CE321 Network Engineering Assignment

Dr. M. Reed v5.2

Submission details (one document, one Packet Tracer file):

You will submit a SINGLE word processed document in one of the following formats:

- Word format (.doc or .docx)
- Portable document format (PDF)

You may either edit this document with the required information (and append answers to the parts you are asked to write), or write your own document containing the required information.

Submission should be on Faser by the deadline shown in Faser.

The parts that you need to fill in, or content to append, are:

- Complete the fields in Table 1
- Complete the fields in Table 2
- Include **only** the configurations and **certain** command outputs specified in Task 6.
- Append the explanation for Task 7.

Additionally, you must submit your working Packet Tracer file with the **same** configuration as that used for the output given in Task 6.
You MUST use Packet Tracer 8.0.1 (or later) for this assignment, it is available for download in Windows/Linux/OS X from the CE321 Moodle page. You must use the provided scenario.pkt file available from the CE321 Moodle page.

Marks will be awarded as follows (marks in Task 1-6 are in proportion to the correct configuration and documentation):

- 5% for Task 1 (Table 1 and Table 2)
- 10% for Task 2 (Basic device configuration)
- 35% for Task 3 (OSPF and router features) (of which 15/40 marks are for extension work, see below in Task 3)
- 15% for Task 4 (Switching and VLAN configuration)
- 10% for Task 5 (Access Control Lists)
- 5% for Task 6, Documentation and correct submission of Packet Tracer file.
- 20% for Task 7, Explanation of recovery of routing and switching after failure of primary DS switch (DS1 or DS2). 5/20 of these marks will be for good presentation including use of English and appropriate use of references. See the table in Task 7 for the marking scheme for this task.

NOTE: this document is a generic description for the whole group. Every student also has a unique combination of IP address ranges, VLAN identifiers and sizes of LANs distributed through the CE321 course pages. Under no circumstances should you use values allocated to another student – doing so will give rise to an investigation of plagiarism. You will find your own individual settings on the CE321 course page using your registration number as a key to your individual page.

