INE 2810 Lab

Version 1.1

Objectives

- Let students have hand-on experience on
  - managing routers and switches
  - network monitoring such as traffic measurement (e.g. MRTG via SNMP), packet analysis (e.g. NTOP, ETHEREAL, TCPDUMP, SNORT)
- Let students have some idea of how an enterprise network is set up and managed
- Let students have some preparation work for the lab work in Advanced Internet Protocol and System course (INE 3010)

Story Line

Let the adventure begin …

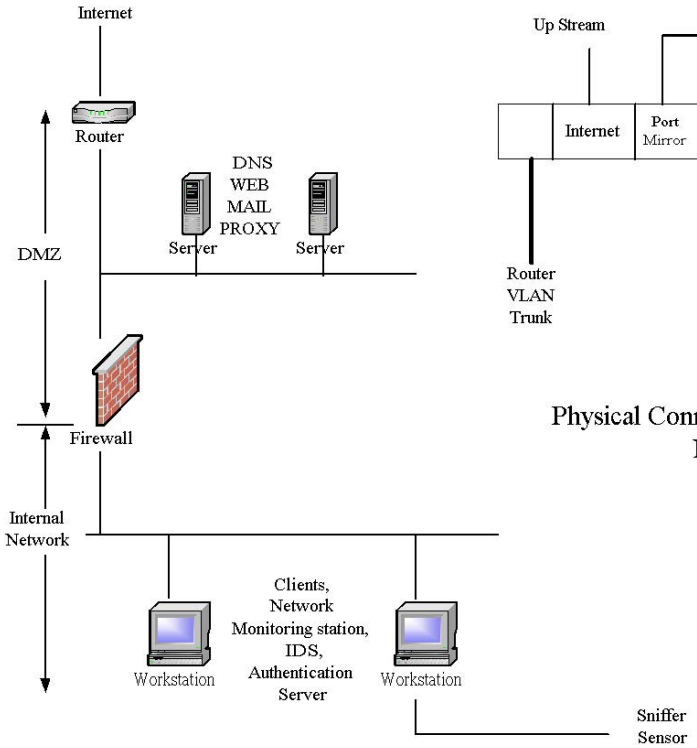
In 200x fall, you are hired to be the technology officers to set up a branch office network for a nationwide enterprise within 12 weeks. The Chief Technology Officer (CTO) in the enterprise headquarter will only give you some general guidelines to set up this network since he is too busy to give you detail steps. As you are the only technical staff in this branch office, you need to figure out the detail implementation procedures by yourselves from manuals and on-line documents. If you encounter any problem, you can post your question to the newsgroup "cuhk.ine.2810" for discussion. You need to report your progress to the enterprise headquarter in each week. In some cases, you may need to explain or justify why you need to take such approach or step to achieve your missions.

Background Information

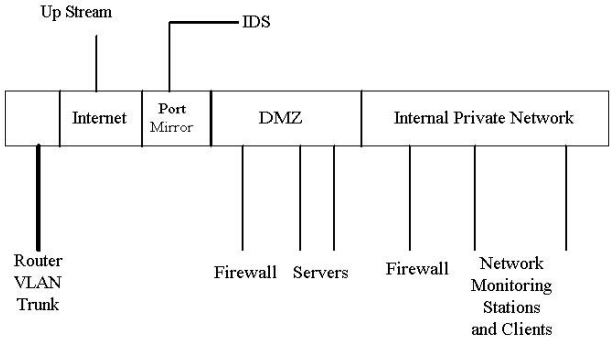
Students are divided into four enterprises and each enterprise has four branch offices. Three students will form a team to set up and manage a branch office network in an enterprise. These branch office network IP address allocation is as follows:

	Branch Office			
Enterprise	**Hong Kong**	**Shanghai**	**Beijing**	**Chengdu**
A	10.2.2.0/24	10.8.2.0/24	10.16.2.0/24	10.32.2.0/24
B	10.2.16.0/24	10.8.16.0/24	10.16.16.0/24	10.32.16.0/24
C	10.2.32.0/24	10.8.32.0/24	10.16.32.0/24	10.32.32.0/24
D	10.2.64.0/24	10.8.64.0/24	10.8.16.0/24	10.32.64.0/24

Your branch office has four departments: Information Technology Service Department (ITSD), Sales Department, Marketing Department, and Accounting Department. You are the only technical staff in ITSD. You will manage one router, one switch, one firewall, and four servers in your branch office. Your office network infrastructure is as follows:



