APPLICATION NOTE

CONFIGURING THE CX111 FOR J SERIES AND BRANCH SRX SERIES DEVICES

How to Configure the CX111 as a Primary or Backup 3G/4G LTE WAN Connection Option for Junos OS-Based Platforms

Table of Contents

Introduction

Due to their ubiquitous presence, the use of 3G/4G LTE wireless networks has become a common deployment option for both primary and backup connectivity. With the introduction of Juniper Networks® CX111 Cellular Broadband Data Bridge, Juniper offers a simple way to provide wireless connectivity as either a backup or primary connection for Juniper Networks J Series Services Routers and branch SRX Series Services Gateways products.

Scope

The purpose of this application note is to provide an overview that shows how to configure and deploy the CX111 as a primary or backup 3G/4G LTE WAN connectivity option for Juniper Networks SRX Series and J Series platforms.

Design Considerations

Supported Hardware

- Juniper Networks SRX Series Services Gateways (SRX100 Services Gateway, SRX200 Services Gateway, SRX550 and SRX650 Services Gateway)
- Juniper Networks J Series Services Routers
- CX111 with enterprise-grade LTE/EV-DO modem MC200LE-VZ, for Verizon Networks

Software Requirements

- Juniper Networks Junos OS release 11.4R5.5 or later
- CX111 firmware 2.1.0 or later
- Configuration examples are based on a factory default configuration

Card Compatibility

As of the date of this writing, about 50 different USB and ExpressCard modems have been certified to work with the CX111. The latest list of modems can be found here: www.juniper.net/techpubs/hardware/junos-cx/cx111/index.html.

Card Activation

Before cards can be used, they need to be programmed with the subscriber information required to access the service provider's network. This is normally referred to as the card activation process. When service is purchased, the carrier will request the card's ESN number, normally found printed on the wireless card. This number is then used for card identification by the different activation protocols.

Cards directly purchased from the wireless carrier can ship pre-activated, or sometimes they will ship with a companion software used to perform the initial activation. In either case, cards already activated do not have to be reactivated.

Optionally, the cards can be activated from the CX111. This requires users to log into the CX111's UI using a Web browser.

Description and Deployment Scenario

The CX111 ships with a default configuration that should accommodate most deployment scenarios. The deployment model assumes that the CX111 is connected to a DHCP-enabled interface.

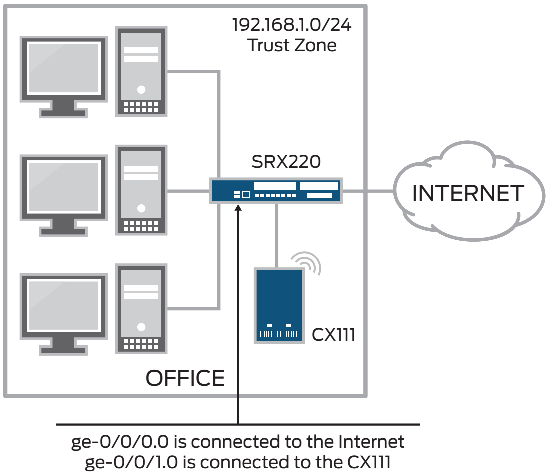

192.168.1.0/24
Trust Zone
SRX220
INTERNET
CX111
OFFICE
ge-0/0/0.0 is connected to the Internet
ge-0/0/1.0 is connected to the CX111

Figure 1: Deployment model

The CX111 will maintain the wireless modem (or modems, if more than one modem is used) in a disconnected state, triggering a new connection as soon as the SRX Series/J Series requests a new lease. The modem(s) will be disconnected as soon as the lease expires, and only reconnected when that gateway requires another new lease.

When using the 3G/4G LTE link as the primary connection, long lease times can be used, as generally there won't be a need to constantly connect and disconnect the line. On the other hand, if the CX111 is used to provide a backup connection, short lease times (in the order of a minute) are commonly used so that, when the primary link is active, the backup link can be disabled, triggering a disconnection, in the worse case, after a lease time.

