A network overview for Apocalypse Petro-Chemicals and ip addressing schemes

Vasileios Balafas, *MSc in DCOM student*,(xwing@otenet.gr)

***Abstract*— In this coursework, a network overview of Apocalypse Petro-Chemicals is analyzed and presented as part of the TCP/IP Networks course in MSc DCOM of TEI of Piraeus. The main case is some possible ip addressing schemes that could be implemented in this enterprise's computer network and the purpose is to practice on a "real by life" example for our course. So it is understood that an imaginary scenario will be developed in this case which does not involve economic or evaluation issues that would required in a real case. Petro-Chemicals is a classic enterprise which is realizing that IT and communications are areas that could help its performance but also this area is neglected. As many enterprises do , it was not right designed or expected to play such an important role in the near future. As a result now the computer network must be correctly established and designed under the present and future needs in order to offer effective and efficient IT solutions.**

I. INTRODUCTION

IN our century it is known that a well based and developed information system is one of the greatest advantages that an organization should have to achieve its economic targets. It is also known and a general consensus that when someone refers to information systems, he practically means a computer network which supports the daily procedures of an organization constantly and securely and provides smooth access to the organization's resources that are requested each time by the employees of every hierarchical level .

Nowadays Major companies have a large number of computers in operation, often located far apart and these computers must be connected with each other or to the needed resources creating a large network or , in technical terms , a WAN (Wide Area Network).

Data and communication technologies are integrating day by day offering to the companies reliable solutions and new services that can support almost every aspect of daily activities. File sharing or generally resource sharing, client-server services, video conference, mobile access, web services and the internet are only some of the implementations that take place in every well respected company nowadays and enhance the productivity and the potency of a modern company.

This sophistication or evolution of communication and data systems is the result of the TCP/IP technology which made the connectivity of the personal computers possible either existing in a house or in a company using a ubiquitous -any longer- middle, the Internet.

In a company's building there is a LAN (Local Area Network) or smaller networks interconnected, creating an intranet consisted by the workstations and the resources servers which exchange data and general information. Those smaller networks are the subnets which can be in the company's central building or everywhere else across the world. Those sub networks are interconnected via devices called routers which can have straight cable connections between them or they just use shared connections like the internet. By this way a company can create its WAN which is a miniature of the Internet. Some of these subjects will be discussed further.

Returning to our case, Apocalypse Petro-Chemicals is a company which is facing the problems that come from the lack of wise use of the networking technology. The systems were developed in an anarchical way without design and consideration of future changes. In other words each new employee could have a new computer, working alone, set up many times by a local "expert" and this computer's job was to do these that could be done locally. In other cases some networks have been created but were operated privately without connectivity to other networks and these networks had low usability. Here is another great positive effect of LANs or WANs; shared resources that grow the utilization of an installed network.

Some of the employees are personally connected to the Internet by various ways but without considering or knowing the dangers of an attack to their systems. Nowadays, it is known by any pc user that Internet encompasses a lot of dangers like viruses, worms and other vulnerabilities which can finally be faced by a person, formatting its own pc and possibly losing its data but an operation like that could be

catastrophic for a company which can not lose its files or sensitive data that keeps in its systems.

As it will be discussed our aim is to offer to Apocalypse Petro-Chemicals a network design which will end to an ip scheme for both required classes as they are demanded from the coursework.

II. The TCP/IP Model

As we discussed above, computers must "talk" with each other and this operation must take place by a standard way for every computer in the world in order to ubiquitous and pervasive IT communication can be achieved. Other terms were also mentioned like LAN, WAN, networks etc. but no further discuss will be done because this could mislead the case of this coursework. But, it is necessary to explicate some points of this lucubration in order to reach a conclusion. One of these points is the TCP/IP model which was mentioned as the technology which gives to the networks the possibility to cooperate. Inspired and originated from the legendary OSI model (Fig.1) the TCP/IP model has 4 layers [1].

Fig. 1 The OSI Model

The application, the transport, the network and the internet layer which can be divided to the datalink and the physical layer resulting a hybrid situation which is why it can be met in many ways in books. The important matter is that this model took its name by the most significant protocols, the TCP (Transmission Control Protocol), and the IP (Internet Protocol) which refer correspondingly to the transport and internet layers. The purpose of this model is to offer an interworking environment and standardization between the network technologies. The IP is, nevertheless, the dominant protocol in networks and we could imagine it as *the glue that holds the Internet together* [2].

