Trabajo Final de Máster Software Libre

Análisis, desarrollo e implantación de plataforma de traceo y monitorización en redes de acceso de telecomunicación basadas en protocolos Ethernet/IP mediante uso de herramientas libres en entornos GNU/Linux

Antonio Gandía

Enero 2012

Índice

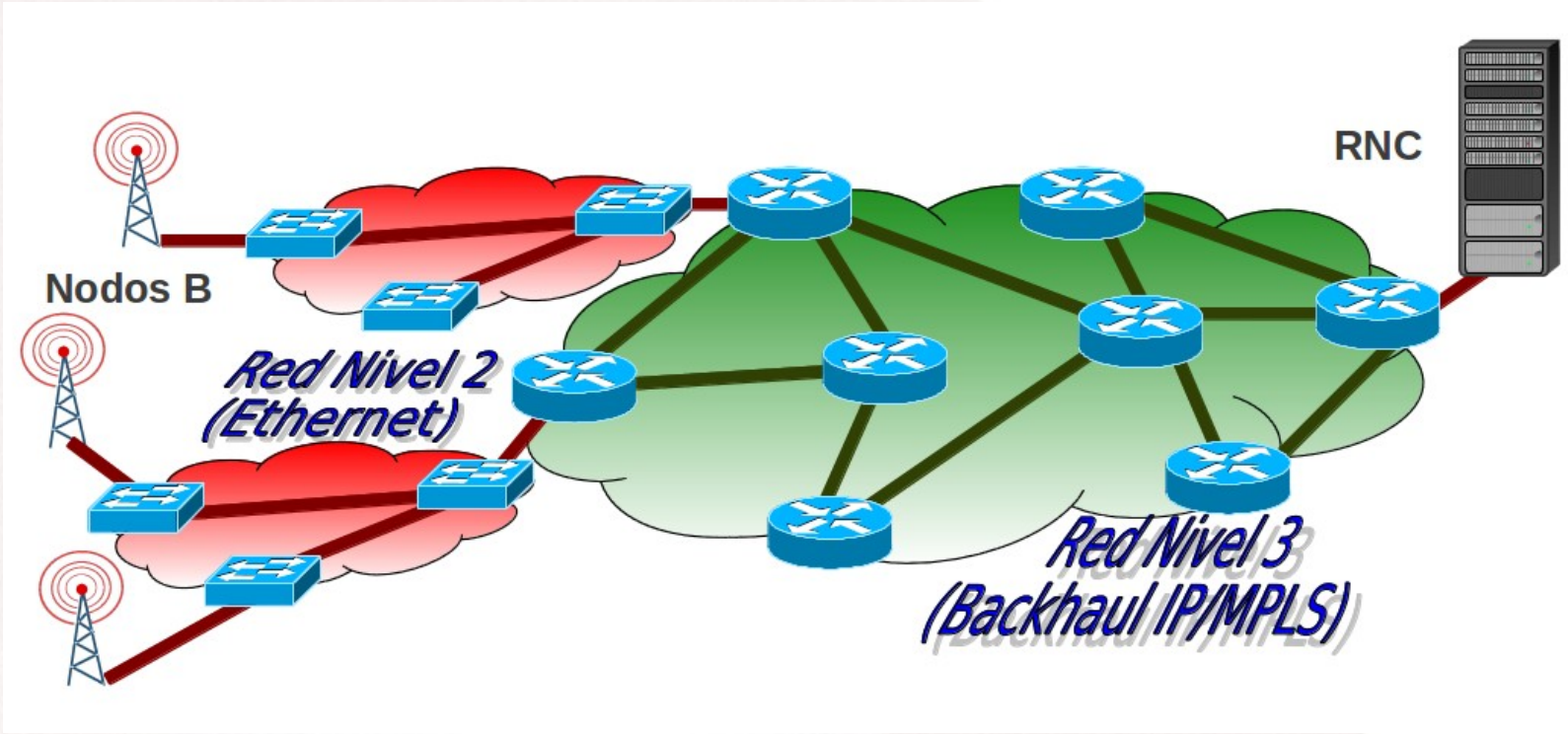
1. Objetivos
2. Estudio de Viabilidad
3. Análisis del Sistema
4. Diseño de Prototipo
5. Desarrollo e Implantación
6. Resultados y análisis de casos de uso
7. Conclusiones

