CCNA Discovery

Working at a Small-to-Medium Business or ISP

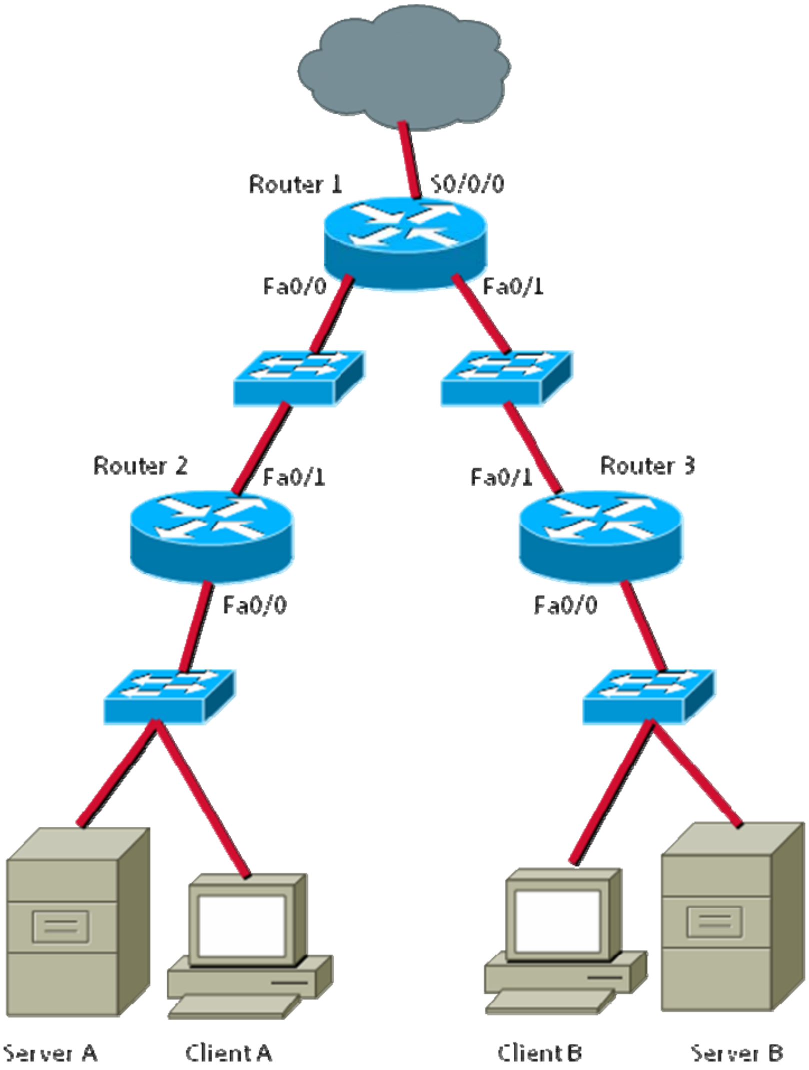
Lab 8.2.1 Planning for Access Lists and Port Filters

Objective

- Based on the predefined network diagram, determine where to implement access lists and port filters to help protect the network.

Background

You are the support technician sent onsite to assess the current network for a business customer that would like to reduce the risk of a security breach on the network.



Identifying where to place access lists

Step 1: Restrict Client A to one subnet

You are asked to restrict Client A to only the subnet to which it is currently attached. Client A needs to be able to access Server A, but it does not need to access the Internet or Server B. Where would you place the access list?

Router	Interface	Allow or Deny?	Input or Output filter?	Why?

Step 2: Restrict Client A access to Server A but allow access to Server B and the Internet

You are asked to restrict Client B from accessing Server A, but Client B needs Internet access and access to Server B. Where would you place the access list?

Router	Interface	Allow or Deny?	Input or Output filter?	Why?

Step 3: Allow only Client A to access the routers using only SSH

You have been asked to secure access to the routers for only Client A, which will be the management PC for those routers. You want to limit access to only SSH from Client A and prevent Telnet access. Where would you place the access list?

Hint: More than one interface on more than one router is needed to control SSH and Telnet access to the routers.

Router	Interface	Input or Output filter?	Port	Allow or Deny?	Why?