Tarefa 2.4.- Vídeo repaso TCP/IP. IPv6 con PacketTracer

PARTE A.- Preguntas previas

Define brevemente os distintos conceptos e o nivel da pila TCP/IP no que traballan, cando sexa o caso:

1. TCP: Protocolo de comunicacións da capa de transporte. É orientado a conexión, confiable, garante que os datos son entregados sen erros e na orde na que se transmitiron
2. UDP: Protocolo de comunicacións da capa de transporte. Non é orientado a conexión, non asegura entrega sen erros nin garante a entrega dos datos.
3. Ping ICMP: **Utililidade de diagnóstico** do protocolo ICMP, que é un protocolo do nivel de rede: ***I**nternet **C**ontrol **M**essage **P**rotocol* de IP. O ping emprégase para ver se unha máquina ten conexión física ata outra.
4. Router: elemento de conexión que traballa a nivel de rede, traballa coas direccións IP. Conecta redes diferentes
5. Switch: elemento de conexión que traballa a nivel de enlace, traballa coas direccións MAC.
6. Proxy: programa ou máquina que intercepta as comunicacións dun equipo coa internet. Estará físicamente entre o equipo e o servidor. O equipo fará unha petición ao proxy e este conectarase co servidor. Traballa a nivel de aplicación
7. Intranet: rede privada dunha organización.
8. Firewall: Dispositivo de seguridade que comproba as comunicacións dunha rede coa internet, permitindo ou denegando acceso a diferente portos. Normalmente trababalla a nivel de rede/transporte
9. Por que chamamos a internet *world wide web*? Rede de araña mundial, cubre unha extensión mundial. Aínda que internet é a rede, na que se poden empregar moitos servicios e protocolos diferentes. A web traballa co protocolo http/https, para navegar empregando páxinas web
10. A que se denominaba "*ping da morte*"? E que é un ataque de denegación de servizo?
    Ping da morte: envío de multitude de paquetes moi pesados a un servidor. É un ataque obsoleto, non existe nos equipos modernos
    Ataque de denegación de servizo ou DOS: ataque a un servidor ata que se satura. O DDOS é un ataque de denegación de servizo distribuído.
11. Que é un porto en redes? Ten relación cun *socket*?
    Un porto é un punto de acceso a unha aplicación ou proceso IP, no nivel de transporte. Está identificado por un número enteiro.
    Un socket está formado por unha dirección de internet e un porto. Exemplo: 192.168.1.211:8080.
12. A que corresponden os portos 21, 23, 25, 53 e 80?
    21: ftp
    23: telnet
    25: SMTP -simple transfer mail protocol
    53: dns
    80: http
13. Define o que é URL e para que se usa. Hai diferencia con URI?

URL: universal resource locator ou Localizador de recursos uniforme: o recurso existe.

URI: universal resource identifier: Identificador de recurso uniforme. (pode ser só un nome único: URN ou un recurso real: URL)

PARTE B.- Vídeo "Warriors of the Net"

Contesta **axustándote** ao que se comenta no vídeo:

1. ¿Cal é o protocolo no que se centra o vídeo?

   O protocolo IP

2. ¿Que describe a "etiqueta" do paquete?

   IP orixe, IP destino, tipo de paquete

3. ¿Que tipos de paquete comenta o vídeo que pode haber na rede?

   Paquetes IP, Novell, Apple Talk, ICMP

4. ¿Que fai o router local na nosa LAN?

   Xestiona os paquetes. Enruta/direcciona/encamiña despois de ler as direccións do paquete, e envíaos a outra rede se é preciso

5. ¿Considérase no vídeo que o router é rápido? E exacto? Sabes por que?

   É exacto: si. Mira as direccións IP e obra en consecuencia.
   Non é tan rápido como o switch porque está nun nivel máis alto da pila de protocolos, no nivel de rede.

6. ¿En que diferencia o vídeo o switch (el chámao o switch router) do router?

   O switch é máis rápido: traballa no nivel de enlace.

