+-----------------------------------------
|     State : CONNECTION_UP
|     DNS1  : 172.16.7.167
|     DNS2  : 172.16.7.167
+-----------------------------------------
ap71xx#show wwan config
+-----------------------------------------
|     Access Port Name :
|     User Name        :
|     Cryptomap        :
+-----------------------------------------
```

One can see in the verification step that there is no configuration for the credentials or APN, yet the 3G card has a status of "**CONNECTION_UP**" and has received the providers DNS servers. Make sure to double-check the connectivity by performing a ping that exits the wwan1 interface to a site to test name resolution as well as IP connectivity.

4.2 Verizon 3G Card Installation

Verizon service will still require login credentials:

1)	Install the 3G card
2)	Activate the card

```
ap71xx(config)#self
ap71xx(config-device-ap71xx)#interface wwan1
ap71xx(config-device-ap71xx-if-wwan1)#username
<vzw_phone_number>@vzw3g.com
ap71xx(config-device-ap71xx-if-wwan1)#password 0 vzw
ap71xx(config-device-ap71xx-if-wwan1)#apn vzw
ap71xx(config-device-ap71xx-if-wwan1)#auth-type chap
ap71xx(config-device-ap71xx-if-wwan1)#no shutdown
ap71xx(config-device-ap71xx-if-wwan1)#commit write
ap71xx(config-device-ap71xx-if-wwan1)#end
```

3)	Verify

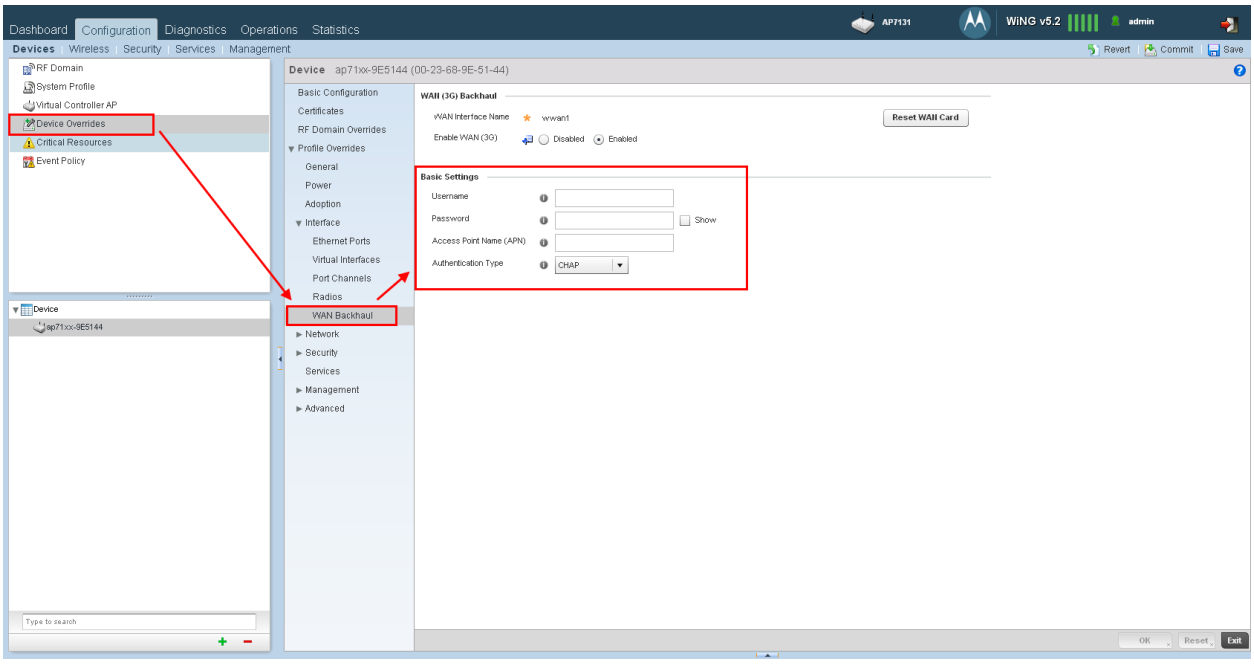
```
ap71xx#show wwan status
>>> WWAN Status:
```

```
+-----------------------------------------
|     State : CONNECTION_UP
|     DNS1  : 209.183.35.23
|     DNS2  : 209.183.35.23
+-----------------------------------------
ap71xx#show wwan config
+-----------------------------------------
|     Access Port Name : vzw
|     User Name        : <vzw_phone_number>@vzw3g.com
|     Cryptomap        :
+-----------------------------------------
```

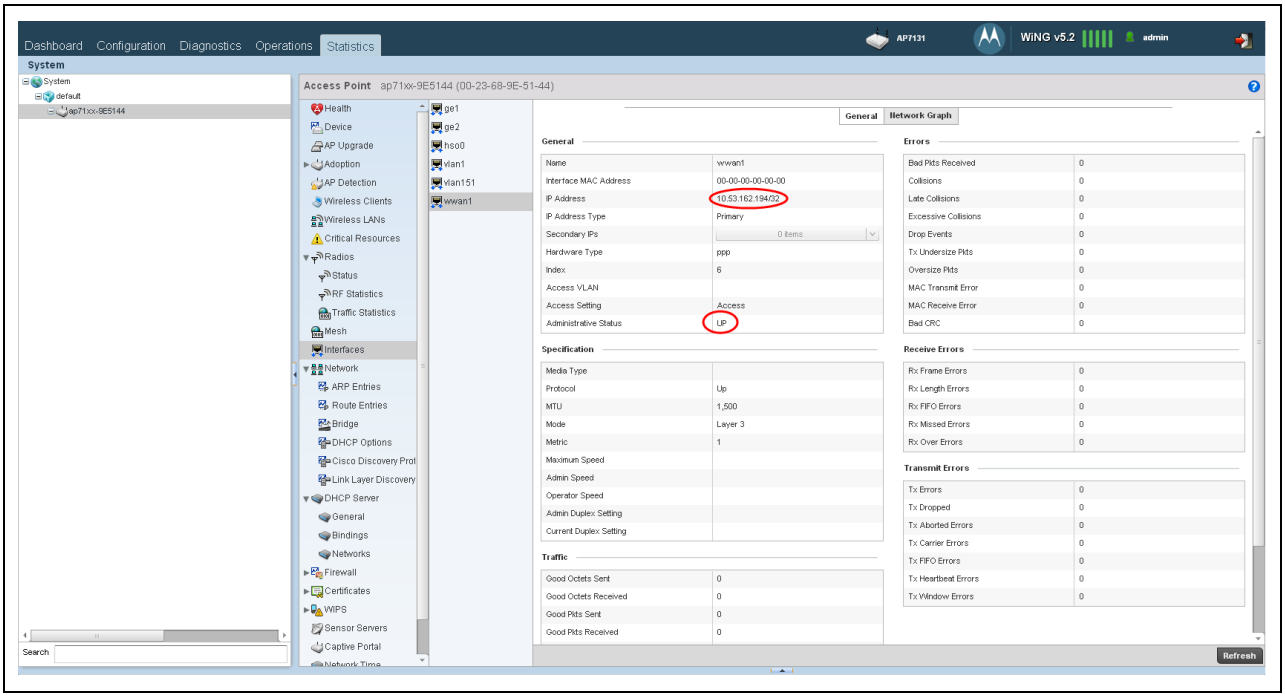
4.2.1 Web-UI Config & Statistics

After logging into the GUI interface, navigate to **"Configuration / Devices / Device Overrides / Interfaces / WAN Backhaul"**

1) AP7131 WWAN Interface Config



2) Statistics / Verification



4.3 NAT Configuration

The WAN backhaul interface (wwan1) is automatically recognized as a nat-outside interface. This means that if traffic is exiting the network via wwan1 on the RFS / AP, that traffic will be translated to the IP address on wwan1 without having to add "**`ip nat outside`**" to that interface. However you do need to add an overload statement for the wwan1 interface.

Though the focus of this paper is 3G WAN backhaul, this section will show how to setup the primary provider NAT translations for reference. In this example, interface "vlan1" is our outside interface on the cable provider network, while interface "vlan151" is our internal, private network. The Ge interfaces have been configured for their respective vlans.

4.3.1 NAT CLI Configuration

1) NAT ACL for allowed networks