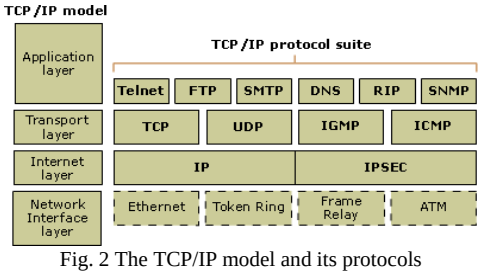

Fig. 2 The TCP/IP model and its protocols

So, we are led to a wide spread concept of networking under

the rules of these famous and well accepted protocols. This concept is that TCP controls the right flow of data from host to host detecting errors and lost data and ip is the middle protocol by witch this data is moving in a network. Data is divided to packets and forwarded based upon the address of the receiver. As in human terms, each host, pc, server and generally every element of the network has a unique ip address which is a 4 byte – 32 bits binary number called the ip number. A 32-bit IP address is a binary number in this form:

10101100000111101000000000010001

This binary number is grouped into four octets, converted to decimal form and finally written in dotted-decimal notation creating the following form [3].

10101100 00011110 10000000 00010001

172 30 128 17

172.30.128.17

This number is not fortuitous but there are authorities that assign ranges of numbers to organizations in order to build and allocate addresses to their LANs. As mentioned before TCP/IP became so popular thanks to its capability to connect different type of networking environments and finally, it can converge the variety of communication technologies. Lot of effort is now made to the integration of TCP/IP to mobile technologies opening a whole new world of services and possibilities. Returning to our issue it is necessary to say that ip numbers are separated to classes A, B, C, D and E. The first 3 classes are used to address actual hosts on IP networks. The ranges of those classes are [4]:

Class	Address Range
A	1.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255

Table 1 Classes ranges

Class A network can have 16 million addresses, class B 65536 and class C 256. Those numbers come from the analysis of the network's 0s and 1s. Class A has a mask of 255.0.0.0. which is in binary form:

11111111 00000000 00000000 00000000

The first octet with 1s represents the net id and the others with the 0s the host id. As we can see, a class A network has 2^{24} hosts. By this way we can resume:

Class B Mask: 11111111 11111111 00000000 00000000

Hosts 2^{16}

Class C Mask 11111111 11111111 11111111 00000000

Hosts 2^{8}

To be accurate, in each network two addresses are excluded. The first and the last, as the first is the network address (the network's name) and the last is the multicast address. So, for example a class C network has 254 addresses for allocating hosts [5]. It was mentioned that each host has to have a unique ip number. Let's see what happened in the past;

as the internet was growing and the ip became dominant, the ip scheme became victim of its own popularity. Organizations when wanted more than 256 hosts were acquiring a class B address and a lot of addresses were unused bringing down the utilization of the ip range by wasting addresses. The concept class A is too big, class C is too small, class B will be right is known as the Three Bears Problem [6] and led to the depletion of ip addresses stressing the authorities to be more careful in giving ip addresses.

Many Class A and B networks do not contain as many hosts as they could, causing address space waste. Reversely if an organization wants to create smaller networks would have to obtain one class C network for each network. To solve this problem, new techniques invented, like CIDR (Classless InterDomain Routing – RFC 1519) and VLSM (Variable Length Subnet Masking - RFC 1009). CIDR practically comes to unite class C networks according to the needs. For example if we need 2000 addresses we can have 8 class C networks which means 2048 hosts. It also offers an easier way to recognize networks by writing prefixes like /24 which means a Class C network as 24 is the number of 0s in the mask (3 octets of 0s). VLSM offers the capability to use different masks in order to create subnets with hosts. The basic idea is that it is possible to split an ip address into smaller networks by borrowing bits from the host's octet which are called subnets in order to support the needs of organizations. When a subnet is designed we can create smaller networks modulated to the hosts needed. Different masks means that we won't use for class C the standard 255.255.255.0 mask but we will change it by changing the 0s and 1s in a way that was explained before [7].