7. ¿Que fai o proxy de saída na empresa ou organización emisora?

   Establece e comparte a dirección de internet aos usuarios da organización. É un intermediario entre cliente e servidor: só deixa pasar o que está autorizado. Aumenta a seguridade da rede.

8. ¿Todos os paquetes que recibe o proxy teñen o mesmo tamaño?

   Non, dependerán do contido.

9. ¿Que fai o firewall?

   Prevén as intromisións indesexadas, evita que información delicada sexa enviada a internet.

10. ¿E o router de saída?

Recolle cada paquete, e reenvía os paquetes para o destino. Pode facer NAT (Network Address Traslation)

11. ¿Que di o vídeo que fai "o **Sr. IP"**? Co que sabes, é correcta esa afirmación?

    Cando non obtén un recibo (ACK) de que paquete chegou envía outro de reemprazo. NON é correcto. Isto pódeo facer TCP.

12. ¿En que diferencia o vídeo intranet de internet?

    Intranet ten un certo control. No vídeo falan de internet como un medio "sen control"

13. Que se di no vídeo do "*ping de la muerte*"?

    Paquetes ICMP moi grandes que colapsaban servidores.

14. Enumera os diferentes camiños físicos que poden seguir os paquetes, segundo o vídeo.

    Satélites, liñas telefónicas e cables transoceánicos.

15. ¿Cando o paquete está chegando ao seu destino, cal é o primeiro elemento que recibe o paquete?

    O firewall

16. ¿Como define os portos do firewall? Cales están abertos, e a que corresponden?

    Como portas de entrada, numeradas. 25 para correo electrónico (SMTP) e o 80 para paquetes HTTP

17. O paquete que vén de volta, ¿que nodos intermedios vai cruzando? Cítaos por orde.

    Firewall, servidor, router, internet, firewall corporativo e PC usuario

18. ¿Onde se fai referencia ás direccións IP?

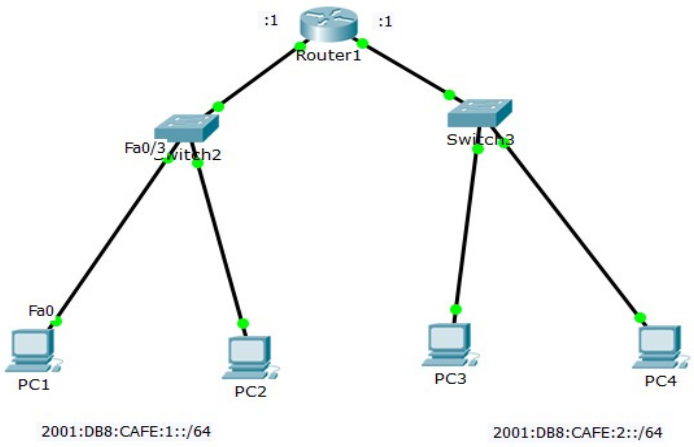
    Non se citan, só se fala das "etiquetas", pero non das direccións IP especificamente.

19. ¿Móstrase no vídeo que as direccións MAC están involucradas?

    NON

PARTE C.- IPv6 con PacketTracer

Configuraremos os equipos en IPv6 para comprobar conectividade entre eles. Partimos de seguinte escenario gardado no ficheiro "***IPv6 1 router.pkt***":



O **Router1** está xa configurado para o enrutamento IPv6 (co comando "*ipv6 unicast-routing*") e tamén están configuradas as súas tarxetas:

1. **FastEthernet0/0:**
   - 2001:DB8:CAFE:1::1/64
   - Link-Local FE80::1/64
2. **FastEthernet0/1:**
   - 2001:DB8:CAFE:2::1/64
   - Link-Local FE80::1/64

Observa que as dúas direccións Link-Local son iguais pero non hai problema porque están en subredes diferentes. Trátase de asignar as IP's correspondentes para os PC's para que teñan comunicación entre eles,empregando só IPv6.

