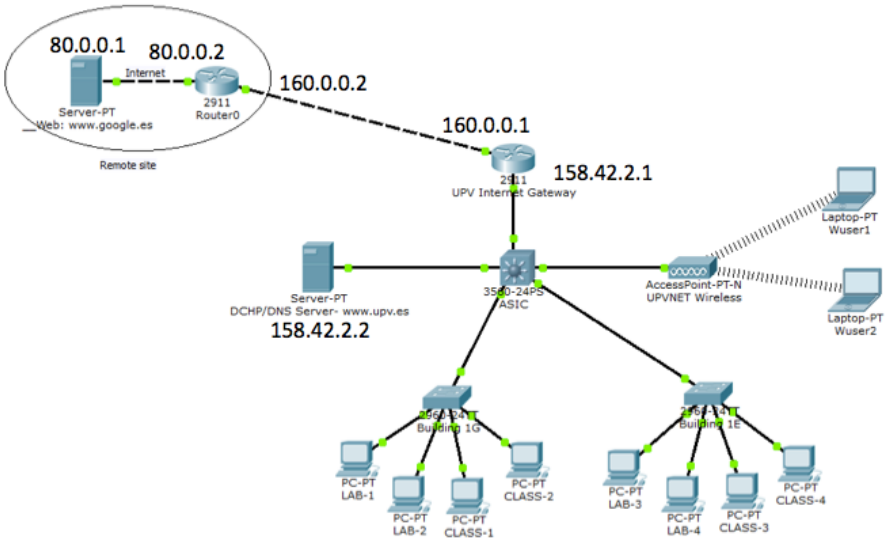
Configuración de una LAN basada en hardware Cisco en entornos corporativos

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 trabajará la competencia de *trabajo en equipo y liderazgo*.

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.

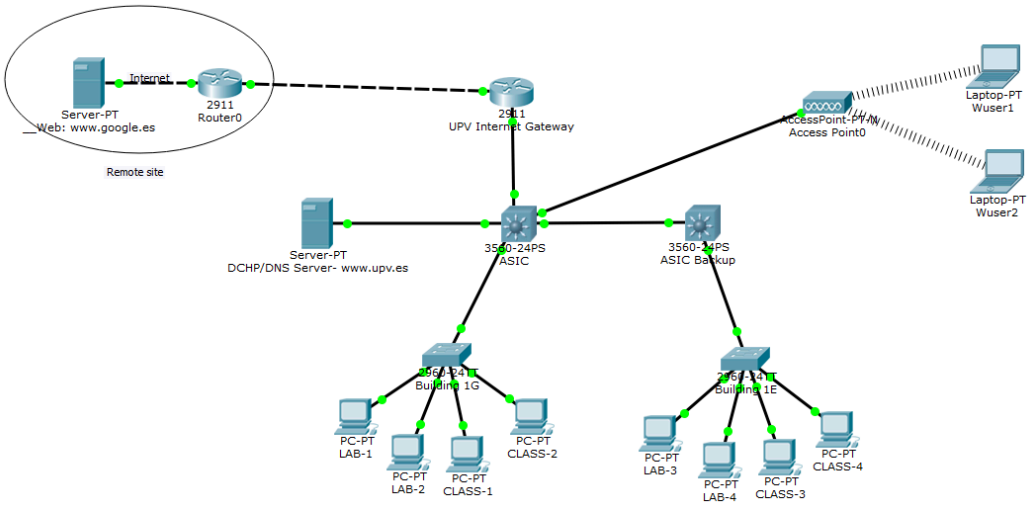
Objetivo

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, añadir la red inalámbrica eduroam, 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

Para empezar con la primera etapa, añada un switch 3560-24PS que deberá ser nombrado “ASIC Backup”. A continuación, modifique las conexiones entre switches para que los switches del ASIC están enlazados entre sí, y para que el switch del edificio 1E se conecte únicamente al switch ASIC Backup, tal y como se ilustra en la figura:

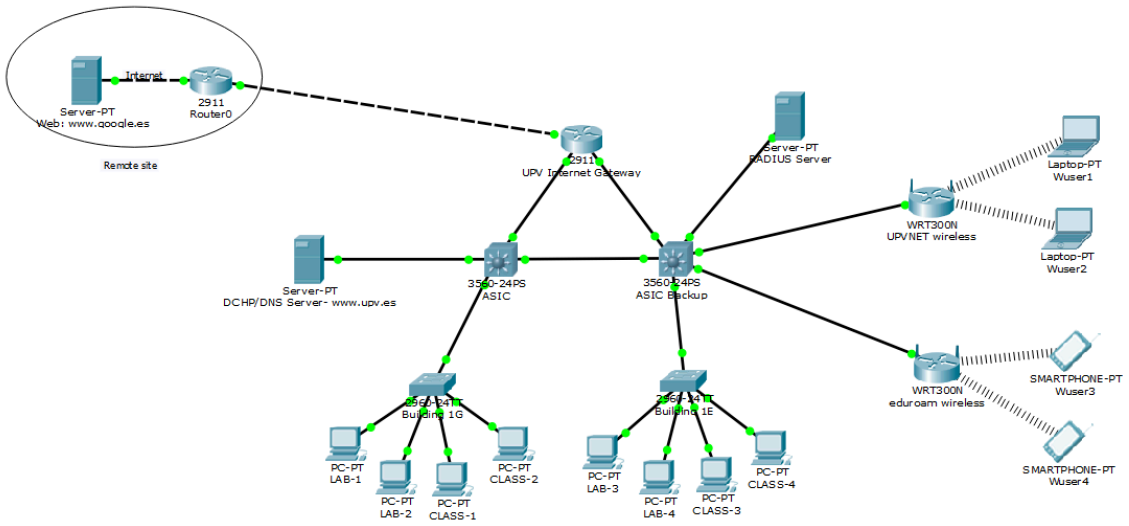


En esta primera etapa hay que realizar las siguientes tareas:

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 ambos Switches del ASIC, y sus enlaces con los Switches 1G y 1E, deberán ser del tipo trunk y solo admitir 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 principal del ASIC.
8. Deberá hacer los cambios necesarios en el switch del ASIC y en el servidor DHCP para que el servidor DHCP pueda servir direcciones IP 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 IP a los clientes de la VLAN 20 en su rango correspondiente.
10. Deberá actualizar la tabla de routing del switch 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”.

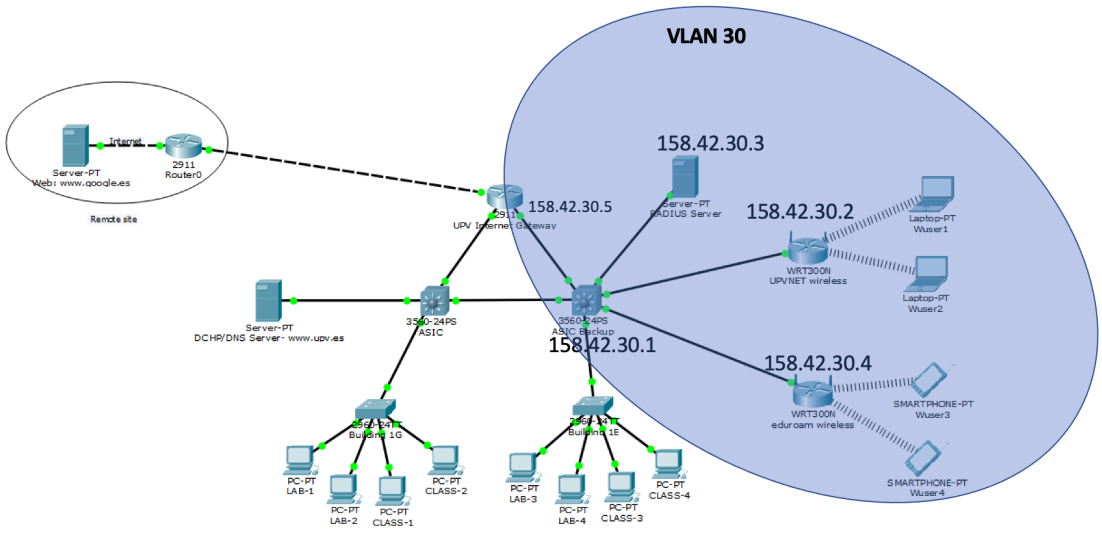
Etapa 2: Mejoras a la seguridad de la red inalámbrica