The CX111 assigns the address received from the wireless service provider to the gateway (normally a public address). For obvious reasons, only a single device can be connected to the CX111 at any given time, or else multiple devices will contend for the only address passed to the CX111. The CX111 works in "pass through" mode, simply relaying all traffic from the wireless network to the DHCP client.

Management Interface

The CX111 provides a web-based management interface, and it can be accessed even when 3G/4G LTE modems are not used. Since "pass through" mode is used instead of a routed connection bridge that doesn't do Network Address Translation (NAT), the management interface cannot be accessed through the normal data channel. When the modem is not active or not inserted, a 192.168.30.x/24 network address is provided and 192.168.30.1 becomes the temporary management address for the CX111

The management interface is still accessible through the Ethernet port, but VLAN tagging is used to separate management from data traffic using the following parameters.

Table 1: Management Network

Card Model	Wireless Technology
Management subnet	192.168.0.0/24
Management address	192.168.0.1
VLAN ID	3900

Power over Ethernet

When available, Power over Ethernet (PoE) can be used to power the CX111. In the event that the CX111 is connected through a switch or a gateway that does not support PoE, an external power supply can be used (provided with the basic install kit).

When PoE is used, the device will require about 3.5 watts of power per modem connected, so plan your power budget accordingly.

Dial Modes

The CX111 can be configured in two modes: "always on" or "dial on-demand." In the "always on" mode, the CX111 connects to the 3G/4G LTE network after booting. The connection is always maintained, as long as there are no network or connectivity problems.

In "dial on-demand" mode, the CX111 only initiates a connection when it receives traffic from the interface connecting the CX111 and gateway. In particular, DHCP request messages will trigger a connection. Similarly, the connection will be dropped after a configurable inactivity timeout.

Regardless of the mode, the CX111 can accept multiple cards simultaneously. In the event of a failure or inability to connect, the remaining card(s) will be used. The connection priority is user configurable through the CX111's management interface.

The default mode at shipping is 'dial on-demand' and set at 20 minutes idle timeout. Most carriers prefer the modem to disconnect if there is no interesting traffic. After the modem times out, the DHCP requests from the SRX Series device will result in a 192.168.30.x/24 response from the CX111. If interesting traffic is observed by the CX111, the modem re-dials. Modem connection takes about 15 to 20 seconds generally. After that, the next DHCP request from the SRX Series device will fetch the actual 3G/4G LTE IP address and Internet connection is re-established.

Deployment Scenarios

In the following section, we will discuss several common deployment scenarios and provide the associated configurations.

CX111 Used for Primary Connectivity

This first scenario shows the gateway configuration when the 3G/4G LTE network is used as the primary WAN link. This can be achieved by simply connecting the CX111 to any interface in the untrust zone. On the SRX Series device, this is ge-0/0/0 when using the default configuration.

