AlliedWare™ OS

How To | Configure WAN Load Balancing

Introduction

With the increasing use of the Internet to service core business functions comes the need for reliable WAN connectivity. A specific aspect of this requirement is for reliable connectivity to particular destinations. A simple and effective method of achieving this is to provide alternative network connections via different Internet Service Providers (ISPs). In this way an outage limited to one network will not result in a loss of connectivity to the essential sites.

When a router simultaneously connects to multiple ISPs, the WAN load balancer tries to distribute the router traffic equally across each network interface.

You can instead achieve connectivity via multiple WAN interfaces by using routing protocols such as RIP, OSPF or BGP, but such protocols usually choose their routing paths on the basis of metrics instead of dynamic load conditions. A router with two WAN ports connected to different ISPs would route most of its traffic via the port that offered the best metric. This provides alternative connectivity if an ISP fails, but under normal operating conditions, it wastes the alternative port's bandwidth. WAN load balancing overcomes this limitation.

Which products and software versions does this information apply to?

WAN load balancing is available for the following products, running software version 2.7.4 or later:

- AR400 and AR700 series routers
- Rapier i series switches
- Rapier 48w switches (non-firewall solutions only)

The Rapier i and Rapier 48w are the only layer 3 switches that support WAN load balancing. WAN LB is possible on these switches because they can house a WAN connection via an optional NSM.

WAN load balancer sessions

The WAN load balancer does not perform balancing on a packet-by-packet basis. Instead, the items being balanced are so-called *WAN load balancer sessions*.

Unique WAN load balancer sessions are distinguished solely based on source IP, destination IP and higher layer protocol, e.g. TCP. Therefore, if a load balancer session has been established, and packets come along which differ from previous packets of the session only in the value of source and/or destination port numbers, then they will still be considered to belong to that same WAN load balancer session. So, even though the packets belong to a new TCP session, they belong to the same WAN load balancer session. That is, WAN load balancer sessions are a different concept to TCP sessions.

Once identified, a WAN load balancer session will always be routed via the same WAN load balancer resource (i.e. gateway) until that session expires. Only traffic that is identified as a new separate WAN load balancer session (i.e. different IP address or protocol) will be routed via a different WAN load balancer resource (gateway).

The behaviour described above is desirable because many Web servers and other servers have security requirements that need to identify the continuity of a user session by source IP address. The WAN load balancer is usually used in conjunction with firewall and network address translation (NAT), so it becomes important to ensure the WAN load balancer always uses the same output interface (load balancer resource) and, therefore, the same NAT translation for any given WAN load balancer session. It would be undesirable for the same user to suddenly connect in from a different source IP address just because a protocol port number had changed. If they did, the server's identification of the user could be lost.

The load balancer manages its sessions (creating, deleting, etc.) by starting a timer for each new session created. Each timer is refreshed when a packet for its particular session passes through the load balancer. When a particular timer reaches its **orphantimeout** value, its associated session is deemed to be orphan and is closed. So, this effectively ‘idles out’ WAN load balancer sessions.

Load distribution methods

There are two load distribution methods that can be configured: round robin and weighted lottery. When a new WAN load balancer session is identified, one of these methods will be used to determine which WAN port to use. The default method is round robin. For more information on these load distribution methods refer to your router’s Software Reference.

How WAN load balancing operates with a firewall

It is not necessary to configure the router as a firewall in order to apply WAN load balancing, although the two features have been designed to operate together, and the load balancing operation operates more effectively when used with a firewall running NAT.

In many practical cases you will need the firewall NAT feature in conjunction with the WAN load balancer.

