6AOSSG0011-42A
April 2014

ADTRAN

Interoperability Guide

Integrating ADTRAN Routers with the CradlePoint CBA750B Mobile Broadband Adapter

This interoperability guide provides instructions for integrating ADTRAN NetVanta 3448 and 4430 routers with the CradlePoint Cellular Broadband Adapter (CBA750B) to provide a 3G/4G Wide Area Network (WAN) backup solution. It provides an overview and instructions for the integration. Also, this guide provides a list of equipment used for testing the integration, the features supported by the integration, and the verified functionality of the integration.

This guide consists of the following sections:

Application Overview

This solution guide provides interoperability support for integrating ADTRAN routers with the CradlePoint CBA750B cellular broadband adapter. This integration uses the CradlePoint CBA750B to provide a 3G/4G WAN backup solution for ADTRAN routers. In addition, the CradlePoint CBA750B can be used as a temporary or mobile primary WAN connection. For example, it can be used while waiting for a primary WAN service to be installed or in mobile applications, such as kiosks.

CradlePoint CBA750B

The CradlePoint CBA750B is a router with an integral USB interface for connecting to a wireless modem. A companion 3G/4G wireless modem module (CradlePoint MC200LE) connects to the USB interface. The CradlePoint ARC Series combines these two products in a bundle solution.

The CradlePoint CBA750B provides a single Ethernet interface for connecting to the LAN. The CBA750B can operate in two modes either **Router** or **IP Passthrough**. When in **IP Passthrough** mode, it connects the attached wireless modem to the LAN interface without performing routing functions. IP Passthrough mode still enables access to the CradlePoint CBA750B management web graphic user interface (GUI) for administration.

Figure 1. CradlePoint CBA750B with attached MC200LE Wireless Modem

Network Topology

Figure 2 shows a network deployment for an ADTRAN router with the CradlePoint CBA750B providing wireless WAN backup. The ADTRAN router Ethernet interface connects to the LAN port on the CBA750B. In this example, the primary WAN uses a static public IP address. The secondary wireless WAN uses DHCP to learn the gateway IP address from the service provider (Verizon). This network topology was used to verify interoperability.

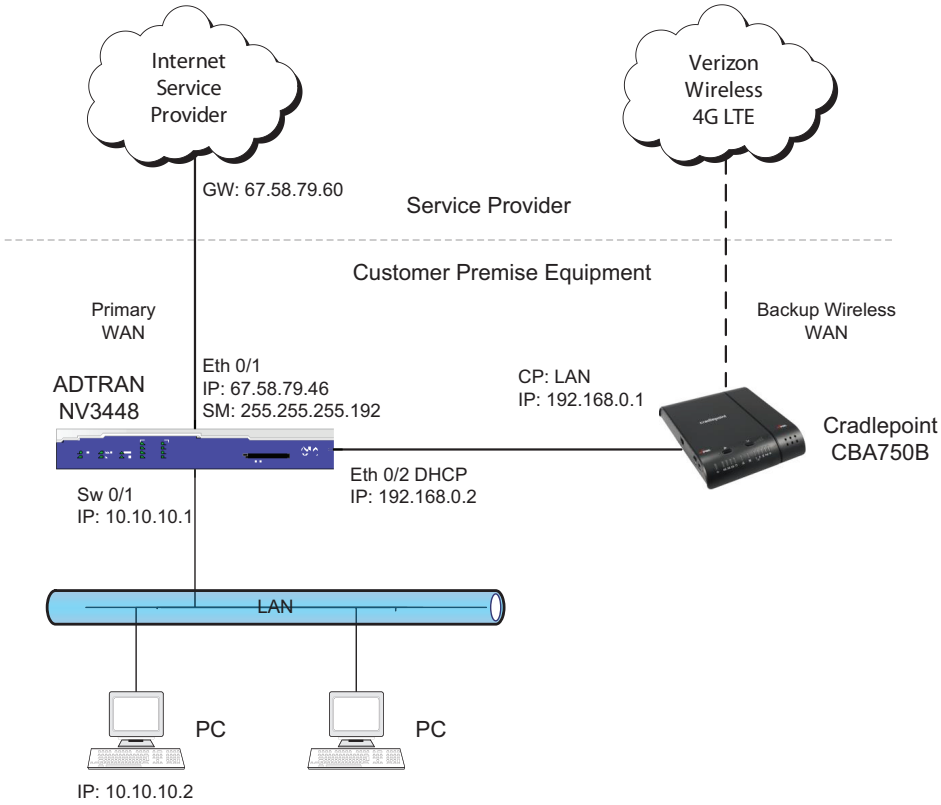


Figure 2. Network Topology Used for Interoperability Verification

Hardware and Software Requirements and Limitations

The CradlePoint CBA750B can be used to provide wireless WAN failover with ADTRAN NetVanta 3448 and 4430 routers. The test equipment, testing parameters, and associated caveats are described in the following sections.

Equipment and Versions

The following sections describe the equipment and versions, features and caveats, and configurations used during interoperability testing:

Table 1. Equipment Verified

Equipment	Version
CradlePoint CBA750B	V4.4.0
CradlePoint MC200LE-VZ (Verizon 4G LTE modem)	33, SWI9600M_03.05.10.06ap r5595 carmden-10527
ADTRAN NetVanta 3448	R10.9.1
ADTRAN NetVanta 4430	R10.9.1
ADTRAN Single Port PoE Power Supply (1200809E1), AULT PW130 48V 420 MA	n/a

Supported Features and Exceptions

The following sections provide information on the feature verification performed and issues discovered during interoperability verification. The features listed in the *Supported Features* section below are the features verified to work. These are the only features you can expect to function with the configuration provided in this guide.