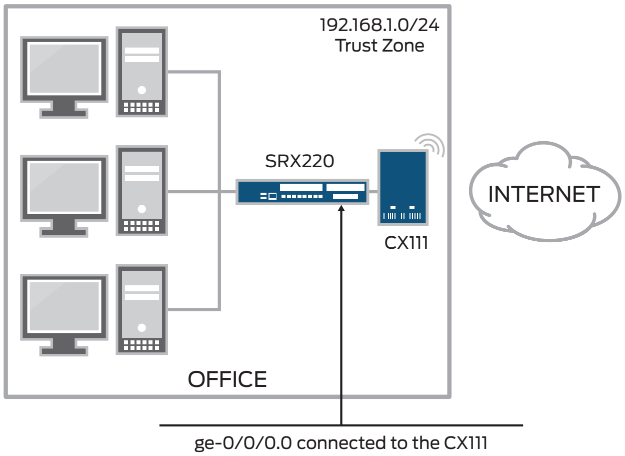


Figure 2: 3G/4G LTE network as the primary link

The relevant sections of the default configuration are shown here, for completeness.

```
set system services dhcp pool 192.168.1.0/24 address-range low 192.168.1.2
set system services dhcp pool 192.168.1.0/24 address-range high 192.168.1.254
set system services dhcp propagate-settings ge-0/0/0.0
set interfaces ge-0/0/0 unit 0 family inet dhcp
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/6 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/7 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces vlan unit 0 family inet address 192.168.1.1/24
set security nat source rule-set trust-to-untrust from zone trust
set security nat source rule-set trust-to-untrust to zone untrust
set security nat source rule-set trust-to-untrust rule source-nat-rule match
source-address 0.0.0.0/0
set security nat source rule-set trust-to-untrust rule source-nat-rule then
source-nat interface
set security policies from-zone trust to-zone untrust policy trust-to-untrust
match source-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust
match destination-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust
match application any
set system services dhcp router 192.168.1.1
set security policies from-zone trust to-zone untrust policy trust-to-untrust
then permit
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces vlan.0
set security zones security-zone untrust screen untrust-screen
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-
traffic system-services dhcp
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-
traffic system-services tftp
set poe interface all
set vlans vlan-trust vlan-id 3
set vlans vlan-trust l3-interface vlan.0
```

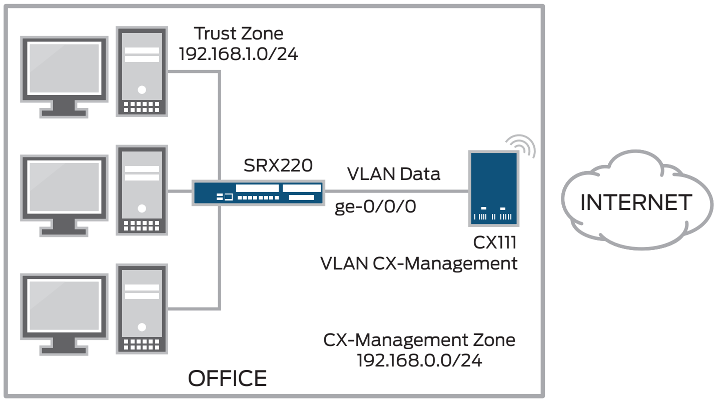
Enabling PoE

On SRX Series devices, it is possible to use PoE to power the CX111. The default configuration has PoE enabled on every PoE-capable interface, so users only have to connect the CX111 to a PoE-capable port. Enabling PoE only requires the addition of the following configuration.

```
/* The priority is optional but it will make sure that, if two many devices are
being powered, the bridge will be given a high priority and will not be powered
off */
set poe interface ge-0/0/0 priority high
```

Management Access

A VLAN-tagged logical interface can be used to provide access to the CX111's management console. NAT can also be used to facilitate access from any device behind the gateway, eliminating the need for complex routing (as all traffic to the CX111's management interface will be translated as if it originated from the management subnet).



Interface ge-0/0/0

VLAN Data
No tagging used for data traffic DHCP assigned address (relayed from the 3G/4G LTE network)