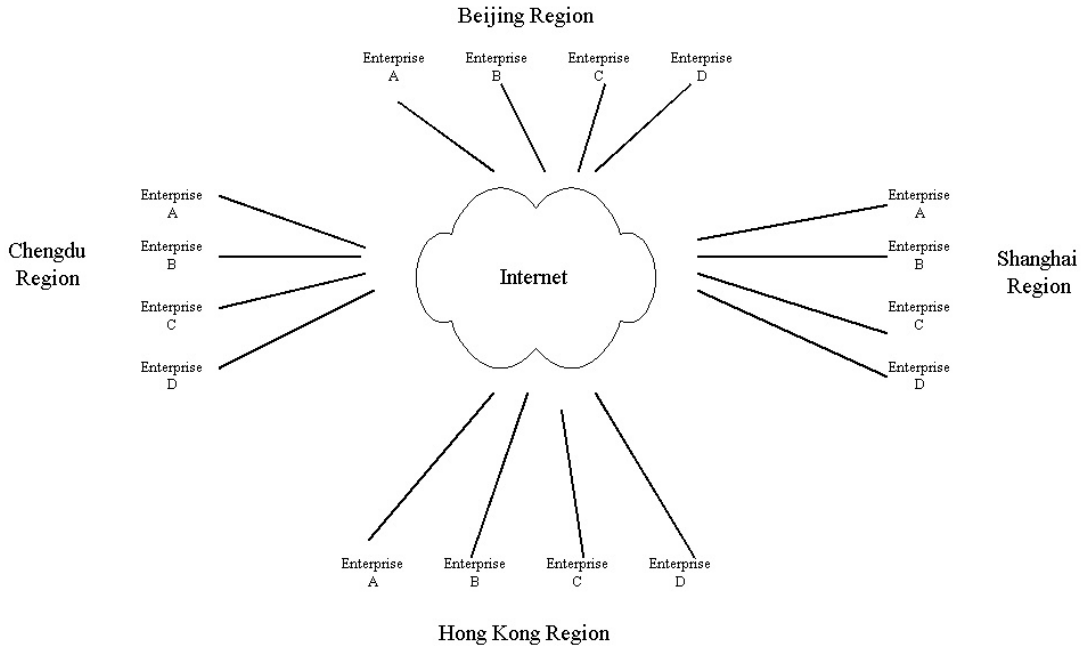
Logical Diagram of a Branch Office Network in a Regional Enterprise



Physical Connection of the Branch Office Network Switch

Your branch office estate manager will provide a patch panel for you connecting the above equipment to your switch.

There are four enterprises and each enterprise has branch offices in Hong Kong, Shanghai, Beijing, and Chengdu respectively. In this early stage, these branch offices are interconnected by the Internet through their ISPs.



Enterprises A and B are partners. They co-operate with each other in business and they are competitors of Enterprise C and D. Enterprises C and D are also partners. They co-operate with each other in business. Enterprise A and B may be their competitors.

Here are the domains and IP address maps of the branch offices of the enterprises.

Enterprise Alpha

Branch Office	**IP Address Range**	**Domain Name and DNS Server IP**	**Router Interface IP to ISP / Netmask**	**Upstream ISP Router IP / Netmask**
Hong Kong	10.2.2.0/24	hk.alpha.ine.cuhk.edu.hk 10.2.2.1 10.2.2.2	10.2.201.249/30	10.2.201.250/30
Shanghai	10.8.2.0/24	sh.alpha.ine.cuhk.edu.hk 10.8.2.1 10.8.2.2	10.8.201.249/30	10.8.201.250/30
Beijing	10.16.2.0/24	bj.alpha.ine.cuhk.edu.hk 10.16.2.1 10.16.2.2	10.16.201.249/30	10.16.201.250/30
Chengdu	10.32.2.0/24	cd.alpha.ine.cuhk.edu.hk 10.32.2.1 10.32.2.2	10.32.201.249/30	10.32.201.250/30

Enterprise Bravo

Branch	**IP Address**	**Domain Name and**	**Router**	**Upstream**

Office	Range	DNS Server IP	Interface IP to ISP / Netmask	ISP Router IP / Netmask
Hong Kong	10.2.16.0/24	hk.bravo.ine.cuhk.edu.hk 10.2.16.1 10.2.16.2	10.2.202.249/30	10.2.202.250/30
Shanghai	10.8.16.0/24	sh.bravo.ine.cuhk.edu.hk 10.8.16.1 10.8.16.2	10.8.202.249/30	10.8.202.250/30
Beijing	10.16.16.0/24	bj.bravo.ine.cuhk.edu.hk 10.16.16.1 10.16.16.2	10.16.202.249/30	10.16.202.250/30
Chengdu	10.32.16.0/24	cd.bravo.ine.cuhk.edu.hk 10.32.16.1 10.32.16.2	10.32.202.249/30	10.32.202.250/30

