

COIT20264 Network Design

ASSIGNMENT 1

SUBMITTED TO:

Lecturer: Ahmed El-Hadad

Tutor: Ahmed El-Hadad

SUBMITTED BY:

RAMANDEEP (12022599)

Radhika Sharma (12022063)

Selvapriyan (12022187)

Charan Prabhu (12026164)

Executive Summary

The divergent cabling options are coaxial cable, unshielded twisted pair and shielded twisted pair, installation guides with Wireless LAN along with fibre optic cable, unshielded twisted cable, in the network. The DHCP has the packet tracer and the Cisco works at the DHCP, on the routers and switches on which the modelling is based. The abstract positions of the network are not understood or even handled by the packet tracer. Incorporating the system of simulation of network protocol, system of authoring and also assessing the systems are certain components. The application layer protocol having the routing set with, the BDP, OSPF and the RIP supports the modelling, to the limit of embedded web server support.

Table of Contents

Executive Summary	2
Project Goals	4
Project Scope	4
Design Requirements	5
Business goals	5
Business constraints	5
Technical goals	6
Trade-offs.....	6
List of Assumptions	7
Logical Network Design	9
Logical Network Diagram	9
Explanation of logical network design	9
Justification of Logical Network Design	10
IP Addressing and Naming	10
Switching and routing protocols	11
Switching Protocol: STP	11
Routing Protocols: (OSPF)	12
Security mechanism	12
References:.....	14

Project Goals

The network has been deployed with Wi-Fi solutions to meet the requirement. The network has to include the deployment for data and application on the network, such that they can be accessed by the students all over the campus. Hence, a simple IP Network has to be used for the deployment, with convergence in the IP. The requirement of the project also includes setting up the data center for the network such that material for the university can be stored online so that student with distance learning program and off campus students can use them. The application that has to be deployed, should also be accessible by the off campus students. The applications would be hosted in the private data center of the university. The security is also a concern in the network deployment, to prevent any data breach. The deployment of Wi-Fi allows the students to access the internally hosted applications on the campus network. The network would be setup in the main campus of the university, and it could be accessible from their other two campuses in two different cities.

Project Scope

The main challenge in setting up this network was in providing the support to the client in the remote location. The complete infrastructure to provide the high speed internet has to be setup. The deployment of the network has also to be done such that clients from the other campuses of the university can access the network, which was a difficult task, given the remote location and distance between campuses. The Cisco always tried to provide its clients the world class network infrastructure, which was a business challenge in setting up the network. The budget has also been a concern in the network setup in this case. The network has to be setup such that it is fully optimized in the budget, and no wastage of resources are done. The deployment has to consider all the requirements of the client, and hence, the

budget had become an important factor. The security implementation was also a concern in the setup of the network.

Design Requirements

Business goals

- BG1: Improve communications- by using the voice and the video transmitting technology in the A4A Organization.
- BG2: Reduce operating costs- The cost related to the network components by having an efficient network design and cost related to the projects can be reduced by Outsourcing the project.
- BG3: Build partnerships with other private universities and colleges.
- BG4: Expand into worldwide markets across Australia and Southeast Asia.
- BG5: Increase employee productivity by recruiting more member institutions.

Business constraints

- BC1: Budgetary Constraint- A4A is a NGO which runs on public funds. So, A4A has to manage all its expenses such as providing facilities to teachers, operating cost. So, Budget is the top most concern for the A4A organization.
- BC2: Staffing Constraints- As A4A organization uses the public fund. So, A4A organization has to limit the numbers of staff required.

- BC3: Time constraint: The A4A organization can only provide the teachers if someone who is interested in providing the volunteering services is registered with A4A or else it needs some time to organize the staff for the member institutions.

Technical goals

TG1: Scalability- To design the network of A4A organization in such way that if needed in the future, it can be expanded easily or more branches can be connected easily (Cisco Network Academy 2014).

TG2: Availability- To make the network available all the time in order to smoothly run all the applications of the A4A organization.

TG3: Network performance- Manage the load and bandwidth utilization in such a way to provide the best network experience to the staff and member institutions.

TG4: Security- To provide the various security features to the information produced by the A4A.

TG5: Affordability- To provide all the network devices which needs to be used in the network design of A4A.

TG6: Adaptability- The network diagram of A4A organization should adapt the changes in the future if required without affecting the current diagram.

