

**ISP High Availability  
on a small budget**

Copyright 2002, MacroscapE Solutions Inc.

1.0 The Problem..... 2

2.0 The three options..... 2

3.0 The assumptions..... 2

4.0 Scenario 1..... 3

5.0 Scenario 2..... 5

6.0 Scenario 3..... 6

7.0 Summary..... 7

8.0 Disclaimer..... 8

## **1.0 The Problem**

Imagine you are a small shop, you have a T-1 to a large provider that promises you the 5 nines, but you find that your grandma's AOL dial-up is more stable. You can keep requesting credits, which take 6 months to appear on your bill, but the fact of the matter is your boss is breathing down your neck every time your T-1 is down.

What can a network admin do to resolve this issue? Well, hopefully you have it in your budget to get another T-1, but with budgets tight as they are, the odds are you will need to resort to a Cable modem or DSL connectivity for you backup connection. In either case, you are probably not going to get a /24 or a slash /25 or even a /27 if you are a small shop, so BGP goes out of the window, especially if you go with DSL or Cable technologies.

So what happens to your mail, ftp and few other servers that sit on your DMZ? What happens when the primary T-1 fails and you need to fall back to your secondary provider?

In this white-paper we will show you how to achieve full-proof redundancy (well almost) even with a small budget. Please note that there are dozens of different scenarios and numerous ways of achieving the redundancy, however we will not be discussing all of them. Also note that we are only trying to design high availability between two ISPs and not concentrating on the other Layer2 and Layer3 points of failure (i.e. switch, firewall, etc.).

## **2.0 The three options**

Well let's first identify a number of scenarios:

Scenario 1: 1 Cisco Router, 2 T-1s from 2 ISPs ([see Figure 1-1](#))

Scenario 2: 2 Cisco Routers, 2 T-1s from 2 ISPs ([see Figure 1-2](#))

Scenario 3: 1 Cisco Router, 1 Cable/DSL router ([see Figure 1-3](#))

## **3.0 The assumptions**

Assumption #1

You already have a firewall on your network and performing network address translation (NAT) at the firewall and not at the ISP facing router.

Assumption #2

You have an adequate number of public addresses. Lets assume you have a /27. This will allow us to subnet it further and allocated a good amount of addresses for your DMZ as well as the external network where you can place some bastion hosts if need be.

Assumption #3

In the third scenario, we are assuming that you have only one IP address and a Cable/DSL router connected to your DSL/Cable modem; hence the port forwarding will be performed on that product. (Refer to the product's documentation)

## **4.0 Scenario 1**

The first scenario presents a situation where you have one router with dual Serial interfaces to support up to two full T-1s from multiple providers. We are going to assume that Provider A gave you a 1.1.1.0/27 and ISP B provided you with

2.2.2.0/29 (this will remain constant through-out all our examples unless specified otherwise).

The basic concept of failover will be to utilize metrics on the static routes to the two providers as follows:

```
ip route 0.0.0.0 0.0.0.0 Serial0/0  
ip route 0.0.0.0 0.0.0.0 Serial0/1 200
```

Now take a look at the routing table and you will see:

```
Router>sh ip route  
<some output is omitted>
```