Enterprise Charlie

Branch Office	IP Address Range	Domain Name and DNS Server IP	Router Interface IP to ISP / Netmask	Upstream ISP Router IP / Netmask
Hong Kong	10.2.32.0/24	hk.charlie.ine.cuhk.edu.hk 10.2.32.1 10.2.32.2	10.2.203.249/30	10.2.203.250/30
Shanghai	10.8.32.0/24	sh.charlie.ine.cuhk.edu.hk 10.8.32.1 10.8.32.2	10.8.203.249/30	10.8.203.250/30
Beijing	10.16.32.0/24	bj.charlie.ine.cuhk.edu.hk 10.16.32.1 10.16.32.2	10.16.203.249/30	10.16.203.250/30
Chengdu	10.32.32.0/24	cd.charlie.ine.cuhk.edu.hk 10.32.32.1 10.32.32.2	10.32.203.249/30	10.32.203.250/30

Enterprise Delta

Branch Office	IP Address Range	Domain Name and DNS Server IP	Router Interface IP to ISP / Netmask	Upstream ISP Router IP / Netmask
Hong Kong	10.2.64.0/24	hk.delta.ine.cuhk.edu.hk 10.2.64.1 10.2.64.2	10.2.204.249/30	10.2.204.250/30
Shanghai	10.8.64.0/24	sh.delta.ine.cuhk.edu.hk 10.8.64.1 10.8.64.2	10.8.204.249/30	10.8.204.250/30
Beijing	10.16.64.0/24	bj.delta.ine.cuhk.edu.hk 10.16.64.1 10.16.64.2	10.16.204.249/30	10.16.204.250/30
Chengdu	10.32.64.0/24	cd.delta.ine.cuhk.edu.hk 10.32.64.1 10.32.64.2	10.32.204.249/30	10.32.204.250/30

As for the internal private network in your branch office, you can choose any class C network in 172.16/12.

Host Naming

In order to facilitate your successors and headquarter to follow up your jobs, you are required to set the hostname of your servers as follow:

Enterprise A

Branch Office	Server Hostname
Hong Kong	vms11-1 (DMZ host) vms11-2 (DMZ host) vms11-3 (Firewall) vms11-4 (internal network host) vms11-5 (internal network host) c2950-n1 (switch) c1721-n1 (router)
Shanghai	vms11-6 (DMZ host) vms11-7 (DMZ host) vms11-8 (Firewall) vms11-9 (internal network host) vms11-10 (internal network host) c2950-n2 (switch) c1721-n2 (router)

Beijing	Vms11-11 (DMZ host) vms11-12 (DMZ host) vms11-13 (Firewall) vms11-14 (internal network host) vms11-15 (internal network host) c2950-n3 (switch) c1721-n3 (router)
Chengdu	vms12-1 (DMZ host) vms12-2 (DMZ host) vms12-3 (Firewall) vms12-4 (internal network host) vms12-5 (internal network host) c2950-n4 (switch) c1721-n4 (router)

Enterprise B

Branch Office	**Server Hostname**
Hong Kong	vms12-6 (DMZ host) vms12-7 (DMZ host) vms12-8 (Firewall) vms12-9 (internal network host) vms12-10 (internal network host) c2950-n5 (switch) c1721-n5 (router)
Shanghai	vms12-11 (DMZ host) vms12-12 (DMZ host) vms12-13 (Firewall) vms12-14 (internal network host) vms12-15 (internal network host) c2950-n6 (switch) c1721-n6 (router)
Beijing	vms13-1 (DMZ host) vms13-2 (DMZ host) vms13-3 (Firewall) vms13-4 (internal network host) vms13-5 (internal network host) c2950-n7 (switch) c1721-n7 (router)
Chengdu	vms13-6 (DMZ host) vms13-7 (DMZ host) vms13-8 (Firewall) vms13-9 (internal network host) vms13-10 (internal network host) c2950-n8 (switch) c1721-n8 (router)