Objetivos

- Análisis de necesidades de un operador en cuanto a herramientas de troubleshooting en redes de acceso basadas en transporte IP.
- Estudio de herramientas (software libre) de análisis, traceo y monitorizado de redes.
- Estudio, análisis y viabilidad de las posibilidades de implantación de plataformas que satisfagan requisitos de análisis y traceo de redes mediante Software Libre teniendo en cuenta aspectos de mantenimiento, eficiencia, acceso remoto, etc.
- Diseño, desarrollo e implantación de un prototipo para tracear/monitorizar un tipo de interfaz de red (p.e. IuB nodo B UMTS).
- Documentación y análisis de ejemplos de uso de la plataforma.
- Aplicación de metodología de desarrollo de proyectos estudiados durante el máster.
- Puesta en conocimiento y difusión dentro de la empresa de herramientas de Software Libre y que pueda servir de base para incrementar su grado de utilización en un futuro.

Estudio Viabilidad. Situación Actual

- Las redes de telecomunicaciones han evolucionado a un transporte basado en protocolo IP sobre Ethernet/PPP
- Típica topología de red UTRAN:



Estudio Viabilidad. Problemática

- Aunque en la actualidad todos los fabricantes de redes IP ofrecen plataformas para ayudar al troubleshooting, éstas tienen varios problemas:
  - Pocas posibilidades de hacer traceos de bajo nivel.
  - Estadísticas muy generales y con pocas condiciones para el segmentado/filtrado.
  - Plataformas muy heterogéneas entre diferentes fabricantes (en una red conviven varios tipos de equipos).
  - En la red de acceso, la capilaridad es muy alta y el acceso a los elementos de red es complejo y por personal no especializado.
  - Suelen ser poco flexibles para hacer análisis complejos en profundidad.
  - Existen fabricantes de plataformas paralelas dedicadas únicamente a traceo y análisis pero son costosas.

Estudio Viabilidad. Necesidades y Requisitos

- **Necesidad:** plataforma (primera fase prototipo) accesible remotamente, con herrramienta para diagnosticar problemas en la red IP de acceso, basándose en capturas y análisis de trazas y estadísticas detalladas de los interfaces.
- **Requisitos Mínimos:**
  - Grabar y Analizar Trazas.
  - Analizar cualquier interfaz de cualquier router frontera del Backhaul IP.
  - Acceso remoto desde cualquier terminal conectado a la intranet corporativa.
  - Estadísticas básicas.
  - Coste económico próximo a cero.
  - Separación de tráfico de telecomunicaciones y tráfico de la red corporativa.
  - Seguridad (accesos autorizados).
- **Requisitos Deseables:**
  - Poder pinchar cualquier interfaz ethernet con la sonda (no sólo el Backhaul).
  - Detalle de desglose/segmentación de estadísticas (p.e. por MAC origen/destino, DSCP, VLAN, tramas erróneas, ancho de banda,...)
  - Filtros de tráfico para que la traza sólo sea del tráfico deseado.
  - Inyección de tráfico. (Pings, traceroute, evaluación ancho de banda e2e,...).
  - Sin desplazamientos de personal a los emplazamientos.
  - Operación remota encriptada.

Estudio Viabilidad. Alternativas y Solución Escogida

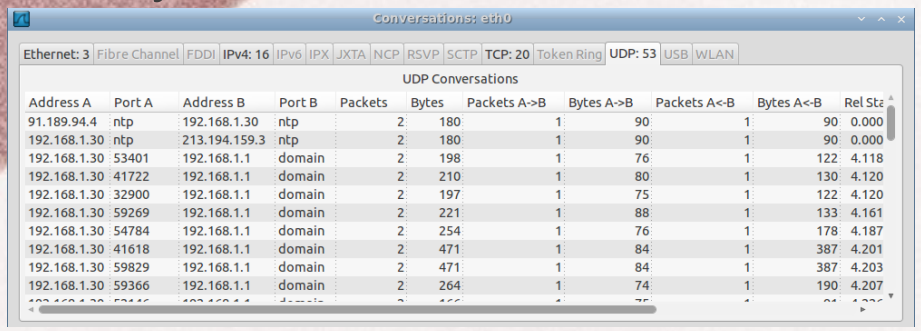
- Herramienta de captura y análisis
  - Posibles: tpcdump/libpcap, snort, netcat, …
  - Solución escogida: Wireshark
- Sistema Operativo base:
  - Posibles: Windows, Fedora, Debian, Ubuntu
  - Solución escogida: Lubuntu
- Máquina:
  - Posibles: instalar en partición de cualquier máquina.
  - Solución escogida: virtualizar en VirtualBox una única máquina que pueda ser replicada e instalada en máquinas fijas conectadas a red (prototipo) o en máquinas portátiles de técnicos de campo (a futuro)
- Modo de capturar/sondar:
  - Posibles: paso a través, port mirroring (no se descarta porque era requisito deseable)
  - Solución escogida: Remote Port Mirroring en Backhaul (para requisito mínimo)