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

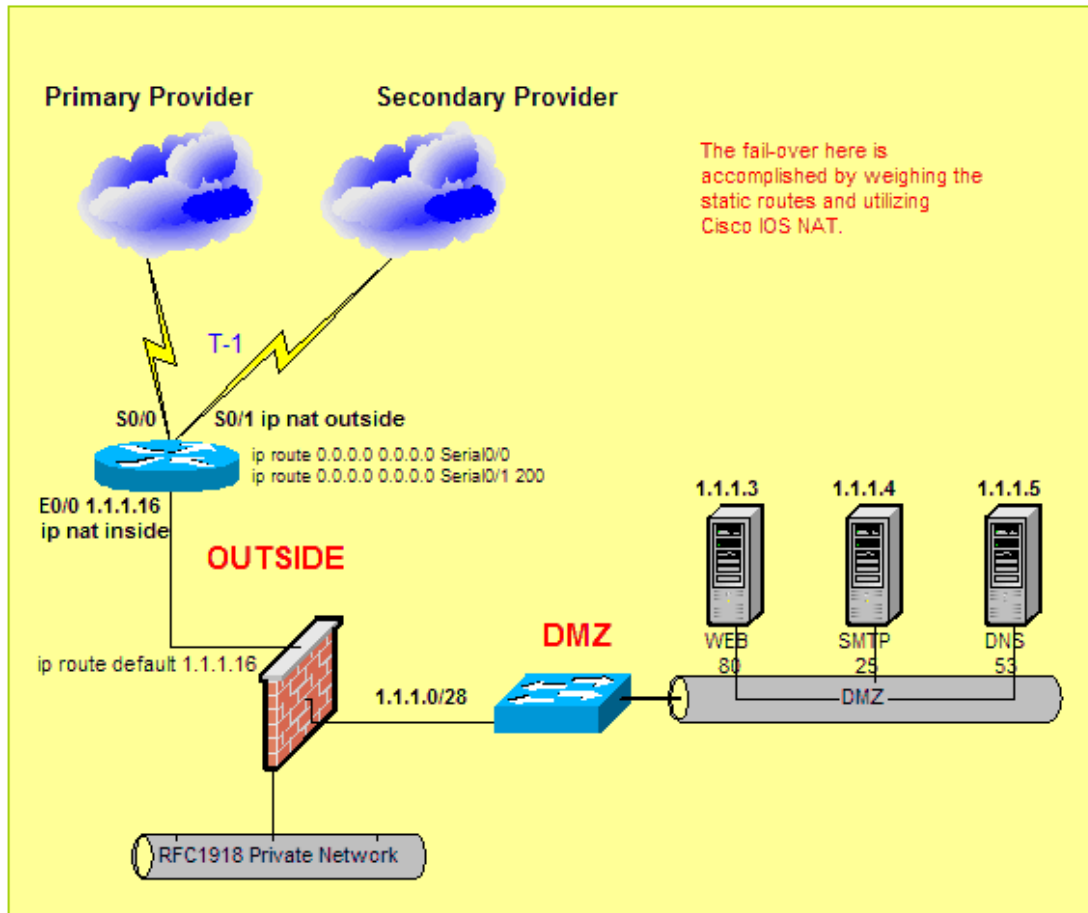
```
S* 0.0.0.0/0 is directly connected, Serial0/0
```

Since you are not running a dynamic protocol to your provider, there might be a number of possible issues on the provider's network that will not cause the interface to go down; therefore the secondary route will never kick-in. A monitoring system that will inform you of internet connectivity is a must. This will enable you to switch over manually to the secondary provider.

Now that we have established the fail-over to the second T-1 from a routing standpoint, let's talk about the translation to the secondary ISP's IP schema in order to enable outbound internet access and inbound services access.

The internet access fail-over, as shown below, is a simple task, however the inbound access for hosted services can get tricky. One of the easiest ways to accomplish this, is to set the TTL (time to live) for the DNS entries in question to zero. Note: We will not discuss DNS configuration in this paper because it is beyond the scope of this document.

Figure 1-1: Two providers, one router router



Basically what needs to be accomplished in the event of a service failure by the Primary ISP, is a static NAT from the Servers located on the 1.1.1.0 network to the backup/secondary public network (2.2.2.0) serviced by the Secondary ISP.

```
! web server
ip nat inside source static 1.1.1.3 2.2.2.3
! smtp server
ip nat inside source static 1.1.1.4 2.2.2.4
! dns server
ip nat inside source static 1.1.1.5 2.2.2.5
```

Also don't forget to translate the address that your firewall is overloading your RFC1918 internal networks.

```
! Firewall NAT address translation
ip nat inside source static 1.1.1.15 2.2.2.6
```

