Matt Tucker

tuckmn1@student.op.ac.nz

Abstract

This document outlines the WAN design for our companies’ network. It includes evidence of choices made, and configuration files for each device.

Phase 2 WAN Design and implementation

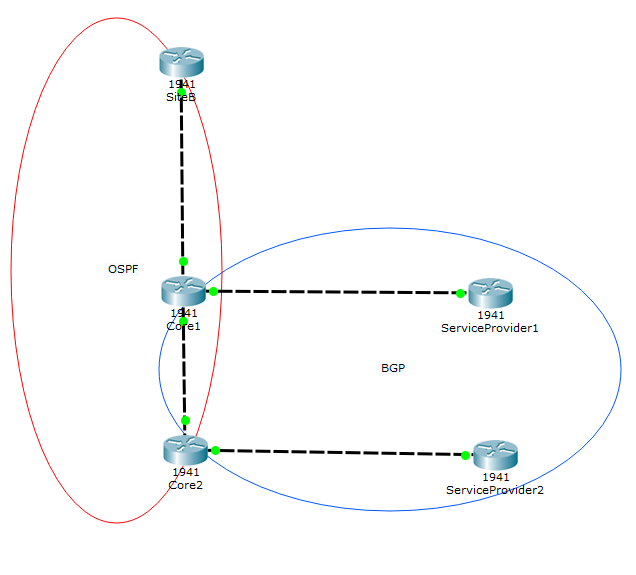
Matt Tucker

# Overview

This document outlines the WAN design for our companies’ network. It includes evidence of choices made, and configuration files for each device.

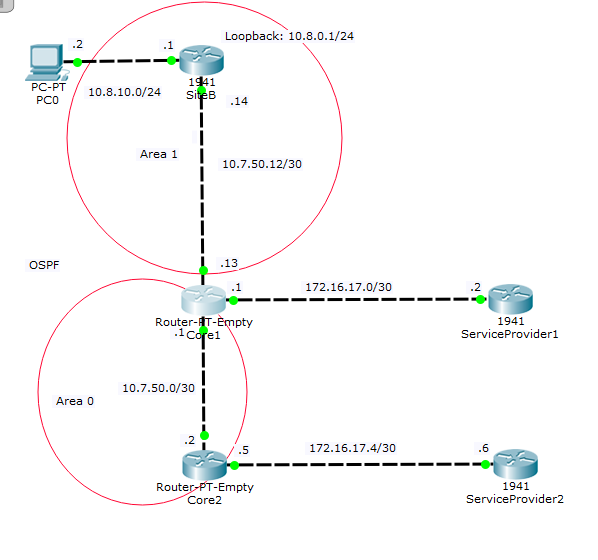
Please refer to Phase One document for the LAN design of the head office.

# Head Office & Site B Physical Topology



MPLS Core

# Logical Topology



# BGP Topology

# 

Site B: Not part of Head Office AS

To stop head office being a transit AS, we apply a route map to both Core 1 and Core 2, that matches on AS-PATH of nothing. If it is a match we advertise the route. If not, the routers have learnt the route from an external AS so will not advertise to other AS’s.

Core 2 prepends 2 more 65007 to AS-PATH so that incoming packets prefer to go via Core 1.

Core 2 has a local preference of 100 (default). Core 1 has a local preference of 200, making it the preferred choice for outgoing packets.

Secondary Path for Incoming and Outgoing packets to ISP

Primary Path for Incoming and Outgoing packets to ISP

# OSPF

Open Shortest Path First (OSPF) will be configured between the gateway routers, distribution switches, and the dark fibre link to Site B. OSPF offers faster convergence and scales to larger network implementations than the older protocol RIP. It is a link state routing protocol (OSPF Design Guide, 2017) that was developed as a replacement for the distance vector routing protocol offered by RIP. RIP uses hop-count as the only metric, which can quickly become problematic, whereas OSPF looks at a number of factors when deciding the best route to take (OSPF Fundamental, 2017). These factors can be customised by the network administration for greater control over network paths.

We will implement multi-area OSPF between the head office and Site B. This will reduce the number of link state advertisements (LSA) flooding the network. The ABR will generate a network summary (type 3 LSA), to send into both areas (Balchunas, 2007). Core 1 router will act as the Area Border Router (ABR). Core 1 will also be the DR by setting the ip ospf priority on all internal interfaces to 5. Core 1 has been chosen as the DR because it is the ABR and the priority connection to the service provider.

Splitting the Head Office and Site B into two different areas has the following benefits:  
(OSPF Design Guide, 2017)

* Smaller routing table, as networks can be advertised as a summary.
* Smaller Link State Database (LSDB), as routers only need to know their area.
* Reduced SPF algorithm calculations, as an ABR only needs to run the SPF algorithm when there is a change an associated area.