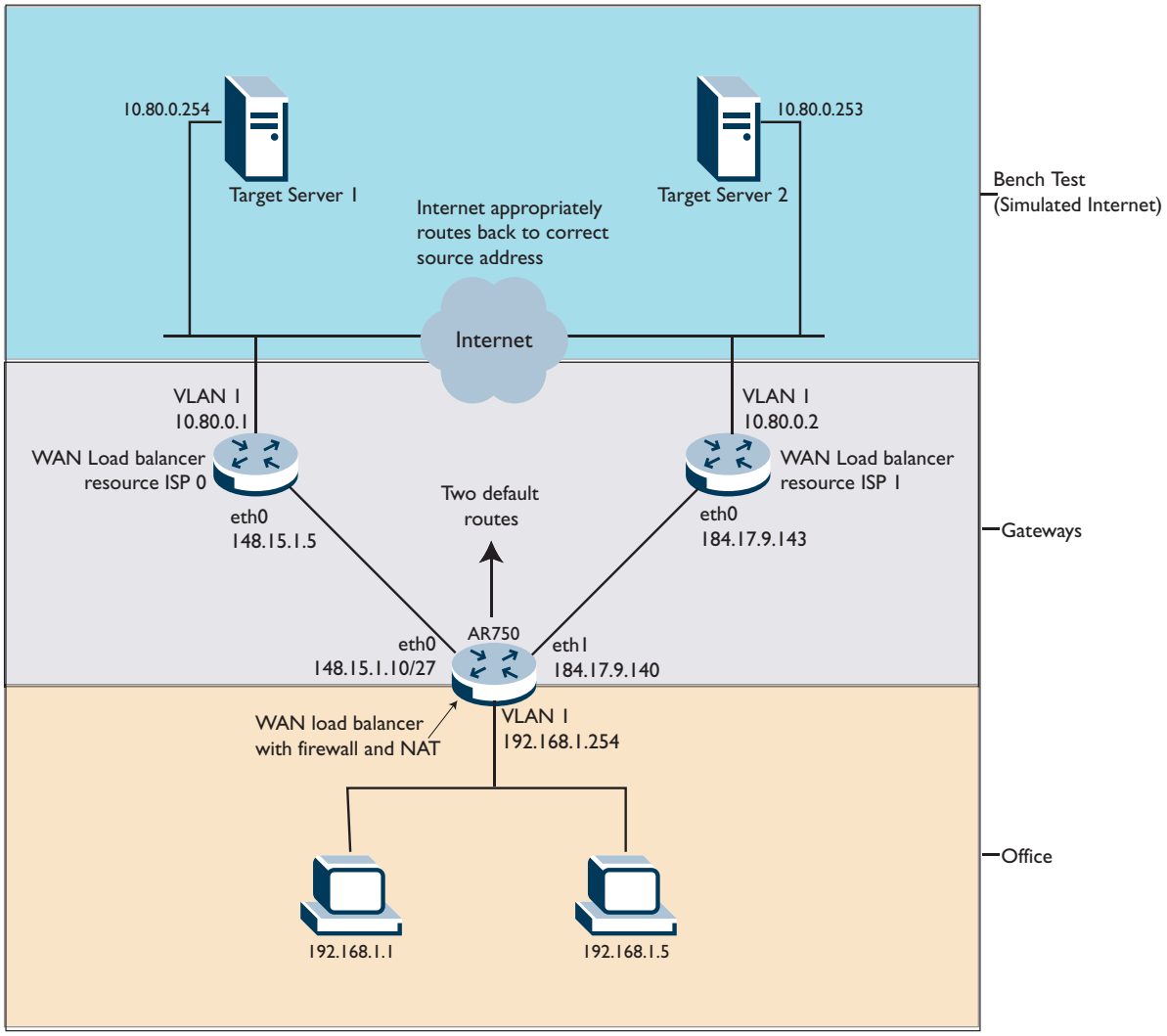
The diagram shown in Figure 1 on page 4 in the following section shows the relationship between the load balancer and the firewall functions within the router. You will need to refer to this when following the configuration examples.

An important aspect to note is that by using firewall NAT, the returning packets are very likely to take the same path (via the same ISP) as the data sent, and therefore achieve a degree of load balancing for the return path.

Example A: WAN load balancer with firewall NAT

Refer to Figure 1 when looking at the following configuration examples. Example A uses WAN load balancing in conjunction with firewall NAT.

Figure 1: Using load balancing in conjunction with firewall NAT



The WAN load balancer/firewall shown has two public interfaces, eth0 (148.15.1.10) and eth1 (184.17.9.140). The interfaces are configured for both NAT and for WAN load balancing. NAT had been defined such that 148.15.1.10 corresponds to ISP 0 and 184.17.9.140 corresponds to ISP 1.

Two upstream network devices are shown, which represent gateways to two separate ISPs. Each new WAN load balancer session will be sent to one of these WAN ISPs, using the load distribution method selected.

The following sections describe the configuration steps for each of the network devices.