Now define the nat inside and outside interfaces

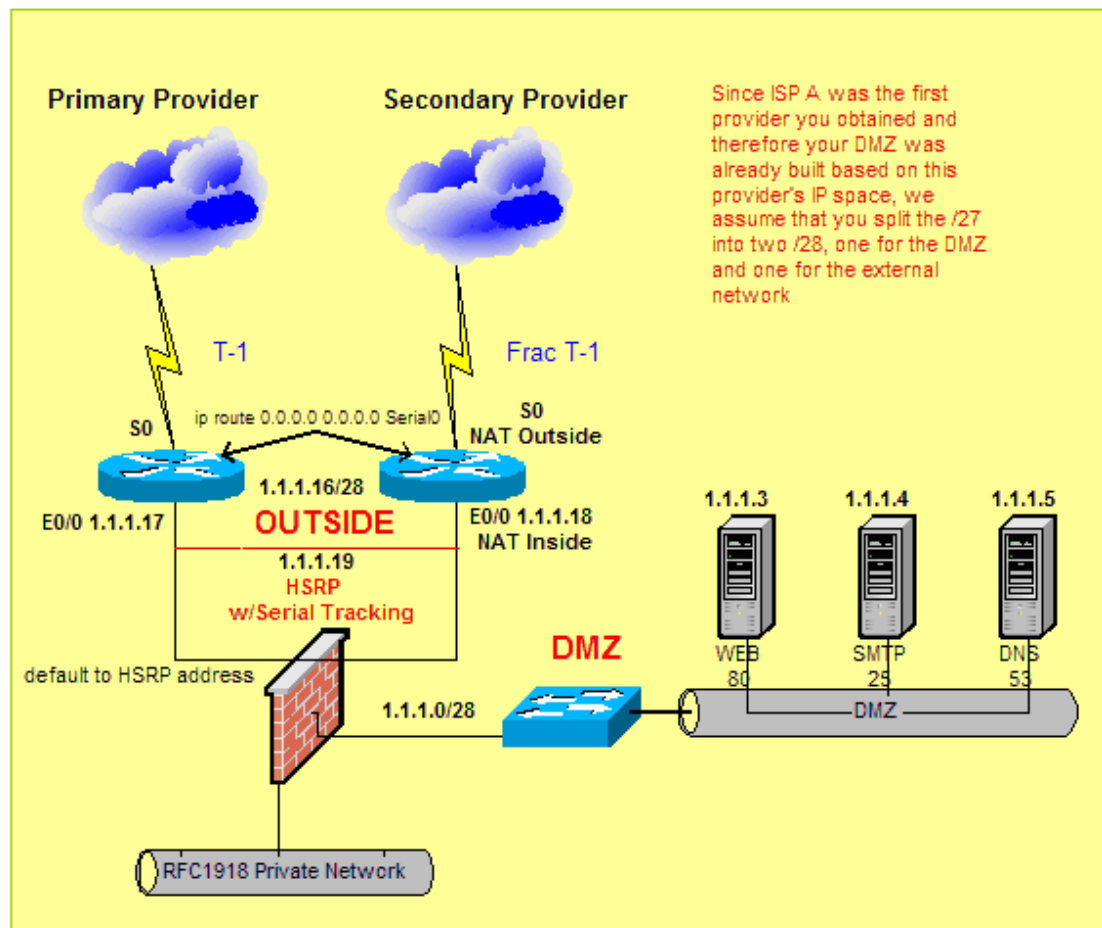
```
Router(config)#int Ethernet 0/0
Router(config-if)#ip nat inside
```

```
Router(config)#int Serial 0/1
Router(config-if)#ip nat outside
```

## 5.0 Scenario 2

Now Let's think big and assume the second option of having two routers, each having its own pipe to a respected provider. Provider A gave you a 1.1.1.0/27 and ISP B provided you with 2.2.2.0/29. (see Fig 1-1)

Figure 1-2: Two providers, two routers



The configuration on Router2 will be identical to the Scenario 1 configuration as far as network address translation is concerned. The only difference is the addition of hot standby routing protocol (HSRP – Cisco's proprietary protocol) to the two routers. The idea behind this is to have Router A as the primary router that all the traffic goes to and Router 2 will take over if and only if the Serial 0 interface on Router A fails.

```
R1 configuration:
interface Ethernet0/0
 ip address 1.1.1.17 255.255.255.248
 standby ip 1.1.1.19
 standby preempt
 standby track Serial0/0 20
```

```
R2 configuration:
interface Ethernet0/0
 ip address 1.1.1.18 255.255.255.248
 standby ip 1.1.1.19
 standby preempt
 standby priority 100
```

### **6.0 Scenario 3**

This is the final scenario we will utilize in this. It is probably the least flexible however it is the most common for those with a small budget.

In this case we will need an extra Ethernet interface on the primary router and will also assume you are only issued one public IP address from your Cable/DSL provider. We will also utilize simple port forwarding features normally provided with current generation of the DSL/Cable routers. We will not go into the details of the Port Forwarding configuration in this document since the mileage varies on each product.

Note: The same failover utilizing static routes applies here as described in the first two scenarios:

```
ip route 0.0.0.0 0.0.0.0 Serial0/0
ip route 0.0.0.0 0.0.0.0 Ethernet1/0 200
```

Basically what needs to be accomplished is each of the servers on the DMZ will need to be translated statically to the RFC1918 network that is connected to the Cable/DSL router.

```
! web server
ip nat inside source static 1.1.1.3 192.168.1.3
! smtp server
ip nat inside source static 1.1.1.4 192.168.1.4
! dns server
ip nat inside source static 1.1.1.5 192.168.1.5
```

Also don't forget to translate the address that your firewall is overloading your RFC1918 internal networks to yet another RFC1918 address.