VLAN CX-Management
VLAN Tag 3900

Figure 3: Management access

```
/* The vlan.2 interface is the L3 interface of the Data VLAN, connecting to the
Bridge */
set system services dhcp propagate-settings vlan.2

/* Interface ge-0/0/0 has 2 VLANS configured, Data and CX-Management */
delete interfaces ge-0/0/0 unit 0
set interfaces ge-0/0/0 description “Connection to CX111”
set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members Data
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members CX-
Management
set interfaces ge-0/0/0 unit 0 family ethernet-switching native-vlan-id Data

/* vlan.2 connects to the bridge (untagged) */
set interfaces vlan unit 2 family inet dhcp

/* vlan.3900 connects to the bridge’s management subnet */
set interfaces vlan unit 3900 family inet address 192.168.0.2/24

/* VLANs */
set vlans Data vlan-id 2
set vlans Data l3-interface vlan.2
set vlans CX-Management vlan-id 3900
set vlans CX-Management l3-interface vlan.3900

/* NAT rule used for CX-Management access to the CX111*/
set security nat source rule-set trust-to-CX-Management from zone trust
set security nat source rule-set trust-to-CX-Management to zone CX-Management
set security nat source rule-set trust-to-CX-Management rule nat-to-CX111 match
source-address 0.0.0.0/0
set security nat source rule-set trust-to-CX-Management rule nat-to-CX111 match
destination-address 0.0.0.0/0
set security nat source rule-set trust-to-CX-Management rule nat-to-CX111 then
source-nat interface

/* Security policies and zones */
delete security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone untrust interfaces vlan.2 host-inbound-traffic
system-services dhcp
set security zones security-zone CX-Management interfaces vlan.3900
set security policies from-zone trust to-zone CX-Management policy CX111-
management-access match source-address any
set security policies from-zone trust to-zone CX-Management policy CX111-
management-access match destination-address any
set security policies from-zone trust to-zone CX-Management policy CX111-
management-access match application junos-http
set security policies from-zone trust to-zone CX-Management policy CX111-
management-access match application junos-ping
set security policies from-zone trust to-zone CX-Management policy CX111-
management-access then permit

/*Complete Configuration*/
set system root-authentication encrypted-password “$1$KMAqVDtM$wDFlcmieLQtxsTg89M
QL.1”
set system name-server 208.67.222.222
set system name-server 208.67.220.220
set system services ssh
set system services telnet
set system services xnm-clear-text
set system services web-management http interface vlan.0
set system services web-management https system-generated-certificate
set system services web-management https interface vlan.0
set system services dhcp router 192.168.1.1
set system services dhcp pool 192.168.1.0/24 address-range low 192.168.1.2
set system services dhcp pool 192.168.1.0/24 address-range high 192.168.1.254
set system services dhcp propagate-settings vlan.2
set system syslog archive size 100k
set system syslog archive files 3
set system syslog user * any emergency
set system syslog file messages any critical
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands error
set system max-configurations-on-flash 5
set system max-configuration-rollbacks 5
set system license autoupdate url https://ae1.juniper.net/junos/key_retrieval
set interfaces ge-0/0/0 description “Connection to CX111”
set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members Data
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members CX-
Management
set interfaces ge-0/0/0 unit 0 family ethernet-switching native-vlan-id Data
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/6 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces ge-0/0/7 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces vlan unit 0 family inet address 192.168.1.1/24
set interfaces vlan unit 2 family inet dhcp
set interfaces vlan unit 3900 family inet address 192.168.0.2/24
set protocols stp
set security screen ids-option untrust-screen icmp ping-death
set security screen ids-option untrust-screen ip source-route-option
set security screen ids-option untrust-screen ip tear-drop
set security screen ids-option untrust-screen tcp syn-flood alarm-threshold 1024
set security screen ids-option untrust-screen tcp syn-flood attack-threshold 200
set security screen ids-option untrust-screen tcp syn-flood source-threshold 1024
set security screen ids-option untrust-screen tcp syn-flood destination-threshold
2048
set security screen ids-option untrust-screen tcp syn-flood timeout 20
set security screen ids-option untrust-screen tcp land
set security nat source rule-set trust-to-untrust from zone trust
set security nat source rule-set trust-to-untrust to zone untrust
set security nat source rule-set trust-to-untrust rule source-nat-rule match
source-address 0.0.0.0/0
set security nat source rule-set trust-to-untrust rule source-nat-rule then
source-nat interface
set security nat source rule-set trust-to-CX-Management from zone trust
set security nat source rule-set trust-to-CX-Management to zone CX-Management
set security nat source rule-set trust-to-CX-Management rule nat-to-CX111 match
source-address 0.0.0.0/0
set security nat source rule-set trust-to-CX-Management rule nat-to-CX111 match
```

```
destination-address 0.0.0.0/0
set security nat source rule-set trust-to-CX-Management rule nat-to-CX111 then
source-nat interface
set security policies from-zone trust to-zone untrust policy trust-to-untrust
match source-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust
match destination-address any
set security policies from-zone trust to-zone untrust policy trust-to-untrust
match application any
set security policies from-zone trust to-zone untrust policy trust-to-untrust
then permit
set security policies from-zone trust to-zone CX-Management policy CX111-
management-access match source-address any
set security policies from-zone trust to-zone CX-Management policy CX111-
management-access match destination-address any
set security policies from-zone trust to-zone CX-Management policy CX111-
management-access match application junos-http
set security policies from-zone trust to-zone CX-Management policy CX111-
management-access match application junos-ping
set security policies from-zone trust to-zone CX-Management policy CX111-
management-access then permit
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces vlan.0
set security zones security-zone untrust screen untrust-screen
set security zones security-zone untrust interfaces vlan.2 host-inbound-traffic
system-services dhcp
set security zones security-zone CX-Management interfaces vlan.3900
set poe interface all
set vlans CX-Management vlan-id 3900
set vlans CX-Management l3-interface vlan.3900
set vlans Data vlan-id 2
set vlans Data l3-interface vlan.2
set vlans vlan-trust vlan-id 3
set vlans vlan-trust l3-interface vlan.0
```