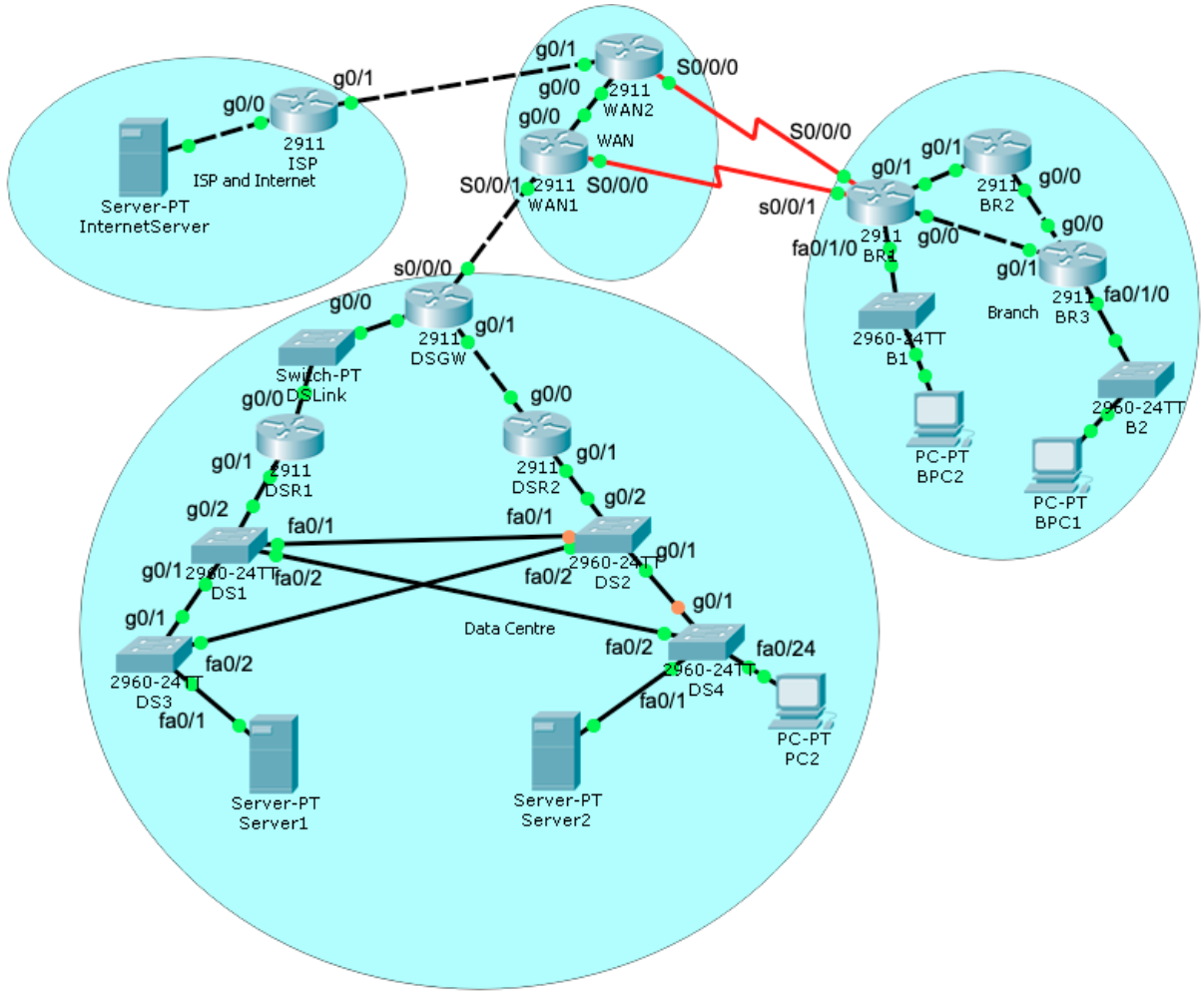

Figure 1 Assignment topology

Scenario

You are to configure the routing and switching for part of the company network shown in Figure 1, in particular the wide area networking routing (including Branch and Data Centre gateways) and the switching for the Data Centre. Some of the systems are pre-configured. You must complete this assignment using Cisco Packet Tracer version 8.0.1 (or later). Some of the assignment (e.g some IP addresses) is specified exactly, but other parts you will have to make sensible design choices based on the scenario as described here and the methods you have learnt from the lab tasks. You are **highly recommended** to use the version of Packet Tracer available on the Moodle page as it is compatible with that from the laboratory.

You will find that the following devices are already configured and **you should not** change their configuration: InternetServer, ISP, B1, B2, BPC1, DSLink.
You can see the configuration of these devices by either using username and password “donotconfigureme” or by exporting the running configuration from the Config tab. The switches, B1, B2 and DSLink, are just running default switching without any VLANs.

You **must** configure the rest of the devices.

All links are operating at the line speed of their interfaces except for the following:

Network name of link (see Table 1 below)	Line rate
DSGW1 (including DSLink)	100 Mb/s (due to DSLink)
BRWAN1	2 Mb/s
BRWAN2	128 kb/s
WANDS	2 Mb/s

The scenario only shows part of the company network, you are to assume that the actual network is very large with many branches (not shown). All the branches connect to the WAN and access the Internet through WAN2.

There is a placeholder for the Internet (InternetServer) accessed through an Internet Service Provider. The router ISP is a placeholder for the Internet Service Providers network. ISP provides one public IP address for the whole company to use (202.202.202.2 on WAN2). The company hosts should be able to access Web servers in the Internet, however, it is not necessary for the Internet to access any hosts in the company network (and in fact the ACLs you will implement will block this traffic).

The data centre needs to have a highly-reliable design and you will note that it has two systems (routers, switches and servers) so that it can cope with a single failure. PC2 is a placeholder for management terminals and only one is shown. There are only two servers and access switches (DS3 and DS4) shown although you should assume there are many more systems to be connected to DS3 and DS4 in the future and not shown. There are no clients or servers directly connected to the distribution layer switches (DS1 and DS2). You should configure the networking so that if there is a failure of any **single** switch, or either router DSR1 or DSR2, then any host will still have network connectivity without any need for manual intervention. You will need to look back at CE231 content to remind you how to allow multiple routers to act as a gateway. (You should assume that DSGW is a highly-fault tolerant router with dual systems and connectivity that are not shown.)