En esta segunda etapa hay que modificar la red de manera que el resultado final sea el que se ilustra en la siguiente figura:



Para lograrlo, en esta etapa hay que realizar las siguientes tareas:

1. Crear la VLAN wireless (30) en el switch de backup. Esta VLAN operará con el rango de direcciones IP 158.42.30.0/24.
2. En el switch ASIC Backup, asignar la IP 158.42.30.1 al interfaz correspondiente a la VLAN 30.
3. Conecte el interfaz Gigabit Ethernet 0/2 del switch ASIC Backup al mismo interfaz del router UPV Internet Gateway. Dé la IP 158.42.30.5 a este último.
4. Reemplazar el punto de acceso actual por el dispositivo Linksys WRT300N, el cual da soporte a autenticación RADIUS. El dispositivo se conecta al switch ASIC Backup en un puerto vinculado a la VLAN 30.
5. Añadir un segundo punto de acceso Linksys WRT300N que haga difusión de la red "eduroam", así como 2 clientes del tipo Smartphone. Este dispositivo también se conecta al switch ASIC Backup en un puerto vinculado a la VLAN 30.
6. Configure ambos routers inalámbricos Linksys para que reciba la IP estática 158.42.30.2 (UPVNET wireless) y 158.42.30.4 (eduroam wireless). Recuerde que estos dispositivos no deberán funcionar como Router/NAT en ningún momento.
7. Añada un servidor RADIUS (AAA), el cual se conectará directamente al switch ASIC Backup, y recibirá la IP estática 158.42.30.3/24.



8. Configure dos claves de seguridad RADIUS distintas en el servidor RADIUS y en los puntos de acceso Linksys (una por punto de acceso). En primer punto de acceso ajuste el SSID a "UPVNET", y en el segundo a "eduroam".
9. Cree credenciales de acceso para los cuatro usuarios en el servidor RADIUS, y configure los portátiles y móviles con sus credenciales correspondientes con el objetivo de tener la mejor configuración de seguridad posible.
10. Verifique que los clientes del tipo laptop se conectan correctamente al router Linksys UPVNET, y que los clientes del tipo Smartphone se conectan correctamente al router Linksys eduroam.
11. Haga los cambios necesarios en el switch ASIC Backup para que este pueda servir direcciones a los clientes de la VLAN 30 en su rango correspondiente. Recuerde deshabilitar el servicio DHCP en ambos routers Linksys.

Nota: evitar servir a los clientes las direcciones usadas por los routers Linksys, el router y el servidor RADIUS, para evitar IPs duplicadas.

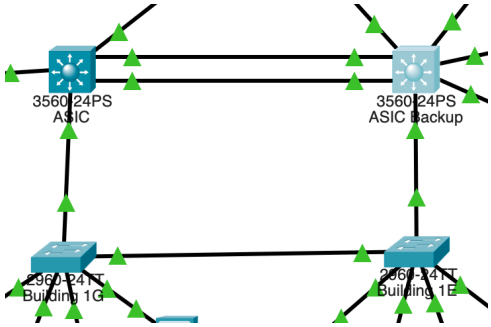
12. Verifique que los clientes reciben su IP por DHCP y se conectan con éxito a www.google.es. Además, confirme que la VLAN 30 queda restringida solamente a su ámbito de red.
13. Si todo es correcto guarde la configuración en switches y routers mediante el comando "write" y pulse "Guardar".

Etapa 3: Aumento de capacidad y tolerancia a fallos

En esta etapa vamos a crear una red con tolerancia a la pérdida de cualquiera de los enlaces entre los switches del ASIC y los switches de los edificios 1G y 1E, así como duplicaremos la capacidad entre los switches ASIC y ASIC backup.