III. Subnetting

As noted before a subnet is a portion of a network that shares a common address component with other portions of the network. For example all devices with ip addresses that start with 206.20.36. would be part of the same network. We can divide networks into subnets using subnet masks which are needed to determine what subnet an ip address belongs to. So the network address 206.20.36.0 with subnet mask 255.255.255.0 means that in this network there are addresses from 206.20.36.0 to 206.20.36.255 = 256 – 2 = 254 hosts. This is a "classic" class C network. By subnetting it is possible to divide this network. If we apply a subnet mask 255.255.255.192 we have in binary form a mask of this type:

11111111 11111111 11111111 11000000

We borrowed two bits from the host portion changing the 0s to 1s. Now we have 2^6 hosts = 64 and 2^2 = 4 subnets. Always we have to keep in mind that the real hosts are 62. By this pattern it is easy to understand that if I borrow one more bit, I will take 8 subnets of 32 hosts. By binary adding the ip address and the subnet mask, we take the network address.

We shall not also now forget that in this example the prefix has changed and became /26 for the first case and /27 for the 8 subnets case. Now the general concept is clear. It is certain that nobody can keep in mind all these operations when designing a large network (LAN or WAN) so there are very useful tools like ip calculators that help to build subnets. In this coursework an ip calculator is used for helping the ip allocation of Apocalypse Petro-Chemicals network.

It must be added that those described techniques help in a determinant way the routing process as when a subnet is divided only the "head" address is needed to be declared. This is significant for the normal creation of the routing tables and for the smoother encounter of changes in a network, something that it is not needed to be analyzed here. Let's see now a simple example of subnetting [8].

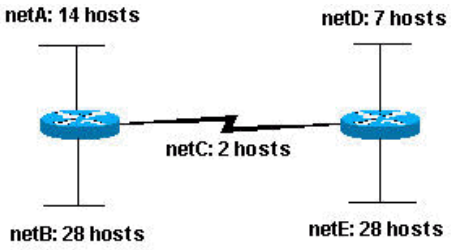

Fig.3 A simple example

Having a Class C network address 204.15.5.0/24 we may divide it in order to create the network shown in Fig.3. Three subnet bits are needed for 6 subnets, and five bits are remaining for the host portion of the address. 2^5 = 32 (30 usable) hosts will be supported and each subnet will have the following ip allocation:

Net A: 204.15.5.0/27 host address range 1 to 30
Net B: 204.15.5.32/27 host address range 33 to 62
Net C: 204.15.5.64/27 host address range 65 to 94
Net D: 204.15.5.96/27 host address range 97 to 126
Net E: 204.15.5.128/27 host address range 129 to 158

It is shown here again that the 1st (network) and the last address (broadcast) of each range are not used. Using now VLSM, this network address becomes more efficient and starting from the largest subnet, the allocation table becomes:

Net B: 204.15.5.0/27 host address range 1 to 30
Net E: 204.15.5.32/27 host address range 33 to 62
Net A: 204.15.5.64/28 host address range 65 to 78
Net D: 204.15.5.80/28 host address range 81 to 94
Net C: 204.15.5.96/30 host address range 97 to 98

As it is shown no waste of addresses happened here because to the Net C, 2 ips were allocated and not a whole 30 hosts subnet [9].

IV. Part I

Now, the technologies that are going to be used in this coursework are clear and the general concept has been given. When a network design is demanded, a scrupulous analysis has to be made in order to predict potential problems and save in many cases, money and valuable time. This is what happened to Apocalypse Petro-Chemicals. Before the consultants report nobody thought the idea of an Intranet which could offer connectivity to the organization's parts and resources. Now an Intranet requirement is assessed and the

network infrastructure has to change. To be able to offer a descent scenario some assumptions are made.

First, we have to collect the information about the topology and the networks that must be deployed. The wanted elements are:

1 HQ Site with 1560 employees
5 Major Sites containing 200-500 staff
10 Medium Sites with 50-200 staff
40 Smaller Sites with 1-50 staff
1 PDC(Primary Domain Controller) per 200 users
1 BDC(Back up Domain Controller) per 200 users
1 File Server per 50 users
3 Application Servers per 50 users
1 Printer per 50 users

Current requirements are for only approximately 7 thousand addresses and it is early shown that the Class C block of addresses given could marginally support those requirements. For simplicity the following assumptions have been made. For the HQ, will be needed approx. 1800 addresses as there are 1560 employees and 8 PDC 8 BDC 31 FS 32 Printers 93 Application Servers and other elements are needed. An allocation of 2040 addresses seems logical here.

