Monitorización de red: Medidas pasivas

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

Grado en Ingeniería en Tecnologías de Telecomunicación, 4º

Hemos visto: NetFlow

1. Create and update flows in NetFlow cache

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src As	Dst Port	Dst Msk	Dst As	NextHop	Bytes /Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	14.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	00A1	/24	180	00A1	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

2. Expiration

- Inactive Timer Expired (15 Sec Is Default)
- Active Timer Expired (30 Min Is Default)
- NetFlow Cache Is Full (Oldest Flows Are Expired)
- RST or FIN TCP Flag

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src As	Dst Port	Dst Msk	Dst As	NextHop	Bytes /Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	0	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

3. Aggregation?

No

Yes

4. Export version

Non-aggregated flows—export version 5 or 9

5. Transport protocol

Export packet: Header | Payload (Flows)

E.g. Protocol-Port Aggregation Scheme Becomes

Protocol	Pkts	Srcport	Dstport	Bytes/Pkt
11	11000	00A2	00A2	1528

Aggregated Flows—Export Version 8 or 9

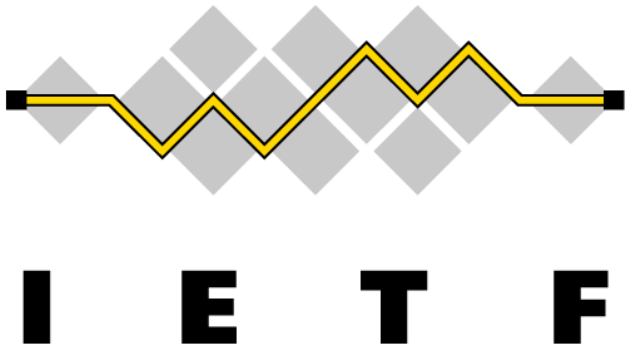
B. Claise y R. Wolter, "Network Management: Accounting and Performance Strategies", Cisco Press

Otras alternativas para flujos

IPFIX

- Cisco publicó RFC 3954 “Cisco Systems NetFlow Services Export Version 9”
- Informativa, simplemente para ser el punto de arranque del desarrollo de IPFIX
- De hecho en la cabecera IPFIX dice que es la versión 10
- RFC 5101 “Specification of the IP Flow Information Export (IPFIX) Protocolo for the Exchange of IP Traffic Flow Information”
- RFC 5102, 5470, 5610, 5655,...
- También se exportan los flujos en modo *push* al *collector*
- Un *template* describe el formato del registro y se envía también al *collector*

(...)



Otras alternativas para flujos

IPFIX

J-Flow

- Juniper
- Paquetes muestreados

sFlow

- InMon Corporation
- Mide flujos hasta L7 con gran cantiad de interfaces mediante packet sampling

IPDR (TM Forum), LFAP (Riverstone), CRANE (RFC 3423)...

¿Los flujos son suficiente?

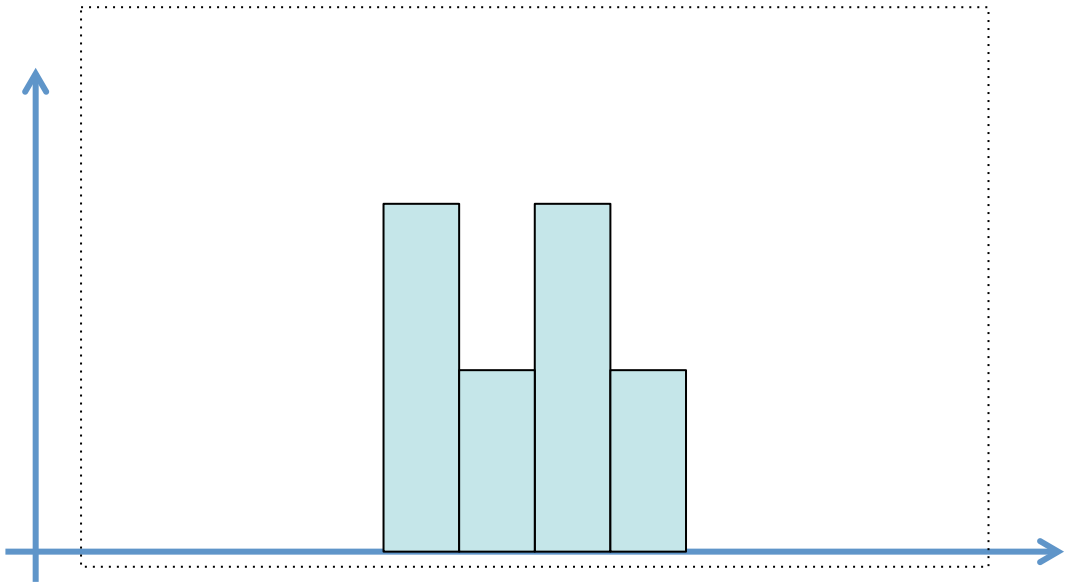
- Los contadores en la MIB son una medida muy agregada que no distingue origen y destino
- Los flujos distinguen a los extremos pero siguen siendo contadores
- Hay cierta temporalidad pues aun estando activo el flujo se envía el registro cada cierto tiempo
- Pero sigue siendo información muy agregada
- Por ejemplo una serie temporal de tráfico tiene como mínimo la escala de exportación
- ¿Qué hacer si queremos la máxima información?