TG7: Usability- Making the services offered by A4A organizations user friendly so that all the members and staff can use the services easily.

Trade-offs

Scalability:	20
Availability:	25
Network performance:	15
Security:	10
Manageability:	5
Usability:	5
Adaptability:	5
Affordability:	15
Total (must add up to 100):	100

The trade-offs have been set according to the requirement of the A4A logical network design. The Scalability, Availability, Affordability and network performance has given the high priority because the services which are offered by A4A must be available, affordable, performable and scalable at all the times.

List of Assumptions

- The members of the private colleges and universities would be 100-200 (users).
- Academic and experienced professional would be 50 to 60.

User communities:

User community Name	User community Users	User community Location	Application used by User community
A4A staff	6	Sydney	Mail, video conference, Web applications
A4A staff	4	Singapore	Mail, video conference, Web applications
Private Universities and Colleges	100-200	Australia, Southeast Asia	Mail, video conference, Web application
Academic and Experienced Professionals	50-60	Australia, Southeast Asia	Mail, video conference, A4A information system

Data Store:

Data Store	User community Users	User community Location	Application used by User community
Database server	A4A staff members	Australia	Database system
E-mail Server	A4A staff members, Volunteers registered with A4A	Australia	E-mail
Application server	A4A staff, Private Universities and Colleges, Academic and Experienced Professionals registered with A4A	Australia	Web application, A4A information system

Traffic load:

	Web Application KB/Sec	Video Conference KB/Sec	E-mail KB/Sec
A4A	256 kbps	512 kbps	128 kbps
Private Universities and Colleges	256 kbps	512 kbps	128 kbps
Academic and Experienced Professionals	256 kbps	Not needed	128 kbps

The speed required for video conference is kept high to provide the uninterrupted Quality of Service and for the rest such as email which and web application are assigned with the required speed based on the requirements of the applications used by the members and staff of A4A.

