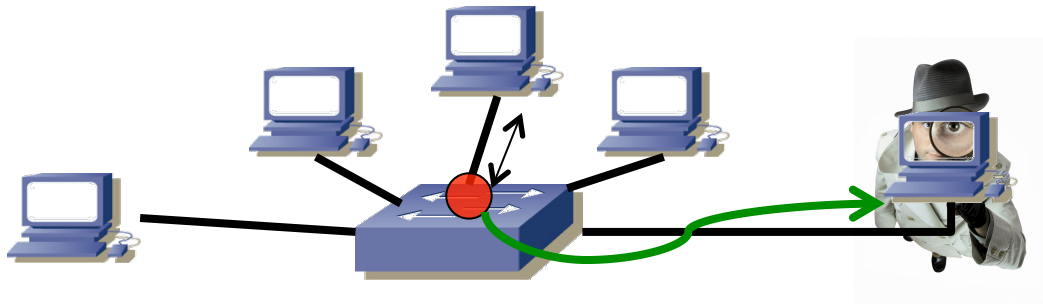
Monitorización de red: Medidas pasivas

Area de Ingeniería Telemática
http://www.tlm.unavarra.es

Grado en Ingeniería en Tecnologías de Telecomunicación, 4º

¿Qué hacer con la medida?

- Supongamos una medida en una Ethernet
- Un *port-mirror*
- O un VSPAN
- ¿Qué información básica se suele extraer?
- Esto no pretende ser una lista exhaustiva
- No es cuestión de hacer cuantas más gráficas se pueda sino de saber qué información se busca y para qué

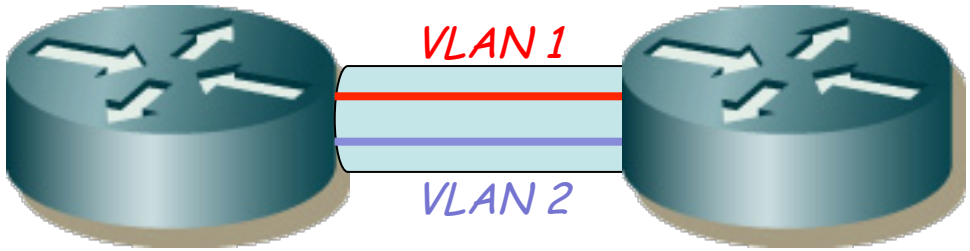


Información en capa 1 y 2

¿Qué hacer con la medida?

¿VLANs?

- Si las hay, se pueden separar con encapsulado 802.1Q? Con otro?
- Para cierto análisis separar por VLAN (no para utilizaciones por puerto, por ejemplo)
- En ocasiones un *mirror* puede eliminar la cabecera 802.1Q, lo cual dificulta diferenciar el tráfico por VLAN solo con capa 2
- Si se monitoriza un enlace puede interesar la serie temporal del tráfico para cada VLAN para detectar responsables de congestión



¿Qué hacer con la medida?

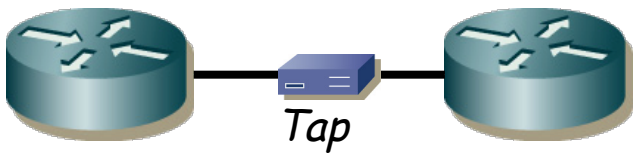
¿Protocolos presentes en la LAN?