Recoger todo el tráfico

- Ventaja: Permite máximo detalle en el análisis
- Inconveniente: La cantidad de datos e información puede ser descomunal
- (…)

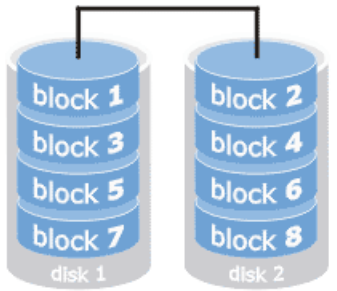
Recoger todo el tráfico

- Ventaja: Permite máximo detalle en el análisis
- Inconveniente: La cantidad de datos e información puede ser descomunal
- ¿Análisis online u offline?
  - 1Gbps = 125MB/s = 450GB/h
  - Digamos utilización del 60% durante 4h + utilización del 30% durante otras 4h y resto 0% = 450x0.6x4 + 450x0.3x4 = 1.6 TB/día
  - (…)



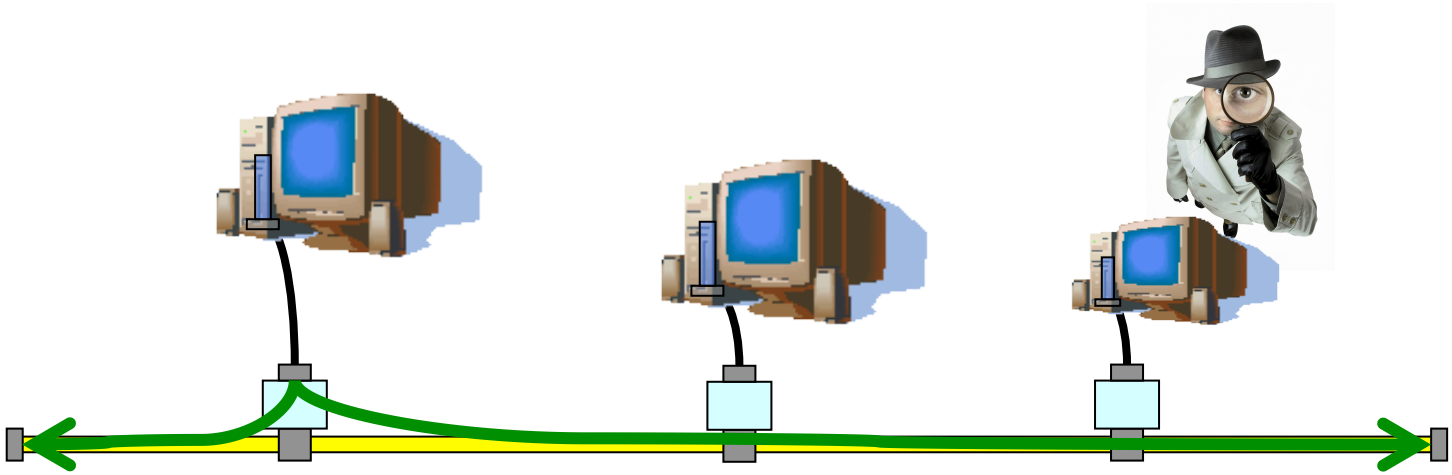
Recoger todo el tráfico

- Ventaja: Permite máximo detalle en el análisis
- Inconveniente: La cantidad de datos e información puede ser descomunal
- ¿Análisis online u offline?
  - 1Gbps = 125MB/s = 450GB/h
  - Digamos utilización del 60% durante 4h + utilización del 30% durante otras 4h y resto 0% = 450x0.6x4 + 450x0.3x4 = 1.6 TB/día
  - Online
    - No requiere gran cantidad de espacio en disco
    - Requiere (según el análisis) considerable capacidad de CPU y RAM (llegando a necesitar múltiples cores o incluso miles en GPGPUs)
  - Offline
    - Requiere almacenar en disco
    - Según el tipo de disco duro hablamos de unas velocidades sostenidas de 100-200MB/s, hasta 300MB/s (enterprise), 500-800MB/s SSD
    - ¿Un interfaz a 10Gbps con picos? Puede requerir varios discos en paralelo



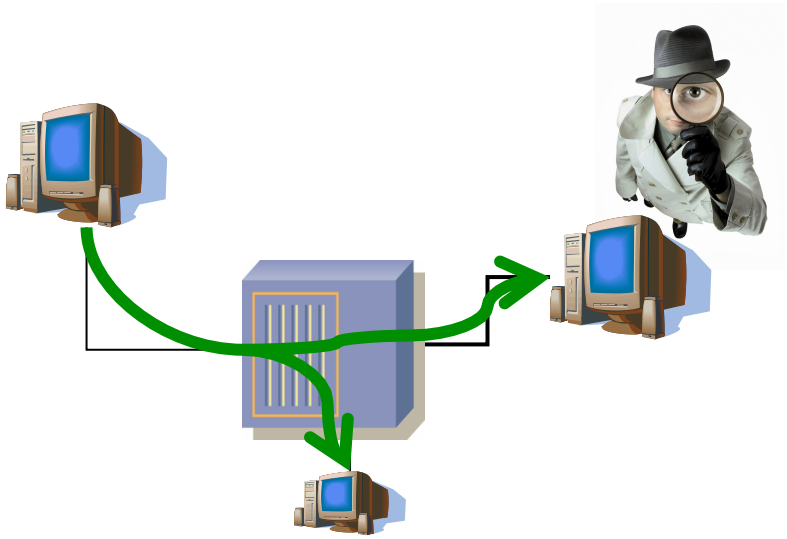
¿Cómo tener acceso al tráfico?

- Sencillo en la Ethernet original pues todos los hosts veían todas las tramas de la LAN
- Solo requería una NIC capaz de trabajar en modo *promiscuo*



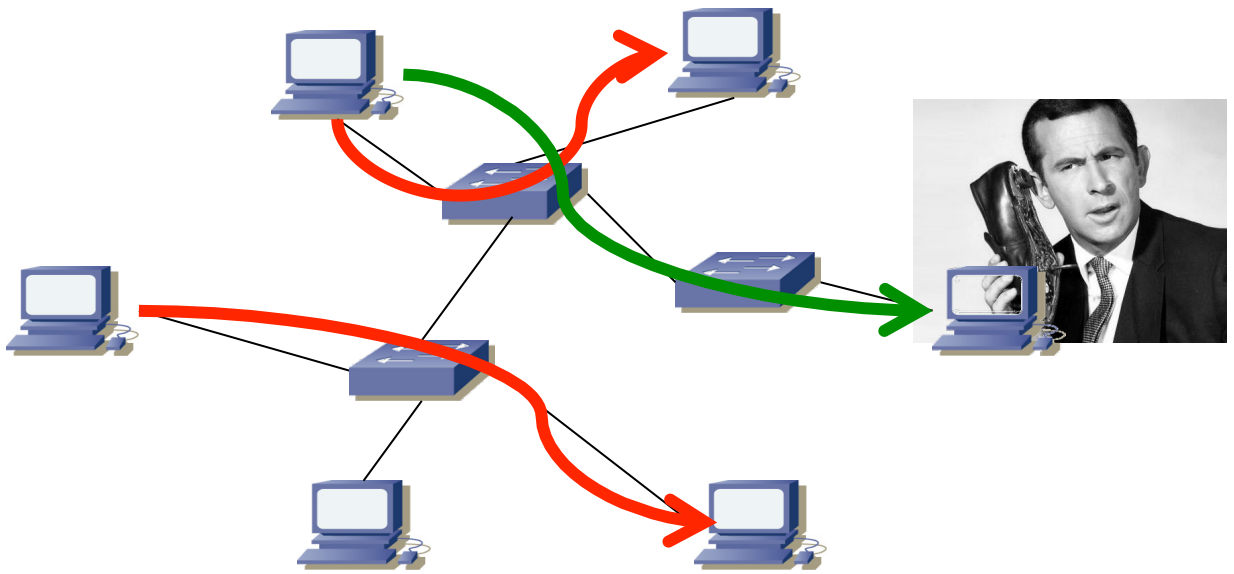
¿Cómo tener acceso al tráfico?