Supported Features

The following features were verified during interoperability testing and are supported by the integration:

- Data application - Internet access only
- CradlePoint CBA750B operation in **Passthrough** mode
- Wireless account activation (initially for a Verizon 4G LTE account)
- CradlePoint CBA750B **Force 24** subnet option for IPv4
- Primary WAN operation with ADTRAN routers
- Backup wireless WAN operation with ADTRAN routers
- AOS Firewall and network address translation (NAT) operation for primary and failover WAN interfaces
- AOS Network Monitor probe operation for keep alive and WAN failover
- ADTRAN Power over Ethernet (PoE) Injector powering for the CBA750B

Exceptions

The following features are not supported by the integration:

- AOS voice over IP (VoIP) operation over the 3G/4G WAN
- CradlePoint CBA750B **Router** mode operation

The following minor issues were observed during interoperability verification:

- The CradlePoint CBA750B should only be connected to an AOS router Ethernet interface and **NOT** to a switchport. The CradlePoint CBA750B temporarily shuts down its Ethernet interface to signal learning a new public IP address from the wireless service provider. Currently, the AOS switchport vlan interface will not trigger a new DHCP discovery based on this event.
- Verizon's 4G LTE wireless DHCP service assigns a private (RFC1918) IPv4 address in the form **10.xxx.xxx.xxx** to the router. Since this is not a publicly routable IP address, some customer premises equipment (CPE) applications are not possible, such as hosting, port forwarding, or remote management access. Customers that require these type of applications will need to obtain a public static IP address from the wireless service provider.
- The CradlePoint CBA750B should be configured to use the **Force 24** subnet option. With the **Force 24** option, the CradlePoint DHCP server will always respond with the first host address (**xxx.xxx.xxx.1**) in the /24 subnet as the gateway WAN address in response to the AOS router DHCP request. This avoids addressing issues with the wireless service provider.

Configuring the ADTRAN Router

This section describes the required CLI configuration for ADTRAN routers when using the CradlePoint CBA750B for wireless WAN failover. It also includes optional instructions for configuring the Network Monitor feature for failover.

> NOTE *This section provides example configurations that may need to be altered to fit your specific network. For additional configuration information please refer to the guides listed in* *Additional Resources on page 24*.

This section consists of the following subsections:

Configuring the ADTRAN Router for Wireless WAN Failover

The following configuration steps are required for all wireless WAN failover deployments:

Step 1: Access the CLI

To access the command line interface (CLI) on the ADTRAN router, follow these steps:

1. Boot up the unit.
2. Telnet to the unit (**telnet** <*ip address*>), for example:

   telnet 10.10.10.1

> NOTE *If during the unit's setup process you have changed the default Internet Protocol (IP) address (**10.10.10.1**), use the configured IP address.*

3. Enter your user name and password at the prompt.

> NOTE *The AOS default user name is **admin** and the default password is **password**. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enter Enable mode by entering **enable** at the prompt as follows:

   >enable

5. Enter your Enable mode password at the prompt.

> *The default Enable mode password is **password**. If your product no longer has the default Enable password, contact your system administrator for the appropriate password.*

6. Enter the unit's Global Configuration mode as follows:

   #configure terminal
   (config)#

Step 2: Configure Policy-Based Routing for Accessing the CradlePoint CBA750B

Configure policy-based routing to access the CBA750B for configuration from a PC on the LAN. Using policy-based routing enables access to the CBA750B even when multiple WAN connections are used for failover applications. Access is also available even if the DHCP server has not resolved the public wireless IP address for the interface.

In the configuration example below, a route map is configured to match the HTTP traffic to the CBA750B's default IP address 192.168.0.1. Matching traffic is routed to the Ethernet connection to the CBA750B. In the example, the **ip access list extended** command is used to create an extended IPv4 ACL named **CPADMIN** and enter the Extended IPv4 ACL Configuration mode. Then, the **permit** command is used to permit TCP packets to port **80** of the default IP address of the CradlePoint CBA750B. After creating an ACL, the **route-map** command is used to create a route map named **CPACCESS**. The **match ip address** command is used to match traffic based on the **CPADMIN** ACL, and the **set interface** command is used to route matching traffic to the Ethernet port connected to the CBA750B.

To configure an ACL to specify the types of traffic permitted to the CBA750B's default IP address and configure a route map to route the permitted traffic to the CBA750B, enter the following commands at the specified command prompts:

```
(config)#ip access-list extended CPADMIN
(config-ext-nacl)#permit tcp any host 192.168.0.1 eq www
(config)#route-map CPACCESS permit 10
(config-route-map)#match ip address CPADMIN
(config-route-map)#set interface eth 0/2 null 0
```

Step 3: Configure the LAN Interface

Configure the LAN interface on the AOS router to provide connections for PCs and other data communications devices that will access the Internet over the wireless WAN. The NetVanta 3448, for example, provides eight Ethernet switch ports that may be used for the LAN connections.

The configuration example below configures the LAN using the default **VLAN 1**. The **ip address** command is used to specify a static ip address and subnet mask for the interface, and the **ip policy route-map CPACCESS** command enables policy-based routing to allow PCs on the VLAN to access the CBA750B for configuration and management. Additionally, the **ip access-policy** command is used to assign the **Private** ACP to the interface to allow PCs on the VLAN to access the ADTRAN router for configuration.

To configure the LAN interface, enter the following commands at the specified command prompts:

(config)#**interface vlan 1**
(config-vlan 1)#**ip address 10.10.10.1 255.255.255.0**
(config-vlan 1)#**ip policy route-map CPACCESS**
(config-vlan 1)#**ip access-policy Private**
(config-vlan 1)#**no shutdown**

Step 4: Configure Policy Classes and Access Lists for Each WAN Connection

Configure separate policy-classes and access-lists for each WAN connection. The firewall uses the separate ACPs to differentiate between the primary and WAN failover interfaces. Having separate ACLs helps maintain stability when making configuration changes.