Logical Network Design

Logical Network Diagram

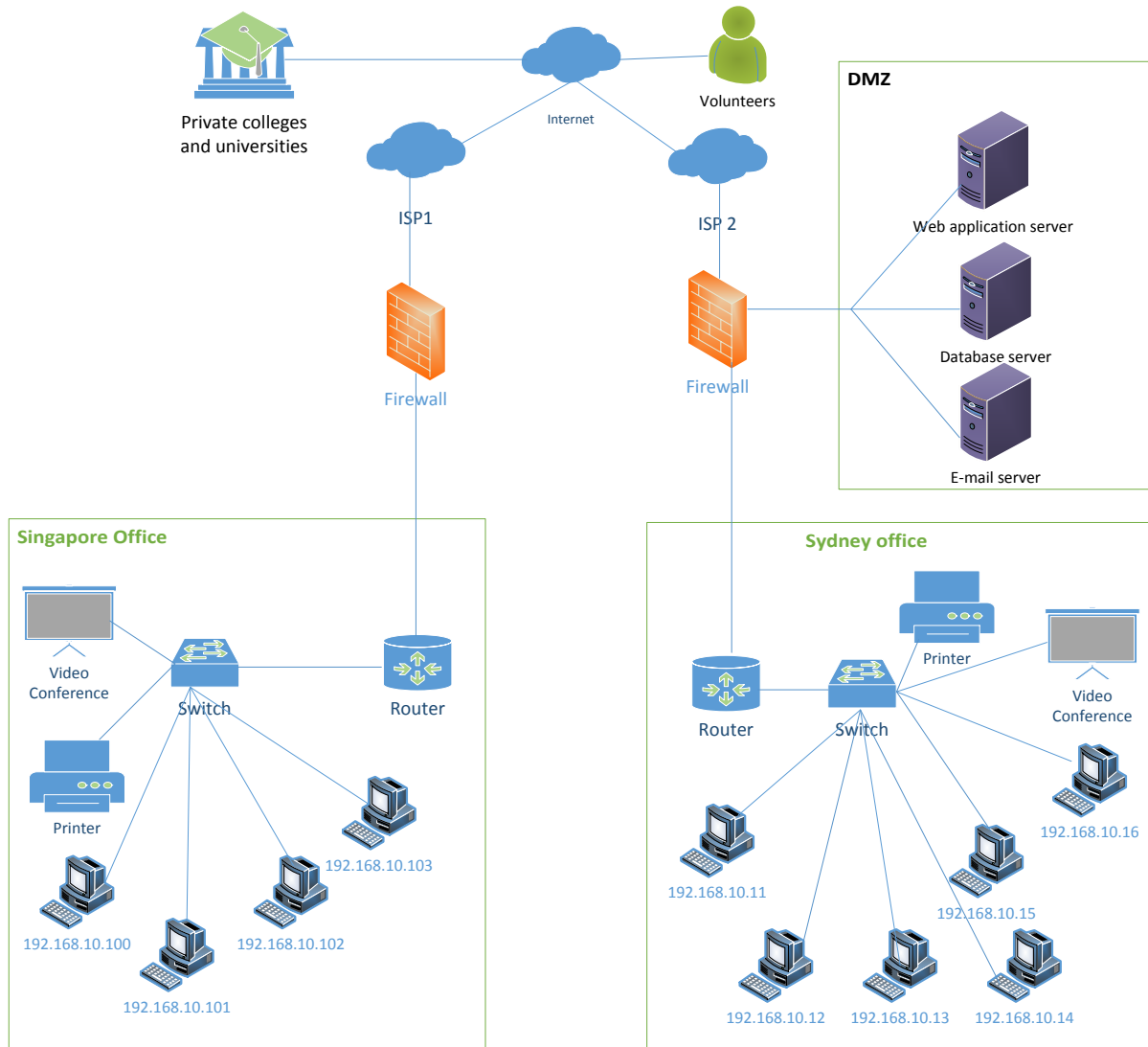


Figure: 3.1 Logical Network diagram

Explanation of logical network design

The logical network design is formed by using the top down hierarchical topology. The Head office situated in Sydney is connected to the branch office in Singapore. There are total two different ISP's connected to the branch office via a router. The DMZ (Demilitarized Zone)

prevents the intrusion or leakage of data and acts as a gate between the ISP's and the branch office to separate the A4A organization private resources and blocking the external users access to data and internal server. The data center includes the services like web services, email, web security appliances. Here, the Access layer starts, where the router then connects to the switches. The users are connected via switches and other devices at the access layer.

Justification of Logical Network Design

A separate core made it possible to scale the size of the A4A organization in such a way that it would minimize the complexity when the size of the A4A organization would grow in the future. The two ISP's are used to prevent the network from going down and provides the high Availability to the network. If there is a problem at one ISP end then another ISP say ISP 2 can be used to keep the services running smoothly. Furthermore, a DMZ is used to provide the control and security to the network servers of A4A organization. It will prevent the intrusion by separating the data center or by not giving the direct access of the services to the external users. Moreover, a switch is used to connect to the PC terminals and several other devices such as printer, video conference etc.

IP Addressing and Naming

In the case of public or private addressing, the public addressing is chosen. And in the case of choosing between static vs dynamic addressing, our design is using dynamic addressing.

Class C IP addresses starting from the IP address range 192.168.10.1/24 is used because A4A is a small organization and for small organization class C addresses are better.

User Name	IP Addresses range	IP address	IP Name
Head office	192.168.10.1/24 192.168.10.100/24	192.168.10.10	www.Aggroup.com
Branch office	192.168.10.100/24 192.168.10.199/24	192.168.10.145	www.branchgroup.com
Servers, staff	192.168.10.199/24 192.168.11.49/24	192.168.11.45	www.Forserver.com

Switching and routing protocols

Switching Protocol: STP

Based on the network traffic characteristics, security and its capability to adapt to changes in the inter-network, the spanning tree protocol STP is more appropriate switching protocol. When a packet is sent, and when there are more possibilities of switches to send the packet to destination, sometimes it kind of forms an endless loop to reach the destination, which is called switching loops (shown in figure.).

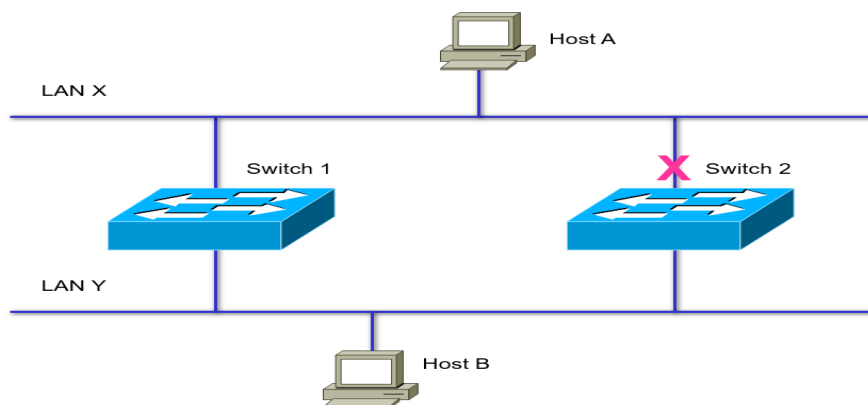


Figure: 7.1 STP to prevent loops

So, here the spanning tree protocol allow us to avoid the switching loops and allows the redundancy helping whenever a switch goes down, it takes the backup from the switch while servicing the switch to make it up and running,