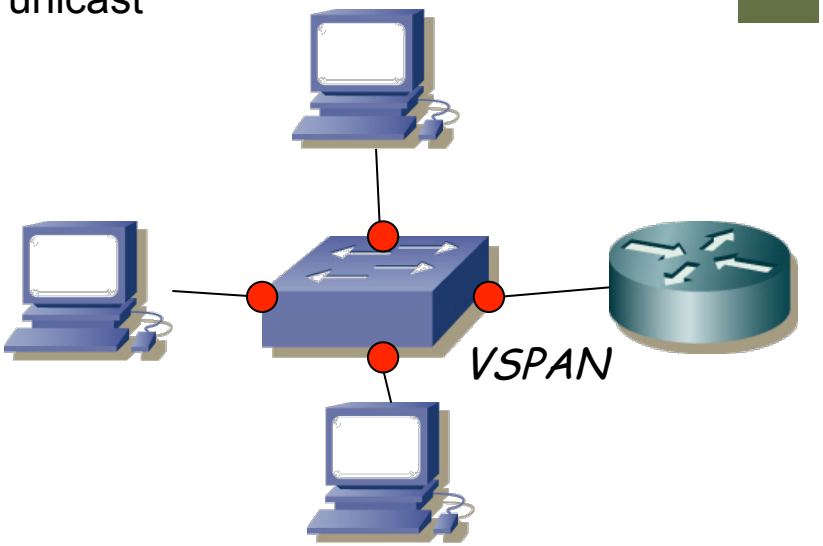
- Protocolos por encima de Ethernet
- IPv4, IPv6, ARP, STP, MPLS, MVRP, MMRP, 802.1x, LLDP
- Una gran cantidad de Ethertypes reservados por empresas: http://standards.ieee.org/develop/regauth/ethertype/eth.txt
- Cantidad de bytes, cantidad de paquetes
- Series temporales de cada uno
- Qué hosts los usan? (ej: hosts IPv6?)
- Podemos descubrir protocolos que no sabíamos que estaban
- O incluso que no queríamos que estuvieran
- O que alguno tenga un uso anormalmente alto

¿Qué hacer con la medida?

¿Estaciones presentes en la LAN?

- Direcciones MAC origen y destino, destinos multicast
- Podemos obtener una matriz de tráfico en capa 2
- La matriz nos da información sobre parejas que envían mucho tráfico
- Agregar por host origen o host destino
- La cantidad de tráfico que genera un host puede ser normal o no
- Puede detectar un host causante de congestión
- Totales en la medida o series temporales
- Escenarios muy variados de red
  - *Tap* entre routers poco más de 2 MACs unicast
  - *VSPAN* una gran cantidad de ellas
  - (otros)

