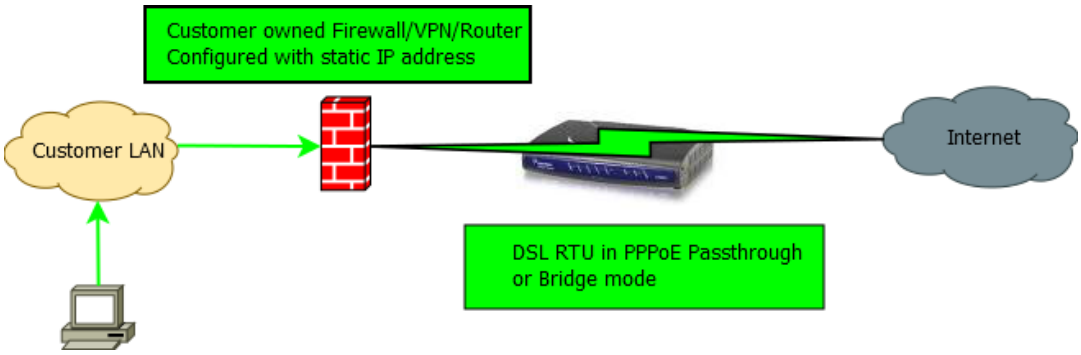
Overview

The Advanced DMZ feature available on Bell Aliant Actiontec routers provides an alternative to RFC 1483 Bridge Mode deployment. This feature delivers the functionality which is usually sought after in a Bridge Mode configuration while maintaining compatibility with service offerings and support capabilities. Use of Advanced DMZ should be encouraged in situations where subscribers desire, require or are already using RFC 1483 Bridge Mode configuration.

Contents

1 Use Case

Business customers using dynamic or static addressed DSL services often have their own network hardware deployed behind a DSL modem in bridged mode. This customer owned equipment can include devices like off-the-shelf broadband routers to specialized VPN or firewall appliances which act as gateways for the customer's existing LAN.