On the Access switches (DS3, DS4), the lower half of the ports (fa0/1-12) are to be allocated to VLAN S, the upper two of the ports (fa0/23-24) are to be allocated to VLAN C. VLAN M is for managing the switches and routers. Other ports are free. All ports not actually connected to a device should be shutdown. VLANs and switch port configuration were covered in CE231.

The company network manager has specified that you use OSPF for routing and to ensure it is configured to route traffic across the whole network and has basic security by limiting where OSPF traffic can be sent/received from to only essential interfaces.

For the OSPF *extension work*:

- OSPF should be reconfigured to be multi-area, the ABRs must be BR1 and DSGW;
- network addresses (routes) between areas must be summarised using a **single** address that is the **smallest** possible summary address to encompass the networks you have been allocated (you are to assume addresses in the summary not used in your scenario are available for expansion at a future date). You will need to find out about this as it is not covered in the Cisco courseware;
- OSPF costs must be correct to allow routing over the fastest path where this is relevant. As the “auto-cost reference bandwidth” command does not work in Packet Tracer link costs must be set manually.

Note that this extension work will require you to look carefully at the multi-area OSPF Packet Tracer Lab example and to carry out your own research in order to complete it. It is **not** covered by the Cisco courseware in any depth.

Task 1: Complete the Addressing Scheme.

The addressing scheme for the network is partially complete, but you will need to allocate the **network addresses** that are blank in Table 1 according to the ranges allocated to you from your individual settings page on Moodle. Fill any blanks or single letters with values that you have been allocated; fill in the WAN addresses marked with "?" using the range allocated to you. Some blank fields will require you to work out suitable values. Any non-applicable fields marked N/A should not have entries.

Document all subnet addresses in Table 1. **Remember that in Table 1 any interfaces with the same Network Name MUST have the same subnet address! For example BR1 G0/0 and BR3 G0/1 are both connected to BR13 and thus have the same subnet. Make sure this applies to the subnets you are allocating (they have been coloured the same to emphasise that they should be the same subnet.**

Table 1

Device	Interface	Network Name	Number of Hosts	Subnet	Subnet Mask
Branch					
BR1	G0/0	BR13	2	10.1.1.128	255.255.255.252
	G0/1	BR12	2	10.1.1.132	255.255.255.252
	VLAN 1 (Fa0/1/0)	BR1LAN	254	10.1.36.0	255.255.255.0
	S0/0/0	BRWAN2	2	172.16.29.120	255.255.255.252
	S0/0/1	BRWAN1	2	172.16.29.124	255.255.255.252
BR2	G0/1	BR12	2	10.1.1.132	255.255.255.252
	G0/0	BR23	2	10.1.1.136	255.255.255.252
BR3	VLAN 1 (Fa0/1/0)	BR3LAN	254	10.1.0.0	255.255.255.0
	G0/1	BR13	2	10.1.1.128	255.255.255.252
	G0/0	BR23	2	10.1.1.136	255.255.255.252
WAN					
WAN1	S0/0/1	WANDS	2	172.16.29.128	255.255.255.252
	G0/0	WAN12	2	172.16.29.132	255.255.255.252
	S0/0/0	BRWAN1	2	172.16.29.124	255.255.255.252
WAN2	G0/0	WAN12	2	172.16.29.132	255.255.255.252
	G0/1	ISP	2	202.202.202.0	255.255.255.252
	S0/0/0	BRWAN2	2	172.16.29.120	255.255.255.252
ISP and Internet					
ISP	G0/0	Internet	254	155.245.0.0	255.255.255.0
	G0/1	ISP	2	202.202.202.0	255.255.255.252
Data Centre					
DSGW	S0/0/0	WANDS	2	172.16.29.128	255.255.255.252
	G0/0	DSGW1	2	192.168.0.0	255.255.255.252
	G0/1	DSGW2	2	192.168.0.4	255.255.255.252
DSR1	G0/0	DSGW1	2	192.168.0.0	255.255.255.252
	G0/1.S	DSS	254	192.168.61.0	255.255.255.0
	G0/1.C	DSC	254	192.168.91.0	255.255.255.0
	G0/1.M	DSM	254	192.168.121.0	255.255.255.0
DSR2	G0/0	DSGW2	2	192.168.0.4	255.255.255.252
	G0/1.S	DSS	254	192.168.61.0	255.255.255.0
	G0/1.C	DSC	254	192.168.91.0	255.255.255.0
	G0/1.M	DSM	254	192.168.121.0	255.255.255.0