```
ap71xx#config terminal
ap71xx(config)#ip access-list nat-list
ap71xx(config-ip-acl-nat-list)#permit ip 192.168.151.0/24 any rule-precedence 10
ap71xx(config-ip-acl-nat-list)#commit
```

2) Establish inside / outside NAT interfaces

```
ap71xx(config-ip-acl-nat-list)#exit
```

```
ap71xx(config)#self
ap71xx(config-device-ap71xx)#interface vlan151
ap71xx(config-device-ap71xx-if-vlan151)#ip nat inside
ap71xx(config-device-ap71xx-if-vlan151)#interface vlan1
ap71xx(config-device-ap71xx-if-vlan1)#ip nat outside
```

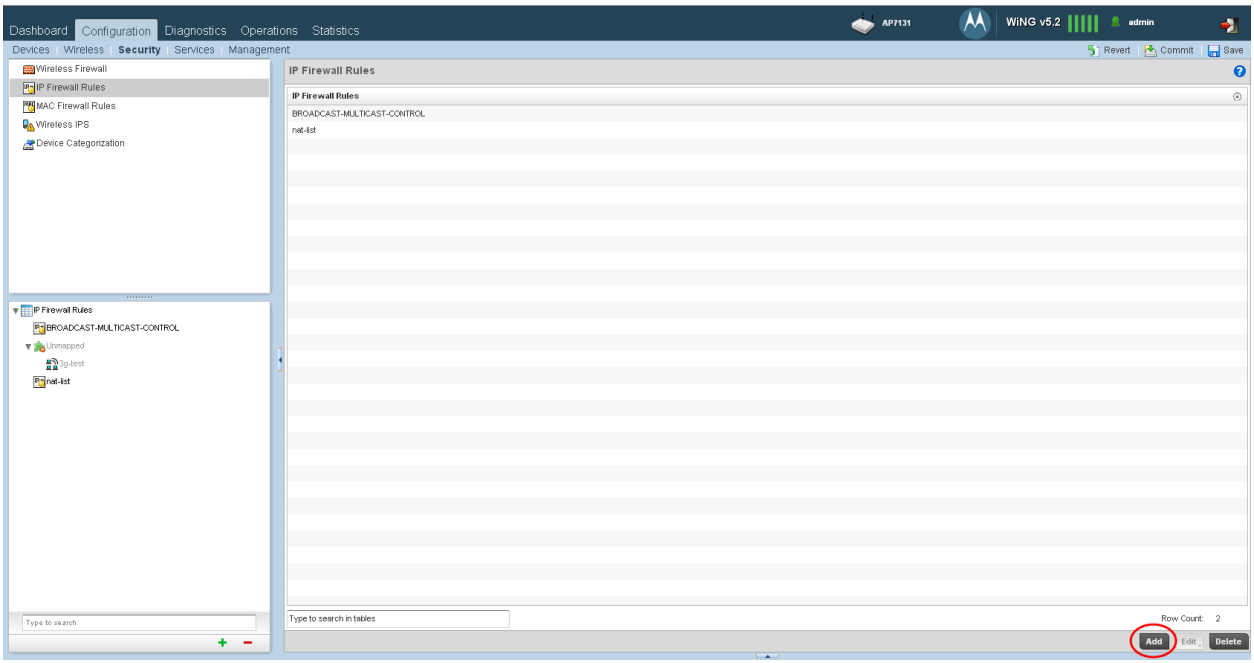
3) Create NAT Overload statements

