1 Purpose

The purpose of this assignment is to teach you to, from a design perspective, architect an actual network solution; replete with an intuition of the ACL's, firewall rules, services and basic configurations for each device on the network.

2 Goal

The goal of this assignment is to help you take a given network architecture and transform it into an enterprise-grade network using all the concepts and ideas we've discussed in this course.

3 Deliverables

You will turn in a document that details all the necessary information to define, architect, and basically implement your design. In this document you should include (note: *this is not a floor or ceiling*):

- design justifications,
- any and all rules needed to be used,
- addressing,
- routes,
- NAT rules,
- vlans,
- services offered,
- general config of the service
- topological map

Pictures and basic diagrams are required to demonstrate topology and architecture. Anything you have learned in class you are expected to apply in some fashion with sufficient justification as to why you chose to use it, e.g., if I used DCHP in my solution, I could do one of two things: I could detail what pool(s) I would use for what ranges or vlans and generally, how it would be configured; or I would give a config that is in the likeness and form of a BIND config (note: this doesn't actually need to be 100% correct).

4 Group Sizes

You will be working in a group size determined by the instructor.

5 Objectives & Expectations

The objective of this project is several-fold:

- Design and "implement" a network
- Understand and parse business needs and requirements
- Work under a specific set of constraints

You are expected to "implement" your network design on paper. You are free to solve this problem however your team sees fit. It must, however, meet the design requirements set forth by the company. Your team's implementation will be graded against the rubric below, in Table 2.

6 Mechanics of the Exercise

As you are building your solution, you will be given a budget of $100,000. This budget will allow you to implement certain aspects of the solution and assume correctness. It effectively let's you not have to write the rules/*some* design decisions/config for a service/function. For instance you might choose to spend $30,000 to build out a DHCP service and assuming the service is configured in the optimal case (optimal being from a security and functional perspective.) The below table gives you the breakdown of what and how you may spend your monies. If it is not on this list it is disallowed. If you choose not to use any

Implement a service (such as DHCP, DNS, Web, MySQL, etc)	$30,000
Implement the ACL's for one router	$30,000
Implement OSPF in the given environment	$70,000
Implement STP in the given environment	$70,000

Table 1: Costs of each contracting job

monies, your team will receive extra credit.

7 Assumptions

You may assume the following:

- All switches have 48 ports available
- All routers have 8 ports available to them
- All firewalls have 8 ports available to them
- All speeds of switchports are >= 1Gbps full duplex

- If we haven't covered a specific service you may use broad generalizations to describe, using principles, what you might do [1](this wouldn't be charged against your budget).
- All firewalls are layer 7 firewalls
- **Any** switch to switch connection requires STP

If you assume something other than what is listed here, you must clearly state it and be able to justify your assumption. Assumptions must be reasonable and obvious. The instructor and TA will judge the assumption as valid or not.

8 Rubric

The rubric will be applied as follows:

- Correct application of security principles:
  - Did the team correctly apply all the applicable principles in network security?
  - How "correct" are the ACL's/network rules at controlling traffic?
  - Is the solution provided optimal given costs?
- Layer 3 topology and technology
  - Did the team use appropriate technologies?
  - Does the solution solve the business problem at this layer?
  - Is there enough room for growth in the future?
  - Is the approach sustainable?
- Layer 2 topology and technology
  - Did the team use appropriate technologies?
  - Does the solution solve the business problem at this layer?
  - Is the approach minimal?
- Clear design justifications
  - Did the team articulate they 'why' behind their decisions?
  - Did the team do anything unconventional, if they did, did they justify it?
  - To what degree does the team's justifications seem sound and reasonable?

[1]for instance, we will not be covering Active Directory(AD) in class, you are not expected to provide a configuration for AD, but you will expected to describe, in some detail, the guiding principles and ideas to configure AD in a generally safe and robust way.

- Correct usage of network services
  - Is the team using each network service correctly?
  - Are the correct ports/applications exposed where they need to be?
  - Does the team solve the business needs given the constraints
- Adherence to business constraints
  - Did the group adhere to the design and objectives set forth by *Acme*, corp?
  - Are the rules, services, and network configuration faithful to the business design goals?