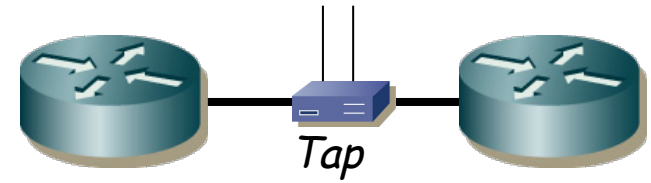


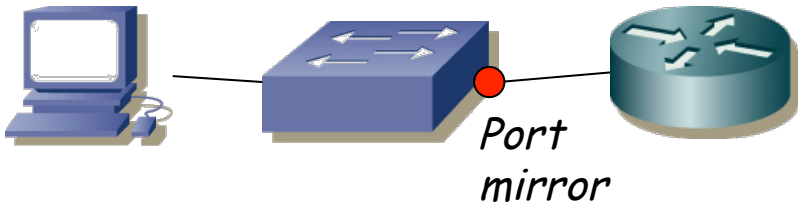


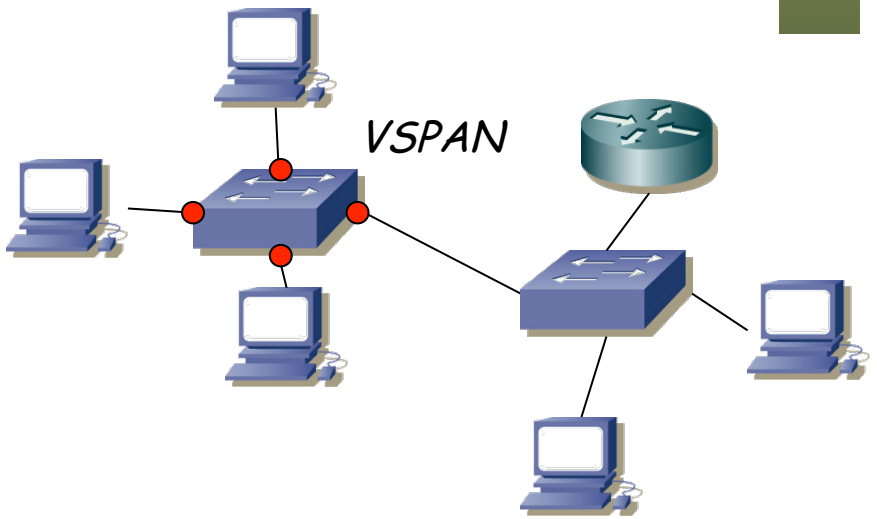
¿Qué hacer con la medida?

¿Utilización de enlaces?

- Series temporales, tiempo/probabilidad exceder una utilización
- Con un *tap* que no haga agregación tenemos los sentidos separados
- Con un *port mirror* hay que separar el tráfico en base a direcciones
- Con un *VSPAN* necesitamos más información sobre la topología
- En el caso de la derecha se recibe tráfico de multiples MACs que provienen del segundo conmutador y no se distingue el enlace





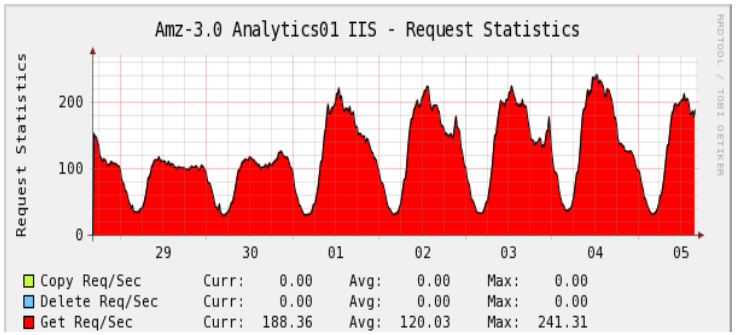


Información en capa 3

¿Qué hacer con la medida?

¿Hosts IPv4

- Direcciones origen y destino, direcciones multicast, direcciones reservadas para ciertos protocolos (IGMP, VRRP, OSPF, PIM...)
- Matrices de tráfico
- Agregación por host
- Patrones de tráfico diarios y semanales
- Con los flujos (NetFlow, IPFIX) se podrían calcular matrices y series en la escala en que se exportan los mismos o en una mayor



¿Qué hacer con la medida?

¿Problemas en IP

- Errores ICMP (puerto UDP inalcanzable, TTL exceeded...)
- Paquetes en bucle de enrutamiento
- Patrón de tráfico generado por un host coherente con un ataque

¿Qué hacer con la medida?

¿Protocolos sobre IP

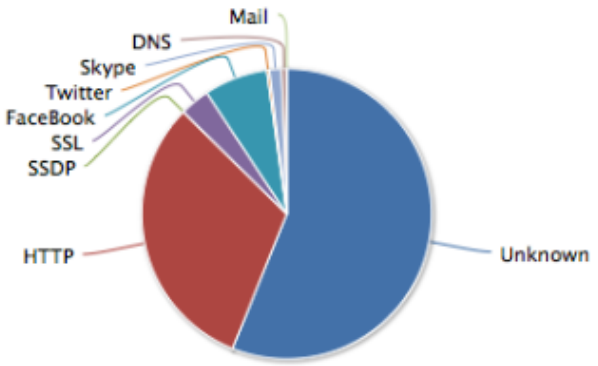
- TCP, UDP, ICMP, IGMP, RSVP, ESP, AH, PIM, SCTP… http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
- Tráfico por cada uno

Información en capa 4

¿Qué hacer con la medida?

¿Aplicaciones sobre TCP o UDP?