```
ap71xx(config-device-ap71xx-if-vlan1)#exit
ap71xx(config-device-ap71xx)#ip nat inside source list nat-list
interface vlan1 overload
ap71xx(config-device-ap71xx)#ip nat inside source list nat-list
interface wwan1 overload
```

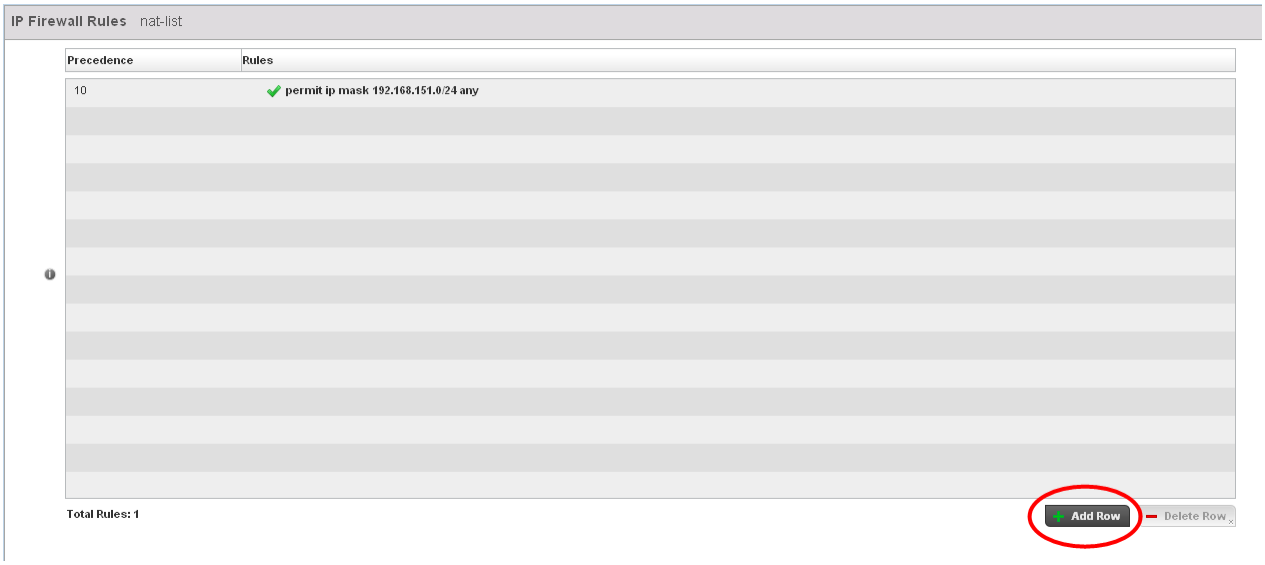
4.3.2 NAT GUI Configuration

Start of by navigating to "**Configuration > Security > IP Firewall Rules**" and add a new IP ACL.

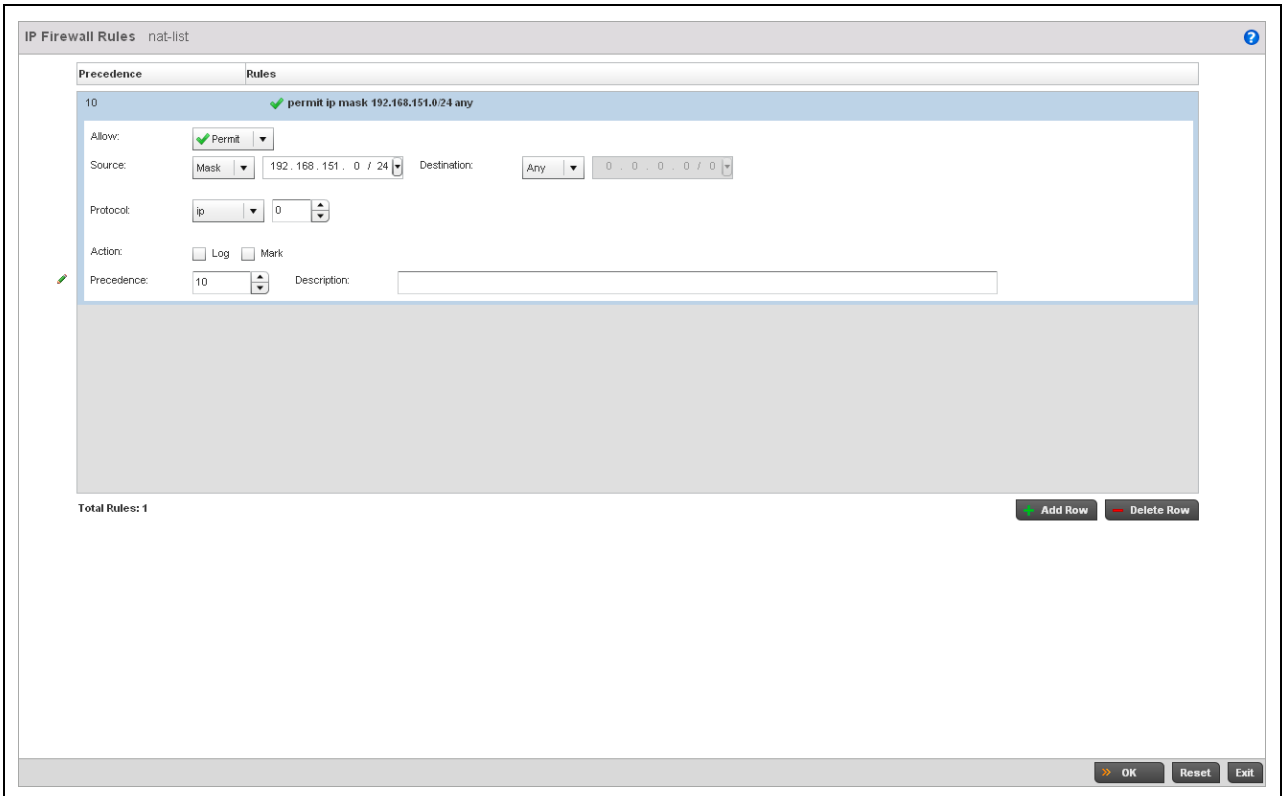
1) Add NAT ACL



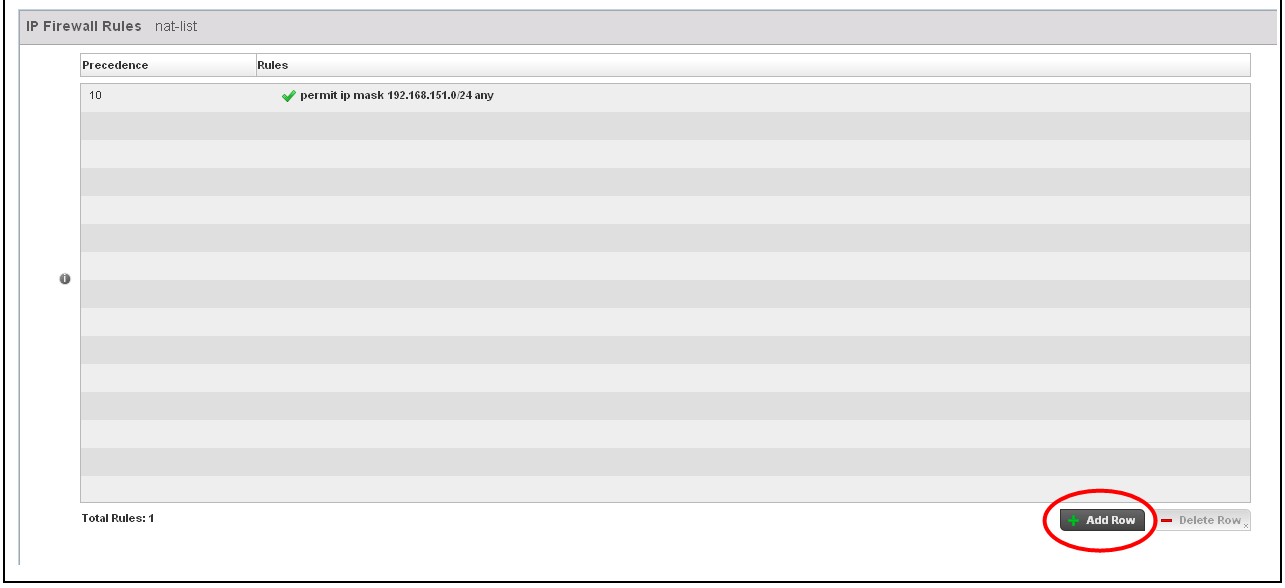
2) Name the ACL and add a new ACL rule