- En Ethernet sobre par de cobre con Hubs, similar



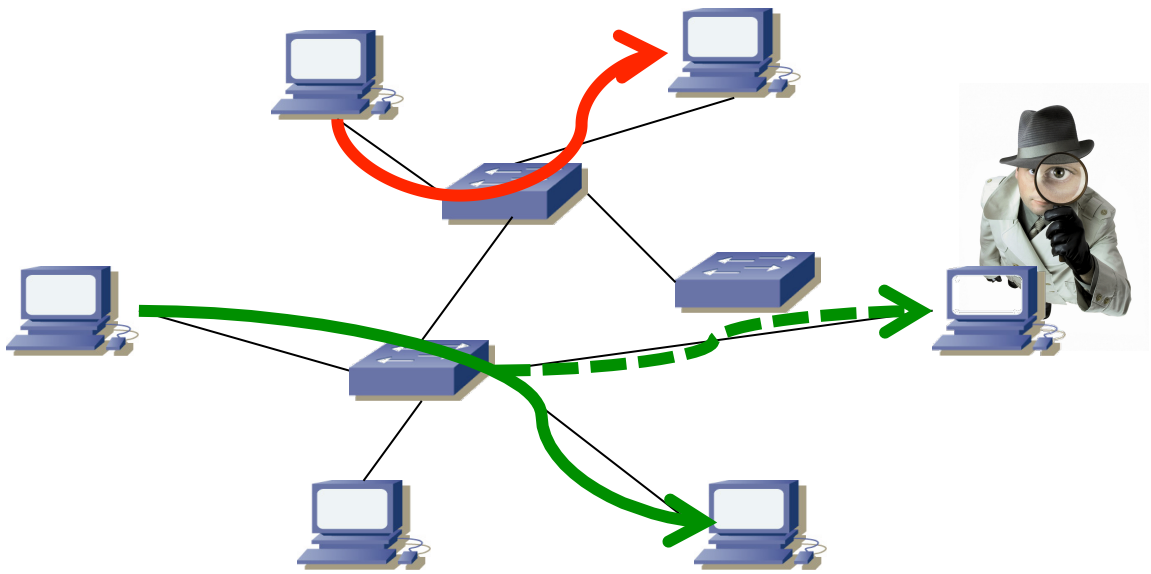
¿Cómo tener acceso al tráfico?

- Al llegar la conmutación Ethernet desaparece el dominio de colisión
- Un host solo puede ver las tramas que se dirijan a él o para las que se haga inundación
- Soluciones (...)



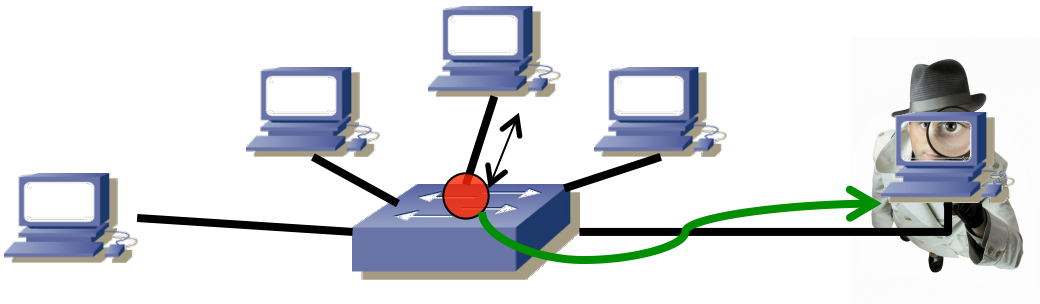
¿Cómo tener acceso al tráfico?

- Al llegar la conmutación Ethernet desaparece el dominio de colisión
- Un host solo puede ver las tramas que se dirijan a él o para las que se haga inundación
- Soluciones:
  - Mirror (...)



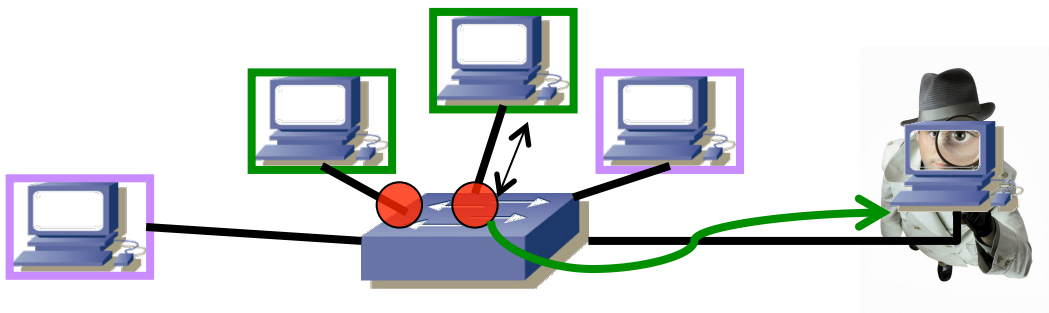
Mirror/SPAN

- Cisco habla de “SPAN” (Switched Port ANalyzer)
- Port-based SPAN (PSPAN):
  - Se especifican uno o varios puertos origen y uno destino
  - Para cada puerto origen también si monitorizar rx, tx o ambos
- (…)