The configuration example below performs several functions: (1) it specifies all traffic on the LAN as trusted, (2) it allows traffic from the LAN destined for an IP address on the ADTRAN router, (3) it enables many-to-one NAT for translating LAN IP addresses to the WAN interfaces, (4) and it allows only HTTPS and SSH traffic from the WAN into the LAN. In total, four extended ACLs are created using the **ip access-list extended** command and are configured to permit traffic to be processed using the **permit** command: (1) a **self** ACL is created to permit management traffic from the LAN to any IP address on the ADTRAN router, (2) an **AdminAccess** ACL is created to permit SSH and HTTPS traffic from the WAN for remote management of the ADTRAN router, (3) a **NAT1** ACL is created for translating private IP addresses on the LAN to the IP address of the primary WAN Ethernet interface (many-to-one NAT), and (4) a **NAT2** ACL is created for translating private IP addresses on the LAN to the IP address of the WAN failover Ethernet interface (many-to-one NAT). Additionally, three ACPs are created using the **ip policy-class command** and are configured to define the actions taken on the packets permitted by the ACLs: (1) a Public ACP is created to **allow** traffic from the primary WAN into the LAN that matches the **AdminAccess** ACL and discard all other traffic, (2) a **Public2** ACP is created to **allow** traffic from the wireless failover WAN into the LAN that matches the **AdminAccess** ACL and discard all other traffic, and (3) a **Private** ACP is created to allow traffic from the LAN destined for an IP address on the ADTRAN router, enable NAT for the primary and failover WAN interfaces, and to only **allow** HTTPS and SSH traffic over the primary and failover WAN interfaces.

*The **Public2** policy and all associated configurations are added as a best practice. Since the IP address the AOS device receives from the 3G/4G network is not publicly accessible, it is not required in most cases.*

This is an example configuration only. This security policy should be configured to fit your network. For more information about configuring the firewall, refer to Configuring the Firewall (IPv4) in AOS available from the ADTRAN support community at https://supportforums.adtran.com.

To configure policy classes and access lists for the primary and WAN failover connections, enter the following commands at the specified command prompts:

(config)**#ip access-list extended self**
(config-ext-nacl)**#permit ip any any**
(config)**#ip access-list extended AdminAccess**
(config-ext-nacl)**#permit tcp any any eq https log**
(config-ext-nacl)**#permit tcp any any eq ssh log**
(config)**#ip access-list extended NAT1**
(config-ext-nacl)**#permit ip any any**
(config)**#ip access-list extended NAT2**
(config-ext-nacl)**#permit ip any any**
(config)**#ip policy-class Public**
(config-ext-nacl)**#allow list AdminAccess**
(config)**#ip policy-class Public2**
(config-ext-nacl)**#allow list AdminAccess**
(config)**#ip policy-class Private**
(config-ext-nacl)**#allow list self self**
(config-ext-nacl)**#nat source list NAT1 interface eth 0/1 overload policy Public**
(config-ext-nacl)**#nat source list NAT2 interface eth 0/2 overload policy Public2**

Step 5: Configure Fast NAT Failover

Enable Fast NAT failover mode to force the ADTRAN router to clear all current IPv4 firewall policy sessions during failover. This allows the router to immediately send traffic to the failover interface. Otherwise, the router tries to send traffic from existing allowed policy sessions out from the failed IP address until the session times out, resulting in a loss of connectivity.

The IPv4 firewall must be enabled for fast NAT failover to be enabled. For more information about configuring the firewall, refer to Configuring the Firewall (IPv4) in AOS available from the ADTRAN support community at https://supportforums.adtran.com.

To enable fast NAT failover, enter the **ip firewall fast-nat-failover** command from the Global Configuration mode:

(config)**#ip firewall fast-nat-failover**

Step 6: Configure the WAN Failover Interface to the CradlePoint CBA750B

Configure the Ethernet interface to the CradlePoint CBA750B to learn its IP address using DHCP, and assign it an administrative distance greater than 1. The ADTRAN router will treat this learned route as a secondary WAN connection, since the default distance for the primary WAN connection is 1. Additionally, the **Public2** ACP created in *Step 4: Configure Policy Classes and Access Lists for Each WAN Connection on page 7* should be assigned to the interface to allow only HTTPS and SSH traffic for ADTRAN router management through the WAN failover interface.

*The **Public2** policy and all associated configurations are added as a best practice. Since the IP address the AOS device receives from the 3G/4G network is not publicly accessible, it is not required in most cases.*

In the example configuration below, the **ip address dhcp** command is used to configure the Ethernet interface to the CBA750B to learn its IP address using DHCP, and assign it an administrative distance of **10**. Additionally, the **ip access-policy** command is used to assign the **Public2** ACP to the interface.

To configure the WAN failover Ethernet interface to the CBA750B, enter the following commands at the specified command prompts:

```
(config)#interface ethernet 0/2
(config-eth 0/2)#ip address dhcp 10
(config-eth 0/2)#ip access-policy Public2
(config-eth 0/2)#no shutdown
```

Step 7: Configure the Primary Ethernet WAN Interface

Configure the primary Ethernet WAN interface with a static IP address and assign it the **Public** ACP created in *Step 4: Configure Policy Classes and Access Lists for Each WAN Connection on page 7* to allow only HTTPS and SSH traffic through the interface for ADTRAN router management

In the example configuration below, the **ip address** command is used to configure the primary Ethernet interface with a static IP address. Additionally, the **ip access-policy** command is used to assign the **Public** ACP to the interface.