Additional Management for the CX111

Using JUNOS CLI, the administrator would be able to pull necessary information from the CX111. These include, but not limited to: modem signal strength, current status, firmware upgrade, syslog information etc.

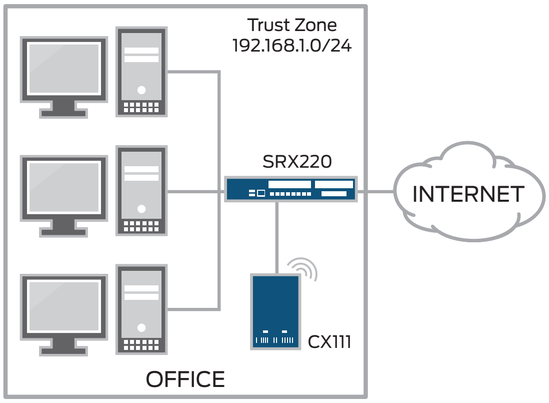
```
/* Name and IP address of the Adapter */
set services wireless-wan adapter CX111 ip-address 192.168.0.1

/* Type of Adapter */
set services wireless-wan adapter CX111 adapter-type cx-bridge

/* Description of modems of each Adapter */
set services wireless-wan adapter CX111 modem usb1 description MC200LE-VZ


/*After commiting the configuration you can verify the CX111*/
root> show wireless-wan adapter
Adapter information
Adapter-name         IP-address
CX111                    192.168.0.1
```

```
root> show wireless-wan adapter CX111
Adapter information
Adapter name : CX111
Adapter firmware version             : “2.1.0”
Number of cellular modems connected  : 1
root> show wireless-wan adapter CX111 detail
Adapter name : CX111
Adapter firmware version             : “2.1.0”
Number of cellular modems connected  : 1
Cellular modem index: 1
Modem information: “MC200LE”
Modem port: “USB1”
Modem signal strength: -64 dBm
root> show wireless-wan adapter CX111 modem usb1
Modem information: “MC200LE”
Modem port: “USB1”
Modem signal strength: -64 dBm
Modem status: established
Modem ecio: 0 dBm
Modem serial number: “990000560131577”
Modem firmware version: “33, SWI9600M_01.00.09.03AP R2492 CARMD-EN-10526
2011/07/01 19:3”
Connection status: Up
IP address:  10.171.122.229
Sent bytes: 1804
Sent packets: 21
Outbound packet discards: 0
Outbound packet errors: 0
Received bytes: 2420
Received packets: 19
Inbound packet discards: 0
Inbound packet errors: 0
```

CX111 Used for Backup

In this example, the CX111 will only be used when the primary interface is down. This is shown mostly for illustrative purposes, as only a failure in the primary interface will trigger a failover.