3) Add network(s) to be NAT'd and click ">>OK"



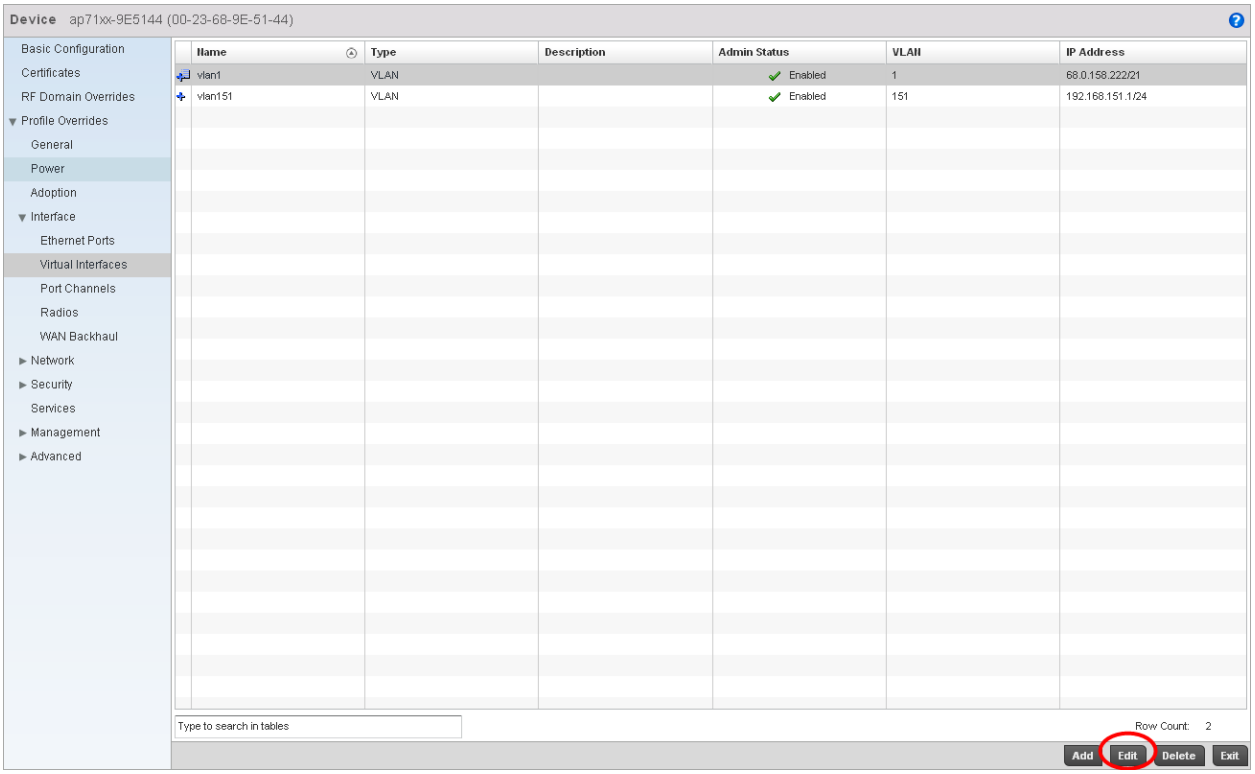
4) Name the ACL and add a new ACL rule



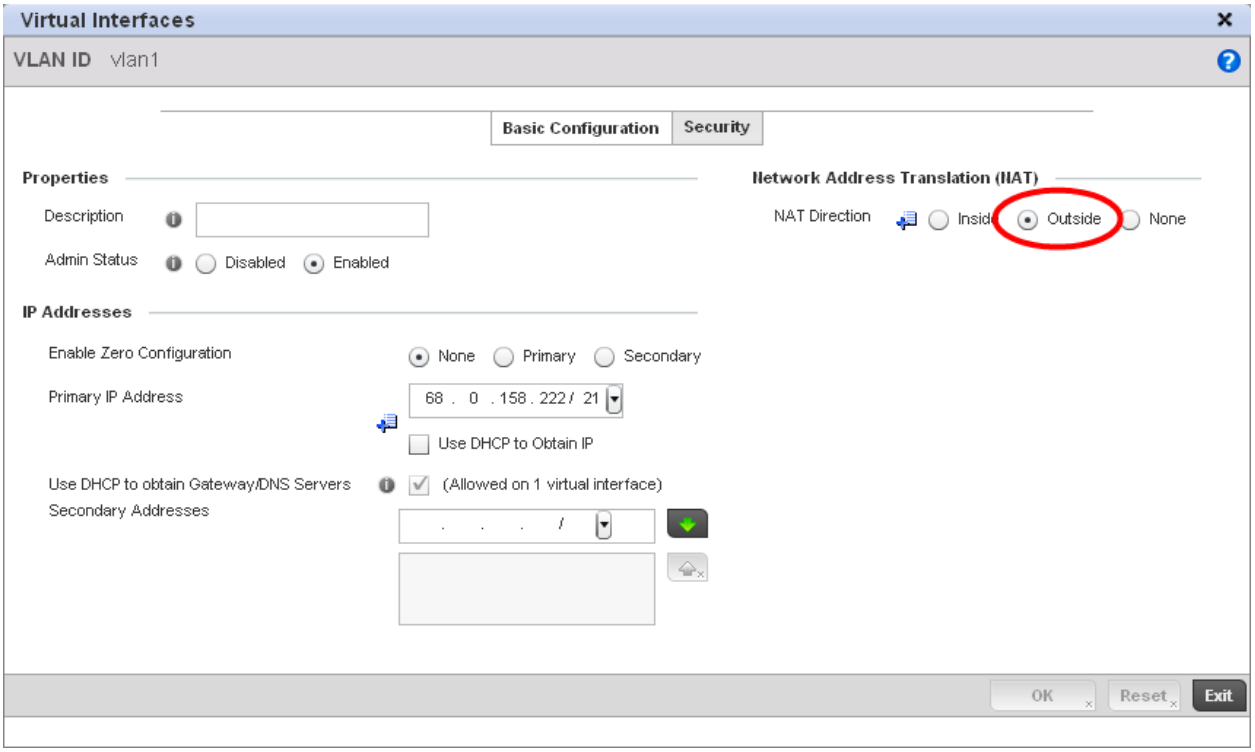
4.3.2.1 Apply to NAT Rules to AP7131

The following configurations will be applied as Device Overrides, as we only want them applied to this specific device. Navigate to "**Configuration > Devices > Device Overrides**" and edit the AP7131 in the device list (right-hand pane).

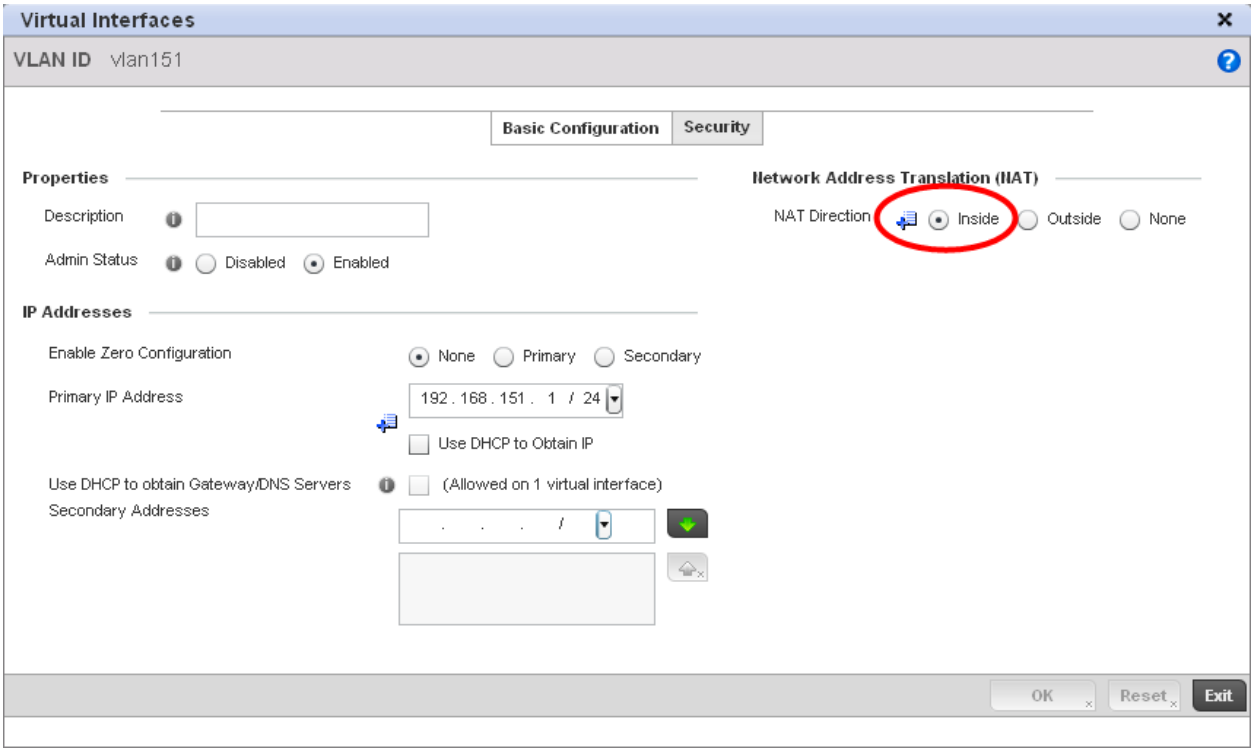
1) Edit interface VLAN1