To configure the primary Ethernet interface, enter the following commands at the specified command prompts:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#ip address 198.51.100.1 255.255.255.192
(config-eth 0/1)#ip access-policy Public
(config-eth 0/1)#no shutdown
```

Step 8: Configure the Default Route to the WAN Gateway

Configure a default route to the WAN gateway. The default route is used as the destination for packets for which no route is present. To set a static default route to the next-hop gateway, use the **ip route** command from the Global Configuration mode:

```
(config)#ip route 0.0.0.0 0.0.0.0 198.51.100.2
```

Optional. Configuring WAN Failover with Network Monitor

Network monitor features for probe, track, and policy-based routing can be used to automatically detect primary WAN failure and switch over to the wireless WAN failover interface for backup. This optional configuration uses Internet Control Message Protocol (ICMP) probes to network servers to detect WAN failures in addition to physical Ethernet interface disruptions.

WAN failover with network monitor provides an additional means of detecting primary WAN failure. The wireless WAN failover configurations provided in Configuring the ADTRAN Router for Wireless WAN Failover on page 5 must also be configured.

> NOTE *The steps in this section show a basic configuration. For detailed configuration information, refer to Configuring WAN Failover with Network Monitor in AOS available from the ADTRAN support community at https://supportforums.adtran.com.*

To configure network monitor for wireless WAN failover, follow these steps:

Step 1: Configure the Primary WAN Probe

Create a primary WAN probe to send Internet Control Message Protocol (ICMP) echo request to detect whether the primary WAN connection is UP or DOWN.

In the configuration example below, the **probe** <*name*> **icmp-echo** command is used to create an ICMP echo probe. The **destination** command is used to configure the **destination IP address** for the ICMP echo request sent by the probe, and the **source** command is used to specify the primary WAN IP address as the source IP address of the ICMP echo requests. The **period** command is used to specify the frequency at which the probe will send ICMP echo request, and the **timeout** command is used to specify how long the probe will wait for an ICMP echo reply from the destination IP address before considering the ICMP echo test a failure. Lastly, the **tolerance consecutive** command is used to specify the consecutive number of times the probe's test must fail or pass in order for the probe to transition from a PASS to FAIL state or FAIL to PASS state, respectively. This command effectively determines when the probe considers the primary WAN to be DOWN or UP.

To configure the ICMP echo probe for the primary WAN, enter the following commands at the specified command prompts:

```
(config)#probe PRIMARYPROBE icmp-echo
(config-probe-PRIMARYPROBE)#destination 4.2.2.2
(config-probe-PRIMARYPROBE)#source-address 198.51.100.1
(config-probe-PRIMARYPROBE)#period 10
(config-probe-PRIMARYPROBE)#timeout 1500
(config-probe-PRIMARYPROBE)#tolerance consecutive fail 3 pass 2
(config-probe-PRIMARYPROBE)#no shutdown
```

Step 2: Configure the Primary WAN Track

Configure a track that monitors the status of the primary WAN probe and FAILs when the probe transitions to the FAIL state (e.g. when the primary WAN fails).

In the configuration example below, the **track** command is used to create a track. The **test list or** command is used to create a Boolean test list. The **or** keyword causes the track to be in the PASS state when the **PRIMARYPROBE** probe (primary WAN) is in the PASS state and causes the track to be in the FAIL state when the **PRIMARYPROBE** probe is in the FAIL state. Finally, the **if probe** command is used to specify that the track's state should be dependent on the state of the **PRIMARYPROBE** probe.

To configure the track for monitoring the **PRIMARYPROBE** probe, enter the following commands at the specified command prompts:

```
(config)#track PRIMARYTRACK
(config-track-PRIMARYTRACK)#test list or
(config-track-PRIMARYTRACK-test)#if probe PRIMARYPROBE
(config-track-PRIMARYTRACK)#no shutdown
```

Step 3: Configure Policy-based Routing for the Probe

Configure policy-based routing to force the probe to only route out of the primary WAN Ethernet interface. Without policy-based routing, during failover, the probe will begin sending ICMP echo requests out the WAN failover interface along with the rest of the traffic, which will transition the probe to a PASS state and cause the unit to try to route out the failed primary WAN interface.

In the configuration example below, the **ip access-list extended** command is used to create an extended IPv4 ACL for the **PRIMARYPROBE**. The **permit** command is used to configure the ACL to permit ICMP packets from any source to the ICMP echo request destination configured in *Step 1: Configure the Primary WAN Probe on page 10*. Next, the **route-map** <*name*> **permit** command is used to create a route-map. The **match ip address** command is used to match traffic based on the **PROBEACL** ACL (traffic from the probe), and the **set interface** command is used to send traffic from the probe out the primary WAN Ethernet interface. Last, the **ip local policy route-map** command is used to globally assign the **PROBEMAP** route map to the ADTRAN router, forcing all traffic generated by the router that matches the ACL to be routed out the primary WAN interface.

To configure policy-based routing for the probe, enter the following commands at the specified command prompts:

```
(config)#ip access-list extended PROBEACL
(config-ext-nacl)#permit ip any host 4.2.2.2
(config)#route-map PROBEMAP permit 10
(config-route-map)#match ip address PRIMARYACL
(config-route-map)#set interface eth 0/1 null 0
(config-route-map)#set ip next-hop 198.51.100.2
(config)#ip local policy route-map PROBEMAP
```

Step 4: Associate the Track with the Primary WAN Route

Associate the track with the default route for the primary WAN interface so that the route will be removed when the ICMP probe fails. To associate the track with the default route, use the **ip route** command from the Global Configuration mode:

The following example creates a default route to **198.51.100.2** and specifies that the route will be disabled when the track **PRIMARYTRACK** fails:

```
(config)#ip route 0.0.0.0 0.0.0.0 198.51.100.2 track PRIMARYTRACK
```


Step 5: Disable the Reverse Path Forwarding Check

Disable the reverse path forwarding (RPF) check on the ACP associated with the primary WAN interface to avoid the possibility that the return probe traffic is not dropped while the backup connection is active. To disable the RPF check, use the **no ip policy-class** <*ipv4 acp name*> **rpf-check** from the Global Configuration mode:

(config)**#no ip policy-class Public rpf-check**

ADTRAN Router Sample Configurations for Verizon Dedicated Internet Access

Reference ADTRAN router sample configurations are listed in the following sections. These should be suitable for providing wireless WAN failover using the CradlePoint CBA750B with Verizon's dedicated Internet access service. The configurations make a few assumptions that may require modification:

1. The router is not acting as a DHCP server, and thus has DNS proxy disabled.
2. The configuration allows **SSH**, **HTTP**, **HTTPS** and **ICMP** packets through the firewall. These can be restricted by modifying the ACLs for additional security.
3. The LAN IP address **10.10.10.1/24** is assigned to the LAN interface. A different subnet can be substituted.
4. The primary WAN is tracked by sending ping probes to address **4.2.2.2**. If a different public address is required, multiple instances of **4.2.2.2** related to the probe configuration will need modification.
5. The DNS servers are assigned to two public servers **8.8.8.8** and **4.2.2.2**. If different DNS servers are required, the name servers should be modified.
6. Time is requested from the public service, **time.nist.gov**. If a different server is required, an SNTP server should be used.

NetVanta 3448 Sample Configuration

The following sample configuration for the NetVanta 3448 provides wireless WAN failover using the CradlePoint CBA750B with Verizon's dedicated Internet access service.

```
!
hostname "CP-3448"
enable password adtran
!
ip subnet-zero
ip classless
ip routing
ipv6 unicast-routing
!
name-server 8.8.8.8 4.2.2.2
!
ip local policy route-map LOCAL
!
no auto-config
!
event-history on
no logging forwarding
no logging email
!
no service password-encryption
!
username <username> password <password>
!
ip firewall
ip firewall fast-nat-failover
no ip firewall alg msn
```



```
no ip firewall alg mszone
no ip firewall alg h323
!
no dot11ap access-point-control
!
probe PRIMARYPROBE icmp-echo
  destination 4.2.2.2
  source-address <primary WAN IP>
  period 10
  tolerance consecutive fail 3 pass 2
  no shutdown
!
track PRIMARYTRACK
  snmp trap state-change
  test list or
    if probe PRIMARYPROBE
  no shutdown
!
vlan 1
  name "Default"
!
no ethernet cfm
!
interface eth 0/1
  description Primary WAN
  ip address  <Primary WAN Public IP and subnet mask>
  ip access-policy Public
  no shutdown
  no lldp send-and-receive
!
interface eth 0/2
  description Secondary wireless WAN
  ip address dhcp 10
  ip access-policy Public2
  no shutdown
  no lldp send-and-receive
!
interface switchport 0/1
  no shutdown
!
interface switchport 0/2
  no shutdown
!
interface switchport 0/3
  no shutdown
!
interface switchport 0/4
  no shutdown
!
```



```
interface switchport 0/5
  no shutdown
!
interface switchport 0/6
  no shutdown
!
interface switchport 0/7
  no shutdown
!
interface switchport 0/8
  no shutdown
!
interface vlan 1
  ip address  10.10.10.1  255.255.255.0
  ip policy route-map CPACCESS
  ip access-policy Private
  no shutdown
!
route-map LOCAL permit 20
  match ip address PRIMARYPROBE
  set ip next-hop <primary WAN gateway IP>
  set interface null 0
!
route-map CPACCESS permit 10
  match ip address CPADMIN
  set interface eth 0/2  null 0
!
ip access-list extended AdminAccess
  remark Admin Access
  permit tcp any  any eq https   log
  permit tcp any  any eq ssh   log
  permit icmp any  any     log
  permit tcp any  any eq www   log
!
ip access-list extended CPADMIN
  remark Management to Cradlepoint
  permit tcp any  host 192.168.0.1 eq www
!
ip access-list extended NAT1
  remark NAT all to primary WAN
  permit ip any  any
!
ip access-list extended NAT2
  remark NAT all to secondary wireless WAN
  permit ip any  any
!
ip access-list extended PRIMARYPROBE
  remark Probe to primary WAN
  permit icmp any  host 4.2.2.2
```



```
!
ip access-list extended self
  remark Traffic to Netvanta
  permit ip any  any
!
ip policy-class Private
  allow list self self
  nat source list NAT1 interface eth 0/1 overload policy Public
  nat source list NAT2 interface eth 0/2 overload policy Public2
!
no ip policy-class Public rpf-check
ip policy-class Public
  allow list AdminAccess
!
no ip policy-class Public2 rpf-check
ip policy-class Public2
  allow list AdminAccess
!
ip route 0.0.0.0 0.0.0.0 <Primary WAN gateway IP> track PRIMARYTRACK
!
no tftp server
no tftp server overwrite
no http server
no http secure-server
no snmp agent
no ip ftp server
ip ftp server default-filesystem flash
no ip scp server
no ip sntp server
!
ip sip udp 5060
ip sip tcp 5060
!
line con 0
  no login
!
line telnet 0 4
  login
  no shutdown
line ssh 0 4
  login local-userlist
  no shutdown
!
sntp server time.nist.gov
!
end
?
```


NetVanta 4430 Sample Configuration

The following sample configuration for the NetVanta 4430 provides wireless WAN failover using the CradlePoint CBA750B with Verizon's dedicated Internet access service.