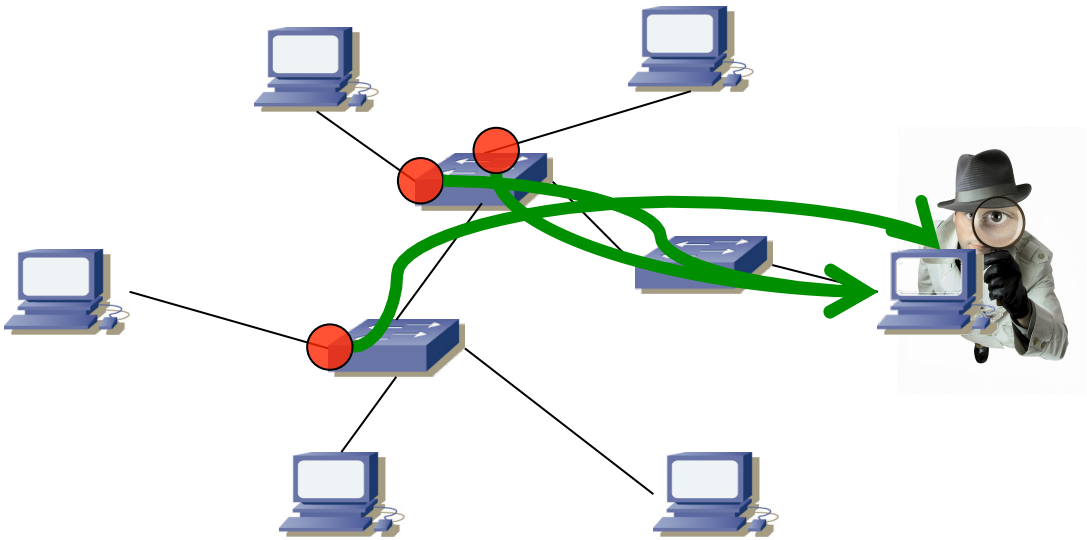
Mirror/SPAN

- Cisco habla de “SPAN” (Switched Port ANalyzer)
- Port-based SPAN (PSPAN):
  - Se especifican uno o varios puertos origen y uno destino
  - Para cada puerto origen también si monitorizar rx, tx o ambos
- VLAN-based SPAN (VSPAN):
  - Origen todos los puertos que pertenecen a una VLAN
- (…)



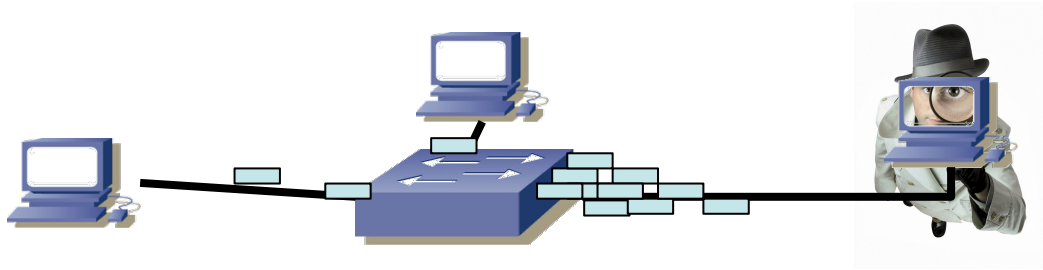
Mirror/SPAN

- Cisco habla de “SPAN” (Switched Port ANalyzer)
- Port-based SPAN (PSPAN):
  - Se especifican uno o varios puertos origen y uno destino
  - Para cada puerto origen también si monitorizar rx, tx o ambos
- VLAN-based SPAN (VSPAN):
  - Origen todos los puertos que pertenecen a una VLAN
- Local SPAN: puertos monitorizados y destino en el mismo switch
- Remote SPAN (RSPAN)
  - Algunos puertos no están en el mismo switch que el puerto destino
  - Requiere una VLAN para transportar el tráfico monitorizado entre switches



Mirror/SPAN: Limitaciones

- El puerto que recibe el tráfico puede congestionarse
  - Porque recibe de varios puertos o de uno pero los dos sentidos
  - Se podría dirigir el tráfico a una agregación de puertos
  - En algunos equipos se pueden crear reglas para indicar los paquetes a copiar al puerto de mirror y así limitarse a un subconjunto
- Suele haber limitaciones en el número de sesiones de SPAN
- No reenvía paquetes estropeados pues no pasan del interfaz entrante
- Pueden aparecer duplicados