Enterprise C

Branch Office	Server Hostname
Hong Kong	vms13-11 (DMZ host) vms13-12 (DMZ host) vms13-13 (Firewall) vms13-14 (internal network host) vms13-15 (internal network host) c2950-n9 (switch) c1721-n9 (router)
Shanghai	vms14-1 (DMZ host) vms14-2 (DMZ host) vms14-3 (Firewall) vms14-4 (internal network host) vms14-5 (internal network host) c2950-n10 (switch) c1721-n10 (router)
Beijing	vms14-6 (DMZ host) vms14-7 (DMZ host) vms14-8 (Firewall) vms14-9 (internal network host) vms14-10 (internal network host) c2950-n11 (switch) c1721-n11 (router)
Chengdu	vms14-11 (DMZ host) vms14-12 (DMZ host) vms14-13 (Firewall) vms14-14 (internal network host) vms14-15 (internal network host) c2950-n12 (switch) c1721-n12 (router)

Enterprise D

Branch Office	Server Hostname
Hong Kong	vms15-1 (DMZ host) vms15-2 (DMZ host) vms15-3 (Firewall) vms15-4 (internal network host) vms15-5 (internal network host) c2950-n13 (switch) c1721-n13 (router)
Shanghai	vms15-6 (DMZ host) vms15-7 (DMZ host) vms15-8 (Firewall) vms15-9 (internal network host) vms15-10 (internal network host) c2950-n14 (switch)

	c1721-n14 (router)
Beijing	vms15-11 (DMZ host) vms15-12 (DMZ host) vms15-13 (Firewall) vms15-14 (internal network host) vms15-15 (internal network host) c2950-n15 (switch) c1721-n15 (router)
Chengdu	vms1-1 (DMZ host) vms1-2 (DMZ host) vms1-3 (Firewall) vms1-4 (internal network host) vms1-5 (internal network host) c2924-n1 (switch) c1721-n16 (router)

Mission (Lab Module Outlines)

Mission 1

- Familiarize with your branch office working environment
- Inspect all your hardware equipment
- Set all your hosts, router and switch hostname and password
    - There is not need to configure IP of these hosts at this moment, as the network connection has not been patched yet.
    - Set the hostname and password according to headquarter prescribed value

Mission 2

- Set up the router to connect to your network upstream ISP and test the connection
- Configure all your host network interfaces
- Configure your switch to link up your hosts

Mission 3

- Set your router and firewall to restrict the traffic to your network (e.g. restrict the access to your colleagues from other branch offices)
- Set up your branch office DNS server and Mail servers so that headquarter and other branch offices can send you e-mails.

Mission 4

- Set up your web server in DMZ to for public access
- Apply for a PKI certificate from headquarter so as to support secure communication on your web server and e-mail communication among other branch offices.
- Set up the firewall to restrict access to your internal private network

Mission 5

- Start building up your internal private network (e.g. internal DNS)
- Open accounts for your staff in your branch office
- Set up a proxy server and mail gateway in DMZ, so that your hosts in the internal network can access the Internet and send e-mails to outsiders.

Mission 6

- Set up a network monitoring station in your internal private network
- Set up the radius authentication server for the router and switch
- Set up the SNMP/MRTG/NTOP/NETFLOW monitoring of your router and switch
- Set up a web reverse proxy in DMZ or NAT in your router/firewall so that headquarter can access your network monitoring station web page

Mission 7

- Set up IDS and Scanner (host and network based) for your network
- Fine tune your firewall and router such that headquarter can login your internal network hosts via NAT and/or VPN

Mission 8

- Conduct a security vulnerability test to your network and other branch office networks in your enterprise.
- Analyze the data get from your IDS
- Write the reports of the security vulnerability test and IDS data analysis. Present them on secure web pages for headquarter review.
- In your report, you should give suggestion or advice to rectify the problems.

Mission 9

- You may find that some services in your network are not working. Try to troubleshoot the problems and write a report to headquarter to explain the incidents. In your report, you should identify the sources of the problems and describe how you solve them.

Mission 10

- As you are leaving the branch office, headquarter wants you to write a risk assessment report to evaluate the risk of your branch office. In the report, you need to identify the assets of your branch office and the nature and impact of potential risks. Headquarter also wants you to work out the contingency plan and recovery plan for unexpected network service interruption and disaster recovery. In your plan, you need to figure out and also justify the service priority, recovery procedures, and minimum downtime.

Mission 11

- Farewell party

  You will be transferred to another department in spring. Before you leave, the headquarter will held a farewell party for you to show her gratitude. In this party, you will present what you have learned from these missions, what difficulties you encountered most, and what improvement can be made in these missions/assignments.