Private side user PCs

The PCs are configured for the 192.168.1.x network with a gateway address of 192.168.1.254

WAN load balancer router

1. Define a system name

```
set system name=wlb
```

2. Enable IP

Enable IP and assign your public side WAN addresses which must be valid for their separate destination ISPs:

```
enable ip
add ip interface=eth0 ip=148.15.1.10 mask=255.255.255.224
add ip interface=eth1 ip=184.17.9.140 mask=255.255.255.0
```

3. Define your private IP address

This represents the gateway address to be used by your private side LAN users:

```
add ip interface=vlan1 ip=192.168.1.254
```

4. Disable multipath IP routing

For WAN load balancing to operate it is necessary to disable multipath IP routing:

```
disable ip route multipath
```

5. Define your WAN default routes

Define your WAN default routes using appropriate next hop addresses for their separate destination ISPs:

```
add ip route=0.0.0.0 mask=0.0.0.0 interface=eth0 next=148.15.1.5
add ip route=0.0.0.0 mask=0.0.0.0 interface=eth1 next=184.17.9.143
```

6. Create your firewall policy

```
enable firewall
create firewall policy=wlb
```

7. Define the firewall interfaces

```
add firewall policy=wlb interface=vlan1 type=private
add firewall policy=wlb interface=eth0 type=public
add firewall policy=wlb interface=eth1 type=public
```

8. Define the firewall enhanced NAT relationships

```
add firewall policy=wlb nat=enhanced interface=vlan1
  gblinterface=eth0
add firewall policy=wlb nat=enhanced interface=vlan1
  gblinterface=eth1
```

9. Enable the WAN load balancer and define its resources

WAN load balancer resources define the available WAN interfaces to separate ISPs:

```
enable wanlb
add wanlb resource=eth1
add wanlb resource=eth0
```

The WAN load balancing resource gateway (Ethernet 0)

Typically these devices are provided and will be configured by the respective ISPs. The following configurations simulate the upstream routing of the ISPs, for bench testing purposes.

The configurations are:

ISP 0

```
enable ip
add ip interface=eth0 ip=148.15.1.5 mask=255.255.255.224
add ip interface=vlan1 ip=10.80.0.1 mask=255.255.0.0
```

ISP 1

```
enable ip
add ip interface=eth0 ip=184.17.9.143 mask=255.255.255.0
add ip interface=vlan1 ip=10.80.0.2 mask=255.255.0.0
```

The ISP will use a default route or routing protocol method for access to the Internet beyond. For the bench test this is not necessary.

Example B: WAN load balancer without firewall NAT

To configure WAN load balancer without firewall NAT, simply use the same WAN load balancer configuration as above and omit the firewall configuration steps. Obviously you need to consider carefully if the upstream routes correctly refer back to the LAN subnet behind your WAN load balancer. If you are connecting to the Internet this means that the LAN will have valid Internet addresses, or that address translation occurs upstream of the WAN load balancer.

If you want to bench test a WAN load balancer without a firewall solution, then you need to add routes back to the WAN load balancer LAN on the target servers and to the WAN load balancer resource router configurations.

Remote site detection

To decide if a particular resource is able to deliver packets to the Internet, ping polls can be configured that will check the health of a path via any given resource. For example, if the path via eth0 seems unreliable, you could configure a ping poll to monitor this path as follows:

```
add ping poll=1 ip=<an-ip-address-accessable-over-the-eth0-link>
  fail=2 norm=10 sample=2

enable trigger

create trigger=1 module=ping event=deviceup poll=1
  script=pingup.scp

create trigger=2 module=ping event=devicedown poll=1
  script=pingdown.scp
```

The pingup.scp script file contains:

```
# Re-add eth0 as a WAN LB resource:

add wanlb resource=eth0
```

The pingdown.scp script file contains:

```
# Remove eth0 as a WAN LB resource:

delete wanlb resource=eth0
```

This ping polling configuration will ping once every 10 seconds while the link is deemed accessable, and every 2 seconds once the link is deemed to have failed. The link is deemed to have failed once the number of pings lost match the value of the **sample** parameter (2 in this example).

Verification of WAN load balancer

When verifying the operation of the WAN load balancer, you should be able to confirm the load distribution behaviour as noted above, i.e. once identified, a WAN load balancer session will always be routed via the same WAN load balancer resource (gateway). Only traffic that is identified as a new separate WAN load balancer session, for example, a different IP address or transport protocol, will be routed via a different WAN load balancer gateway.

To verify the activity of the WAN load balancer session, use the following command:.

```
show wanlb session
```

```
WAN Load Balancer Sessions
Resource  Source IP         Destination IP   Prot    Expiry
-----------------------------------------------------------
eth0
          192.168.1.5      10.80.0.253       TCP      294

eth1
          192.168.1.1      10.80.0.254       TCP      524
-----------------------------------------------------------
```

To verify the WAN load balancer resource configuration, use the command:

```
show wanlb resource
```

```
WAN Load Balancer Resources

Resource            Status              State
-----------------------------------------------------
eth0                ENABLED             UP
eth1                ENABLED             UP
-----------------------------------------------------
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

C613-16064-00 REV B