The main assumptions are made for the other sites as in this coursework the average numbers are taken and some server economy was applied. So, for the Major Sites it is assumed that there are on the average 250 users needing 1 PDC 1 BDC 5 FSs 15 App Servers and 5 Printers reaching a number of approx. 300 hosts including switches hubs and routers for each site. For the Medium Sites the same concept is followed, assuming there are 100 hosts on the average with 2 FS 6 App S and 2 Printers and some PDCs and BDCs will be attached to some networks in order to implement shared resources as they can serve more than one network's users. This results to a number of 110 addresses for each medium network. Finally for the smaller sites, on the average 30 ips or more should be enough for their needs.

V. Class C scenario

Starting from the class C scenario for the HQ site 8 class C networks are required, so addresses from 204.217.64.0 to 204.217.71.255 can be offered in order to donate 2048-2=2046 hosts. This 8 Class C addresses network can be expressed as 204.217.64.0/21 applying the CIDR rules. This operation is called supernetting [10].

For the Major sites, where more than 300 hosts are needed 2 Class C blocks will be allocated to each one. As a result for the first Major Site 204.217.72.0 and 204.217.73.0 will be offered, expressed by 204.217.72.0/23 containing 510 hosts. By the same way ip addresses will be given to the rest 4 major sites with the following network addresses:

204.217.74.0/23
204.217.76.0/23
204.217.78.0/23
204.217.80.0/23

For the Medium sites approx. 110 hosts are needed for each one, creating the following allocation:

204.217.82.0/25
204.217.82.128/25
204.217.83.0/25
204.217.83.128/25
204.217.84.0/25
204.217.84.128/25
204.217.85.0/25
204.217.85.128/25
204.217.86.0/25
204.217.86.128/25

This allocation offers 126 usable hosts to each network. Note that now the prefix has become /25 as 1 bit is borrowed from each address' host portion.

For the smaller networks needing approx. 30 hosts each, the prefix will become /27 offering 8 subnets of 30 hosts in each Class B address starting from 204.217.87.0/27

#	ID	Range	Broadcast
1	204.217.87.0	204.217.87.1 - 204.217.87.30	204.217.87.31
2	204.217.87.32	204.217.87.33 - 204.217.87.62	204.217.87.63
3	204.217.87.64	204.217.87.65 - 204.217.87.94	204.217.87.95
4	204.217.87.96	204.217.87.97- 204.217.87.126	204.217.87.127
5	204.217.87.128	204.217.87.129-204.217.87.158	204.217.87.159
6	204.217.87.160	204.217.87.161-204.217.87.190	204.217.87.191
7	204.217.87.192	204.217.87.193-204.217.87.222	204.217.87.223
8	204.217.87.224	204.217.87.225-204.217.87.254	204.217.87.255

Above the first 8 subnets coming from the first block are analyzed a little more in order to show the range of the hosts addresses and the broadcast addresses. Remember that the binary subnet mask is here:

11111111 11111111 11111111 11100000 /27 1s
255 255 255 224
255.255.255.224 in decimal

By this concept, we manage to create 40 subnets of 30 hosts using 5 Class C network addresses and reaching the last of those which is 204.217.91.224/27. So we have 4 class C addresses left which can be used for offering remote access to remote users or for future needs.

Here it is needed to underline that one Class C will be used to offer the interconnection addresses of routers dividing it to 64 subnets of 2 hosts using a /30 prefix and a 255.255.255.252 subnet mask. In the next page a general design of Apocalypse Petro-Chemicals is shown, drawn with Smart Draw Suite Edition v.7.0, including the assumptions made and a possible hierarchical representation of the whole organization's WAN.