Concept	Points Available
Correct application of security principles	30
Layer 3 topology and technology	30
Layer 2 topology and technology	20
Clear design justifications	10
Correct usage of network services	10
Bonus: Used no $$$$	10
Total:	100

Table 2: Rubric

9 ACL Form

The form of the ACL's should be in the following:

Src Zone	Dst Zone	Src Addr	Dst Addr	Src Port	Dst Port	App	Allow/Deny

Table 3: ACL Form

You will need to enumerate all the ACL's for each router/firewall you install. Use the form in table 3 for how the form your rules should take.

10 Problem Definition

You are a systems administration for *Acme*, Corp. *Acme* employees constantly complain that the network is slow, goes down frequently, and weird things happen on their machines and network all the time. Fortunately, *Acme* is growing and has a strong budget of $100,000 for their new network. Their current network is described in the topology in fig 1. *Acme* employs about 200 employees:

- 100 Sales,
- 10 HR,
- 60 Engineering,
- 10 Executives, and
- 20 R&D

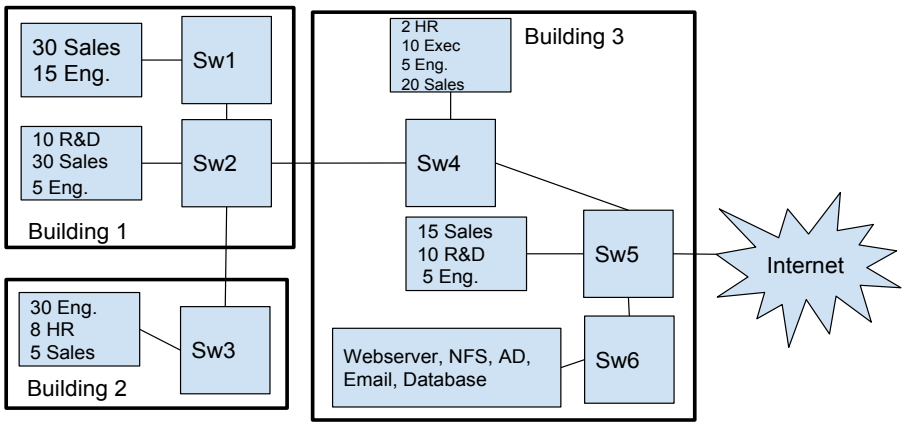

Figure 1: Current topology of *Acme*, corp

Currently, as per fig 1, this network is completely layer 2 with *switch 5* handling NAT for the network. The executives want this network to never go down, be fast, secure, and redundant. As per the network diagram in fig 1 employees are randomly distributed throughout the building (e.g., there is no sales floor or research location). You must upgrade their network and services given the following constraints:

1. Network Access
   (a) Engineering and R&D employees should be able to communicate with each other,
   (b) Sales employees should be completely isolated from the rest of the groups,

(c) Executives should be able to talk to anyone, but no one can talk to them,

(d) HR should be able to talk to everyone but the Executives,

(e) NAT rules need to be updated with new network,

(f) Each device plugged into a switchport is the only device allowed to use that switchport

(g) The CEO hates memes. As such, memes.com should be completely blocked.

(h) The executives want a redundant layer 3 OSPF network.

2. NFS

   (a) Their NFS should be restricted to the same rules as network access on a folder level

3. Webserver

   (a) Sales should be able to access this internally and externally[2],

   (b) The backing database needs to be accessible to only HR

4. Email

   (a) Everyone should be able to access email from wherever they are on the network, or external to the network

5. Firewall & Security [3]

   (a) The executives are asking for the most secure implementation possible,

   (b) this includes ACLs, Firewall rules, zoned traffic, etc.

   (c) Perhaps a honeypot?

6. AD (user login)[4]

   (a) User accounts are required to log onto the network

7. DNS/DHCP

   (a) This is a request from the executive,

   (b) DNS is required to host their own webserver,

[2]Anyone, technically, could access this if it is exposed externally, but how would you ensure that only sales people can access the service?

[3]Note that there is no firewall present in fig 1, you must implement one

[4]I don't expect you implement AD user accounts. I do expect you to do some research on what AD is and be able to articulate, at a high level, what you could do to assign roles and users to accomplish what you want.

(c) You must adequately subnet your network to allow for future growth of *Acme*, corp at 10% in each department each year for the next 2 years

8. Configuration Management

   (a) You should implement an ability to quickly bring a new machine/network device up on the network, back-up configs, etc.