- Permite detectar aplicaciones (suele haber sorpresas) y reconocer las que más consumen, así como las que emplea cada usuario
- (...)



Aplicaciones sobre TCP o UDP

¿Aplicaciones sobre TCP o UDP?

- ¿Cómo identificar esos servicios?
- En tiempos había TCP/IP en los UNIX, IPX de Novell, SNA de IBM…
- Hoy en día TCP/IP fundamentalmente (los anteriores sobre él)
- Tradicionalmente el campo protocolo de IP o el puerto servidor lo identifican
- Con flujos podríamos identificar los servicios reconocibles por puerto
- (...)

FTP, POP, SMTP, IMAP, DNS, IPP, HTTP, MDNS, NTP, NETBIOS, NFS, SSDP, BGP, SNMP, XDMCP, SMB, SYSLOG, DHCP, PostgreSQL, MySQL, TDS, DirectDownloadLink, I23V5, AppleJuice, DirectConnect, Socrates, WinMX, VMware, PANDO, Filetopia, iMESH, Kontiki, OpenFT, Kazaa/Fasttrack, Gnutella, eDonkey, Bittorrent, OFF, AVI, Flash, OGG, MPEG, QuickTime, RealMedia, Windowsmedia, MMS, XBOX, QQ, MOVE, RTSP, Feidian, Icecast, PPLive, PPStream, Zattoo, SHOUTCast, SopCast, TVAnts, TVUplayer, VeohTV, QQLive, Thunder/Webthunder, Soulseek, GaduGadu, IRC, Popo, Jabber, MSN, Oscar, Yahoo, Battlefield, Quake, VRRP, Steam, Halflife2, World of Warcraft, Telnet, STUN, IPSEC, GRE, ICMP, IGMP, EGP, SCTP, OSPF, IP in IP, RTP, RDP, VNC, PCAnywhere, SSL, SSH, USENET, MGCP, IAX, TFTP, AFP, StealthNet, Aimini, SIP, Truphone, ICMPv6, DHCPv6, Armagetron, CrossFire, Dofus, Fiesta, Florensia, Guildwars, HTTP Application Activesync, Kerberos, LDAP, MapleStory, msSQL, PPTP, WARCRAFT3, World of Kung Fu, MEEBO, FaceBook, Twitter, DropBox, Gmail, Google Maps, YouTube, Skype, Google, DCE RPC, NetFlow_IPFIX, sFlow, HTTP Connect (SSL over HTTP), HTTP Proxy, Netflix, Citrix, CitrixOnline/GotoMeeting, Apple (iMessage, FaceTime…), Webex, WhatsApp, Apple iCloud, Viber, Apple iTunes, Radius, …

Aplicaciones sobre TCP o UDP

¿Aplicaciones sobre TCP o UDP?

- El puerto puede ser dinámico, anunciado por otro servicio (ej: RPC portmap)
- Muchos protocolos hoy en día en nivel de aplicación no usan un puerto bien conocido o lo cambian (para ocultarse, por configuración, etc)
- Muchos son servicios sobre el mismo protocolo (HTTP es muy popular)
- Hace falta DPI (*Deep Packet Inspection*) para identificar los servicios
- Pero contra encriptación, poco que hacer sin las claves
- Algunas sondas aceptan la clave privada del servidor para desencriptar flujos SSL

