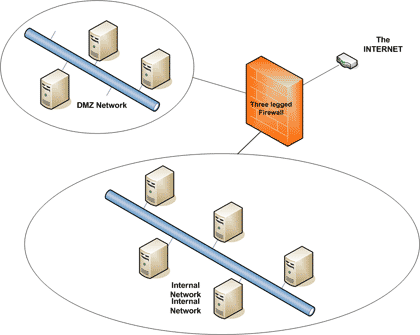
**DMZ: DeMilitarized Zone**

Arun Baalaaji.S Vasudevan.P

II Year B.TECH E.C.E II Year B.TECH E.C.E

DeMilitarized Zone(network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a usually larger and untrusted network, usually the Internet. It is an additional network configuration which is deployed for security purposes. It is being used in most parts of the world.DMZ is also used in most tense borders in the world.

For example,DMZ is used in the border between South Korea and North Korea.

DMZ is also an area of the network where you can place your internet services such as FTP server,E-mail server or Web server that you want public to access.

The purpose of a DMZ is to add an additional layer of security to an organization's LAN; an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.There are multiple configurations,the one which is experimented here is a single firewall network.The DMZ is used to create an isolated network which can be reached from the inside (private) network and the Internet (public) network, but cannot act as a transit point for traffic between the two.

**Now coming to the part why do we need this?**

This is very much important in network security as it can protect the network from cyber attacks.

A DMZ divides splits such a network into two parts by taking one or more devices inside the firewall and moving them to the outside. This configuration better protects the inside devices from possible attacks by the outside (and vice versa).

Also a DMZ is useful in homes when the network is running a [server](https://www.lifewire.com/servers-in-computer-networking-817380). The server could be set up in a DMZ so that Internet users could reach it via its own [public IP address](https://www.lifewire.com/what-is-public-ip-address-818383), and the rest of the home network was protected from attacks in cases where the server was compromised.

**What we need to make it?**

Here in this project we use a tool i.e a development environment which we can use to simulate our network layout virtually , it is called Cisco Packet Tracer. The version we have used in this project is 6.3. Cisco Packet Tracer allows us to simulate any network of our choice without the the bulky need of actual hardware. Cisco Packet Tracer creates virtual machines like routers, switches, servers and many more network and end-network devices with the their entire features and functionalities for us to work on. These virtual machines are near to the actual thing as resemble in every way (in the software front) to the actual hardware you may get in the market.