Document router/switch interface and PC addresses in Table 2 (these should match the network addresses you assigned in Table 1). Note that interfaces *in italic like this* have already been configured for you. **Make sure where two interfaces are on the same Network you allocate compatible and different IP addresses (again those you are allocating in the same subnet have been coloured the same to help you).**

Table 2

Device	Interface	Network Name	IP Address	Subnet Mask	Gateway
BR1	*G0/0*	*BR13*	*10.1.1.129*	*255.255.255.252*	N/A
	G0/1	*BR12*	*10.1.1.133*	*255.255.255.252*	N/A
	VLAN 1 (Fa0/1/0)	BR1LAN	10.1.36.254	255.255.255.0	N/A
	S0/0/0	BRWAN2	172.16.29.121	255.255.255.252	N/A
	S0/0/1	BRWAN1	172.16.29.125	255.255.255.252	N/A
BR2	*G0/1*	*BR12*	*10.1.1.134*	*255.255.255.252*	N/A
	G0/0	*BR23*	*10.1.1.137*	*255.255.255.252*	N/A
BR3	*VLAN 1 (Fa0/1/0)*	*BR3LAN*	*10.1.0.254*	*255.255.255.0*	N/A
	G0/1	*BR13*	*10.1.1.130*	*255.255.255.252*	N/A
	G0/0	*BR23*	*10.1.1.138*	*255.255.255.252*	N/A
WAN1	S0/0/1	WANDS	172.16.29.129	255.255.255.252	N/A
	G0/0	WAN12	172.16.29.133	255.255.255.252	N/A
	S0/0/0	BRWAN1	172.16.29.126	255.255.255.252	N/A
WAN2	G0/0	WAN12	172.16.29.134	255.255.255.252	N/A
	G0/1	*ISP*	*202.202.202.2*	*255.255.255.252*	202.202.202.1
	S0/0/0	BRWAN2	172.16.29.122	255.255.255.252	N/A
ISP	*G0/0*	*Internet*	*155.245.0.254*	*255.255.255.0*	N/A
	G0/1	*ISP*	*202.202.202.1*	*255.255.255.252*	N/A
DSGW	~~S0/0/1~~ S0/0/0	WANDS	172.16.29.130	255.255.255.252	N/A
	G0/0	*DSGW1*	*192.168.0.1*	*255.255.255.252*	N/A
	G0/1	*DSGW2*	*192.168.0.5*	*255.255.255.252*	N/A
DSR1	*G0/0*	*DSGW1*	*192.168.0.2*	*255.255.255.252*	N/A
	G0/1.S	DSS	192.168.61.1	255.255.255.0	N/A
	G0/1.C	DSC	192.168.91.1	255.255.255.0	N/A
	G0/1.M	DSM	192.168.121.1	255.255.255.0	N/A
DSR2	*G0/0*	*DSGW2*	*192.168.0.6*	*255.255.255.252*	N/A
	G0/1.S	DSS	192.168.61.2	255.255.255.0	N/A
	G0/1.C	DSC	192.168.91.2	255.255.255.0	N/A
	G0/1.M	DSM	192.168.121.2	255.255.255.0	N/A
DS1	VLAN M	DSM	192.168.121.11	255.255.255.0	
DS2	VLAN M	DSM	192.168.121.22	255.255.255.0	
DS3	VLAN M	DSM	192.168.121.33	255.255.255.0	
DS4	VLAN M	DSM	192.168.121.44	255.255.255.0	
InternetServer	*NIC*	*Internet*	*155.245.0.1*	*255.255.255.0*	*155.245.0.254*
BPC1	*NIC*	*BR3LAN*	*10.1.0.1*	*255.255.255.0*	*10.1.0.254*
BPC2	NIC	BR1LAN	10.1.36.1	255.255.255.0	10.1.36.254
Server1	NIC	DSS	192.168.61.11	255.255.255.0	
Server2	NIC	DSS	192.168.61.22	255.255.255.0	
PC2	NIC	DSC	192.168.91.11	255.255.255.0	

