ACL

Access Control List

Scenario

Design a Wide area network to serve all kind of customers through DSL (Digital Subscriber Line), Cable Frame-relay, and 3G network. All devices on the network should be able to browse the internet but FTP (File Transfer Protocol); TFTP (Trivial File Transfer Protocol) should be allowed to a handful of devices in belonging to the BIT LANs

Design

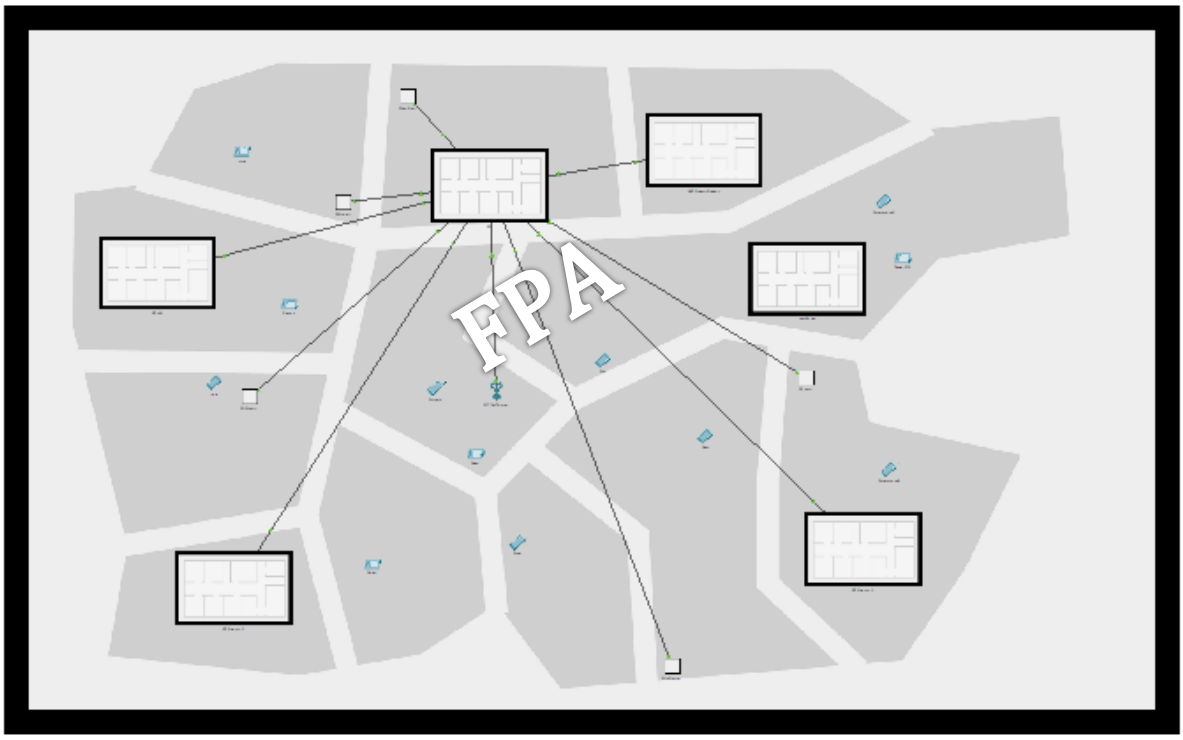

Figure 1 Physical topology

The ISP (Internet Service Provider) represented in the light green bubble has the central infrastructure to serve the entire network.

- **3G Service:** Offers a Cell Tower in the region to which all subscribers (Purple free form) can connect to and browse the internet.
- **DSL Service:** the DSL is serving a private business (A&T Beauty in the light blue bubble) and a branch of BIT (Green Square on the right)
- **Cable Modem:** is used to serve the general public and BIT second branch office (Green Square on the left).
- BIT HQ (Green Bubble) and the Internet Network (Yellow and Blue square) are respectively connected via Frame relay and direct serial link and interact with the core network using static route.