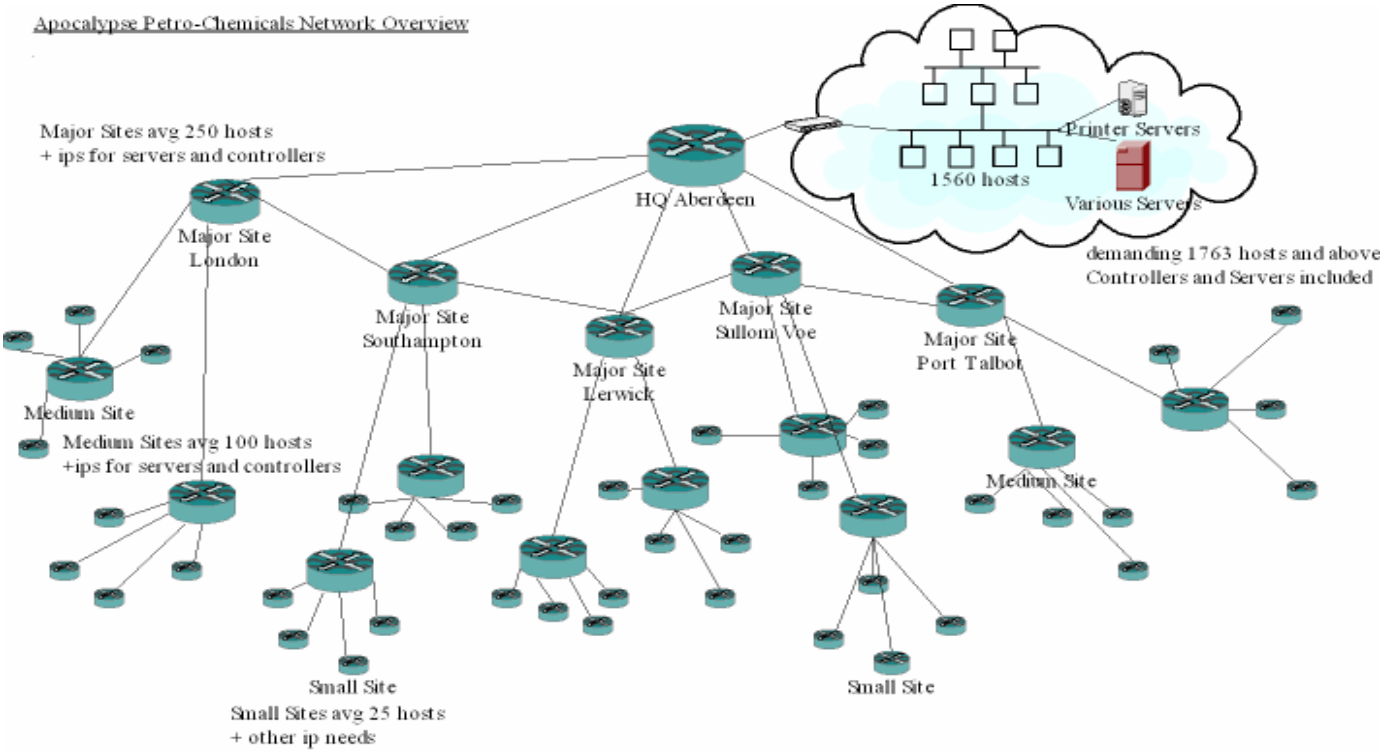

Fig.4 Apocalypse Petro-Chemicals Network Design

The Class C scenario is a stretched one and doesn't leave space for great future implementations or diversification. Here the bear just fits in its bed and is hard-bested!

VI. Class B Scenario

In Class B scenario the situation is more comfortable. The given Ip address 150.23.0.0 has a mask:

11111111 11111111 00000000 00000000
255 255 0 0 /16 prefix

This address can support 65534 active hosts giving to the examined Apocalypse's network great efficiency and the convenience to manipulate any future changes and demands.

But as it is going to be proved, on a network that will need over the next three – six years, 3-4 thousand more hosts (or just double its demands) and reaching approx. 12 thousand addresses, the waste of address space is enormous from the early beginning of this analysis.

Here in the Class B scenario the use of VLSM (RFC 1878) will be more rousing, as by using variable length masks this network address will be distributed to the member networks.