Mirror: Ejemplo

- Juniper EX2200 Ethernet Switch

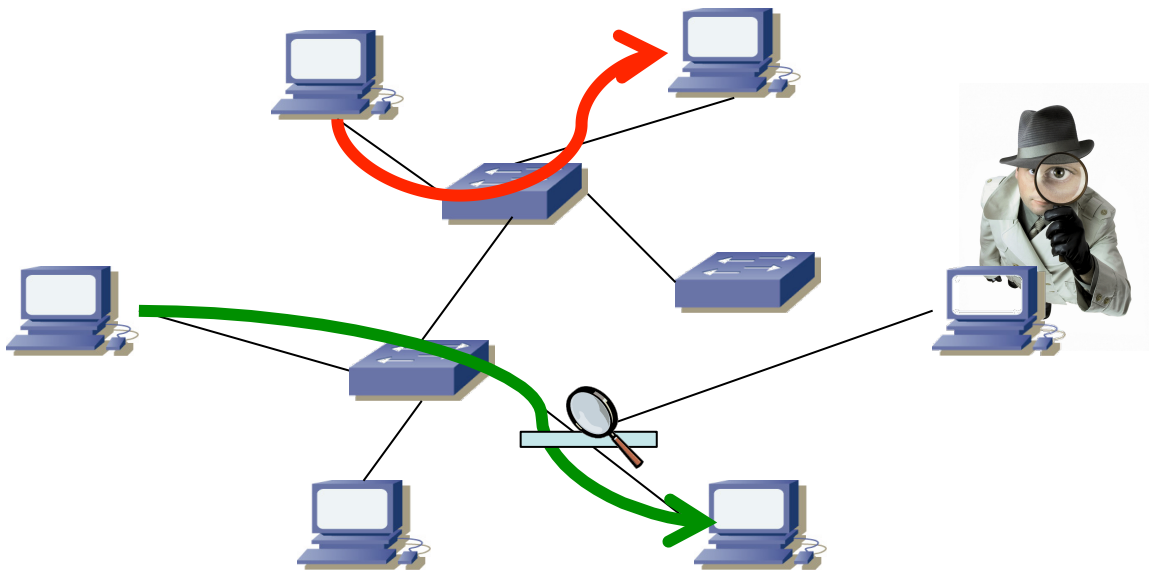
Troubleshooting

- Debugging: CLI via console, telnet, or SSH
- Diagnostics: Show and debug command statistics
- Traffic mirroring (port)
- Traffic mirroring (VLAN)
- ACL-based mirroring
- Mirroring destination ports per system: 1
- LAG port monitoring
- Multiple destination ports monitored to 1 mirror (N:1)
- Maximum number of mirroring sessions: 1
- Mirroring to remote destination (over L2): 1 destination VLAN
- IP tools: Extended ping and trace
- Juniper Networks commit and rollback

LAG = Link Aggregation Group

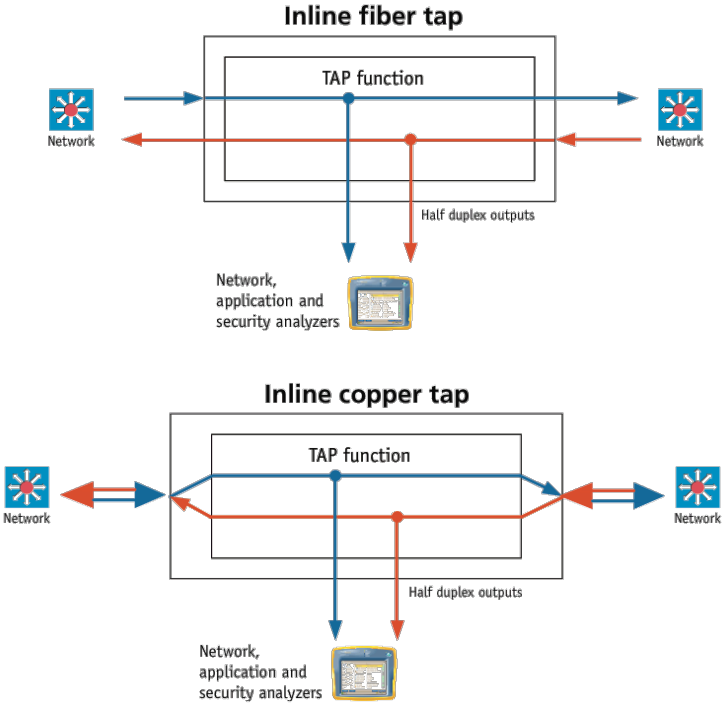
¿Cómo tener acceso al tráfico?

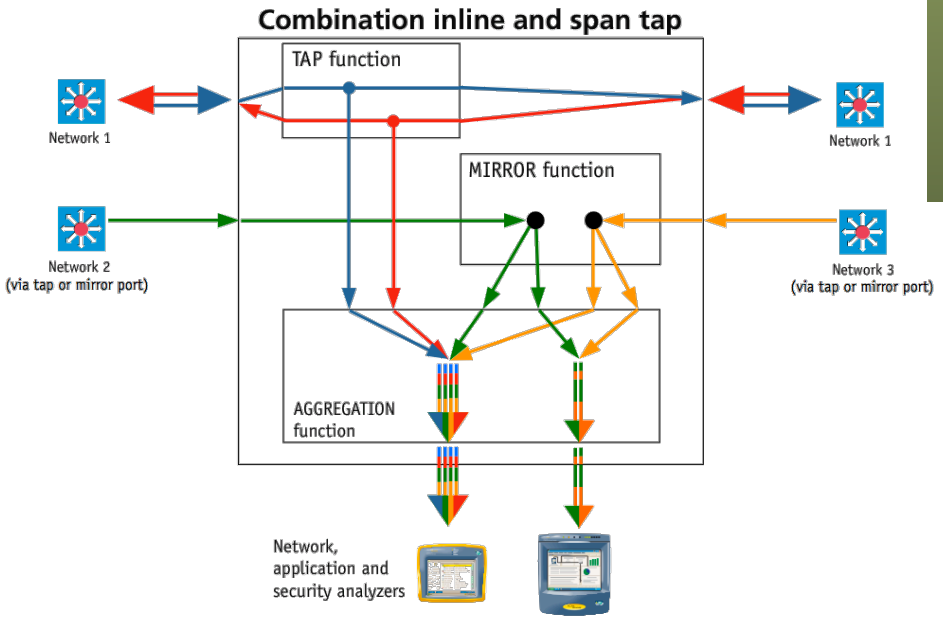
- Soluciones:
  - **Mirror**
  - **Network Tap**
    - Solo para el tráfico que circule por un enlace
    - Ante fallo de corriente mantienen el enlace de datos
    - En fibra, *splitters* (...)



¿Cómo tener acceso al tráfico?

- Soluciones:
  - **Mirror**
  - **Network Tap**
    - Solo para el tráfico que circule por un enlace
    - Ante fallo de corriente mantienen el enlace de datos
    - En fibra, *splitters*