```
hostname "CP-4430"
enable password adtran
!
ip subnet-zero
ip classless
ip routing
ipv6 unicast-routing
!
name-server 8.8.8.8 4.2.2.2
!
ip local policy route-map LOCAL
!
no auto-config
!
event-history on
no logging forwarding
no logging email
!
no service password-encryption
!
username <username> password <password>
!
ip firewall
ip firewall fast-nat-failover
no ip firewall alg msn
no ip firewall alg mszone
no ip firewall alg h323
!
no dot11ap access-point-control
!
probe PRIMARYPROBE icmp-echo
  destination 4.2.2.2
  source-address <primary WAN IP>
  period 10
  tolerance consecutive fail 3 pass 2
  no shutdown
!
track PRIMARYTRACK
  snmp trap state-change
  test list or
    if probe PRIMARYPROBE
  no shutdown
!
no ethernet cfm
!
```



```
interface eth 0/1
  description Secondary wireless WAN
  ip address dhcp 10
  ip access-policy Public2
  no shutdown
  no lldp send-and-receive
!
interface gigabit-eth 0/1
  description Primary WAN
  ip address <primary WAN Public IP and subnet mask>
  ip access-policy Public
  no shutdown
  no lldp send-and-receive
!
interface gigabit-eth 0/2
  ip address  10.10.10.1  255.255.255.0
  ip access-policy Private
  no shutdown
!
route-map LOCAL permit 20
  match ip address PRIMARYPROBE
  set ip next-hop <primary WAN gateway IP>
  set interface null 0
!
route-map CPACCESS permit 10
  match ip address CPADMIN
  set interface eth 0/1  null 0
!
ip access-list extended AdminAccess
  remark Admin Access
  permit tcp any  any eq https   log
  permit tcp any  any eq ssh   log
  permit icmp any  any     log
  permit tcp any  any eq www   log
!
ip access-list extended CPADMIN
  remark Management to Cradlepoint
  permit tcp any  host 192.168.0.1 eq www
!
ip access-list extended NAT1
  remark NAT all to primary WAN
  permit ip any  any
!
ip access-list extended NAT2
  remark NAT all to secondary wireless WAN
  permit ip any  any
!
ip access-list extended PRIMARYPROBE
  remark Probe to primary WAN
```