Por exemplo PC1 terá a *2001:DB8:CAFE:1::1/64.*

1. Escribe as MAC de PC1 e PC3

   PC1: 00:60:70:1B:D3:D9

   PC3: 00:D0:D3:C9:AB:53

2. Teñen relación as direccións IPv6 Link-Local coas MAC de cada equipo?

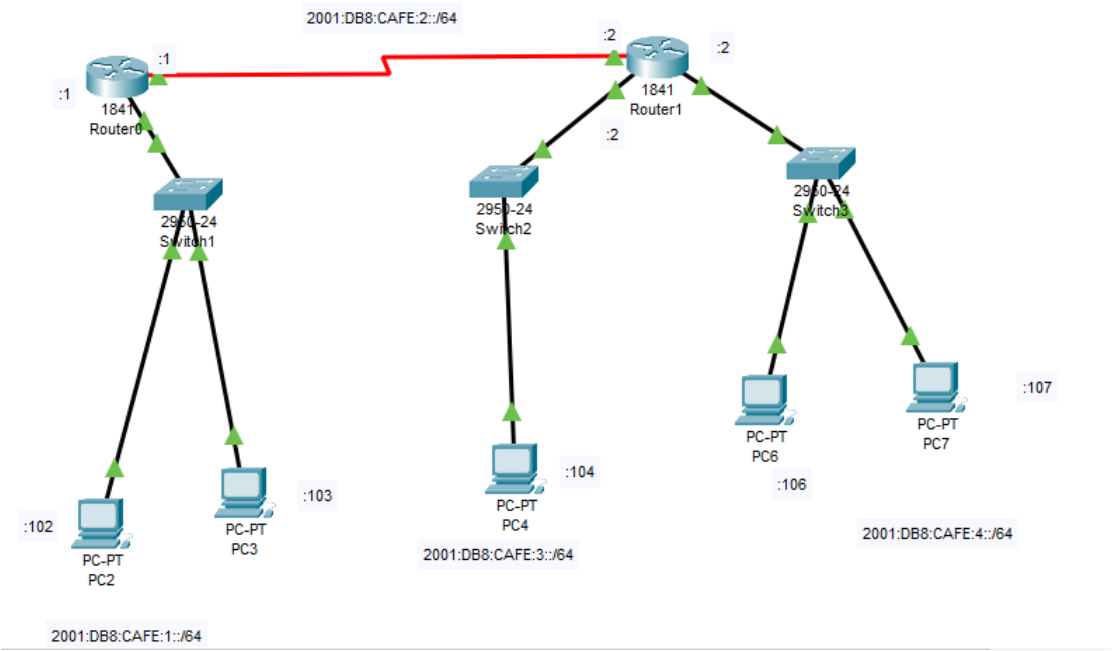
   PC1: 00:60:70:1B:D3:D9 , IPv6 FE80::260:70FF:FE1B:D3D9

   Si, as IPv6 Link-local neste caso están formadas empregando o proceso EUI64: parte de 48 bits da MAC e insire FFFE no medio da MAC, invirte o 7º bit do primeiro grupo (00 pasa a 02), e antepón FE80::

   A partir de Windows Vista, Windows prefire empregar unha IPv6 Link-local aleatoria, en vez de empregar o proceso EUI64.

3. Asigna direccións Globais e configurar as portas de enlace para que todos os equipos poidan facer ping entre si. Indica aquí a configuración de cada PC, e mostra os seguintes **pantallazos**:
    - PC1 facendo ping a PC3 e obtendo resposta
    - PC2 facendo ping a PC4 e obtendo resposta.

4. Fai o mesmo para o escenario do ficheiro *"**IPv6 2 routers.pkt**":*



Asigna as IP's que corresponden (...102, ...103, ...104, etc.) , *e m*ostra un **pantallazo** con:

- PC2 facendo un ping6 a PC6 e obtendo resposta
- PC4 facendo un ping a PC7 e obtendo resposta
- PC3 facendo un ping a PC4 e obtendo resposta