http://es.flukenetworks.com/enterprise-network/network-monitoring/Tap-Solutions

Network Tap

NetOptics®

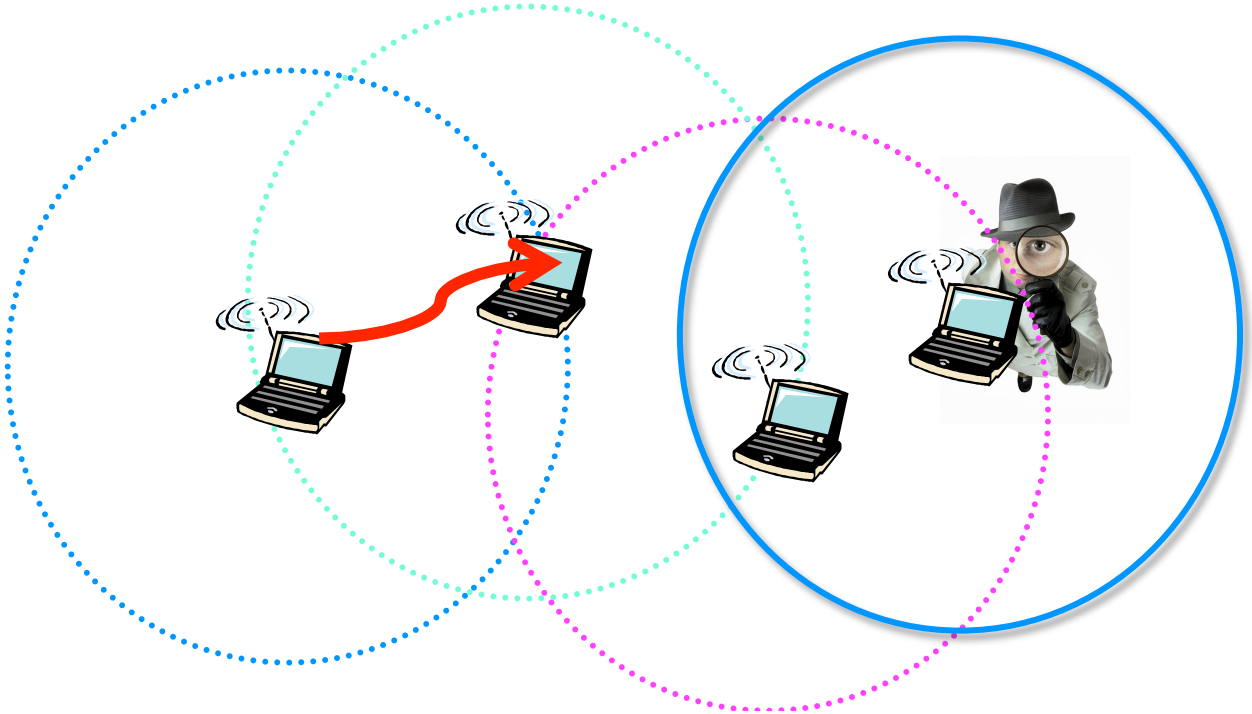
Gig Zero Delay Tap

The Gig Zero Delay Tap is the industry's only 10/100/1000BaseT Tap with true Zero Delay operation. Using innovative new technology, this Tap guarantees absolutely zero packet loss on the network link even during power outages. With the Gig Zero Delay Tap, power glitches and failures no longer mean dropped packets and lengthy renegotiation sequences. Your network operates more smoothly and your critical business applications remain responsive with the Gig Zero Delay Tap in your monitoring infrastructure.

Get total traffic visibility for 10/100/1000 monitoring and security devices by deploying Net Optics Gig Zero Delay Taps on critical network links as permanent monitoring access ports. The Gig Zero Delay Tap sends copies of traffic moving in each direction on the link to a separate NIC on the monitoring device for comprehensive full-duplex monitoring. The Tap has no IP address, so monitoring devices are isolated from the network, dramatically reducing their exposure to attacks. The monitoring device connected to the Tap sees all full-duplex traffic as if it were in-line, including Layer 1 and Layer 2 errors.

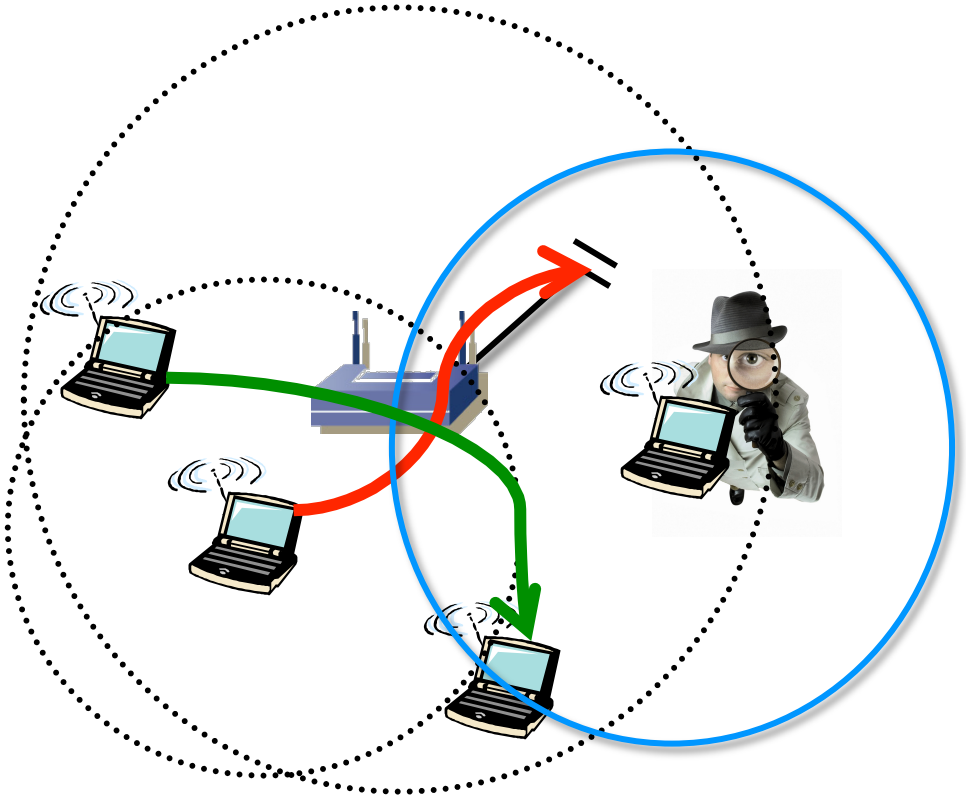
¿Cómo tener acceso al tráfico?

- En WLANs de nuevo un interfaz ve lo que envían otros
- Pero solo si está dentro del alcance
- ¿ En escenario BSS (con AP) ? (...)



¿Cómo tener acceso al tráfico?