Task 2: Configure basic device settings.

Configure the routers and switches that you have been told to configure according to the following guidelines:

- Routers and switches should be secured against unauthorised access and passwords should be stored in a secure manner. Use only the password “cisco” in your configurations.
- There is no DNS server in the network.
- Configure a message-of-the-day banner that warns against unauthorized use and states “This router is managed by 0123456”, where 0123456 is **replaced with your registration number**.
- Console input should not be broken with console output messages.
- Any systems that you configure should be capable of being remotely managed using the most secure manner possible. (The systems that you should not configure have not been, and should not be, configured for remote management).

Task 3: Configure routing and router features.

Configure the routing and router features to meet the requirements in the scenario using your judgment to make sensible decisions. You should note that the company network is using a private address space that is not allowed to be used in the Internet. These basic OSPF and other routing settings are worth 20/35 of the marks in this task.

Extension work
The extension work is worth 15/35 of the Task 3 marks. While not strictly optional, be aware that you will need to do some self-study and spend some time to complete this part properly.

This extension work requires you to find out how to implement the multi-area OSPF with correct routing costs as described below, and then implement the features in your scenario. The laboratory experiments or lecture slides do not contain enough detail to show you how to implement them. The features are:

- OSPF should be reconfigured to be multi-area, the area border routers (ABRs) must be BR1 and DSGW;
- network addresses (routes) between areas should be summarised using a single address that is the smallest possible summary address to encompass the networks you have been allocated (you are to assume addresses in the summary not used in your scenario are available for expansion at a future date);
- costs should be correct to allow routing over the fastest path where this is relevant. As the “auto-cost reference bandwidth” command does not work in Packet Tracer, link costs **must** be set manually to their correct values.

The extension work only requires changes to the OSPF settings, all other settings can be kept the same.

Note that this extension work will require you to look carefully at the multi-area OSPF Packet Tracer Lab example and to carry out your own research in order to complete it. It is not covered by the Cisco courseware in any depth.

Task 4: Configure switching

Configure switching as specified in the scenario using your judgement to make sensible decisions.
Configure clients and servers.
Test full connectivity (e.g. company hosts can access the Internet).

Task 5: Access Control Lists

Configure ACLs to implement the following policy:

- The whole company network should allow HTTP/HTTPS traffic from the company to the Internet and related HTTP/HTTPS traffic back in. *i.e.*, any company users or systems should be able to browse the Web in the Internet. But all other traffic to/from the Internet should be blocked.
- Traffic should be allowed to move freely within the company network **except** for the following policy for the Branch network which should:
  - allow access to any TCP server in the company network from Branch hosts;
  - allow users in Branch to browse the Web in the Internet (as specified in the first policy point);
  - allow PC2 (a system administrator) to connect to any hosts in Branch using SSH to manage the systems;
  - allow any OSPF traffic;
  - block any other traffic *i.e.*, systems outside of Branch should not be able to initiate TCP connections into Branch.

Task 6: Document *certain* specified parts of the configurations and include in your submitted document.