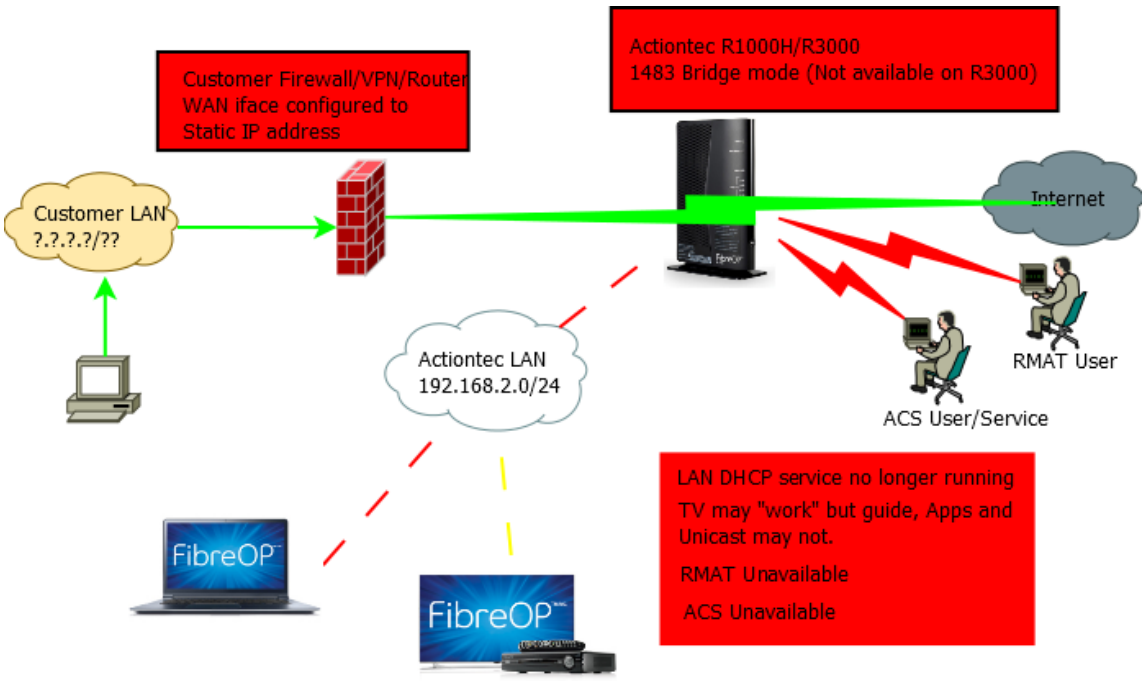


Customers switching from this configuration to a FibreOP service are provided with an Actiontec R1000H, or an Actiontec R3000 router. It is intended that the customer should utilize the port-forwarding functionality in their Actiontec router if they need to make services (HTTP, FTP, SSH, etc.) residing behind the Actiontec available to the Internet. For the majority of customers, with a bit of planning and configuration this option should be sufficient to meet their requirements. In cases where customer owned routers are deployed, there is a chance that placing them behind Network Address Translation (**NAT**) on the Actiontec LAN can result in problematic behavior of some protocols.

In cases such as these the outcome will often be that the customer or a 3rd party technical support provider contracted by the customer will configure the Actiontec router's WAN interface to use RFC 1483 Bridge mode, which allows the customer owned equipment to request an address directly from the FibreOP DHCP service over VLAN 35. The use of RFC 1483 Bridge mode on the WAN interface of the Actiontec router has the following side effects:

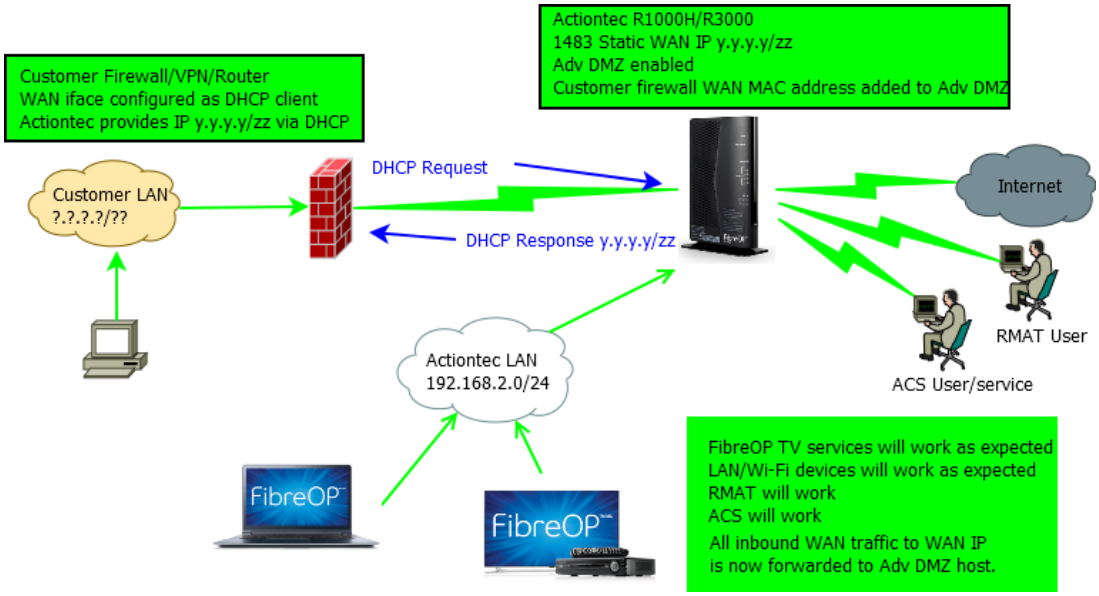
- Communication with ACS no longer works, subsequently firmware and configuration changes cannot be pushed to the Actiontec router. This affects our ability to troubleshoot and support the service/device.
- RMAT no longer works, which can affect our ability to troubleshoot and support the service/device.
- TV service cannot work as designed or expected.
- Unified Communications service cannot work as designed or expected.