Routing Protocols: (OSPF)

As, the name states “the routing protocols,” the routing protocols allows routers to dynamically learn on how to reach other networks. And these protocols allow to exchange information of the system with other routers or hosts.

Selecting a routing protocol is difficult because of wide range of protocols being available. So, out of all the protocols, based on the trade-offs such as scalability, availability, Adaptability, OSPF is chosen as a routing protocols.

Open Shortest Path First (OSPF)

- Link state routing protocol
- Uses Shortest Path First or Dijkstra Algorithm
- Metric: Cost
- Required numbers of hop count and ability to scale if required.
- Uses Areas
- Standard compatible protocol.

Security mechanism

- The firewall is used which allows only authorized users.

- The use of IPS (Intrusion Prevention System) and IDS (Intrusion Detection System).
- Use of Anti-virus software.
- Regular updates of all the application used by the A4A organization.
- Use of VPN software to do wireless networking.
- The server is placed in a DMZ that would be protected by a firewall.

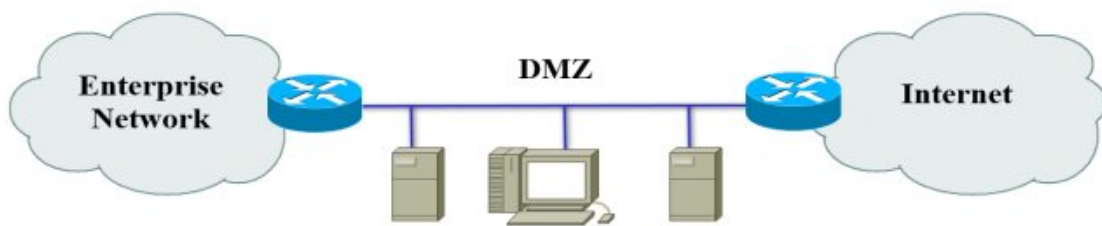


Figure: 8.1 DMZ security feature

The hardware that has been used in the network setup are all manufactured by CISCO. The hardware that has been used include:

1. Wireless controllers for the 300 APs:
Cisco 6509E Switch with WiSM
2. Security Device for central authorization and authentication on the network:
Cisco ACS server
3. The network security with firewall of Cisco ASA 5550 Firewall. It has a throughput of 1Gpbs
4. The routers in the network with BGP links: Cisco 7206 routers
5. The switched in the network for branching and connection to multiple devices: 10 Gigabit Switched Backbone
6. The other switched for connections: 2960 series switches

References:

Cisco Networking Academy 2014, 'Cisco Networking Academy Connecting network companion Guide: Hierarchical Network Design', viewed on 30/08/2017

<http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=6>

Purser, J 2008, 'Networking Geek to Geek', viewed on 10/09/2017

<https://www.networkworld.com/article/2346494/cisco-subnet/top-5-branches-office-design-tips.html>

Ccexpert 2017, 'Enterprise Branch Design', viewed on 10/09/2017

<https://www.ccexpert.us/network-design/enterprise-branch-design.html>

Cisco Validated Design 2008, 'Campus Network for High Availability Design Guide', viewed on 4/09/2017

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html

Oppenheimer, P 2004, 'Analysing Business Goals and Constraints of Network Design',
viewed on 5/09/2017

<http://www.ciscopress.com/articles/article.asp?p=328773&seqNum=4>

Bright, P 2012, 'How much bandwidth does your office *really* need?', viewed on 8/09/2017

<https://arstechnica.com/information-technology/2012/05/the-speed-of-networking-today-and-tomorrow/>

Oppenheimer, P 2010, 'Developing Network Security Strategies', viewed on 5/09/2017

<http://www.ciscopress.com/articles/article.asp?p=328773&seqNum=4>