FTP, POP, SMTP, IMAP, DNS, IPP, HTTP, MDNS, NTP, NETBIOS, NFS, SSDP, BGP, SNMP, XDMCP, SMB, SYSLOG, DHCP, PostgreSQL, MySQL, TDS, DirectDownloadLink, I23V5, AppleJuice, DirectConnect, Socrates, WinMX, VMware, PANDO, Filetopia, iMESH, Kontiki, OpenFT, Kazaa/Fasttrack, Gnutella, eDonkey, Bittorrent, OFF, AVI, Flash, OGG, MPEG, QuickTime, RealMedia, Windowsmedia, MMS, XBOX, QQ, MOVE, RTSP, Feidian, Icecast, PPLive, PPStream, Zattoo, SHOUTCast, SopCast, TVAnts, TVUplayer, VeohTV, QQLive, Thunder/Webthunder, Soulseek, GaduGadu, IRC, Popo, Jabber, MSN, Oscar, Yahoo, Battlefield, Quake, VRRP, Steam, Halflife2, World of Warcraft, Telnet, STUN, IPSEC, GRE, ICMP, IGMP, EGP, SCTP, OSPF, IP in IP, RTP, RDP, VNC, PCAnywhere, SSL, SSH, USENET, MGCP, IAX, TFTP, AFP, StealthNet, Aimini, SIP, Truphone, ICMPv6, DHCPv6, Armagetron, CrossFire, Dofus, Fiesta, Florensia, Guildwars, HTTP Application Activesync, Kerberos, LDAP, MapleStory, msSQL, PPTP, WARCRAFT3, World of Kung Fu, MEEBO, FaceBook, Twitter, DropBox, Gmail, Google Maps, YouTube, Skype, Google, DCE RPC, NetFlow_IPFIX, sFlow, HTTP Connect (SSL over HTTP), HTTP Proxy, Netflix, Citrix, CitrixOnline/GotoMeeting, Apple (iMessage, FaceTime…), Webex, WhatsApp, Apple iCloud, Viber, Apple iTunes, Radius, …

¿Qué hacer con la medida?

¿Comportamiento de TCP?

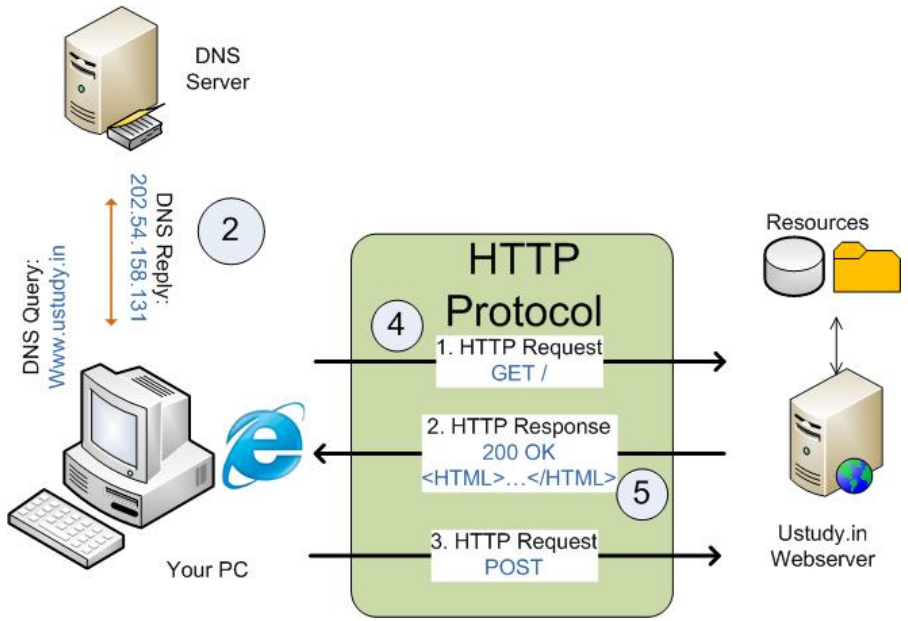
- ¿RST? (se abortan conexiones o no está el servidor corriendo?)
- ¿SYN no confirmado? (no está el host servidor encendido? En la misma LAN fallaría a nivel ARP)
- ¿Ventana de control de flujo = 0 ? (receptor saturado?)
- ¿Retransmisiones? (pérdidas?)
- etc

Información en capa de aplicación

¿Qué hacer con la medida?

¿Comportamiento de aplicaciones?