```
  permit icmp any  host 4.2.2.2
!
ip access-list extended self
  remark Traffic to Netvanta
  permit ip any  any
!
ip policy-class Private
  allow list self self
  nat source list NAT1 interface gigabit-ethernet 0/1 overload policy Public
  nat source list NAT2 interface eth 0/1 overload policy Public2
!
no ip policy-class Public rpf-check
ip policy-class Public
  allow list AdminAccess
!
no ip policy-class Public2 rpf-check
ip policy-class Public2
  allow list AdminAccess
!
ip route 0.0.0.0 0.0.0.0 <primary WAN gateway IP> track PRIMARYTRACK
!
no tftp server
no tftp server overwrite
no http server
no http secure-server
no snmp agent
no ip ftp server
ip ftp server default-filesystem flash
no ip scp server
no ip sntp server
!
sip udp 5060
sip tcp 5060
!
line con 0
  no login
!
line telnet 0 4
  login
  no shutdown
line ssh 0 4
  login local-userlist
  no shutdown
!
sntp server time.nist.gov
!
end
```


Configuring the CradlePoint CBA750B

> NOTE *The following sections provide general instructions for configuring the CradlePoint CBA750B for integration with an ADTRAN Router. Refer to the CradlePoint CBA750B User Manual for detailed instructions on how to configure the CBA750B.*

To configure the CradlePoint CBA750B to provide a wireless WAN connection to the ADTRAN router, follow these steps:

Step 1: Remove the MC200LE-VZ Wireless Modem from the CBA750B Router

If the CradlePoint MC200LE-VZ wireless modem is attached to the CBA750B router, the modem must be removed in order to enable **Passthrough** mode on the CBA750B router and insert a Verizon subscriber identity module (SIM) card into the wireless modem. If the wireless modem is already detached from the router, you may skip this step. To remove the MC200LE-VZ wireless modem from the CBA750B router, follow these steps:

1. Remove the three screws on the bottom of the assembly that affix the modem to the router.
2. Remove the modem from the router.

Step 2: Enable Passthrough Mode

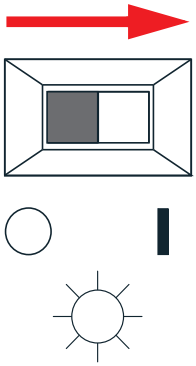
The CradlePoint CBA750B can operate in two modes either **Router** or **Passthrough**. **Passthrough** mode forces the integrated USB wireless modem to pass IP packets through to the LAN Ethernet port without the attached router performing any routing functions. In this mode, load balancing is disabled, the **Routing Mode** is set to **IP Passthrough**, the **Subnet Selection Mode** is set to **Automatically Create Subnet**, and any secondary networks are disabled. The CBA750B must be in **Passthrough** mode to properly operate with the AOS router.

A miniature, sliding switch on the right side of the CBA750B is used to toggle between **Router** mode and **Passthrough** mode; however, this switch is obstructed by the wireless modem when it is installed. Consequently, the modem must first be removed from the router to access the switch.

> NOTE *By default, **Passthrough** mode is enabled; however, because this setting is necessary for the operation of the CBA750B with ADTRAN routers, you should verify that this mode is enabled by following the steps below.*

To enable **Passthrough** mode on the CBA750B, follow these steps

1. On the right side of the CBA750B router, identify the miniature sliding switch labeled with an **O** and **I**. The switch should be adjacent to the ExpressCard slot.
2. Slide the switch to the **I** position to enable **Passthrough** mode. If the router is receiving power, the LED under the switch will be unlit while the unit is in **Passthrough** mode.



Step 3: Insert a Verizon SIM Card into the MC200LE-VZ Wireless Modem

> NOTE *In order to activate and use the wireless modem, a Verizon data plan must be purchased and a SIM card obtained. Contact Verizon or the CradlePoint reseller to setup an account.*

Insert the Verizon 4G LTE SIM card (DIRECTSIM4G-D) into the SIM card slot in the CradlePoint MC200LE-VZ modem with the circuit side down.

Step 4: Connect the MC200LE-VZ Wireless Modem to the CBA750B Router