**How does it work?**

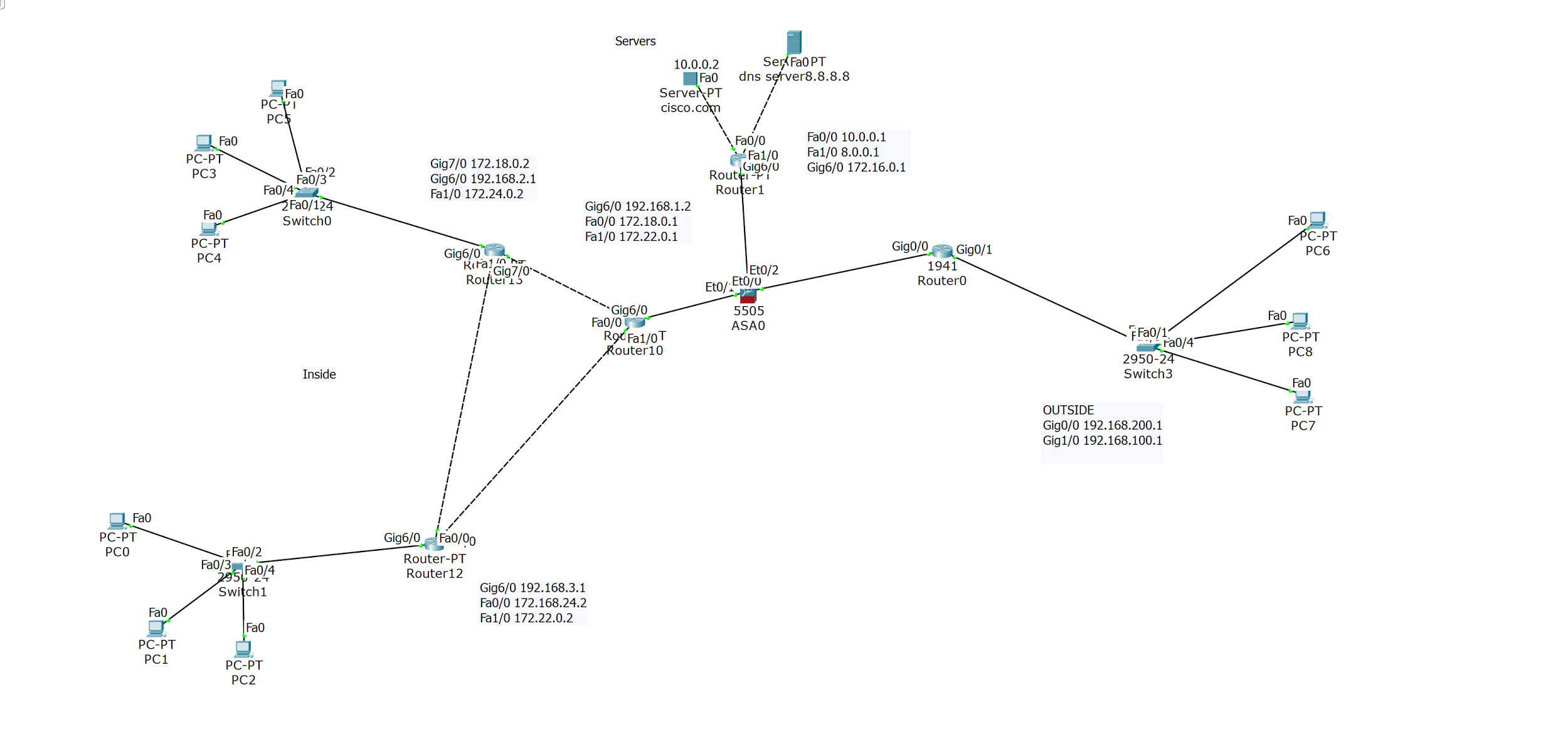
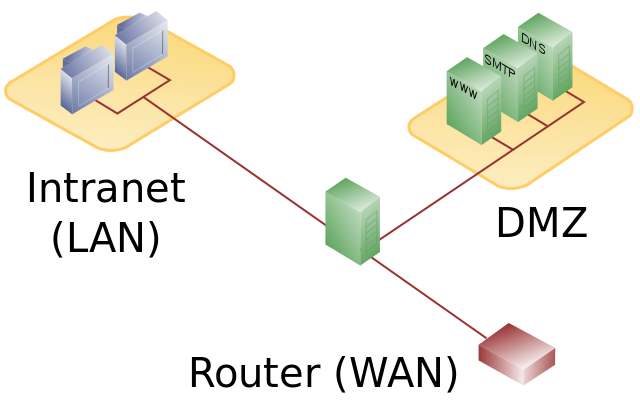


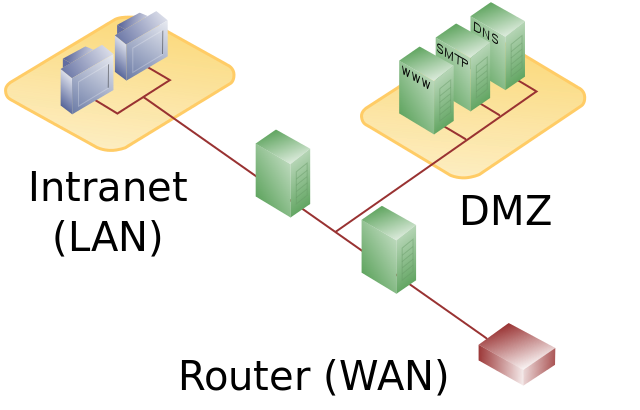
Fig1.0

The above figure shows us the configuration of DMZ we have worked on in this project. There are many different ways to design a network with a DMZ. Two most basic methods are :

1.Single Firewall



2.Dual Firewall



Here in this project we will work with Single Firewall architecture. These designs can be expanded to create very complex architectures depending on the network requirements.

A single firewall with at least 3 network branches can be used to create a network architecture containing a DMZ. The external network is formed from the public network or ISP to the firewall on the first network interface, the internal or private network is formed from the the second network interface, and the DMZ is formed from the third network interface The firewall becomes a single point of failure for the network and must be able to handle all of the traffic going to the DMZ as well as the internal network.