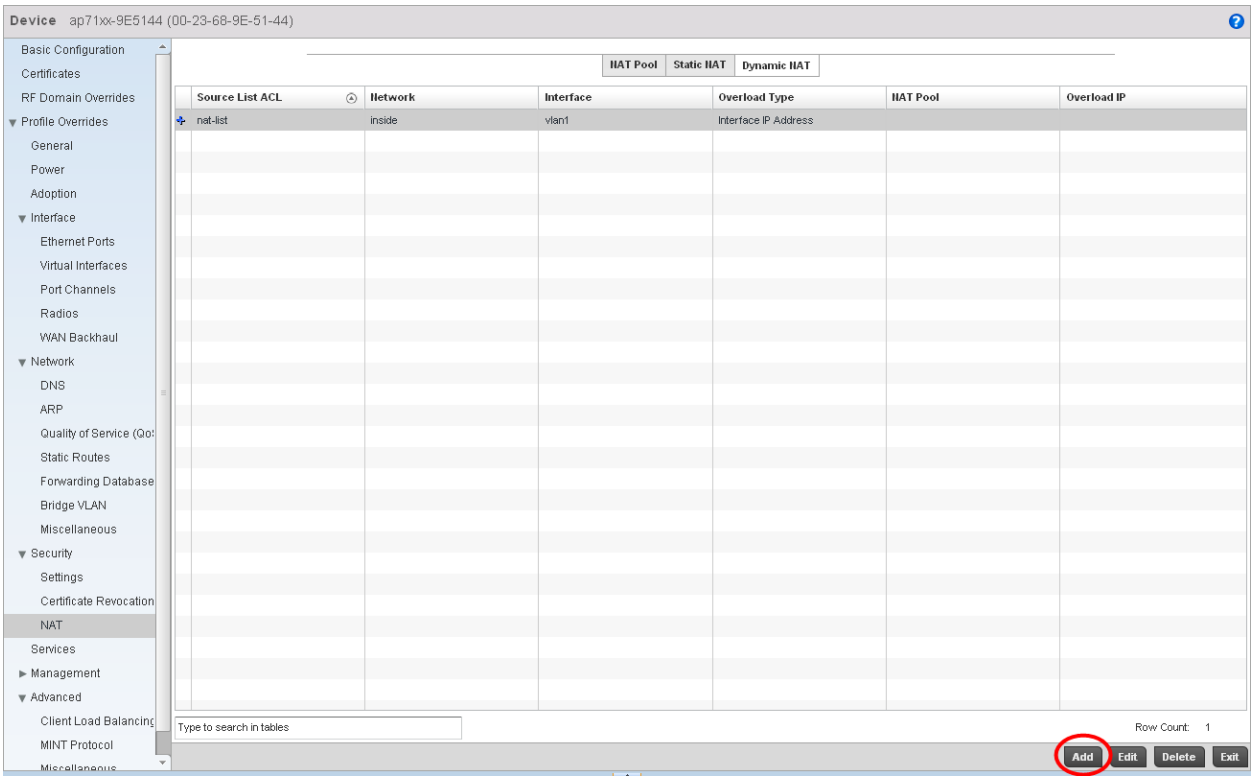
2) NAT Outside interface



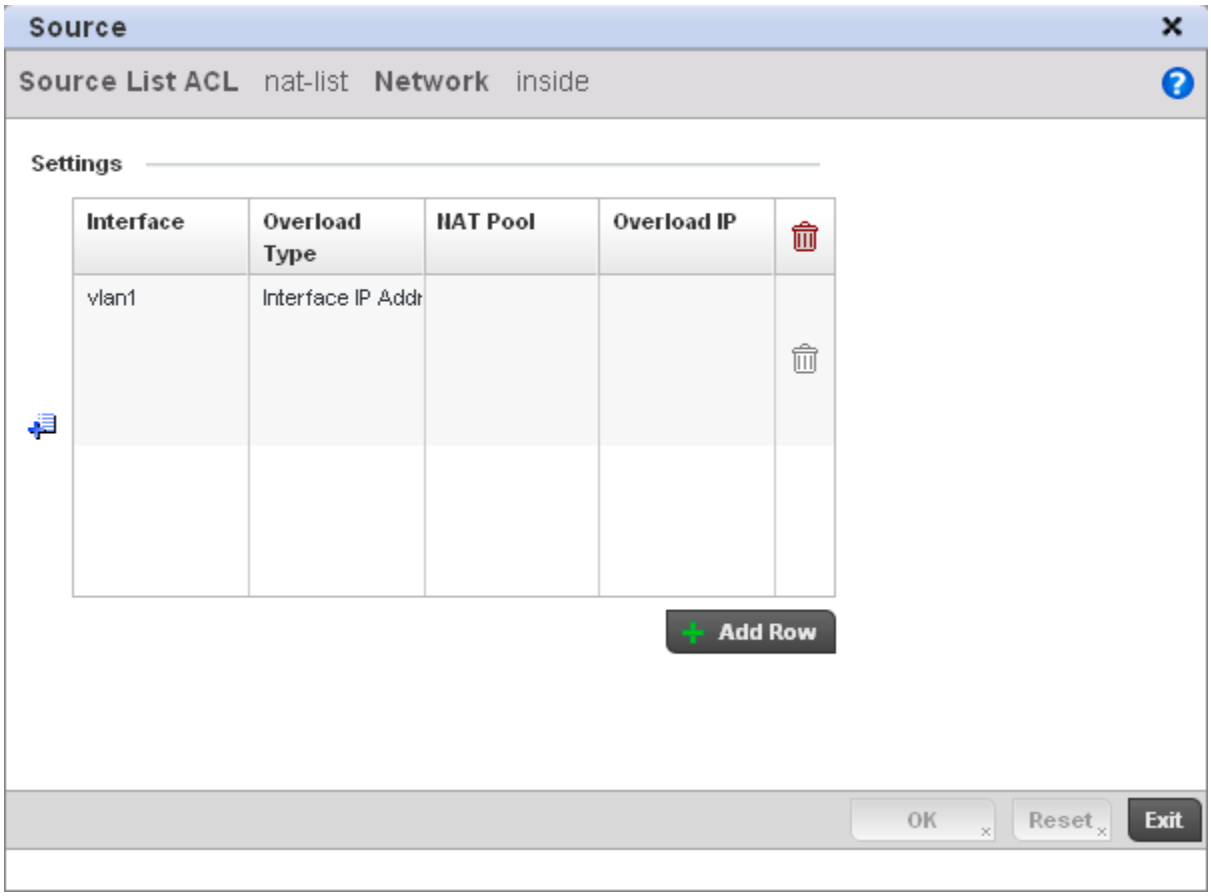
3) Make interface “VLAN151” NAT Inside

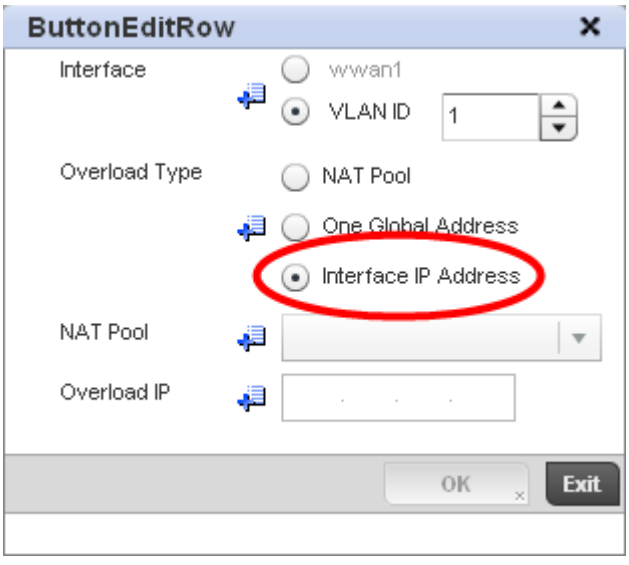


4) Navigate to “**Configuration > Devices > Device Overrides > Security > NAT**” and add overload statement



5) Add row and select AP7131's IP as the overload IP





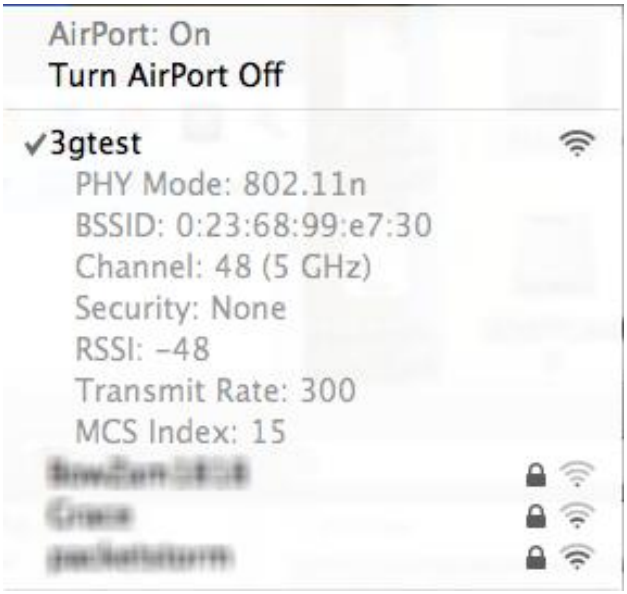
Remember to complete step 5 above for the “wwan1” interface as well.