Also, this example can only be used with the CX111 operating in “always on” mode, as once connected, the DHCP requests from the SRX Series will keep the connection up. (Increasing the lease times is not a good idea, since there are no guarantees that, after a new connection, the modem will be assigned the same IP. Thus, this situation requires short lease times to make sure that the gateway is notified of the address change).



ge-0/0/0.0 is connected to the Internet
ge-0/0/1.0 is connected to the CX111

Figure 4: Interface backup

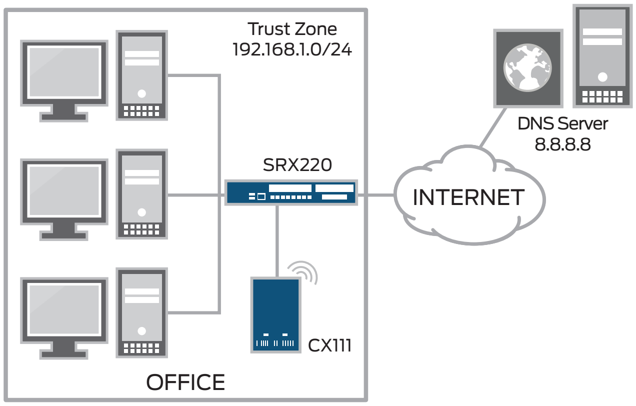
Please make sure that your unit has a default configuration.

```
/* Interface Configuration */
delete interfaces ge-0/0/1 unit 0
delete interfaces ge-0/0/0 unit 0

/* Main Internet Link */
set interfaces ge-0/0/0 unit 0 family inet address 10.50.1.100/24

/* CX111 backup link */
set interfaces ge-0/0/1 unit 0 family inet dhcp
set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-
traffic system-services dhcp

/* Default route points to the primary link and it takes precedence over the DHCP
assigned default */
set routing-options static route 0.0.0.0/0 next-hop 10.50.1.1
```

Detecting Network Failures Using IP Monitoring

Although quite simple, our previous example presents a major drawback—the primary interface's status is not always a good indicator of the network's connectivity. In some instances, when layer 2 protocols are not able to detect end-to-end failures, or when multiple network hops separate the Juniper Networks SRX220 Services Gateway from remote resources, other means to trigger a failover are desired.

This example shows how to configure IP Monitoring to check the reachability of an IP address and take action if the IP address is not reachable.



ge-0/0/0.0 is connected to the Internet
ge-0/0/1.0 is connected to the CX111

Figure 5: IP Monitoring

Using IP Monitoring we will use RPM probes to monitor the DNS Server 8.8.8.8. When the DNS Server is down we will disable interface ge-0/0/0.0 so that the default gateway of interface ge-0/0/1.0 will be active and all the traffic will continue thru the CX111.

