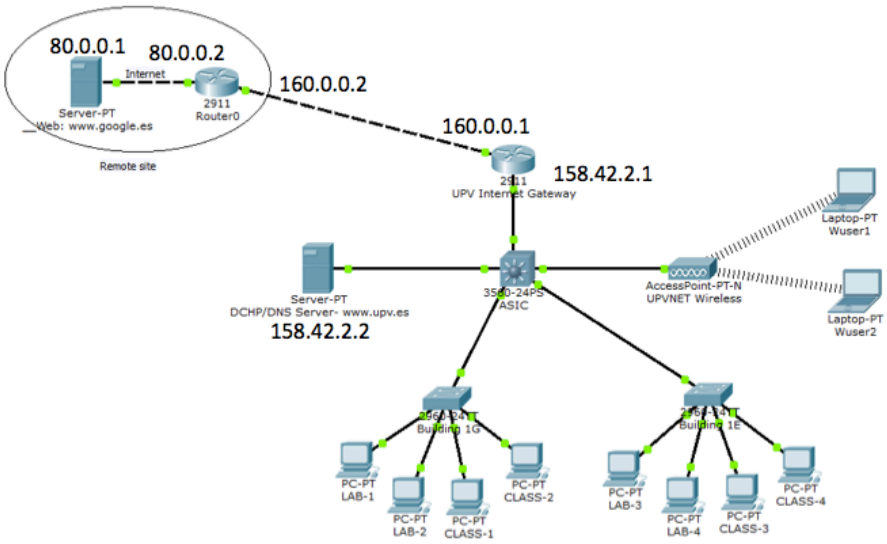
Configuración de una LAN basada en hardware Cisco en entornos corporativos

Descripción general

En este trabajo se pretende que el alumno adquiera conocimientos y destrezas en el ámbito de la gestión de dispositivos de red avanzados en entornos corporativos. Para ello se propone el uso de la herramienta Packet Tracer de Cisco, la cual permite gestionar diferentes tipos de dispositivos de red de manera muy similar a los dispositivos reales.
En lo que respeta a competencias transversales, se trabajarán las competencias de *trabajo en grupo y liderazgo* y *aprendizaje permanente*:
http://competencias.webs.upv.es/wp/

Escenario inicial

En este trabajo el alumno parte de un escenario dónde se representa una red corporativa de tamaño reducido (UPV), así como una red externa (80.0.0.0/8) accesible mediante en Internet Gateway de la UPV, y en la cual está alojado el servidor web del dominio www.google.es:



La red de la UPV se caracteriza por un elemento central situado en el ASIC, y que consiste de un Layer-3 Switch:

- Cisco Catalyst 3560-24PS: 24 Ethernet 10/100 ports with PoE and 2 SFP-based Gigabit Ethernet ports; 1 RU

El escenario incluye también dos switches situados en los edificios 1G y 1E, del modelo:

- Cisco Catalyst 2960-24TT-L

Inicialmente todos los dispositivos de la red UPV están en la VLAN por defecto (1), y se usa únicamente una subred (158.42.2.0/24) del conjunto de direcciones disponible (158.42.0.0/16).
La red de la UPV dispone de un único servidor (158.42.2.2), el cual realiza las funciones de servidor DNS, servidor DHCP y servidor web del dominio: www.upv.es.
Todos los PCs y portátiles solicitan su dirección IP a este servidor, el cual inicialmente les asigna direcciones en el rango utilizado (158.42.2.0/24).
Los portátiles se autentican usando WPA2-PSK (clave compartida).

La red inicialmente propuesta tiene varios problemas a nivel de seguridad y prestaciones, por lo que hará falta mejorarla para obtener una configuración más robusta.

Objetivo

El objetivo del trabajo es introducir múltiples mejoras a la red de la UPV representada de manera a mejorar sus prestaciones, seguridad y funcionalidad. Siendo así, la configuración final de la red deberá segmentar el tráfico en diferentes VLANs, introducir autenticación basada en servidor RADIUS para los clientes inalámbricos, mejorar el ancho de banda entre el switch del ASIC y los switches de los edificios 1G y 1E, e introducir redundancia en la red.