As a result it is recommended and preferred that RFC 1483 Bridge mode not be used in order to support customer owned equipment; doing so limits our ability to support the existing service and upsell new services (TV and UC).



New installs going forward from 2015 are deployed with the Actiontec R3000 router. The R3000 router does not provide a configuration option for RFC 1483 Bridge mode. This can complicate installation/migration for DSL customers who rely on their own equipment to manage their Internet connection. A solution to this complication and an alternative for customers currently using an Actiontec R1000H in RFC 1483 Bridge mode is to use the Advanced DMZ feature available on both the Actiontec R1000H and R3000 routers. DMZ stands for "*Demilitarized Zone*". In computer networking the term "DMZ" is used to describe a perimeter network where you expose some services with less security – effectively putting them outside the firewall. Enabling Advanced DMZ allows one device on the Actiontec LAN to a) obtain the router's WAN IP address via the router's LAN DHCP server and b) receive every packet received on the router's WAN interface. This differs from "DMZ Host" in that the device in Advanced DMZ actually has the router's WAN address configured on its own WAN interface, while a device configured as "DMZ Host" has an IP address from the router's LAN subnet configured on its WAN interface. Packets to and from the device in Advanced DMZ won't need to be modified as they traverse the firewall since they were constructed using the WAN IP address to begin with. With "DMZ Host", traffic to any port on the router's WAN interface which isn't explicitly forwarded to another LAN host will be forwarded to the DMZ Host's LAN IP address, which requires address translations and possibly other packet mangling like protocol fix-ups by ALGs.

A device using Advanced DMZ mode behind an Actiontec router will behave as though the Actiontec router were configured in RFC 1483 Bridge mode. RMAT and ACS services will work as designed, and intended compatibility with TV, UC and ability to deliver other services to the Actiontec LAN remains unbroken.



2 Configuration Steps

Prerequisites: The WAN interface of the device being placed into the Advanced DMZ will need to be configured as a **DHCP client**. This needs to be done before or during service installation by the customer or a technical support resource contracted by the customer to manage their network. The best case scenario is that the customer or their technical support resource are available during install and can access and configure the customer owned device. The customer owned device must be able to respond to ARP requests received at its WAN interface (some firewall devices may not respond to these in their default configuration). Note: *The built-in Dynamic DNS client does not work when Advanced DMZ is enabled. If Dynamic DNS is required, advise the customer that they must deploy a Dynamic DNS client on their device, or somewhere on the LAN behind their device.*

2.1 Reboot

If this Actiontec router has already been running for a while it should be rebooted or reset to factory defaults before configuring Advanced DMZ mode.

2.2 Enable Customer Owned Device DHCP Client

The customer device should already be configured as a DHCP client and have its WAN interface connected to any LAN port on the Actiontec router and have a LAN address provided by the Actiontec router's LAN DHCP server. Confirm that this is so.