Following the assumptions made for the HQ network using 4 subnet bits, the mask the mask will be converted as below:

11111111 11111111 00000000 00000000
11111111 11111111 11110000 00000000
255 255 240 0
255.255.240.0 = /20

The first subnet emerging, offers 4094 active hosts with 150.23.0.0/20 as network address,150.23.0.1 - 150.23.15.254

as address range and the 150.23.15.255 as the broadcast address. As it can be understood, it is possible here to give more than the demanded hosts, in order to satisfy any future demands or additional needs that may occur.

For the major sites we can afford giving them 1022 active hosts by subnet using a 6 subnet bits mask which is 255.255.252.0 = /22. By this way 5 subnets can be provided for the 5 major sites:

#	ID	Range	Broadcast
1	150.23.16.0	150.23.16.1 - 150.23.19.254	150.23.19.255
2	150.23.20.0	150.23.20.1 - 150.23.23.254	150.23.23.255
3	150.23.24.0	150.23.24.1 - 150.23.27.254	150.23.27.255
4	150.23.28.0	150.23.28.1 - 150.23.31.254	150.23.31.255
5	150.23.32.0	150.23.32.1 - 150.23.35.254	150.23.35.255

Following this pattern, the ip allocation can be continued to the medium sites by applying a 7 subnet bits mask to the next available address and creating 10 networks by 510 active hosts each. So now the result is:

#	ID	Range	Broadcast
1	150.23.36.0	150.23.36.1 - 150.23.37.254	150.23.37.255
2	150.23.38.0	150.23.38.1 - 150.23.39.254	150.23.39.255
3	150.23.40.0	150.23.40.1 - 150.23.41.254	150.23.41.255
4	150.23.42.0	150.23.42.1 - 150.23.43.254	150.23.43.255
5	150.23.44.0	150.23.44.1 - 150.23.45.254	150.23.45.255
6	150.23.46.0	150.23.46.1 - 150.23.47.254	150.23.47.255
7	150.23.48.0	150.23.48.1 - 150.23.49.254	150.23.49.255
8	150.23.50.0	150.23.50.1 - 150.23.51.254	150.23.51.255
9	150.23.52.0	150.23.52.1 - 150.23.53.254	150.23.53.255
10	150.23.54.0	150.23.54.1 - 150.23.55.254	150.23.55.255

Offering to the smaller networks 254 active hosts to every

one, we will reach the last active network witch will be the 150.23.96.0/24. Of course some more interconnecting addresses are needed for the routers.

The given class B block has the 150.23.255.254 address as the last host ip address that could be allocated. It is obvious that a waste of address space is happening in this scenario leaving a lot of hosts for future use and it is much possible that they will never be activated.

VII. General And Future considerations

As the discussion comes to practical matters it is obvious that Apocalypse Petro-Chemicals has to develop a new network infrastructure, use Ethernet technologies and install UTP cables and leased lines through its network. It is also wise to install fibre between the HQ, the Major and the Medium sites in order to achieve high speed in its network. Some of the already existent network elements can be used but generally, potential issues of compatibility could rise as some of the parts installed can't fulfil the new standards.

By the system proposed, network efficiency can be achieved and better administration control can be practiced. Specific rights can be given to the users in order to have access to the resources needed and not to every data that could be kept in the Information System. Resources can be shared, saving money and time and the danger of duplicated data can be averted by shared network disks and synchronization of the documents.

Application and File Servers can provide the information needed and create a distributed system which obeys the lines and the decisions of the HQ. A (SAN) Storage Area Network could provide a reliable back up system that ensures the organisation's information. Telephony expenses will decrease radically as a VoIP system could be developed using the new installed network infrastructure. Plus to those advantages can be added the possibility, which offers a well structured WAN, for more powerful and efficacious security policies against attacks providing that the new WAN will be connected to the Internet.

By connecting to the Internet new applications and new services to the employees can be practiced like remote access through VPNs (Virtual Private Networks) [11], and moreover if wireless and mobile technology is going to be applied, possibilities like mobile access to shared information can be achieved. As it is obvious, such implementations demand a scalable ip address space and this can't be practiced with the given class C scenario.