Our Head Office site is going to act as our backbone area, or Area 0. Site B will be Area 1. To further reduce the flooding on LSA’s we are making Site B a stub area. This will stop Area 1 receiving Type 4 and 5 LSA’s (Balchunas, 2007). This is appropriate as there is only a single point of entry to and from the area, and no ASBR inside the area (Lesson 3 Stub Areas, 2017). The ABR will automatically advertise the default route (with a cost metric of 1) into the stub area.

Using another router as the ABR was considered, however it was determined that due to a relatively low number of employees, a single router acting as the ABR, and part of the Head Office network, would easily meet our requirements.

OSPFv4 is being used in our network as we are using IPv4 as our IP protocol. A further advantage of OSPF is that MD5 can be implemented, to improve network security. This means that routers will only accept OSPF updates from peers with the same pre-shared password.

# BGP

## What is BGP?

Border Gateway Protocol (BGP) is an exterior routing protocol. It allows routers to send packets to router in different networks / Autonomous Systems (AS) (Understanding BGP, 2017). BGP uses TCP as the transport protocol, on port 179 (BGP Case Studies, 2008). This allows BGP routers to peer with other BGP routers that are more than one hop away – provided the hop count is increased with external BGP (this does not effect us).

Before BGP routers can exchange routing information, the routers must become BGP neighbours/peers. Once a BGP peer is established, the peer initially exchanges full BGP routing tables (Balchunas, 2007). After this, the peers send incremental updates as the routing table changes, for example: a new network being advertised with BGP (BGP Case Studies, 2008). All BGP neighbours keep the same version number of the BGP table, which increments whenever the routing information changes (BGP Case Studies, 2008).

Internal BGP is when routers are peers within the same autonomous system. External BGP is where routers are peered from different AS’s. In our network, we will use internal BGP to peer the two core routers to each other, and external BGP to peer the core routers to the ISP routers.

## Head Office Setup

Our Head Office Site is connected to every other site in our company (excluding Site B), using BGP into an MPLS service provider network. The aim is to be able to see each remote site in our route table, and advertise Site B and Head Office network to the other sites.

As we have two connections to our service provider, but want only 1 of those connections to be used for both incoming and outgoing traffic, we need to apply some BGP policy. The secondary link must be able to take over in the case of an outage.

Core 1’s link to the service provider is the primary link that will be used for incoming and outgoing traffic. In order to make Core 1 the preferred link for outgoing traffic, we have decided to set the default local-preference of Core 1 to be 200. This is greater than the default local-preference of Core 2 (100), so Core 1 will be used for all outgoing traffic (Balchunas, 2007).

To make Core 1 the primary path for incoming traffic, we need to use AS-PATH prepending on Core 2. This will make Core 2 be the least preferred option when deciding whether to send traffic to Core 1 or 2. To do this we created a route map, and matched any as-path that originated in the Head Office network. We then prepended two more instances of the AS 65007 to all outgoing traffic.

We do not want the Head Office site to be a transit site for any of other sites. In order to stop this happening, we have chosen to only advertise networks that originate in the Head Office AS. We do this by creating a route map on both Core 1 & 2 that matches an as-path access list. This access list uses a regular expression to check that the as-path contains nothing (therefore originating locally). The route map denies by default any other paths that may want to be advertised.

# Frequently Asked Questions

## Assumptions

There are very few assumptions with this project. The specifications are well documented. The only assumption we are making is about company growth. We have planned for the foreseen growth, but any large increase in numbers might have an effect on the network (unlikely however).

## Constraints

As we are using an MPLS core, we have no say over how the packets are routed once they reach the core. However, we are confident the service provider can meet our needs.

## Security

We are using password protected connections for BGP and OSPF. We will ensure that passwords are of sufficient strength for any we define.

## Scalability

By using an ISP MPLS core, we can add as many new company sites as we desire without any effect on other sites.  
Our head office site setup has been designed for continual growth. As technology needs continue to increase there will come a time when we might choose to use a Fibre connection to the ISP. When this happens, we will need to ensure that our OSPF routing is calculating cost correctly and that our hardware has gigabit ports which can handle the increased speeds.

## Administration & Support

Head office has a management network configured on all devices so that config can be accessed only by those authorised. Once the network build has been completed we will provide a dedicated, on-call service representative should any issues arise.

# Work Log

29/09/17 – Started researching BGP. (2hrs)

3/10/17 – Drew a physical and logical network schema out by hand. Created more available networks where required. Started building example network in packet tracer. (2hrs)

5/10/17 – 12/10/17 – Began documentation. Took screen shots of topologies. Started writing down router config for the network. Completed further research. (6hrs)

13/10/17 – Consulted with Michael about implementing BGP and to resolve some OSPF issues. Continued with documentation.