A continuación se definen diferentes etapas, las cuales permitirán alcanzar el objetivo final de manera incremental.

Etapa 1: Creación de las VLANs Main, Lab y Class

En esta primera etapa hay que realizar las siguientes tareas:

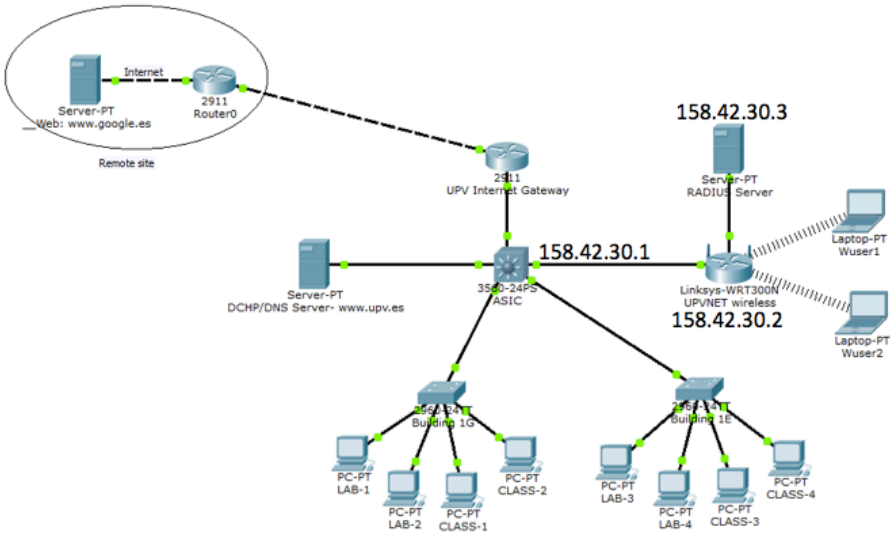
1. Crear las VLANs main (2), lab (10) y class (20) en todos los switches.
2. El Gateway de la UPV, el servidor y el punto de acceso deberán estar en la VLAN 2.
3. Todos los PCs con nombre Lab-x deberán estar en la VLAN 10.
4. Todos los PCs con nombre Class-x deberán estar en la VLAN 20.
5. Las conexiones entre el Switch del ASIC y los Switches 1G y 1E deberán ser trunk que solo admiten tráfico de las VLANs 10 y 20.
6. El switch del ASIC deberá disponer de interfaces de red para las VLANs 2, 10 y 20 con las siguientes IPs:
    a. VLAN 2: 158.42.2.3/24
    b. VLAN 10: 158.42.10.1/24
    c. VLAN 20: 158.42.20.1/24
7. Deberá habilitar la función de router en el switch del ASIC
8. Deberá hacer los cambios necesarios en el switch del ASIC y en el servidor DHCP para que este último pueda servir direcciones a los clientes de la VLAN 10 en su rango correspondiente.

9. Deberá hacer los cambios necesarios en el switch del ASIC para que el propio switch pueda servir direcciones a los clientes de la VLAN 20 en su rango correspondiente.
10. Deberá actualizar la tabla de routing del switch del ASIC de manera a poder alcanzar destinos fuera de la red de la UPV.
11. Compruebe que todo funciona correctamente: los clientes reciben sus IPs por DHCP y pueden visitar la web www.google.es sin problemas.
12. Si todo es correcto guarde la configuración en switches y routers mediante el comando "write" y pulse "Guardar".