**Configuration of the network:**

Now as we look at Figure1.0 we need to configure the interfaces of the router and enable DHCP on the inside and outside routers to dynamically allocate IP address to the client machines. This can be done using the following commands:

Router>en

Router#configure terminal

Router(config)#int Gig6/0

Router(config-if)#ip address 172.16.0.2 255.255.0.0

Router(config-if)#no shut

To enable DHCP feature , default route and dns in the router we use these commands:

Router(config)#ip dhcp pool <name>

Router(config-dhcp)#net 172.16.0.0 255.255.0.0

Router(config-dhcp)#exit

Router(config)#ip dhcp exclude 172.16.0.1 172.16.0.10

Router(config)#default-router 172.16.0.1

Router(config)#dns-server 8.8.8.8

Now we need to enable OSPF routing functionality in routers in the internal network. For that we use the commands:

Router(config)#router ospf <area number>

Router(config-router)#do show ip route connect

(shows all directly connected adjacent interface)

Router(config-router)#network 192.168.0.1 0.0.0.255 area <number>

Router(config-router)#network 172.18.0.1 0.0.255.255 area <number>

(continue until all adjacent interfaces are added to the configuration)

Router(config)#exit

Now we must configure the Firewall a.k.a the ASA(Adaptive Security Appliance).First we configure the ASA settings and interface security using the CLI:

ciscoasa>en

ciscoasa#conf t

ciscoasa(config)#hostname CISCOASA

CISCOASA(config)#domain-name ccnasecurity.com

CISCOASA(config)#clock set 22:16:00 Jan 28 2017

Now we must configure the ASA interfaces VLAN 1 (inside) will have the highest security setting of 100 and VLAN 2(outside) will have lowest security setting of 0. This is done by using the commands:

CISCOASA(config)#int vlan <nummber>

CISCOASA(config-if)#nameif <name>

CISCOASA(config-if)#ip add 192.168.0.1 255.0.0.0

CISCOASA(config-if)#security-level 100

Now we configure a static route on the ASA outside interface to enable the AS to reach the external networks:

CISCOASA(config)# route outside 0.0.0.0 0.0.0.0 192.168.200.1

Now configure address translation using PAT and network objects.

CISCOASA(config)#object network inside-net

CISCOASA(config-network-object)#subnet 192.168.0.1 255.255.255.0

CISCOASA(config-network-object)#nat (inside,outside) dynamic interface

CISCOASA(config-network-object)#end

Now modify the default the MPF application inspection global service policy:

CISCOASA(config)#class-map inspection\_default

CISCOASA(config-cmap)#match default-inspection-traffic

CISCOASA(config-cmap)#exit

CISCOASA(config)#policy-map global\_policy

CISCOASA(config-pmap)#class inspection\_default

CISCOASA(config-pmap-c)#inspect icmp

CISCOASA(config-pmap-c)#exit

CISCOASA(config)#service-policy global\_policy

Now let us configure DMZ on interface VLAN 3 on the ASA:

CISCOASA(config)#int vlan 3

CISCOASA(config-if)#nameif dmz

CISCOASA(config-if)#ip add 172.16.0.1 255.255.0.0

CISCOASA(config-if)#security-level 70

Assign ASA physical interface E0/2 to DMZ VLAN 3:

CISCOASA(config-if)#int ethernet0/2

CISCOASA(config-if)#switchport access vlan 3

Configure a static NAT to the servers using a network object.

CISCOASA(config)#object network dmz-server

CISCOASA(config-network-object)#host 10.0.0.2

CISCOASA(config-network-object)#nat (dmz, outside) static 192.168.200.3

CISCOASA(config-network-object)#exit

Configure a named access list OUTSIDE -DMZ that permits TCP protocol on port 80 from any external host to the internal IP address of the servers. Apply access list to the ASA outside interface in the ‘IN’ direction.

CISCOASA(config)#access-list OUTSIDE-DMZ permit icmp any host 10.0.0.2

CISCOASA(config)#accss=list OUTSIDE-DMZ permit tcp any host 10.0.0.2 eq 80

CISCOASA(config)#access-group OUTSIDE-DMZ in interface outside

These are the steps needed to create a DMZ network. Complexity will vary according the internal and external network configurations and the type of DMZ architecture you use.

**References:**

* Cisco.com
* Pluralsight.com
* CCNA by Todd Lammle

**Mentor:**

Sandeep Kundala B.Tech E.C.E