15/10/17 – Continued with documentation. (1hr)

22/10/17 – Tested BGP config in VIRL. – Will need to do again as config file didn’t push to github. (4hrs)

25/10/17 – Continued with documentation. Getting references written down correctly. Looked into OSPF stub areas and implemented it in my network design. (3hr)

27/10/17 – Spoke to Michael about final few questions. Added password security to BGP connections. (1hr)

28/10/17 – Finished writing report. Added company questions. Handed in report. (2hr)

## Core1:

**Interface Config**

int g0/0

ip address 10.7.50.0 255.255.255.252

no shut

int g0/1

ip address 10.7.50.1 255.255.255.252

no shut

int g0/2

ip address 10.7.50.13 255.255.255.252

no shut

int g0/3

ip address 172.16.17.2 255.255.255.252

no shut

int lo0

ip address 1.1.1.1 255.255.255.255

int range g0/0-2

ip ospf priority 5

**OSPF Config:**

router ospf 1

router-id 1.1.1.1

log-adjacency-changes

area 1 range 10.8.0.0 255.255.0.0

network 10.7.50.9 0.0.0.0 area 0

network 10.7.50.1 0.0.0.0 area 0

network 10.7.50.13 0.0.0.0 area 1

area 0 authentication message-digest

area 1 authentication message-digest

area 1 stub

exit

int g0/0

ip ospf message-digest-key 1 md5 P@ssw0rd

int g0/1

ip ospf message-digest-key 1 md5 P@ssw0rd

int g0/2

ip ospf message-digest-key 1 md5 P@ssw0rd

**BGP Config:**

router bgp 65007

no sync

bgp router-id 1.1.1.1

neighbor 2.2.2.2 remote-as 65007

neighbor 2.2.2.2 update-source lo0

neighbor 2.2.2.2 next-hop-self

neighbor 2.2.2.2 password BGP-P@ssword

neighbor 172.16.17.2 remote-as 4700

neighbor 172.16.17.2 password ISP-P@ssword

network 10.7.0.0 mask 255.255.0.0

network 10.8.0.0 mask 255.255.0.0

bgp default local-preference 200

neighbor 172.16.17.2 route-map LOCAL-ONLY out

route-map LOCAL-ONLY permit 10

match as-path 1

ip as-path access-list 1 permit ^$

## Core2:

**Interface Config**

int g0/0

ip address 10.7.50.5 255.255.255.252

no shut

int g0/1

ip address 10.7.50.2 255.255.255.252

no shut

int g0/3

ip address 172.16.17.5 255.255.255.252

no shut

int lo0  
ip address 2.2.2.2 255.255.255.255

**OSPF Config:**

router ospf 1

router-id 2.2.2.2

log-adjacency-changes

network 10.7.50.2 0.0.0.0 area 0

network 10.7.50.5 0.0.0.0 area 0

area 0 authentication message-digest

area 1 stub

exit

int g0/0

ip ospf message-digest-key 1 md5 P@ssw0rd

int g0/1

ip ospf message-digest-key 1 md5 P@ssw0rd

**BGP Config:**

router bgp 65007

no sync

bgp router-id 2.2.2.2

neighbor 1.1.1.1 remote-as 65007

neighbor 1.1.1.1 update-source lo0

neighbor 1.1.1.1 next-hop-self

neighbor 1.1.1.1 password BGP-P@ssword

neighbor 172.16.17.6 remote-as 4700

neighbor 172.16.17.6 password ISP-P@ssword

neighbor 172.16.17.6 route-map LOCAL-ONLY-PREPEND out

network 10.7.0.0 mask 255.255.0.0

network 10.8.0.0 mask 255.255.0.0

route-map LOCAL-ONLY-PREPEND permit 10

match as-path 1

set as-path prepend 65007 65007

ip as-path access-list 1 permit ^$

## SiteB

**Interface Config:**

Int g0/0

ip address 10.7.50.14 255.255.255.252

ip ospf priority 0

no shut

int g0/1

ip address 10.8.0.1 255.255.255.0 #(example address to represent link to site B network)

no shut

**OSPF Config:**

router ospf 1

router-id 5.5.5.5

log-adjacency-changes

network 10.8.10.1 0.0.0.0 area 1

network 10.8.0.1 0.0.0.0 area 1

network 10.7.50.14 0.0.0.0 area 1

# References

Balchunas, A. (2007). *Open Shortest Path First v1.31*. Retrieved From: http://www.routeralley.com/guides/ospf.pdf

Balchunas, A. (2007). *Border Gateway Protocol v2.01*. Retrieved From: http://www.routeralley.com/guides/bgp.pdf

BGP Case Studies. (2008). *Cisco*. Retrieved from: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html#howbgpwork

Lesson 3 Stub Areas. (2017). *IN723*. Retrieved From: Otago Polytechnic I: Drive.

OSPF Design Guide. (2017). *Cisco*. Retrieved From: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

OSPF Fundamental. (2017). *Computer Networking Notes****.*** Retrieved From: https://www.computernetworkingnotes.com/ccna-study-guide/ospf-fundamental-terminology-explained.html

Understanding BGP. (2017). *Juniper Networks*. Retrieved From: https://www.juniper.net/documentation/en\_US/junos/topics/concept/bgp-routing-overview.html