2.3 Configure static IP on R3000 WAN

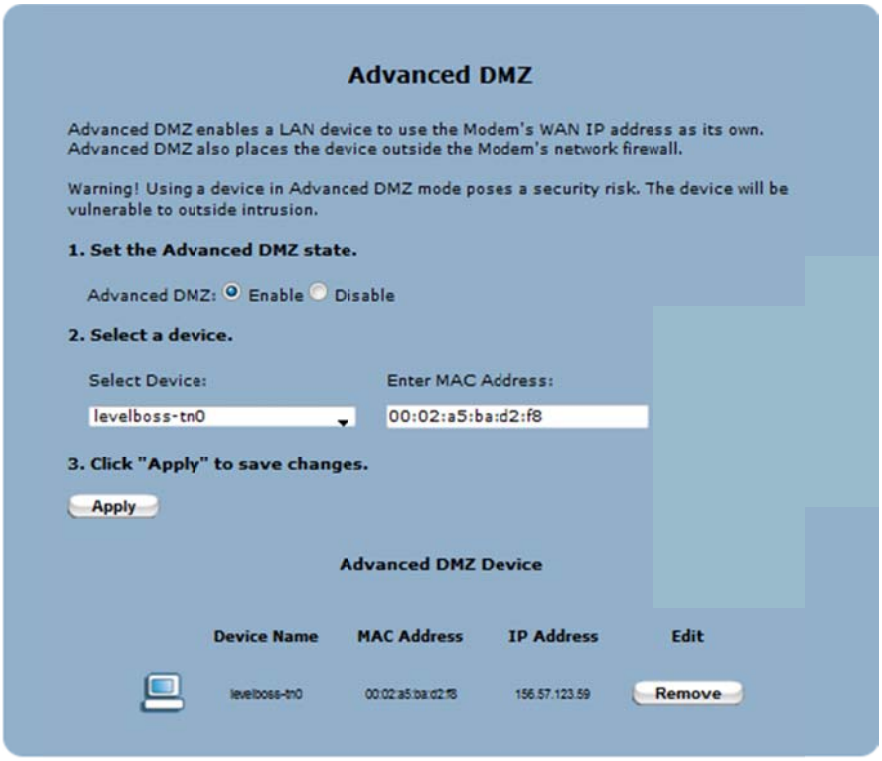
Optional - If this is a static IP service, proceed with configuring the Actiontec router's WAN interface with the appropriate settings and apply the configuration as normal.

2.4 Navigate to Advanced DMZ Screen

In the Actiontec router's Web UI, navigate to the Firewall section and select "Advanced DMZ" from the menu at the left side of the screen.

2.5 Enable Advanced DMZ

Click the “Enable” button in section 1, and then either use the drop-down menu to locate the customer owned device to be placed into the Advanced DMZ, or manually enter the device’s MAC address in the field provided. The dropdown will either contain a device name (if one has been determined) or the MAC address of the WAN interface of the customer owned device. Click the Apply button. After a short wait, the screen will return and the Advanced DMZ status can be observed at the bottom. The host configured for Advanced DMZ can be removed from the configuration by pressing the “Remove” button next to its entry at the bottom of the screen.



2.6 Reboot Actiontec Router

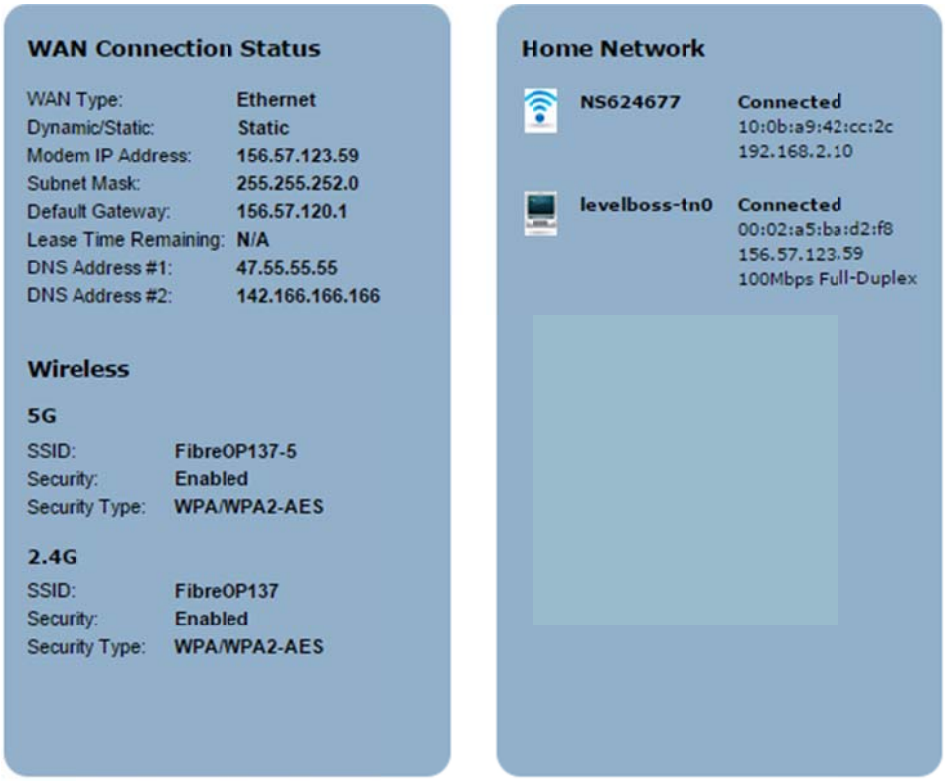
Now that the configuration is applied, reboot the Actiontec router.