One could establish a dedicated IP address to overload to or a pool of IP’s, it is the choice of the user.

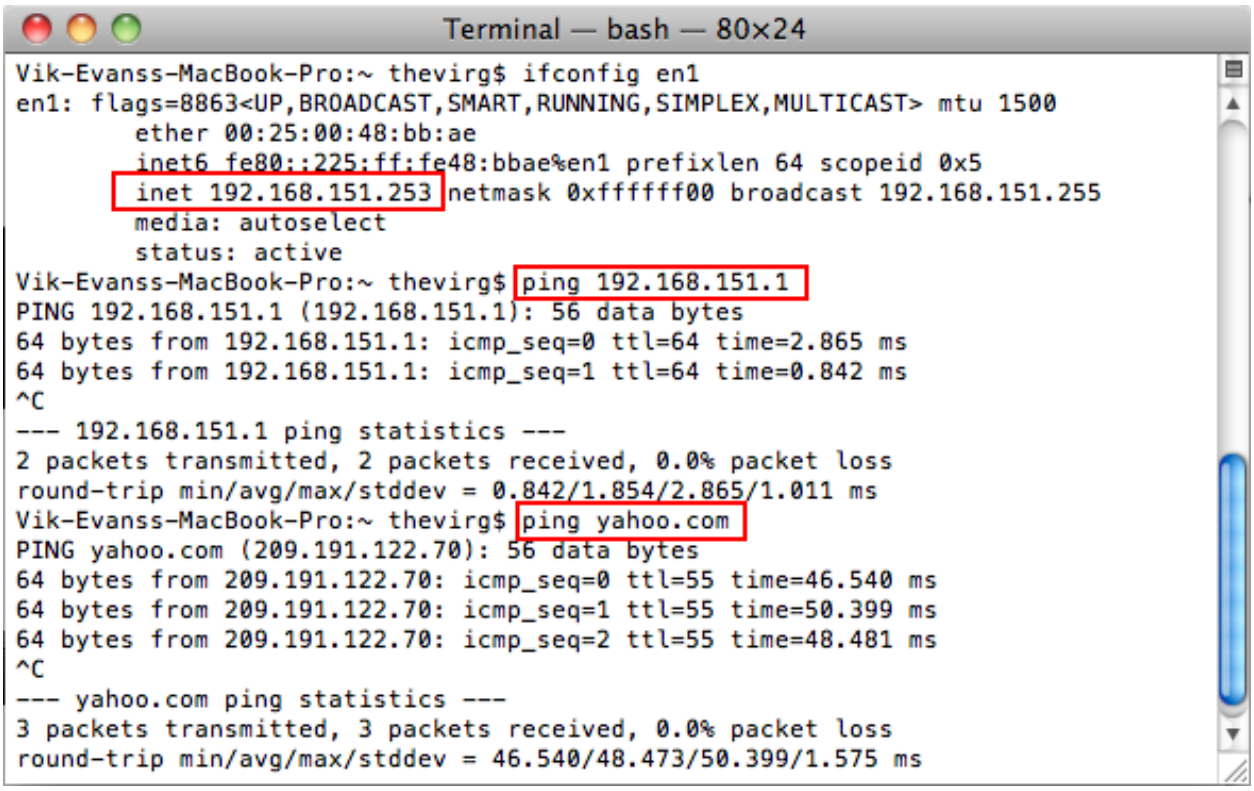
5. Testing:

Both the internal wired network and our WLAN in the example share VLAN 151. We will test connectivity of both our AP7131 router and a wireless client. Our test will consist of a client on our “3gtest” WLAN on vlan 151 pinging out to the Internet; in this case we will use “yahoo.com” as it is a website that will respond to pings.

1)	Connect to WLAN



2)	Ping Test / Pre-failover



3) Verify translations on AP7131