Para eso hay que realizar las siguientes tareas:

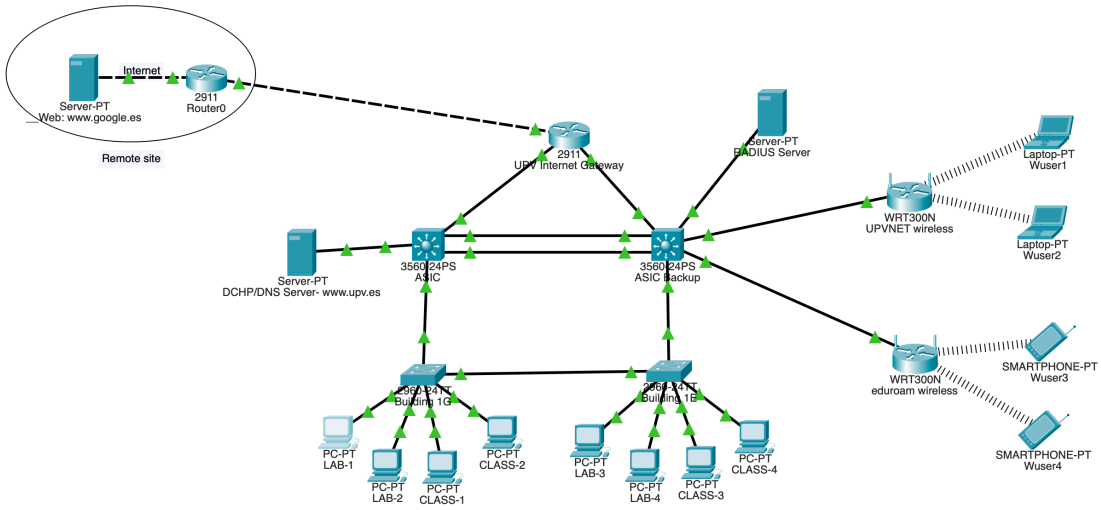
1. Añadir un enlace adicional ente los switches ASIC y ASIC backup, como ilustrado en la figura de abajo. Se sugiere usar el puerto FE 0/5 en ambos switches para simplificar la corrección.
2. Configurar el nuevo enlace de manera similar a la conexión entre switches ya existente (FE 0/3).
3. Crear un Port Channel con propiedades similares a los enlaces entre switches, y a continuación vincular los enlaces al port channel. Comprobar que se ha ejecutado correctamente mediante el comando "*show etherchannel port-channel*"
4. Para todos los switches, definir como protocolo spanning tree la variante *rapid-pvst*.
5. Definir el switch del ASIC como *root primario* para la VLAN 10 y como *root secundario* para la VLAN 20.
6. Definir el switch ASIC Backup como *root primario* para la VLAN 20 y como *root secundario* para la VLAN 10.
7. En la consola de cada switch, comprobar que el protocolo spanning tree está funcionando correctamente, y que todos aceptan el switch del ASIC correspondiente como root.
8. Añadir un nuevo enlace del tipo trunk entre los switches 1G y 1E con las VLANs 10 y 20 habilitadas (y únicamente esas VLANs…).



9. Verificar la configuración de spanning tree de todos los switches, y en particular verificar que el nuevo enlace creado sale como bloqueado desde el switch 1E para una VLAN, y el switch 1G para la otra VLAN.

10. Si todo es correcto, guardar la configuración en switches y routers mediante el comando “write” y después “Guardar”.

El resultado final debería de ser el siguiente:



La red deberá estar totalmente operativa, con las diferentes estaciones fijas y móviles siendo capaces de tener acceso a todas las máquinas de su entorno, incluidos ambos servidores web (UPV y Google).

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 (¡no realizar dos envíos!).

Enlaces útiles

General:

- Documentación del Switch Catalyst 2960
- Documentación del Switch Catalyst 3560
- http://www.study-ccna.com
- http://www.freeccnaworkbook.com/workbooks/ccna
- https://www.netwrix.com/cisco_commands_cheat_sheet.html
- http://www.ciscopress.com/articles/article.asp?p=358549

VLANs:

- https://www.dummies.com/article/technology/information-technology/networking/general-networking/cisco-networking-all-in-one-for-dummies-cheat-sheet-208539/
- https://www.freeccnaworkbook.com/workbooks/ccna/configuring-a-management-vlan-interface

STP:

- https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/RPVSpanningTree.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/72836-rapidpvst-mig-config.html

Port channels:

- https://www.freeccnaworkbook.com/workbooks/ccna/configuring-a-port-channel-interface

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.