You **must not** include all the running configurations in your submitted document. Instead you should **only show the items below from the running configurations:**

- the "router OSPF" block of the running configuration for the routers DSGW and BR1
  - *i.e.*, the router block from the output `show running-config | begin router`
- interface specifications for configured interfaces on routers DSR1 and DSR2
  - *i.e.*, the interface settings from `show running-config | begin interface`
- the complete running configuration of WAN2
  - *i.e.*, the output of `show running-config`
- any ACLs by specifying the router they are running on and showing the ACLs and the relevant interface configurations
  - to show interfaces config use `show running-config | begin interface`
  - to show ACLs use `show running-config | begin access-list`

Additionally, you **must** show the output of the following command:

- the output of `show ip route` on DSGW and BR1

For the first **four** items above (the parts of the running configurations), add comments describing the significant features in the configuration using the "!" symbol at the start of a comment line and by using the `description` command for all interfaces and a `remark` for ACLs.

```
The configurations and command output should be in a fixed width font
such as this. If you are simply using this document as a template you
can paste the necessary output here (with a suitable title before
each one).
```


IT IS VITAL THAT YOUR PACKET TRACER FILE CONTAINS THE SAME CONFIGURATIONS THAT YOU SUBMIT IN THE DOCUMENT. ANY FAILURE TO DO SO WILL MEAN ZERO MARKS FOR THE DOCUMENTATION PART AND THE MARKER MAY TAKE THE LOWER OF THE FUNCTIONALITY IN EITHER OF THE CONFIGURATIONS. IF YOU SIMPLY DUMP WHOLE CONFIGURATIONS, NOT IN THE LIST ABOVE, IN YOUR SUBMITTED DOCUMENT YOU WILL SCORE ZERO FOR DOCUMENTATION.

Task 7: Explain switching and routing recovery after failure of either switch DS1 or DS2

You have implemented a resilient design in the Data Centre. If either switch DS1 or DS2 fails it should still be possible for an external host such as BPC1 to contact a server without any manual intervention.

From Server 1 ping WAN2 (or another device outside the Data Centre) and determine which **router** (DSR1 or DSR2) is used to send the packet beyond the Data Centre using your design. Once you have determined this you must consider what happens when the neighbouring switch fails; *i.e.* if DSR1 is the router to send the packet to DSGW then consider what happens when DS1 fails.

Describe the recovery from failure by explaining how the routers and switches handle the failure. You should describe the protocols that are used to recover from the failure and how they operate **in the context of your network**. You do not need to give details of exact messages as there are too many involved; however, you should explain in general terms the messages needed to recover from the failure.

It is recommended that you attempt this part even if you do not have a complete network design. You will still receive marks for the description.

You should aim for approximately two sides for this explanation (not including any diagrams) and it should not contain unnecessary background information. It should read as a self-contained document and have a suitable structure (i.e. an introductory paragraph and a closing paragraph). You **must** use references for sources that support your description and would give more information to the reader – an example might be the standards documents for protocols (e.g. RFCs) and/or a textbook. **Web references are not suitable.** However, IETF RFC's are allowed (even though they are normally distributed via the web).

Mark Task 7	Task 7 Guideline attributes
100% (20/20)	Full description in the switching and routing layers of the recovery after failure. The necessary protocols are fully described using examples from the network. The description is written to a professional standard with excellent grammar and has full list of citations to authoritative sources for each system or protocol.
70% (14/20)	A good description in the switching and routing layers of the recovery after failure. The necessary protocols are described in some depth using examples from the network. The description is written to a professional standard with good grammar and has good list of citations to authoritative sources.
60% (12/20)	A good description in the switching and routing layers of the recovery after failure including the necessary protocols using examples from the network; although one of the protocols or systems may be described in less depth. The description is written to a reasonable standard with reasonable grammar and has a list of citations to authoritative sources.
50% (10/20)	A description in the switching and/or routing layers of the recovery after failure with some protocols described using examples from the network. The description is written to a reasonable standard but with some grammatical errors, some citations to, mostly, authoritative sources are given.
40% (8/20)	A description in the switching or routing layers of the recovery after failure with at least one protocol described using examples from the network. The description is

	written to an acceptable standard but with some grammatical errors, some citations are given.
<40% (<8/20)	A failure to describe even one of either the switching or routing layers used for recovery after failure.

Marking Descriptors for Task 7

End of Assignment