We are just talking about future considerations that urge the organisation to apply for 16384 addresses to the authorities. The future needs – as the organisation tends to grow by acquiring 3 more companies in the next two years – and the new technologies that could be applied, justify this demand as a larger address space could, more effectively, support the organisation's needs. Provided that this demand will be accepted more ip addresses can be allocated to every subnet in order to meet new host demands and allow expansion of the network. A central network administration department has to be established and provide support for any potential problems or expansion that could happen as the routing administration is crucial for the new network infrastructure in order to achieve connectivity availability and consistent services offered. That's why the backbone network has to encompass some spare connections for ensuring that a casual disruption would not affect the whole network.

VIII. Part II option 3

As mentioned before Internet Access is required for the Apocalypse Petro-Chemicals organisation. This capability can offer a lot of advantages to an enterprise but there may be serious security dangers as well.

It is well known that the best way to keep away from internet dangers is not to connect to it. This suggestion cannot be accepted, without dispute. Multiple techniques have been proposed to offer Internet Access through organisations with dominant ones the Proxy Server and the NAT system. In this part, some other answers to the coursework's issues will be given. An interesting one is the case of private addresses which refers to the internet access issue and to the potential growth of a network as well. How these two issues can be connected will be shown.

Beginning from the main matter, earlier in this coursework public addresses were discussed. Here, it is important to remind that in each addresses Class there are some private addresses assigned for private networks and experimental purposes. If somebody wants to create a home network, he will use those addresses without needing renting them but those addresses cannot be public. We may have in our home more than 1 pc (most of us nowadays have). The solution offered to connect them is to create a home LAN allocating those private addresses to our pcs.

Class	Private Start Address	Private End Address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Table 2 Private Addresses Ranges

Those addresses shown in Table 2 are given and determined in RFC 1918 and cannot be used for public networks. But we can offer a shared internet connection by using a proxy server.

A proxy server is indeed a gateway application and can be software or hardware. Intranets connect to the "outside world" through the proxy and the other systems respond to the proxy. Those systems cannot see the internal network. All outgoing traffic appears to be coming to others by one and only ip address. To differentiate a connection the proxy server uses protocol and port numbers [12]. Proxy servers usually work at layer 4 (transport) and this is one of their disadvantages as they become slower. In other words proxy servers operate as translators to clients of an intranet. When requests are done the proxy initiates these requests and when a reply is coming back, it re-translates the ip addresses and sends the traffic to the internal host. A great positive point of some proxies is that

they can cache the incoming data and for example when 3 pcs are asking the same url, the proxy downloads one copy of the requested url and the internal hosts take this url from its cache memory. This saves bandwidth and offers faster replies to url requests. There are many implementations of proxy servers and lots of them in software form can be downloaded freely from the internet and support a little home network. One of them is AnalogX Proxy and can be found at www.analogx.com. There are more complicated implementations like Microsoft Proxy Server and others which have more possibilities and can offer better performance, better configuration utilities and can be more effective in sectors like controlling the network internet traffic and enforce security policies and different access to web pages for each proxied host. Generally there are two types of proxy servers, the application and the socks proxies. Application Proxies can authenticate users by asking them to login before a connection. Socks proxies act like a switch board by simply crossing wires through the system to an outside connection like it was happening to old telephone centrals [13].

The main drawback of proxy servers is that they can't support direct connections and applications like direct mailing to the internal hosts and don't support UDP.

Another option is NAT (Network Address Translation). NAT can be found as a separate piece of hardware or software in routers, firewalls and other types like the Alcatel Router Adaptor offered by the public telephone organization in our country for ADSL connections. It works by converting the source address of datagrams, leaving the internal network, from private addresses to official addresses allocated. It has several advantages and the most significant is the conservation of ip addresses. NAT makes possible for organizations to use a large space of private addresses, as discussed before, for configuring the intranet and use a small space of public addresses for internet connections. It also hides the internal structure if the network offering a strong solution against dangerous attacks [14]. Whenever an internal host wants internet access, NAT associates a valid public ip address to the original requesting private ip address. Then all traffic is re-written from public NAT address to NAT public address. This operation is shown in Fig.5. When traffic stops the public ip address returns to the NAT public pool from which the internal hosts drag available public addresses. This is similar to a queue and creates the problem that the hosts must wait to satisfy their requests when this pool is empty [15].