- En WLANs de nuevo un interfaz ve lo que envían otros
- Pero solo si está dentro del alcance
- ¿ En escenario BSS (con AP) ?
- Debería ver todo el tráfico reenviado por el AP a la WLAN
- Pero podría no ver el que vaya al DS (sí los ACK)

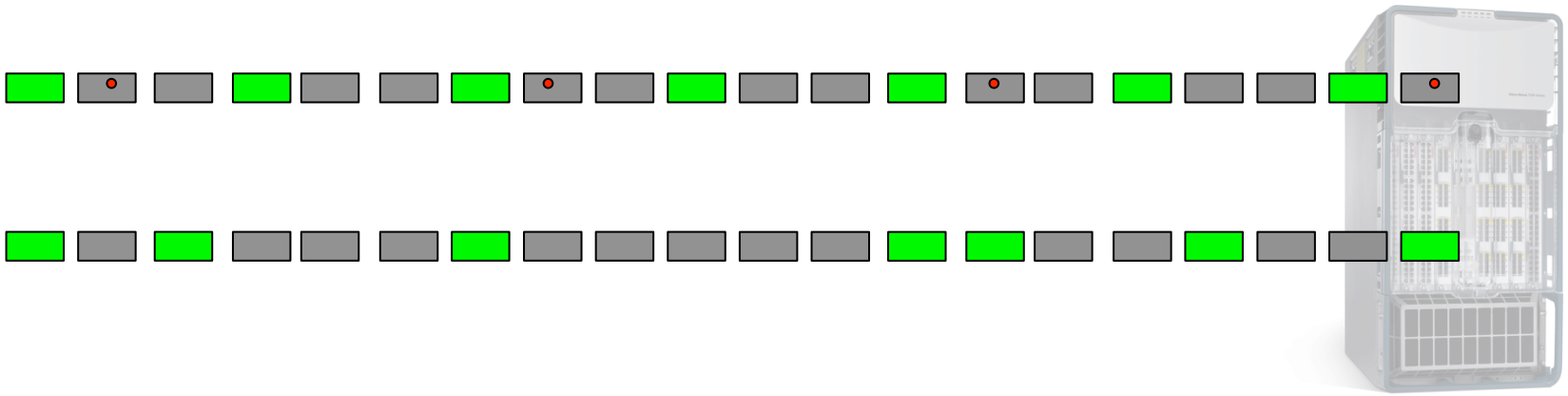


Completo vs muestreado

- Para medición de flujos o registros de paquetes
- Podemos analizar/recoger todos los paquetes o solo una fracción
- Completo
  - No nos dejamos nada, no hay error de medida
  - Podemos seguir el estado de sesiones
  - Podemos inspeccionar contenido de aplicación
  - Pero gran cantidad de información recogida (número de paquetes o flujos)
  - Puede llegar a tener requisitos serios de CPU y throughput a disco, throughput de registros en red (NetFlow), etc
- Muestreado (...)

Completo vs muestreado

- Muestreado
  - En conmutadores/routers de gama alta puede que la medición tenga que ser “muestreada”
  - Se analiza/recoge 1 de cada N paquetes o cada N ms
  - Escala mejor para grandes tasas de tráfico
  - Pero podemos dejarnos algo importante (por ejemplo para facturar)
  - Muestreo determinista o probabilístico (1 de cada N al azar o para cada uno una probabilidad)
  - Determinista puede sesgar los resultados ante patrones periódicos
  - IETF PSAMP (RFC 5474 “A Framework for Packet Selection and Reporting”)



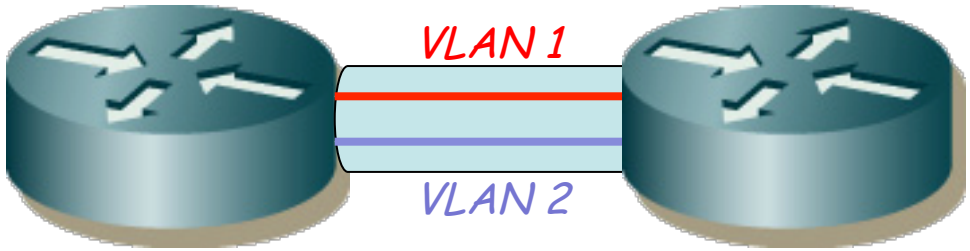
¿Qué hacer con la medida?

- 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
- (...)

¿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?

VLANs?

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

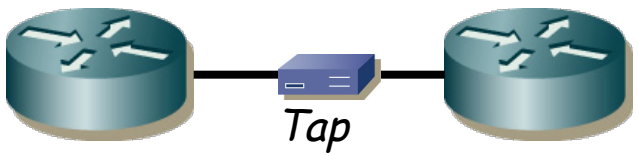
¿Qué hacer con la medida?

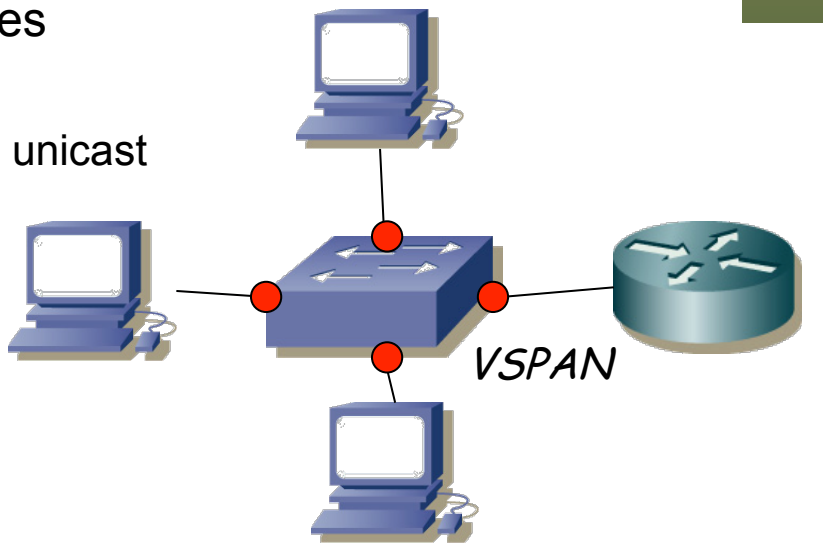
VLANs?

Protocolos presentes en la LAN?

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?