Etapa 2: Mejoras a la seguridad de la red inalámbrica

En esta etapa hay que realizar las siguientes tareas:

1. Crear la VLAN wireless (30), la cual operará con el rango de direcciones IP 158.42.30.0/24.
2. En el switch del ASIC, asignar la IP 158.42.30.1 al interfaz correspondiente a la VLAN 30.
3. Reemplazar el punto de acceso actual por el dispositivo Linksys WRT300N, el cual da soporte a autenticación RADIUS. El dispositivo se conecta al switch del ASIC en un puerto vinculado a la VLAN 30.
4. Configure el router inalámbrico Linksys para que reciba la IP estática 158.42.30.2. Deshabilite el servidor de DHCP. Recuerde que el dispositivo no deberá funcionar como Router/NAT en ningún momento.
5. Añada un servidor RADIUS (AAA), el cual se conectará directamente al router Linksys, y recibirá la IP estática 158.42.30.3/24.



6. Configure la clave de seguridad RADIUS en el servidor RADIUS y en el punto de acceso Linksys. En el punto de acceso ajuste el SSID a "UPVNET".
7. Cree credenciales de acceso para dos usuarios en el servidor RADIUS, y configure los portátiles con sus credenciales correspondientes.
8. Verifique que los clientes se conectan correctamente al router Linksys.
9. Deberá hacer los cambios necesarios en el switch del ASIC y en el servidor DHCP para que este último pueda servir direcciones a los clientes de la

VLAN 30 en su rango correspondiente.
Nota: evitar servir las direcciones usadas por el router Linksys y el servidor RADIUS para evitar IPs duplicadas.

10. Verifique que los clientes reciben su IP por DHCP y se conectan con éxito a www.google.es.
11. Si todo es correcto guarde la configuración en switches y routers mediante el comando "write" y pulse "Guardar".

Etapa 3: Mejoras a la capacidad de los enlaces entre ASIC y edificios 1G/1E

En esta etapa vamos a crear Etherchannels para mejorar la capacidad entre switches:
http://es.wikipedia.org/wiki/EtherChannel

Para eso hay que realizar las siguientes tareas:

1. Crear la interfaz 1 del tipo port-channel en el switch del ASIC y en el switch del edificio 1G.
2. Crear la interfaz 2 del tipo port-channel en el switch del ASIC y en el switch del edificio 1E.
3. Crear un segundo enlace entre el switch del ASIC y el switch del edificio 1G conectado al puerto FastEthernet 0/6 en ambos switches.
4. Crear un segundo enlace entre el switch del ASIC y el switch del edificio 1E conectado al puerto FastEthernet 0/7 en ambos switches.
5. Asegurarse que los nuevos enlaces y los port-channel creados son del tipo trunk, y solo aceptan las VLANs 10 y 20.
6. Añada los enlaces entre switches a los port-channel correspondientes. Se sugiere utilizar el modo siempre "ON", ya que tanto PAgP como LACP dan problemas en Packet Tracer.
7. Si todo es correcto (todos los enlaces están activados con color verde claro y no verde oscuro, rojo o amarillo) guarde la configuración en switches y routers mediante el comando "write" y pulse "Guardar".

Etapa 4: Entrega del trabajo

Después de verificar que la configuración del escenario es correcta, y asegurarse que las comunicaciones funcionan correctamente, sube el fichero con el escenario Packet Tracer (.pkt) a la plataforma Poliformat para evaluación. Se habilitará una "Tarea" con ese propósito. Solo uno de los miembros del grupo deberá subir el trabajo a la plataforma.

Enlaces útiles

General:

- Documentación del Switch Catalyst 2960
- Documentación del Switch Catalyst 3560
- http://www.study-ccna.com

- http://www.freeccnaworkbook.com/workbooks/ccna
- http://www.cisco.com/en/US/docs/ios/12_2/switch/command/reference/fswtch_r.html
- http://www.ciscopress.com/articles/article.asp?p=358549

VLANs:

- http://www.dummies.com/how-to/content/cisco-networking-switch-management-interface-confi.html
- http://www.freeccnaworkbook.com/workbooks/ccna/configuring-a-management-vlan-interface

Trunking:

- http://blog.alwaysthenetwork.com/tutorials/etherchannel-tutorial/

Nota importante:
Los dispositivos Cisco simulados en la herramienta Cisco Packet Tracer solo soportan un conjunto reducido de los comandos disponibles en un dispositivo real.