After enabling **Passthrough** mode on the CradlePoint CBA750B router and inserting a Verizon 4G LTE SIM card into the MC200LE-VZ wireless modem, connect the modem to the router, and insert the three screws on the bottom of the assembly to affix the modem to the router.

Step 5: Connect the CBA750B to the ADTRAN Router

After connecting the MC200LE-VZ modem to the CBA750B router, use an Ethernet cable to connect the Ethernet port of the CBA750B to the Ethernet port on the ADTRAN router.

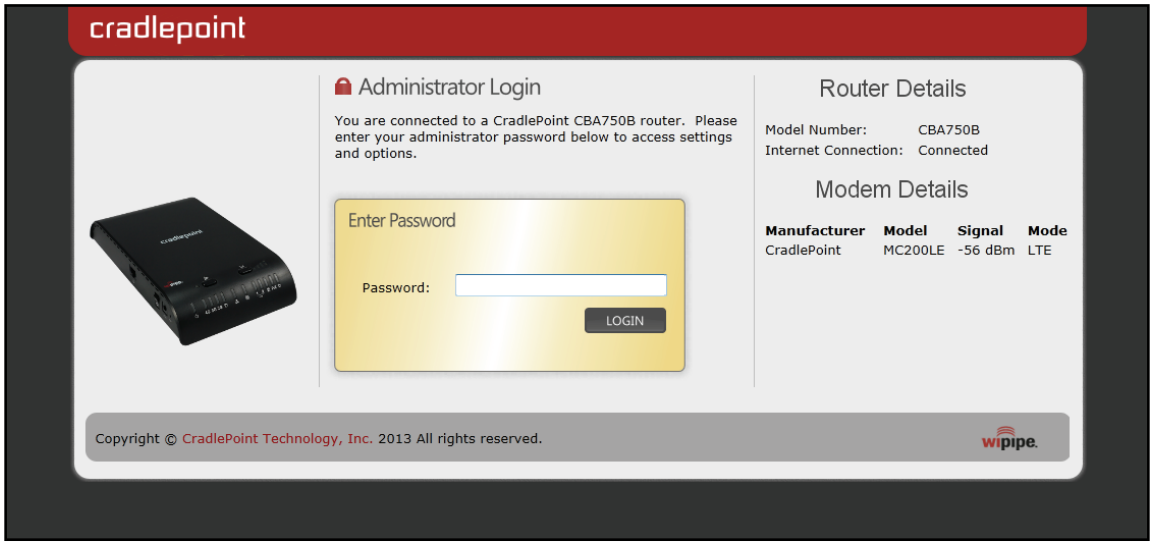
Step 6: Log in to the CradlePoint CBA750B

The CradlePoint CBA750B is configured through a Web browser. To log in to the CBA750B, follow these steps:

1. Open a new web page in your Internet browser.
2. To log in to the administrator GUI, enter the CBA750B IP address in the Internet browser's address field. The default IP address for the CBA750B is **192.168.0.1**.
   The following example accesses the administrator GUI login for a CBA750B with a default IP address:

   http://192.168.0.1

3. Enter the administrator password for the CBA750B in the **Password** field. The default login password is the last 8 characters of the CBA750B MAC address. Then, select **Login**.

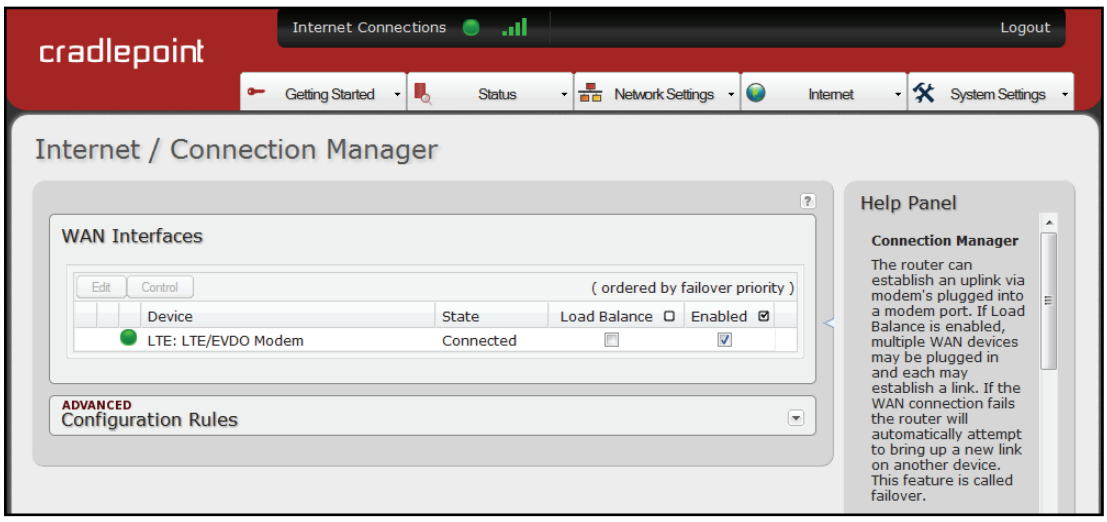


Step 7: Verify Modem Activation with Verizon

Normally, no additional configuration is required to activate the modem with Verizon. After connecting the modem to the CBA750B, connecting the CBA750B to the NetVanta router, and powering up the units, the modem should automatically activate with Verizon.

To verify the modem is activated, follow these steps:

1. In the CBA750B GUI, use the **Internet** drop-down menu to select **Connection Manager**. The **Connection Manager** menu will appear.
2. In the **WAN Interfaces** section of the **Connection Manager**, the **State** of the **LTE: LTE/EVDO Modem** should appear as **Connected** if it has been activated with Verizon.



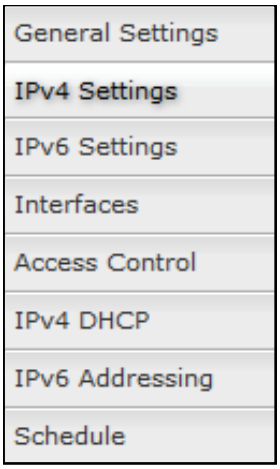
Step 8: Enable the Force 24 Subnet Option

The CradlePoint CBA750B must be configured with the **Force 24** subnet option for reliable operation with Verizon and other wireless 3G/4G LTE service providers. Verizon uses GGSN to assign wireless user IP addresses. These addresses may fall on a subnet boundary and cause routing issues. To avoid these issues, the **Force 24** option must be enabled.

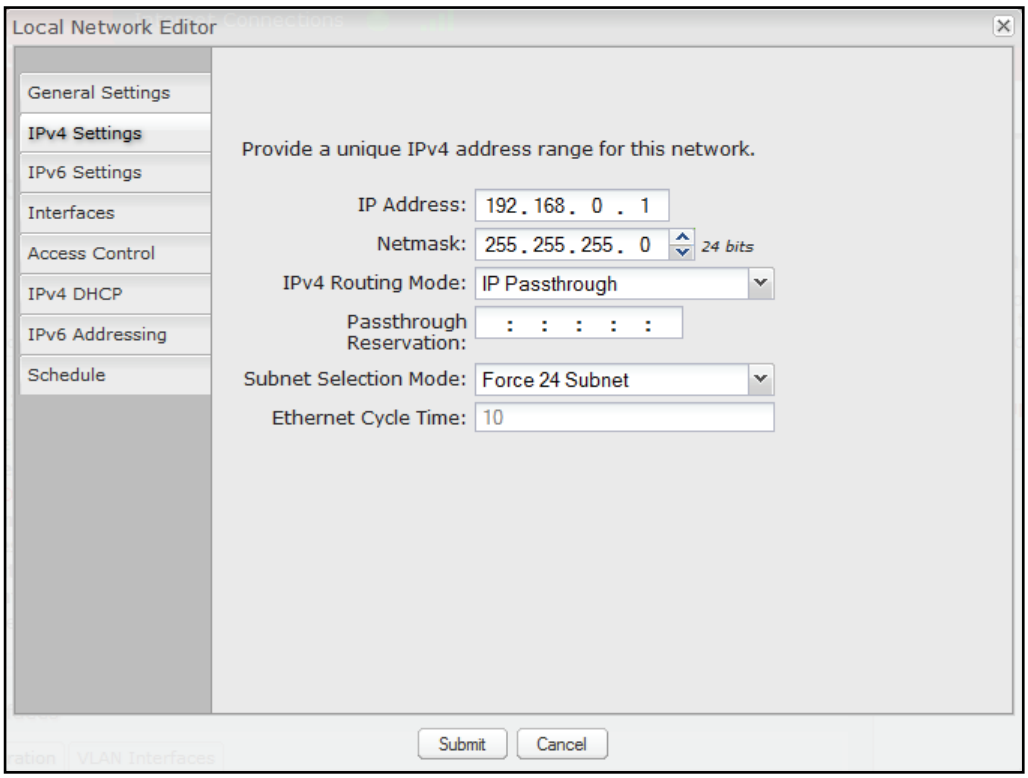
When using the **Force 24** option, the CBA750B's DHCP server will assign the gateway IP address of **xxx.xxx.xxx.1** in the /24 subnet for the LAN interface that connects to the ADTRAN router.

To configure **Force 24** option, follow these steps:

1. From the CBA750B web interface, use the **Network Settings** drop-down menu to select **Local Networks**. The **Local Networks** menu will appear.
2. In the **Local IP Networks** section of the **Local Networks** menu, select the check box next to **Primary LAN**. Then, select the **Edit** button. The **Local Network Editor** will appear.
3. In the **Local Network Editor**, select the **IPv4 Settings** tab.



4. Use the **Subnet Selection Mode** drop-down menu to select **Force 24 Subnet** Then, select the **Submit** button to save the change.



Additional Resources

There are additional resources available to aid in configuring your ADTRAN router. Many of the topics discussed in this guide are complex and require additional understanding, such as using the CLI,WAN Failover, and Network Monitoring. The documents listed in *Table 2* are available online at ADTRAN's Support Forum at https://supportforums.adtran.com.

Table 2. Additional ADTRAN Documentation

Feature	Document Title
All AOS Commands Using the CLI	*AOS Command Reference Guide*
WAN Failover with Network Monitoring	*Configuring WAN Failover with Network Monitor in AOS*
Network Monitoring	*Network Monitoring in AOS*
Multiple WAN Connection Failover	*Configuring Multiple WAN Connection Failover in AOS*
Firewall (IPv4)	*Configuring the Firewall (IPv4) in AOS*
Access Control Lists	*Configuring IP Access Control Lists (ACLs) in AOS*
Access Control Policies	*Configuring Access Policies in AOS*