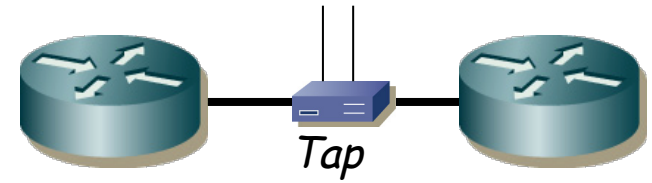
VLANs?

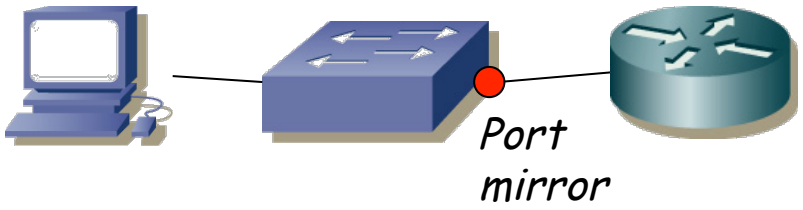
Protocolos presentes en la LAN?

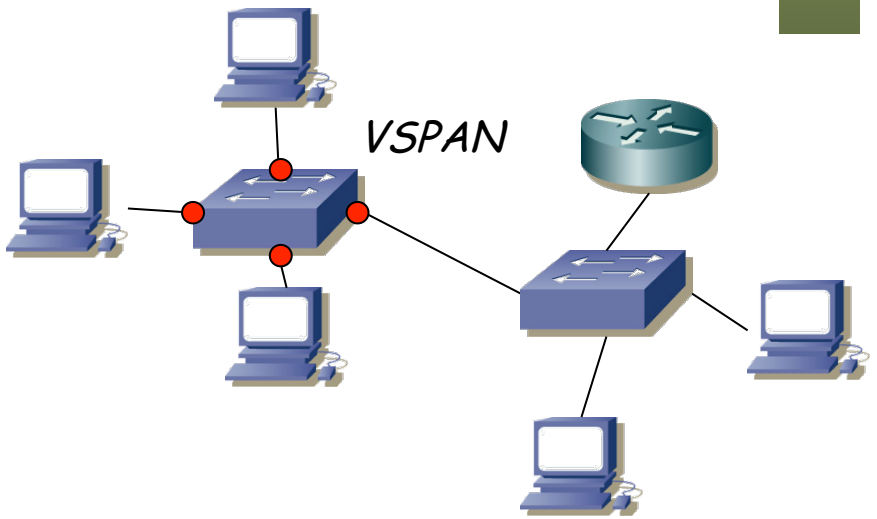
Estaciones presentes en la LAN?

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







¿Qué hacer con la medida?

VLANs?

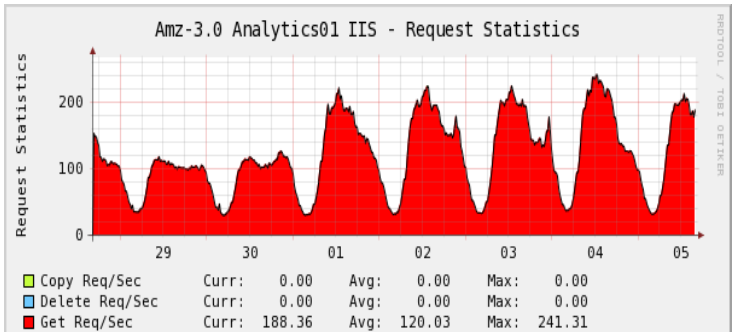
Protocolos presentes en la LAN?

Estaciones presentes en la LAN?

Utilización de enlaces?

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?

VLANs?

Protocolos presentes en la LAN?

Estaciones presentes en la LAN?

Utilización de enlaces?

Hosts IPv4

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?

VLANs?

Protocolos presentes en la LAN?

Estaciones presentes en la LAN?

Utilización de enlaces?

Hosts IPv4

Problemas en IP

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

¿Qué hacer con la medida?

VLANs?

Protocolos presentes en la LAN?

Estaciones presentes en la LAN?

Utilización de enlaces?

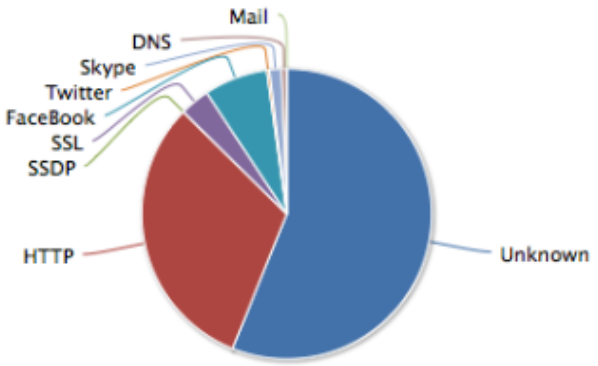
Hosts IPv4

Problemas en IP

Protocolos sobre IP

Aplicaciones sobre TCP o UDP

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



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
- 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

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?

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

- 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?)

¿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

- 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 pasivas en WLAN

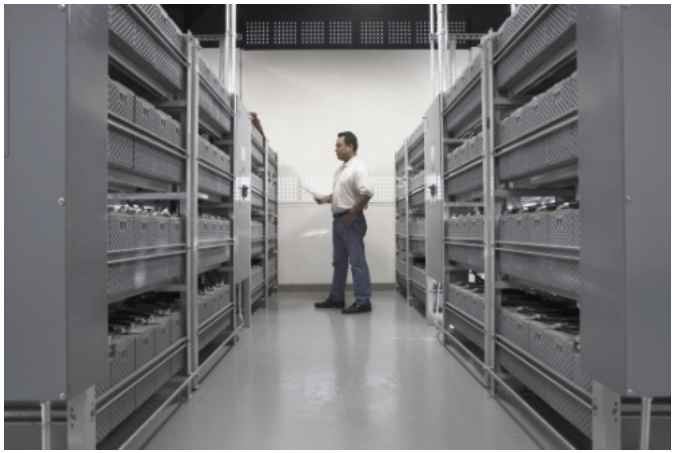
- Características específicas del medio y nivel MAC
- Potencia, SNR, canales empleados, WLANs en mismos canales
- WLANs “piratas”
- *Access Points* localizados
- Seguridad implementada en cada WLAN
- Detección de intentos de intrusión

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