2.7 Verify Settings

When the Actiontec router finishes booting up, verify that it has a WAN IP address, and that the Advanced DMZ settings are still applied.

2.8 Reboot Customer Owned Device

Reboot the customer owned device and then check its IP address. The address on the Customer Owned Device's WAN interface should now be the same as the address assigned to the Actiontec router's WAN interface. This can be checked from the Actiontec router's home screen.



2.9 Check Customer Owned Device Internet Connectivity

Verify that the customer can connect to and from the Internet using their device as expected.

3 Troubleshooting

The primary objective when troubleshooting an Actiontec router in Advanced DMZ mode should be to verify whether the Actiontec router and things on its LAN can reach the Internet. Take any normal steps to troubleshoot a static or dynamic FibreOP service. If the Actiontec router in Advanced DMZ mode is suspected of experiencing an issue, begin troubleshooting it like you would any other Actiontec router. To determine if there might be a problem with the Advanced DMZ feature, or with the customer owned device:

3.1 Ping WAN

Using the Actiontec router's Web UI (via RMAT), can you ping an address on the Internet? If yes proceed to step 3.2. If no, proceed to step 3.2.

3.2 Test Actiontec LAN Connectivity

The end user will plug a computer or client device directly into a free LAN port on the Actiontec router, or connect it to the wireless network on the Actiontec router. Can this device reach the Internet? If yes, we know that a) Internet connectivity is working and b) the Actiontec LAN is working properly. If the customer owned device in Advanced DMZ is not able to connect to the Internet proceed to step 3.3.

3.3 Reboot

If Advanced DMZ mode had already been working and then abruptly stopped working, then rebooting the Actiontec router and the customer owned device in some sequence might clear the condition:

3.3.1 Reboot Customer Owned Device

This will trigger DHCP events and refresh the CPE's IP address. At this stage we are assuming that there is not a problem with the Actiontec router. If this does not restore expected functionality to the CPE then move on to step 3.3.2

3.3.2 Reboot Actiontec router

Using the Web UI on the Actiontec router, reboot it and wait for it to come back online. In the event that there is an issue with the Actiontec router, rebooting it might at least temporarily clear the condition. When it becomes available again after the reboot, verify it has Internet connectivity and move on to step 3.3.3

3.3.3 Reboot Customer Owned Device

A final refresh of the CPE's WAN interface after a clean boot of the Actiontec router allows the customer's device to boot up and refresh its DHCP lease.

3.4 Escalate to or Notify Tier3

Tier3 can be engaged once it has been determined that the above steps have not resolved connectivity issues for the device in Advanced DMZ mode in the following cases:

- If the customer owned device in the Advanced DMZ is still unable to connect to the Internet, but the Actiontec router and its LAN connected devices are able to do so, Tier 3 should be engaged to troubleshoot further.
- If the ticket history indicates that there is a pattern emerging wherein it is required that some combination of reboots be used in order to restore connectivity for customer owned device in the Advanced DMZ, then Tier 3 should be notified in order to investigate further.

Please feel free to discuss any questions or concerns around the Advanced DMZ feature with Tier 3.