Filter access to resources using ACL

Definition

Access lists are configured to allow control of devices access to and from network and/or nodes. Many appliances and software are available for the implement of network and traffic filtering, however ACL control List is available to network technician help design and implement solutions that can prevent certain traffic from entering or exiting a network.

More robust design will be ACL configured on Firewalls (ASA …) devices, however most cisco support ACL capabilities and this is helpful for small companies looking at the cost of implementing their infrastructure.

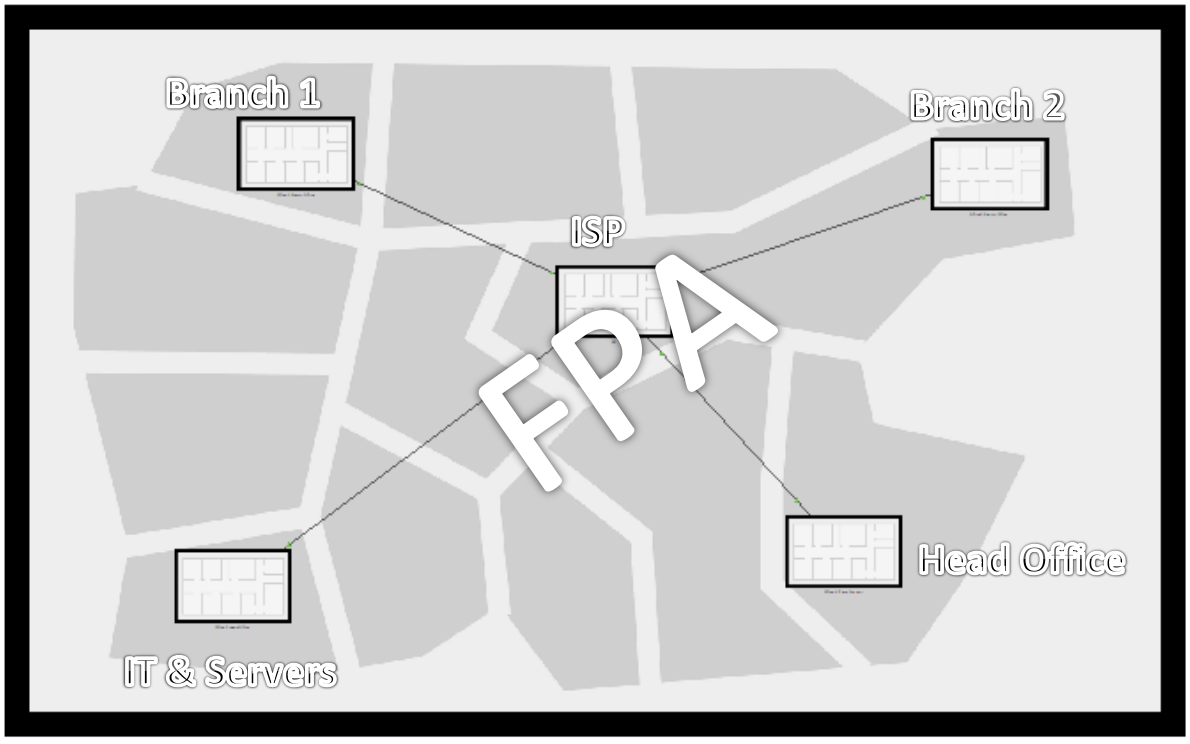
Design Scenario

Design and implement a network with four (4) sites, each assigned a range of public IP addresses to allow internet connectivity.

