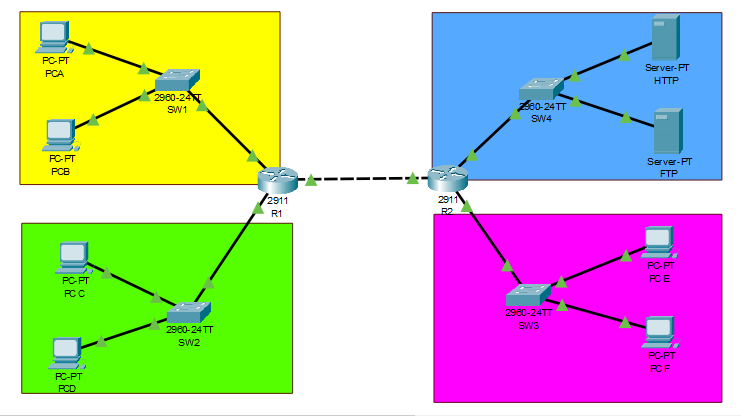
Task 2: Packet Filtering Using Access Control List

Objective: Filter packets and restrict traffic on the network by configuring standard IPv4 ACLs.

Table for configuration:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | ````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````` |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

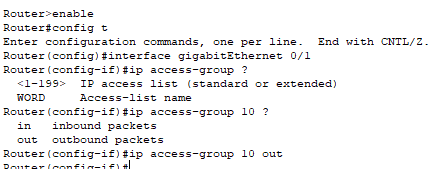
Following working network is obtained after configuration using above table.



Part 1: Configure a standard IPv4 ACL to Restrict Access to PINK LAN

Step 1: Access-List

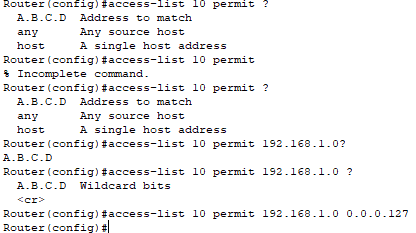
* Access list number is 10



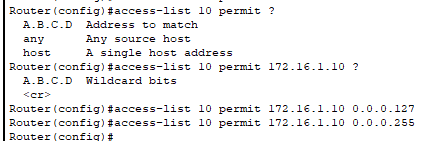
* Permit PC C to reach pink LAN



* Permit only first half of hosts PC A on the yellow LAN so they reach Pink LAN

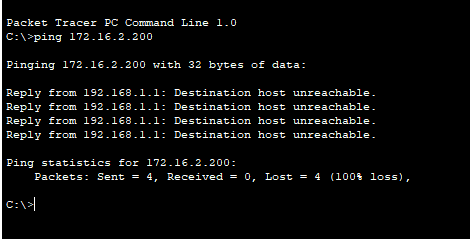


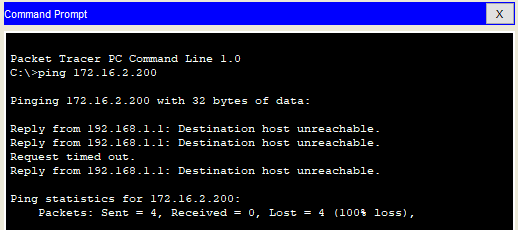
* Permit all of the servers on the blue LAN to reach Pink LAN



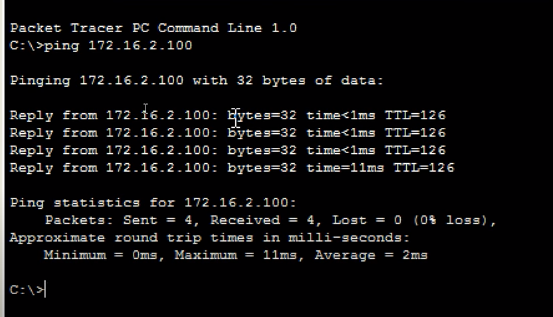
Step 2: Create, Apply and Test Access List

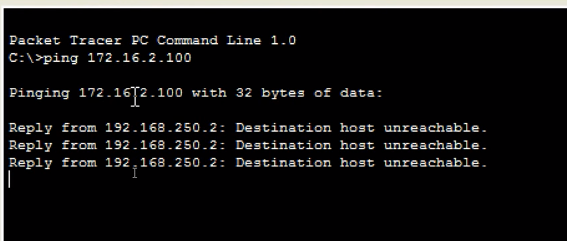
1: All pings from PINK LAN to Yellow LAN are successful but pings from PC B are denied:



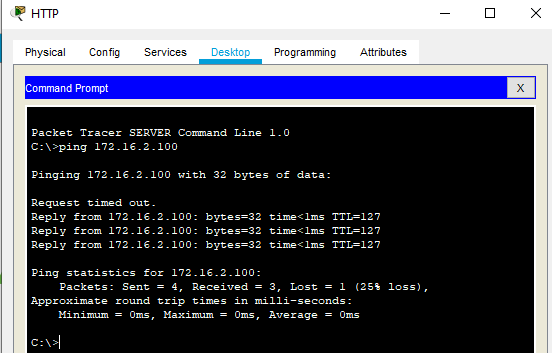


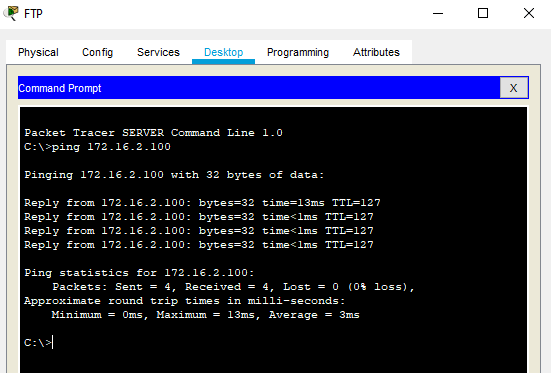
2: A ping from PC C to PINK LAN is Successful while ping from PC D to PINK LAN is denied:





3: Pings from BLUE LAN Servers to PINK LAN are Successful:





Part 2: Configure an extended IPv4 ACL to Restrict Access to Blue LAN

Access list has three access control entries

* Access list number is 199
* 
* Deny Yellow LAN from reaching HTTP server in Blue LAN



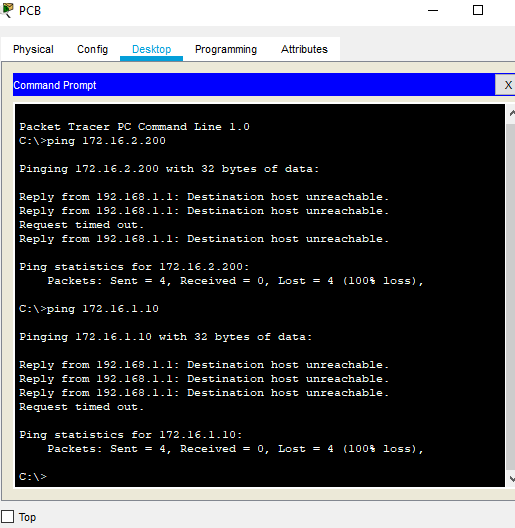


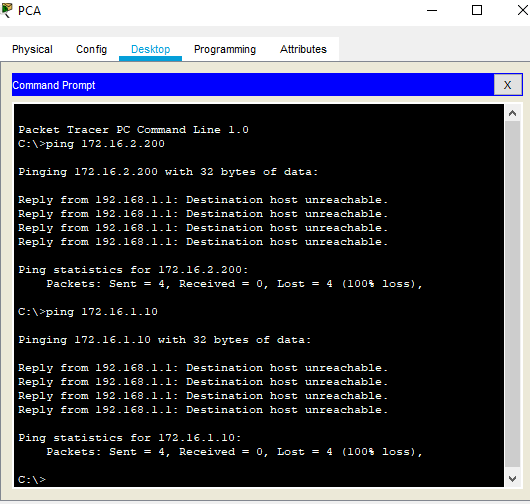
* Allow all other network to reach Blue LAN



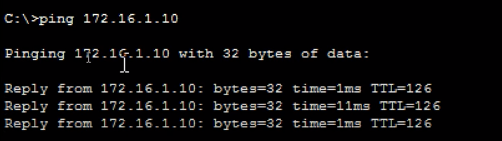
Step 2: Create, Apply and Test Access List

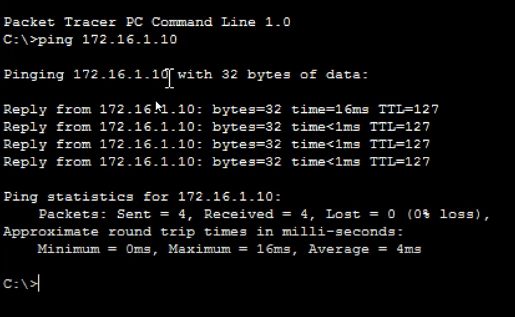
1: All the PCs in the Yellow LAN will not be able to access hosts of blue LAN





2: All hosts in PINK and BLUE LAN are able to access servers in BLUE LAN





These Access Control List (ACL) statements need to be applied inbound on the interface that joins the Pink and Blue Local Area Networks (LANs), using the Router2's interface GigabitEthernet0/2.

Conclusion:

In conclusion, the mission entailed the establishment of IPv4 Access Control Lists (ACLs) that were both conventional and upgraded in order to enforce certain traffic limits on the structure of the network configuration (Grout, 2007). The purpose of the standard Access Control List (ACL) was to allow communication from local area networks (LANs) that were not the Yellow LAN to access the Yellow LAN, while at the same time restricting communication from the Pink LAN to the Yellow LAN (Mythrei, 2014). Through the successful implementation of Access Control List (ACL) number 10 on the outward direction of Router1's interface Fa0/1, this objective was successfully accomplished. For the sole purpose of limiting access to the FTP server located on the Blue LAN, the expanded Access Control List was developed (Thakar, 2012). It restricts access to it to just those hosts that are part of the Pink Local Area Network (LAN), while allowing all other LAN traffic to continue unimpeded. To accomplish this, Access Control List (ACL) number 199 was built on the Gigabit Ethernet0/2 interface of Router2 in the direction of incoming traffic. It is the responsibility of this interface to connect the Pink and Blue local area networks. The network was able to retain connectivity for legitimate communication demands while simultaneously enforcing traffic limitations thanks to the configurations of the access control list (ACL). Adaptations were made to the IP addresses, interface names, and access control list entries in order to fulfil the particular requirements of the network configuration through the implementation of modifications (Simanjuntak, 2012).

References

Grout, V., McGinn, J., & Davies, J. (2007). Real-time optimisation of access control lists for efficient Internet packet filtering. *Journal of Heuristics*, *13*, 435-454.

Mythrei, S., & Dharmaraj, R. (2014). Packet classification based on standard access control list. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *3*(1).

Thakar, U., Purohit, L., & Pahade, A. (2012, September). An approach to improve performance of a packet-filtering firewall. In *2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN)* (pp. 1-5). IEEE.

Simanjuntak, P., & Suharyanto, C. E. (2017). Analisis Penggunaan Access Control List (Acl) Dalam Jaringan Komputer Di Kawasan Batamindo Industrial Park Batam. *Journal Information System Development (ISD)*, *2*(2).