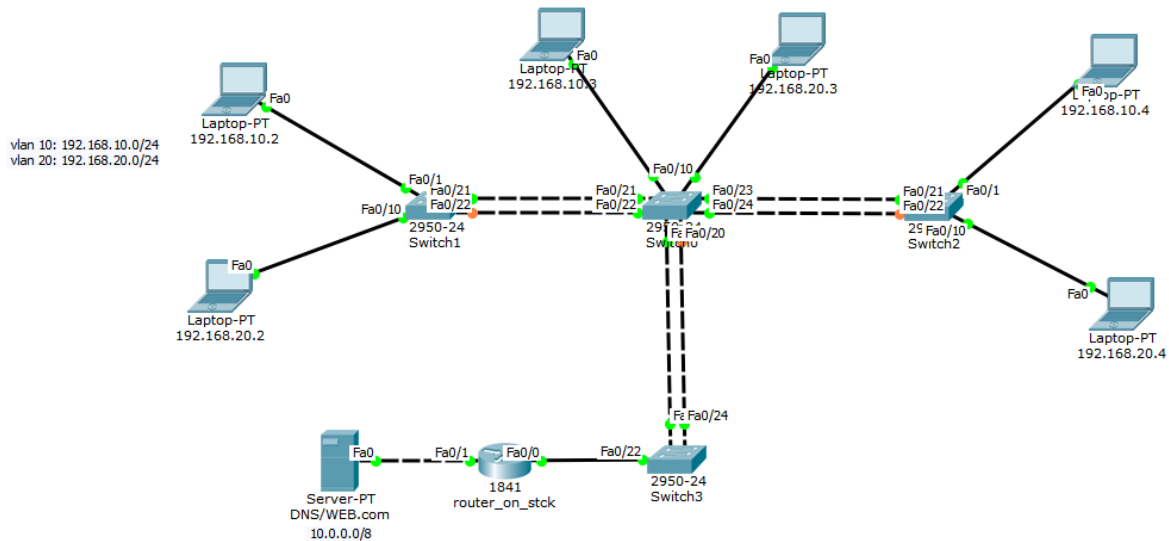


Laboratorio 6 y 7 e investigación 2 (fecha de entrega: sábado 5 de diciembre)

Se tiene el siguiente escenario de red el cual contiene 2 vlans 192.168.10.0/24 (vlan10) y la 192.168.20.0/24 (vlan20), tal y como se muestra a continuación:



LAB#6: diseñe la red tal que todas la vlans tengan acceso al server cuya red es la 10.0.0.0/8, en donde se encuentran el DNS y WEB.com, a usted le entregan esa red así y no dicen nada más valore con los conocimientos obtenidos dentro del curso si debe implementar algo más, debe hacer uso de dhcp en router_on_stick.

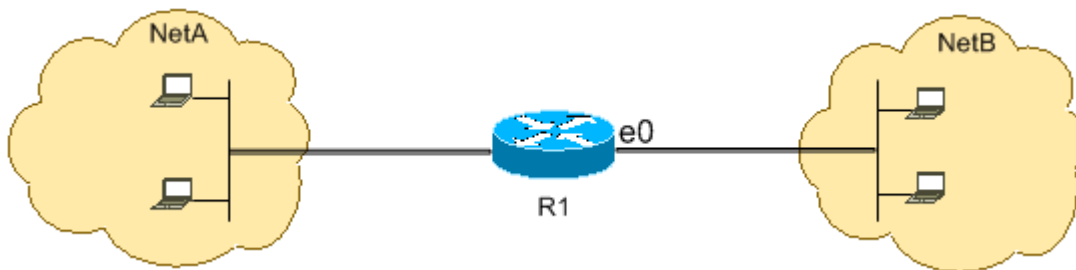
Lab#7: ahora le solicitan que pase a una solución inalámbrica al problema anterior ya que la implementación es de interés de la empresa para ambas alternativas y así valorar cual es la más viable para ser implementada.

Vale por la investigación 2: la investigación 2 requiere de filtros extendidos y se le solicita a usted que bloquee el puerto 80 (acceso vía www) de la vlan 2 al servidor web, pero no así los pings por ejemplo de esa vlan 2 a la red 10.0.0.0/8, ahora la vlan 1 deberá tener la posibilidad de acceder vía browser y hacer pings no habrá restricciones para ella. De igual manera evalúe sus soluciones y escoja la mejor que se pueda.

Les incluyo algunos ejemplos de cómo se verían los comandos para que tengan una idea de cómo deben guiar su investigación

Permita el HTTP, Telnet, correo, POP3, FTP

En esta figura, se muestra que se permite solo el tráfico FTP, POP3, Simple Mail Transfer Protocol (SMTP), Telnet y HTTP, y que se niega el resto del tráfico con origen en la Red B y destino en la Red A.



Esta configuración permite el tráfico TCP con valores de puerto de destino que coincidan con datos FTP (puerto 20), FTP (puerto 21), POP3 (puerto 110), SMTP (puerto 25), Telnet (puerto 23) y WWW (puerto 80). Tenga en cuenta que una cláusula total de negación implícita al final de una ACL niega el resto del tráfico, que no coincide con las cláusulas de permiso.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any any eq www
access-list 102 permit tcp any any eq telnet
access-list 102 permit tcp any any eq smtp
access-list 102 permit tcp any any eq pop3
access-list 102 permit tcp any any eq 21
access-list 102 permit tcp any any eq 20
```