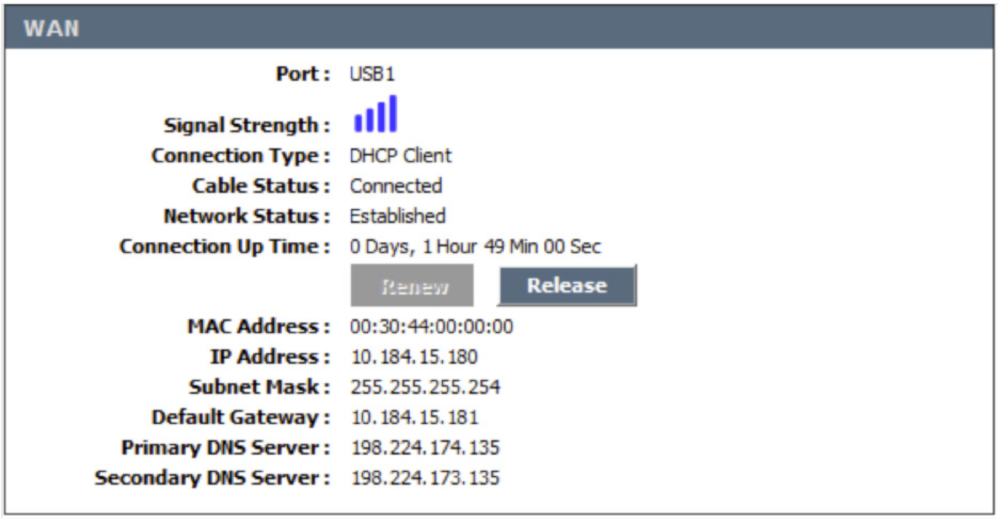
```
/* Configure the RPM probe */
set services rpm probe Probe-DNS-Server test dnssvr target address 8.8.8.8
set services rpm probe Probe-DNS-Server test dnssvr probe-count 5
set services rpm probe Probe-DNS-Server test dnssvr probe-interval 5
set services rpm probe Probe-DNS-Server test dnssvr test-interval 3
set services rpm probe Probe-DNS-Server test dnssvr thresholds successive-loss 5
set services rpm probe Probe-DNS-Server test dnssvr destination-interface ge-
0/0/0.0
```

```
set services rpm probe Probe-DNS-Server test dnssvr hardware-timestamp
set services rpm probe Probe-DNS-Server test dnssvr next-hop 10.50.1.1

/* Configure IP Monitoring */
set services ip-monitoring policy test-remote-server match rpm-probe Probe-DNS-
Server
set services ip-monitoring policy test-remote-server then interface ge-0/0/0
disable

/* Monitoring rpm and IP Monitoring before failure */
root# run show services rpm probe-results
    Owner: Probe-DNS-Server, Test: dnssvr
    Target address: 8.8.8.8, Probe type: icmp-ping
    Destination interface name: ge-0/0/0.0
    Test size: 5 probe
    Probe results
      Response received, Tue Dec 18 07:51:12 2012, Client hardware timestamps
      Rtt: 76714 usec
      Results over current test
       Probes sent: 1, Probes received: 1, Loss percentage: 0
       Measurement: Round trip time
       Samples: 1, Minimum: 76714 usec, Maximum: 76714 usec, Average: 76714 usec,
Peak to peak: 0 usec, Stddev: 0 usec, Sum: 76714 usec
    Results over last test:
       Probes sent: 5, Probes received: 5, Loss percentage: 0
       Test completed on Tue Dec 18 07:51:09 2012
       Measurement: Round trip time
       Samples: 5, Minimum: 76713 usec, Maximum: 77720 usec, Average: 77173 usec,
Peak to peak: 1007 usec, Stddev: 325 usec, Sum: 385863 usec
   Results over all tests:
       Probes sent: 26, Probes received: 26, Loss percentage: 0
       Measurement: Round trip time
       Samples: 26, Minimum: 76515 usec, Maximum: 77720 usec, Average: 76817
usec, Peak to peak: 1205 usec, Stddev: 269 usec, Sum: 1997233usec

root# run show services ip-monitoring status
Policy - test-remote-server (Status: PASS)
     RPM Probes:
           Probe name                Test Name     ddress            Status
           ----------------------     --------------- ---------------- ---------
           Probe-DNS-Server    dnssvr          8.8.8.8             PASS
  Interface-Action:
       interface         policy action   admin state     action status
       ----------------- ---------------   -----------           ---------------
--
      ge-0/0/0          Disable            UP                     NO-ACTION


root# run show route
inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
0.0.0.0/0          *[Static/5] 00:00:10
                    > to 10.50.1.1 via ge-0/0/0.0
                          [Access-internal/12] 00:00:24
                     > to 10.186.19.180 via ge-0/0/1.0
10.50.1.100/32     *[Local/0] 00:28:47
                      Reject
10.186.19.180/31   *[Direct/0] 00:26:23
```

```
                    > via ge-0/0/1.0
10.186.19.181/32   *[Local/0] 00:26:23
                      Local via ge-0/0/1.0
192.168.1.0/24     *[Direct/0] 00:31:32
                    > via vlan.1
192.168.1.1/32     *[Local/0] 00:31:45

/* Monitoring rpm and IP Monitoring after failure */
root# run show services rpm probe-results
    Owner: Probe-DNS-Server, Test: dnssvr
    Target address: 8.8.8.8, Probe type: icmp-ping
    Destination interface name: ge-0/0/0.0
    Test size: 5 probes
    Probe results:
      Request timed out, Tue Dec 18 08:13:32 2012
      Results over current test:
      Probes sent: 3, Probes received: 0, Loss percentage: 100
    Results over last test:
      Probes sent: 5, Probes received: 0, Loss percentage: 100
      Results over all tests:
      Probes sent: 298, Probes received: 221, Loss percentage: 25
      Measurement: Round trip time
         Samples: 221, Minimum: 76505 usec, Maximum: 79577 usec, Average: 76927
usec, Peak to peak: 3072 usec, Stddev: 385 usec, Sum: 17000802 usec

root# run show services ip-monitoring status
Policy - test-remote-server (Status: PASS)
     RPM Probes:
           Probe name               Test Name     ddress            Status
           ----------------------     --------------- ---------------- ---------
           Probe-DNS-Server    dnssvr          8.8.8.8             FAIL
  Interface-Action:
       interface         policy action   admin state        action status
       ----------------- ---------------   -----------           ---------------
--
      ge-0/0/0          Disable           DOWN              FAILOVER

root# run show route
inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
0.0.0.0/0          *[Access-internal/12] 00:00:24
                     > to 10.186.19.180 via ge-0/0/1.0
10.50.1.100/32     *[Local/0] 00:28:47
                      Reject
10.186.19.180/31   *[Direct/0] 00:26:23
                    > via ge-0/0/1.0
10.186.19.181/32   *[Local/0] 00:26:23
                      Local via ge-0/0/1.0
192.168.1.0/24     *[Direct/0] 00:31:32
                    > via vlan.1
192.168.1.1/32     *[Local/0] 00:31:45
```