```
ap71xx#show ip nat translations verbose

PROTO ACTUAL SOURCE          ACTUAL DESTINATION     NATTED SOURCE
NATTED DESTINATION

-------------------------------------------------------------------------------

TCP   192.168.151.253:57324 74.125.235.2:443       68.0.158.222:56793
74.125.235.2:443

TCP   192.168.151.253:57167 199.47.216.146:80      68.0.158.222:64230
199.47.216.146:80

TCP   192.168.151.253:57386 208.89.13.133:80       68.0.158.222:35672
208.89.13.133:80

TCP   192.168.151.253:57323 74.125.235.2:443       68.0.158.222:44010
74.125.235.2:443

UDP   192.168.151.253:59241 192.168.150.55:8612    68.0.158.222:45065
192.168.150.55:8612

TCP   192.168.151.253:57381 23.11.88.100:80        68.0.158.222:58349
23.11.88.100:80

TCP   192.168.151.253:57307 74.125.235.16:80       68.0.158.222:41577
74.125.235.16:80
```

5.1 Failover Test

To test our failover, we will simply kill the connection between the AP7131's VLAN1 interface and the cable modem. This connection goes through a switch, so we will pull the cable modem Ethernet connection to the switch.

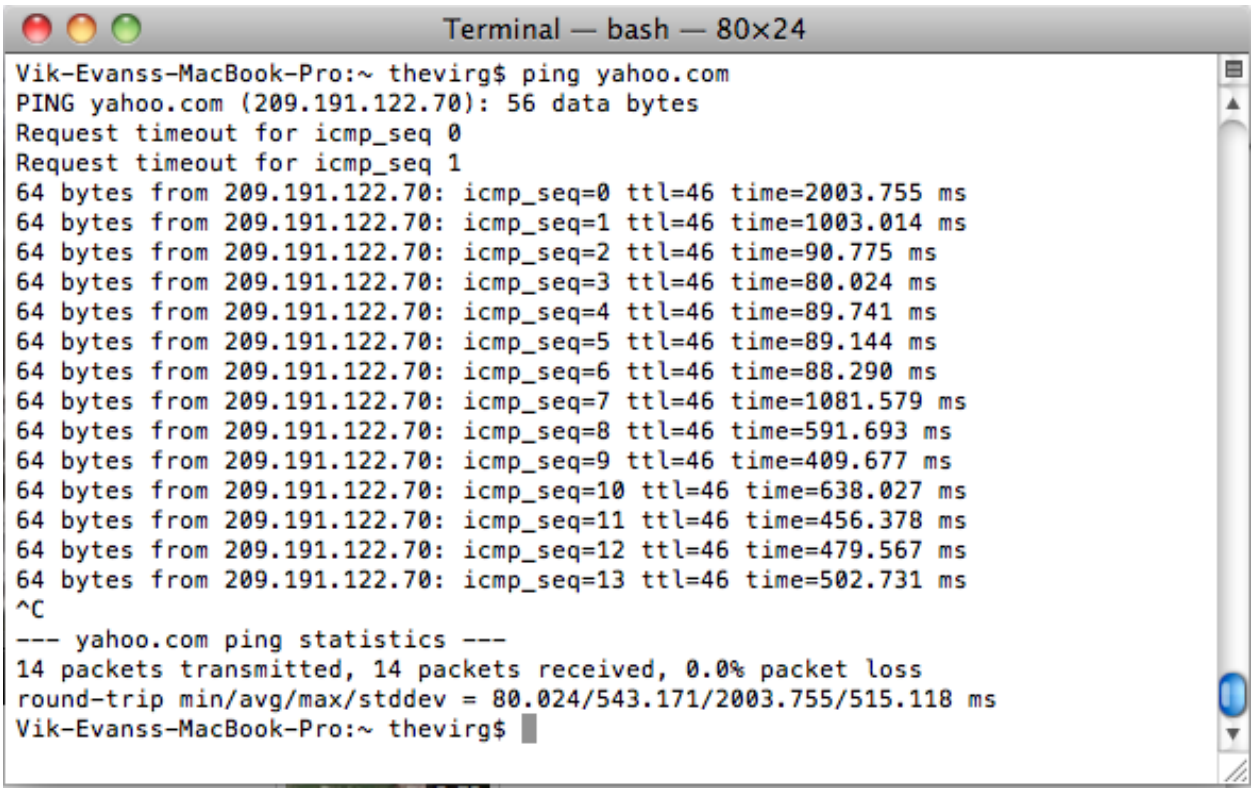
1) AP7131 Routing Table pre-failover

```
ap71xx#sho ip route
------------------------------------------------------------------------------
        DESTINATION               GATEWAY            FLAGS        INTERFACE
------------------------------------------------------------------------------
  192.168.151.0/24       direct                  C            vlan151
  10.64.64.64/32         direct                  C            ppp0
  68.0.158.0/21          direct                  C            vlan1
  default                68.0.152.1            CG           vlan1
------------------------------------------------------------------------------
Flags:  C - Connected G - Gateway
ap71xx
```

2) AP7131 Routing Table post-failover

```
ap71xx#sho ip route
------------------------------------------------------------------------------
        DESTINATION               GATEWAY           FLAGS         INTERFACE
------------------------------------------------------------------------------
  192.168.151.0/24          direct                C            vlan151
  10.64.64.64/32            direct                C            ppp0
  68.0.158.0/21             direct                C            vlan1
  default                   10.64.64.64           CG           ppp0
------------------------------------------------------------------------------
Flags:  C - Connected G - Gateway
```

3) Ping test / Post-failover



4) Verify NAT translations via WWAN1

```
ap71xx#sho ip nat translations verbose

PROTO ACTUAL SOURCE          ACTUAL DESTINATION    NATTED SOURCE
NATTED DESTINATION

-------------------------------------------------------------------------------

TCP   192.168.151.253:57655 107.20.249.111:443    10.64.64.64:58380
107.20.249.111:443

TCP   192.168.151.253:57649 174.129.211.231:443   10.64.64.64:38071
174.129.211.231:443

TCP   192.168.151.253:57643 199.47.216.146:80     10.64.64.64:47231
199.47.216.146:80

TCP   192.168.151.253:57644 74.125.113.125:443    10.64.64.64:56020
74.125.113.125:443

TCP   192.168.151.253:57646 174.129.218.106:443   10.64.64.64:46419
174.129.218.106:443

TCP   192.168.151.253:57648 199.47.216.174:443    10.64.64.64:52470
199.47.216.174:443

TCP   192.168.151.253:57650 199.47.216.174:443    10.64.64.64:59970
199.47.216.174:443

TCP   192.168.151.253:57659 74.125.73.103:443     10.64.64.64:39693
74.125.73.103:443
```

As seen in the ping times between the two tests, the 3G connection is much slower. However it does suffice as a backup connection for many installations. As well, it makes a perfectly functional primary method of connecting to the Internet for small branch locations. As long as the use is not too heavy (i.e. many users or bandwidth-demanding traffic types), a 3G connection works quite well for email, web browsing and of course VPN connectivity to a central location.

6. Troubleshooting / Configuration:

The main element to troubleshoot in this scenario is connectivity to the 3G provider. As mentioned before, you may see that your interface goes to an "Active" status, the router obtains the provider's DNS entries and yet the router will not ping anything out the "wwan1" interface. This is usually due to an issue with the provider APN (the cell your 3G card connects to) not registering your device properly. In this case, simply shutdown the wwan interface and then bring it up again – *don't forget a "commit" must be done after each of these two actions*.

Another scenario is when you run the command "**`show wwan status`**" and the state shows "connecting" without ever changing. There have been to reasons for seeing this:

- 3G credentials were typed in wrong (username / password)
- Unsupported 3G card – drivers may not be available in WiNG 5 for the installed card.

You can perform the following debug to watch the wwan interface activate and deactivate as connectivity to the wired default-gateway is lost and then re-established:

1) Debug NSM