The Network belongs to a company called BIT and is to be designed as follow:

1. Server site: The site host all of the company servers and is the base to the IT department
2. Main Office site: Were the coy operational will be based. A small team of IT technicians will be based on site for local supports
3. Branches: to branches will be used for supporting operation duty and will also have IT teams on site for support

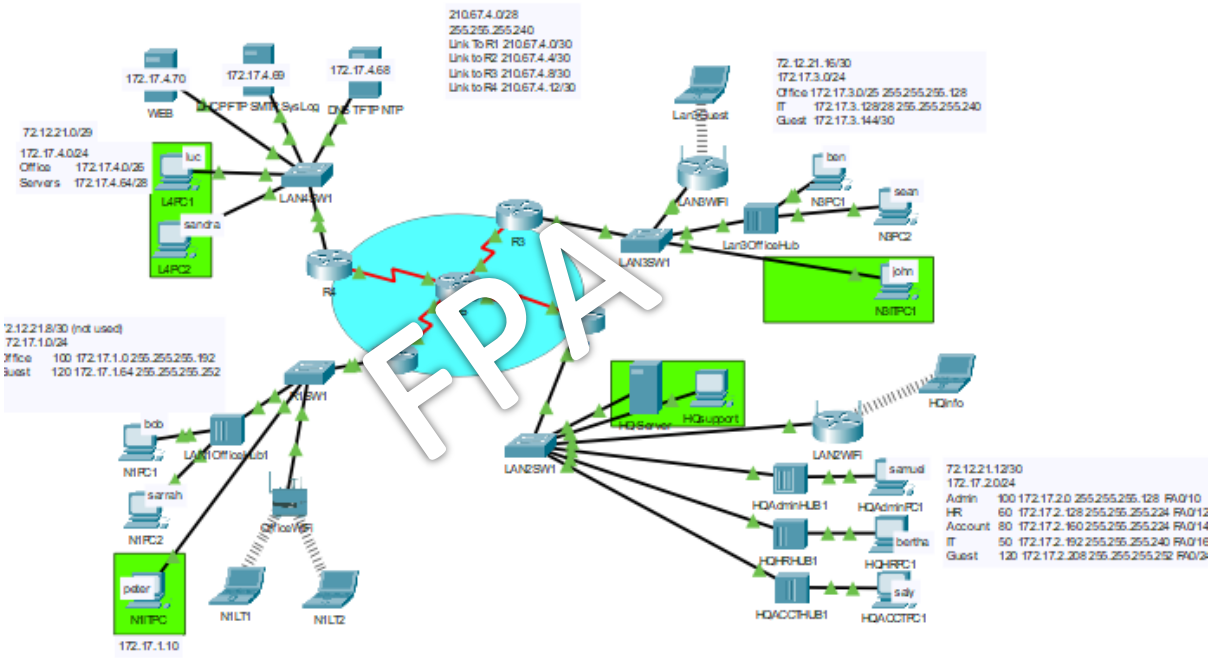
All sites are connected together through an ISP and have dedicated lines using static routes for connectivity.



The packet tracer file associated allows users to navigate through site and view the physical configuration of the devices.

Services in the network

- WEB - All users are allowed access to the WEB service only. The web server is preconfigured with the DNS server which allows users to enter the site name www.bit.com instead of its IP address 72.12.21.4. This can be done using any machine linked to the network
- FTP - Only IT devices can access the FTP server. Access control has been configured to only allow IT Technicians (In Green rectangle in Figure below) access to FTP services
- SMTP and POP3-All users can access the mail server. Every user in the network has had an email configured and can send and receive email using SMTP or POP3. The mail domain name is bit.com and an example of email will be; bob@bit.com
- Syslog -Configuration to allow routers log secured to be used by the layer 3 devices as log server
- DNS – Access allowed to all users for domain name translation service.
- TFTP -Reserved for only the routers in the network to save configuration
- NTP -Used by routers to update system time



For configuration commands please refer to the packet tracer file associated.

Additional

An extra layer of security was added to allow only SSH access to the company Routers. Only members of the IT department can remotely connect to the routers. At this stage, everyone in IT has full access to the routers configuration commands. This is not practical and CISCO allows for privileged user configuration to define which user does what on the device (Feature to be demonstrated in future posts).

IP Addressing

- Network 1 (R1) 72.12.21.8/30
- Network 2 (R2) 72.12.21.12/30
- Network 3 (R3) 72.12.21.16/30
- Network 4 (R4) 72.12.21.0/29