Guía de Trabajo

De acuerdo a el ejercicio dado en Packet Tracer, realizar:

• Configurar Los puertos de acceso de los Switches, de modo que los equipos pertenecientes a las VLAN 15,30 y 100

• Almacenen de forma manual el direccionamiento físico de los dispositivos. MANUAL

• Asegúrese que en caso de recibir una dirección física diferente a la configurada, se envié un mensaje de LOG a el servidor “LOGGG”, pero que el puerto siga recibiendo información (Drop)

• Asegúrese de que al momento de hacer un “show interface trunk”, nunca aparezca el mensaje “n-802.1q” (Todos los puertos de acceso jamás deben mostrar este mensaje”

• Realice prunning de VLAN de forma manual

• Al momento de recibir una BPDU superior el switch debe descartarla y junto con eso si llegase a recibir cualquier BPDU el puerto debe quedar en “Error Disable”

• Asegurece de que el host conectado al puerto sea capaz de enviar información inmediatamente desde que es conectado a la red.

• Configurar Los puertos de acceso de los Switches, de modo que los equipos pertenecientes a las VLAN 25 y 95

• Almacenen de forma dinámica el direccionamiento físico de los dispositivos. DHCP

• Asegúrese que en caso de recibir una dirección física diferente a la configurada, el puerto incremente el contador y que se apague.

• Asegúrese de que al momento de hacer un “show interface trunk”, nunca aparezca el mensaje “n-802.1q” (Todos los puertos de acceso jamás deben mostrar este mensaje”

• Realice prunning de VLAN de forma manual

• Al momento de recibir una BPDU superior el switch debe descartarla y junto con eso si llegase a recibir cualquier BPDU el puerto debe quedar en “Error Disable”

• Asegurece de que el host conectado al puerto sea capaz de enviar información inmediatamente desde que es conectado a la red.

• Implemente una solución capaz de evitar el ataque VLAN Hopping

• Asegúrese que no pueda existir un ataque de DHCP en la red

• En caso de recibir Broadcast desde el acceso, los puertos deben limitarlos a 4 Mbps máximo y en caso de recibirlos desde sus uplinks, deben ser limitados a 30 mbps. Storm-control

• Asegúrese de que la tabla CAM, se “refresque” cada 10 segundos más de su valor por defecto.

• Los links entre DLS1 y DLS2, deben ser parte de un link de agregación, y el protocolo a configurar debe ser capaz de operar con otras marcas.

• Configure un FHRP, en donde DLS1 sea Default Gateway de la VLAN 15 y 95 y DLS2 Default Gateway de la VLAN 25 y 30

• Optimice STP, y en caso de que los ROOT reciban un BPDU superior, estos deben descartarlo. (Para optimizarlo solo puede ocupar valores numéricos, jamás que los switches auto descubran las prioridades que tienen los otros switches.)

• Todo el Ruteo, debe ser realizado con EIGRP. Asegúrese de que los Host en el acceso jamás puedan recibir algún mensaje del protocolo, y en caso de hacerlo este mensaje debe estar cifrado.

• El Router de Borde, debe realizar NAT para llegar a el Servidor HTTP (www.entel.cl) de ENTEL, desde todos los equipos internos de la red (No DMZ)

• El servidor DMZ-http debe ser alcanzable al menos via IP (No URL) desde Internet (Probar este punto desde Servidor DNS del ISP)

• Recuerde en este punto que todas las redes pertenecientes a la RFC1918 no pueden ser publicadas hacia internet.

• El Router de Borde, debe ser capaz de mantener la visualización de todas las conexiones originadas desde el interior de su RED y al exterior de su red (Internet). Los protocolos de los que debe tener visibilidad son HTTP, DNS, Ping, todos los demás protocolos no se deben inspeccionar, solo permitirlos pasar.

• El Router del ISP, debe implementar una tecnología, capaz de tener visibilidad a nivel de Capa 7. Esta tecnología deberá manejar Firmas y debe ser capaz de contar todo el tráfico “en línea¨ (IN-LINE). Lo que debe verificar es que no se realicen ICMP-Request a el servidor HTTP