NAT was originally defined in RFC 1631 and extended in RFC 3022. The last one sets itself to solve the queue problem by adopting the proxy concept and assigning each connection a different port number using a single public ip address. So NAT can be either static or dynamic using the ports model. That's why this type is called PAT (Port Address Translation) [16]. Here it is important to note that one difference between NAT and Proxy is that NAT is a layer 3 (network) protocol.

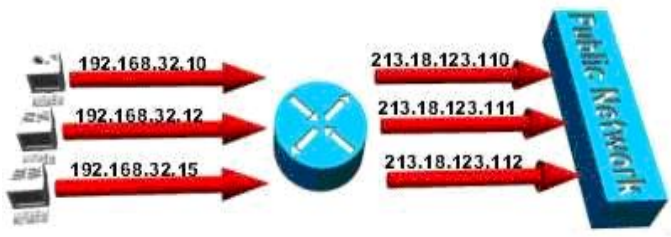

Fig.5 NAT operation

NAT may add cost for new hardware and optional software. It also adds overhead to the processing of every datagram affecting the performance because when an address changes the checksum must be recalculated. An additional negative point is that NAT is a new technology and there is not great experience of using it and this causes instabilities. Among the disadvantages of NAT is the lack of authentication and problems noticed referring to encryption cases.

But, despite their problems Proxies and NAT can give useful solutions to networks which don't have or can't afford the demanded public addresses. So in this coursework's examined organisation NAT and Proxies could be a useful suggestion for Internet Access. Private addresses as they were presented here can be the solution to the potential future growth of the network hosts.

IX. Conclusion

Summarizing, in this coursework, a network overview of the Apocalypse Petro-Chemicals was presented and some suggestions has been made towards the implementation of a more sophisticated network. It is obvious that this model, as presented, is the case that could be met in modern organisational networks.

REFERENCES

[1] A.S. Tanenbaum , *Computer Networks*, 3rd ed., Prentice Hall, 1996, pp. 28-39.

[2] A.S. Tanenbaum , *Computer Networks*, 3rd ed., Prentice Hall, 1996, pp. 412-413.

[3] Cisco CCNP 1: Advanced IP Addressing Management guide.

[4] A.S. Tanenbaum , *Computer Networks*, 3rd ed., Prentice Hall, 1996, pp. 416.

[5] J.F. Kurose, K.W. Ross, *Computer Networking – A Top-Down Approach Featuring The Internet*, 3rd ed., Addison Wesley, 2005, pp. 331-339

[6] http://courses.dce.harvard.edu/~cscie131b/handouts/module4.pdf (URL)

[7] J.D. Wenger, R. Rockell, *IP Addressing and Subnetting Including IPv6*, Syngress, 2000, pp. 13-33

[8] Charles M. Kozierok , The TCP/IP Guide - http://www.TCPIPGuide.com (URL)

[9] http://networking.ittoolbox.com/lp (URL)

[10] J.D. Wenger, R. Rockell, *IP Addressing and Subnetting Including IPv6*, Syngress, 2000, pp. 231-233

[11] .F. Kurose, K.W. Ross, *Computer Networking – A Top-Down Approach Featuring The Internet*, 3rd ed., Addison Wesley, 2005, pp. 491

[12] http://www.unix.org.ua/orelly/networking/tcpip/ch04_02.htm (URL)

[13] http://www.grennan.com/Firewall-HOWTO.html (URL)

[14] http://en.tldp.org/howto/ip-masquerade-howto/what-is-masq.html (URL)

[15] http://www.suse.de/~mha/linux-ip-nat/diplom/nat.html (URL)

[16] J.D. Wenger, R. Rockell, *IP Addressing and Subnetting Including IPv6*, Syngress, 2000, pp. 145-151.

BIBLIOGRAPHY

[A] A.S. Tanenbaum , *Computer Networks*, 3rd ed., Prentice Hall, 1996

[B] J.F. Kurose, K.W. Ross, *Computer Networking – A Top-Down Approach Featuring The Internet*, 3rd ed., Addison Wesley, 2005

[C] J.D. Wenger, R. Rockell, *IP Addressing and Subnetting Including IPv6*, Syngress, 2000

FIGURES

Figures 1, 2, 3 and 5 can be found at http://computer.howstuffworks.com (URL) and many others as they are widely used and their origin is not unique.