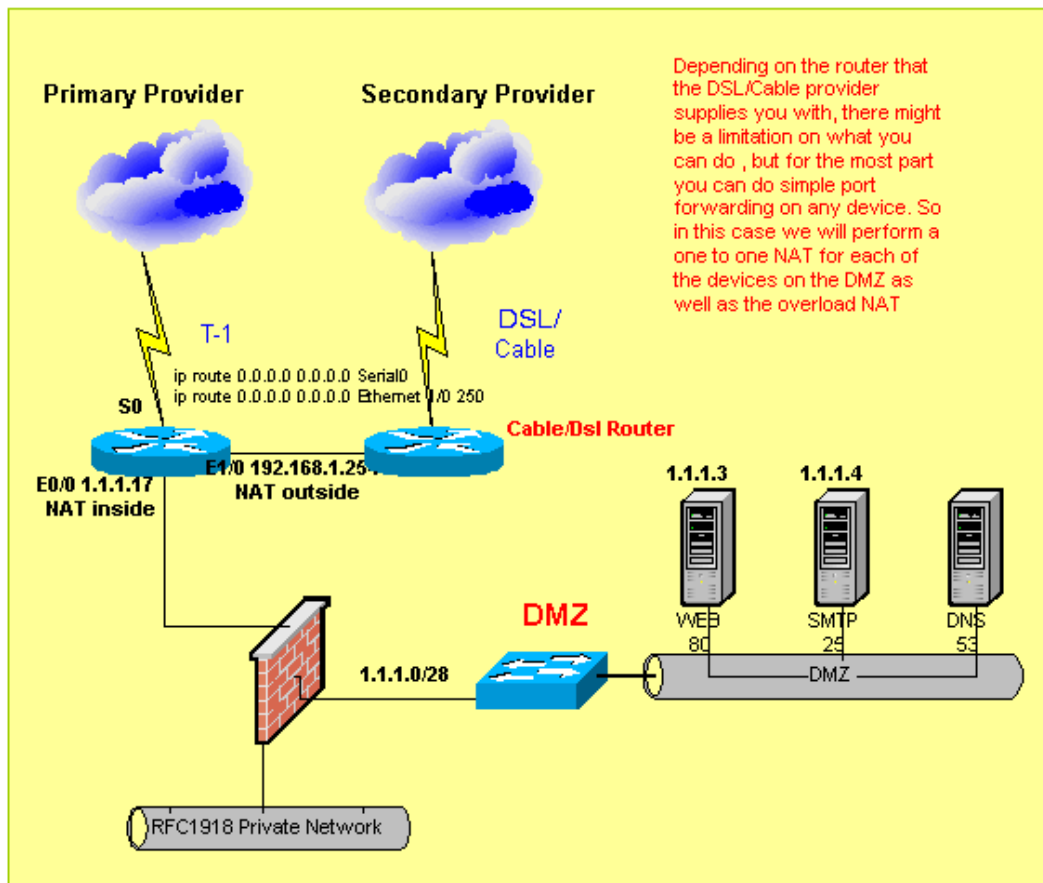
```
! Firewall NAT address translation
ip nat inside source static 1.1.1.15 192.168.1.15
```

Now define the nat inside and outside interfaces

```
Router(config)#int Ethernet 0/0
Router(config-if)#ip nat inside
```

```
Router(config)#int Ethernet 1/0
Router(config-if)#ip nat outside
```

Figure 1-3: 1 Router, 1 Cable/DSL router



## 7.0 Conclusion and Summary

The work presented in this whitepaper covers only a limited amount of scenarios that can be used to achieve high availability between multiple providers. We hope the above documentation will become useful to the network administrators and as always we are looking for feedback based on your personal experiences with implementing such solutions. Please feel free to contact us at [feedback@macroscAPE.com](mailto:feedback@macroscAPE.com)

## **8.0 Disclaimer**

The materials in this whitepaper are for technical informational purposes only. MacroscapE Solutions Inc. does not guarantee the accuracy or completeness of any information contained herein. While MacroscapE Solutions Inc. has obtained its information from internal and external sources we deem to be reliable, MacroscapE assumes no responsibility for any error or omission, nor shall it be liable but not limited to any downtime and/or lost revenue caused by implementing any of the suggested solutions.

No statement in this whitepaper should be construed or understood as definitive solution of implementing high availability. **MacroscapE strongly recommends the expertise of a network professional when considering implementing any changes in the production environment.**

All reproduction, copy, retransmission or reprinting of all or any portion of this document is encouraged as long as credit is given to MacroscapE Solutions, Inc. where appropriate.

**Cisco, and other third parties mentioned in this whitepaper are registered trademarks of the respected Corporations.**