```
ap71xx#logging monitor 7
ap71xx#debug nsm all
Sep 14 21:54:20 2011: NSM: WWANProcCheckCritResScriptStatus: The critical-resource 68.0.152.1 is not connected
Sep 14 21:54:20 2011: NSM: wwan_handle_event: WIRED_GW_DOWN
Sep 14 21:54:20 2011: NSM: state_transition_gw_down: state CONNECTION_UP event WIRED_GW_DOWN
Sep 14 21:54:20 2011: NSM: ifc address 20b0fa07 destiantion a404040
Sep 14 21:54:20 2011: NSM:  nsm_rib_add_ipv4: type=10 p=0.0.0.0 ifindex=8
Sep 14 21:54:20 2011: NSM:  nsm_rib_add_ipv4: gate=10.64.64.64 flags=1 metric=0
Sep 14 21:54:20 2011: NSM:  nsm_rib_add_ipv4: About to Add def route to RIB
Sep 14 21:54:20 2011: NSM: nsm_nexthop_ipv4_ifindex_add: rib=0x100fad20 gate=10.64.64.64 ifindex=8
Sep 14 21:54:20 2011: NSM: nsm_nexthop_add: rib=0x100fad20 nexthop=0x100faec8
Sep 14 21:54:20 2011: NSM: nsm_rib_add: rib=0x100fad20 p->prefix.u.prefix4=0.0.0.0 same=(nil)
```

```
Sep 14 21:54:20 2011: NSM: nsm_nexthop_active_update: rib=0x100fad20 active=1
nexthop=10.64.64.64

Sep 14 21:54:20 2011: NSM: nsm_nexthop_active_update: rib=0x100faef8 active=1
nexthop=10.64.64.64

Sep 14 21:54:20 2011: NSM: nsm_nexthop_active_update: rib=0x100fae40 active=1
nexthop=10.64.64.64

Sep 14 21:54:20 2011: NSM: nsm_nexthop_active_update: rib=0x100fad90 active=1
nexthop=10.64.64.64

Sep 14 21:54:20 2011: NSM: nsm_nexthop_active_update: rib=0x100fa5b0 active=1
nexthop=68.0.152.1

Sep 14 21:54:20 2011: NSM: nsm_rib_process: rn=0x100fa580 fib=0x100faef8
select=0x100faef8

Sep 14 21:54:20 2011: NSM:  nsm_rib_add_ipv4: Successfully Added def rt

Sep 14 21:54:20 2011: NSM: installed ppp0 route 10.64.64.64

Sep 14 21:54:20 2011: NSM: wwan_activate_wwan_gw: /bin/sh
/usr/scripts/failover start 10.64.64.64 &

Sep 14 21:54:20 2011: NSM: state_transition_gw_down: new state ACTIVE

..

..

Sep 14 21:54:50 2011: NSM: nsm_nexthop_active_update: rib=0x100fa5b0 active=1
nexthop=68.0.152.1

Sep 14 21:54:50 2011: NSM: nsm_rib_process: rn=0x100fa580 fib=0x100faef8
select=0x100faef8

Sep 14 21:54:50 2011: NSM: wwan_deactivate_wwan_gw: failover stop

Sep 14 21:54:50 2011: NSM: state_transition_gw_up: new state CONNECTION_UP

Sep 14 21:54:55 2011: NSM: RestartCheckCriticalWWANResource: Executing
/bin/sh /usr/scripts/check_a_critical_resource 68.0.152.1 wwan vlan1 &

Sep 14 21:54:55 2011: NSM: RestartCheckCriticalWWANResource: 1 critical
resource found

ap71xx-9E5144(config-device-00-23-68-9E-51-44)*#comSep 14 21:55:05 2011: NSM:
WWANProcCheckCritResScriptStatus: The critical-resource 68.0.152.1 is
connected

Sep 14 21:55:05 2011: NSM: wwan_handle_event: WIRED_GW_UP

Sep 14 21:55:05 2011: NSM: Ignored event: state CONNECTION_UP event
WIRED_GW_UP
```

6.1 Running-Config

```
ap7131-9E5144#show run
!
! Configuration of AP7131 version 5.2.0.0-057R
!
!
```

```
version 2.1
!
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all
TCP traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description
"permit DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-
description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP
multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description
"deny IP local broadcast"
 permit ip any any rule-precedence 100 rule-description "permit all IP
traffic"
!
ip access-list nat-list
 permit ip 192.168.151.0/24 any rule-precedence 10
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit
all IPv4 traffic"
 permit any any type arp rule-precedence 20 rule-description "permit
all ARP traffic"
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
igmp-snoop-policy default
 no igmp-snooping
 no querier
 unknown-multicast-fwd
!
!
mint-policy global-default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
wlan 3g-test
 ssid 3gtest
 vlan 151
 bridging-mode local
 encryption-type none
 authentication-type none
!
dhcp-server-policy 3g-dhcp
```

```
 dhcp-pool 3g-pool
  network 192.168.151.0/24
  address range 192.168.151.100 192.168.151.254
  default-router 192.168.151.1
  dns-server 4.2.2.2 172.16.7.167
!
!
management-policy default
 no http server
 https server
 ssh
 user admin password 1
79d69b7a103e47661ba2571b838d5e4b32aad1b19666856f467bab5da5e19153 role
superuser access all
 user operator password 1
466f1ecaa278bdfb71a03922b3105ce8d722e9143d2a57d350b296369b327008 role
monitor access all
 no snmp-server manager v2
 snmp-server community public ro
 snmp-server community private rw
 snmp-server user snmpoperator v3 encrypted des auth md5 0 operator
 snmp-server user snmptrap v3 encrypted des auth md5 0 motorola
 snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola
!
profile ap71xx default-ap71xx
 autoinstall configuration
 autoinstall firmware
 interface radio1
 interface radio2
 interface radio3
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface vlan1
  ip address dhcp
  ip address zeroconf secondary
  ip dhcp client request options all
 interface wwan1
 use firewall-policy default
 service pm sys-restart
!
rf-domain default
 country-code us
!
ap71xx 00-23-68-9E-51-44
 use profile default-ap71xx
```

```
 use rf-domain default
 hostname ap7131-9E5144
 ip default-gateway 68.0.152.1
 interface radio1
  shutdown
 interface radio2
  power smart
  wlan 3g-test bss 1 primary
 interface ge2
  switchport mode access
  switchport access vlan 151
 interface vlan1
  ip address 68.0.158.222/21
  ip nat outside
 interface vlan151
  ip address 192.168.151.1/24
  ip nat inside
 interface wwan1
  no shutdown
 use dhcp-server-policy 3g-dhcp
 ip dns-server-forward
 logging on
 no logging console
 logging buffered warnings
 ip nat inside source list nat-list interface vlan1 overload
 ip nat inside source list nat-list interface wwan1 overload
!
!
end
```

7. Reference Documentation:

Description	Location
Motorola Solutions WiNG 5 CLI Reference Guide	http://support.symbol.com


MOTOROLA