IP Addresses

In order to reach the outside world, each LAN is assigned Public IP addresses represented as follow:

BIT

1. HQ 11.21.4.0/29 255.255.255.248
2. Branch One(1) 11.21.4.8/30 255.255.255.252
3. Branch Two(2) 11.21.4.12/30 255.255.255.252

A&T Beauty 132.32.12.64/29 255.255.255.248

INTERNET

1. Servers 8.8.8.0/29 255.255.255.248
2. Support 8.8.8.8/30 255.255.255.252

Core Network

1. Link to BIT HQ 200.12.21.0/30 255.255.255.252
2. Link to DSL 200.12.22.0/24 255.255.255.0
3. Link to Cable 200.12.23.0/24 255.255.255.0
4. Link to 3G 200.12.24.0/30 255.255.255.0

Private LAN

All private LAN's in the network are assigned private IP addresses. To be able to reach outside networks, edge routers to each LANs have been configured with NAT (Network address translation)

In most cases, devices get their IP addresses through DHCP but essential devices are configured with static Private addresses and are mostly translated using static NAT.

<u>Solving the problem</u>

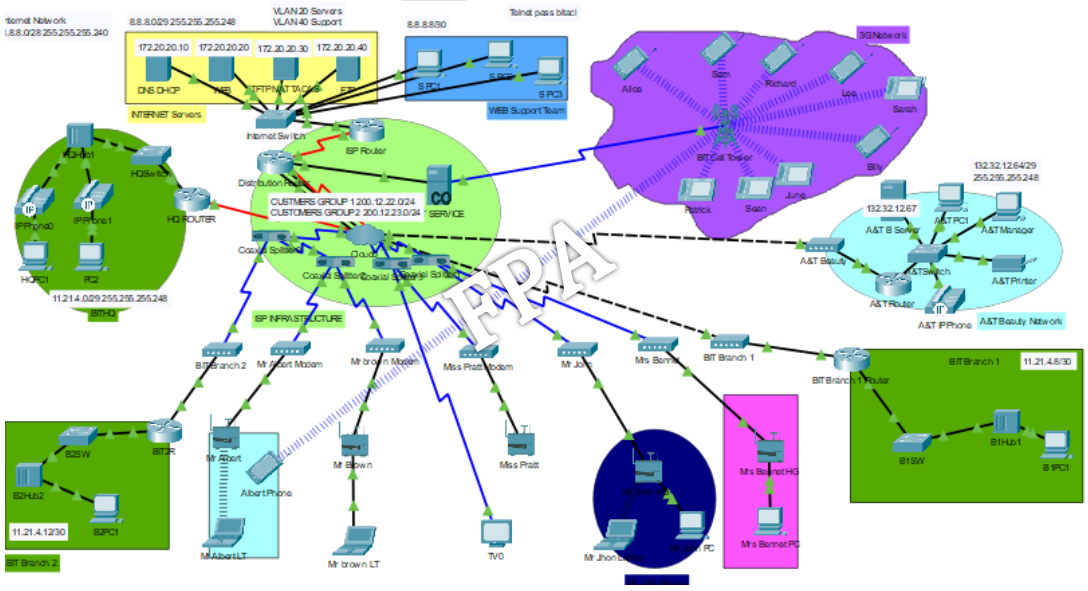

Figure 2 Logical View

Prior to implementing ACL, all devices on the network were able to ping each other. Static routes were used to route information in the core network.

Implementing ACL where ever needed allows only certain devices to have connectivity with every other device on the network. Restrictions were implemented to allow the majority of devices only DNS and HTTP service on the network.

Please refer to each device startup configuration for the command used to implement the topology.

A much robust way to implement this would have been the use of specialised security devices such as the Cisco Adaptive Security Appliance (ASA). In a production environment, each LAN owner will be responsible for the traffic entering or leaving its network. With an ASA at the INTERNET site, traffic could be filtered using more options to implement robust security.

Connect Happily

FPA