Monitoring

The 3G/4G LTE signal strength and connection status can be monitored from the CX111's management interface, which is found under status -> device info tab.



WAN

Port : USB1

Signal Strength :

Connection Type : DHCP Client

Cable Status : Connected

Network Status : Established

Connection Up Time : 0 Days, 1 Hour 49 Min 00 Sec

MAC Address : 00:30:44:00:00:00

IP Address : 10.184.15.180

Subnet Mask : 255.255.255.254

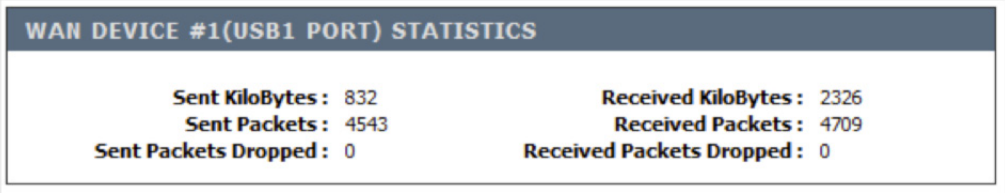
Default Gateway : 10.184.15.181

Primary DNS Server : 198.224.174.135

Secondary DNS Server : 198.224.173.135

Figure 6: Modem status

Traffic statistics can be found under the Status->Statistics page.



WAN DEVICE #1(USB1 PORT) STATISTICS

Sent KiloBytes : 832

Sent Packets : 4543

Sent Packets Dropped : 0

Received KiloBytes : 2326

Received Packets : 4709

Received Packets Dropped : 0

Figure 7: Modem statistics

Summary

As more and more wireless carriers expand their coverage and upgrade their networks to offer 3G/4G LTE wireless data services, enterprises worldwide can look to use 3G/4G LTE as a backup connectivity solution for many deployments and in some cases, even use 3G/4G LTE wireless as primary data access.

Juniper Networks SRX Series Services Gateways provide world-class security and routing features, and now combined with the flexible and optimized CX111 Cellular Broadband Data Bridge, the SRX Series can offer additional WAN connectivity solutions to customers for increased WAN uptime coupled with reduced operational expense. The CX111 is simple to configure and deploy, which can be installed easily in existing and new SRX Series and J Series deployments.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: 31.0.207.125.700
Fax: 31.0.207.125.701

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

3500184-002-EN Jan 2013 ♻ Printed on recycled paper