- Errores en protocolo de nivel de aplicación
- Tiempos de respuesta (relevantes según la proximidad del punto de medida a los extremos)
- Servicios que involucran flujos/conexiones en paralelo con el mismo o distinto host
- Tiempos de transacción



¿Qué hacer con la medida?

VLANs

Protocolos presentes en la LAN

Estaciones presentes en la LAN

Utilización de enlaces

Hosts IPv4

Problemas en IP

Protocolos sobre IP

Aplicaciones sobre TCP o UDP

Comportamiento de TCP

Comportamiento de aplicaciones

etc...

Medidas en otros escenarios

Medidas pasivas en WLAN

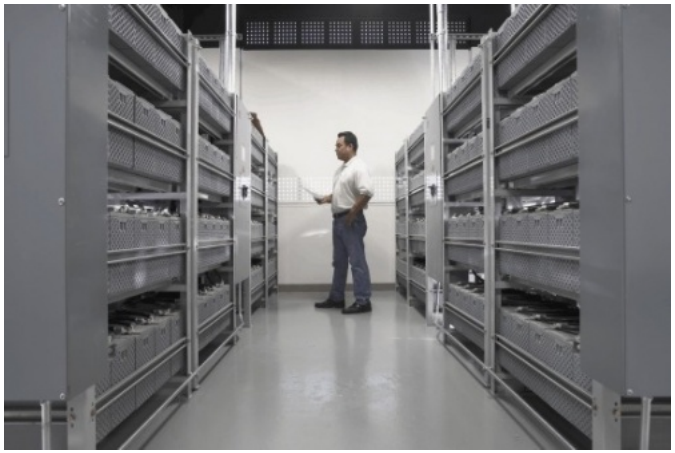
- Características específicas del medio y nivel MAC
- Potencia, SNR, canales empleados, WLANs en mismos canales
- WLANs “piratas”
- *Access Points* localizados
- Seguridad implementada en cada WLAN
- Detección de intentos de intrusión

Medidas fuera de LAN

- Según la tecnología
  - MPLS
    - Según el encapsulado que lo transporte
    - Señalización
  - ATM
    - Llegada de celdas
  - En tecnologías de paquetes más datos que en circuitos por su transparencia
  - Redes de señalización en redes de circuitos
- Según la capacidad
  - En enlaces de baja capacidad pueden interesar otros datos
  - Por ejemplo el tamaño de los paquetes puede tener un efecto apreciable
  - La calidad de la implementación del planificador (QoS) es crítica

¿Dónde medir?

- Depende de lo que se quiera saber
- Puede valer un punto de medida o necesitar varios
- Físicamente
  - En un host (diferente O.S., no cargarlo)
  - En un conmutador (L2 ó 3)
  - En un enlace (*tap*, *splitter*)
  - En un segmento LAN (hoy WLAN)
- Lógicamente (desde el punto de vista de una empresa)
  - La entrada/salida a la red corporativa (enlace con Internet)
  - La entrada/salida de un CPD
  - Interior de CPD cerca de granja de servidores
  - Cerca de servidor
  - Cerca de usuario remoto
- Lógicamente en “Internet”
  - En el Backbone de un ISP
  - En enlace de *peering* de un ISP
  - En un Internet Exchange Point



Agregación de medidas

- La cantidad de datos de monitorización crece
- Es común agregar datos antiguos para reducir espacio
- Normalmente con medias o máximos
- Por ejemplo RFC 1857 (informativa) recomienda:
  - Datos de hace más 1 día agregar en intervalos de 15min
  - Datos de hace más de 1 mes agregar en horas
  - Datos de hace más de 1 año agregar en días

Seguridad y privacidad

- Según el país o empresa puede estar prohibido recoger información por usuario
- Puede hacer referencia a los datos transferidos (eliminar datos de paquetes)
- O incluso lo que permita identificar al usuario (anonimizar cabeceras)
- Generalmente un proceso de agregación elimina la posibilidad de identificación
- Si no se puede identificar al usuario es más difícil actuar ante violaciones de seguridad