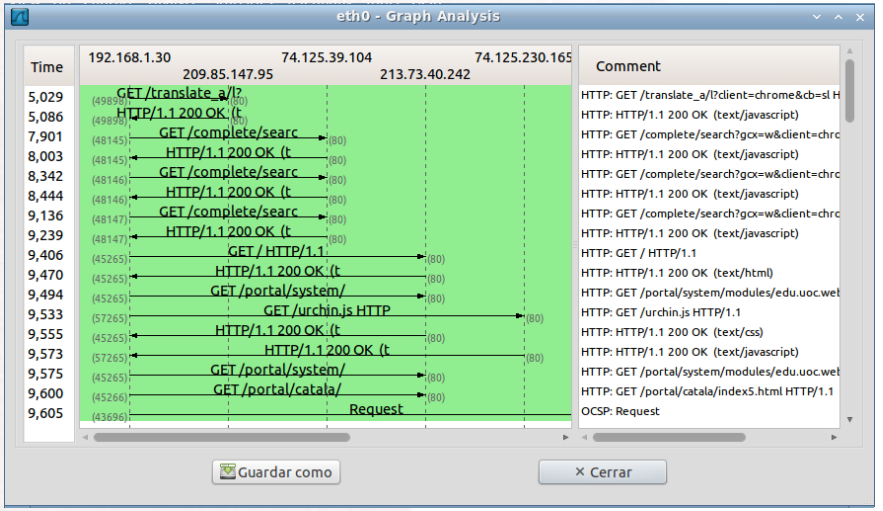
Análisis de la Solución. Seguridad

- Máquina Virtual Huésped:
  - No va a ver la red corporativa (intranet). Sólo interfaz ethernet a monitorizar (separación de los 2 tráficos).
  - Escritorio remoto accesible gracias a la las funcionalidades de VirtualBox que lo pondrá disponible en la intranet (con password).
  - Intercambio de ficheros: a través del anfitrión mediante funcionalidad de carpeta compartida de VirtualBox.
  - Un único usuario compartido por los usuarios.
- Máquina Anfitriona:
  - Si es Windows => administrada por IT.
  - Si es Lubuntu (prototipo):
    - Acceso de administración por SSH.
    - Se habilita un usuario sin acceso a consola para acceder “enjaulado” a la carpeta compartida mediante FTP.

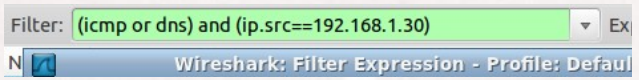
Análisis de la Solución. ¿Wireshark suficente?

- Cumple Wireshark todos los requisitos funcionales?
- Grabar y Analizar Trazas: Sí excelentemente

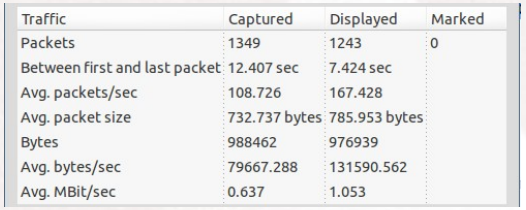




- Filtros de Tráfico: Sí

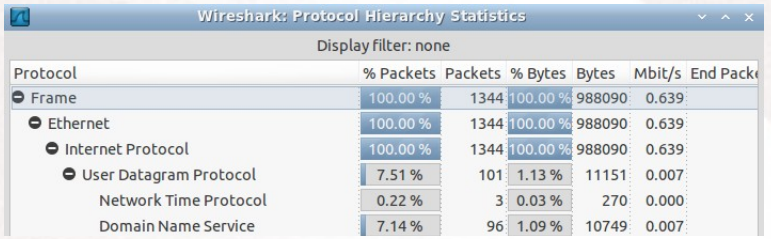


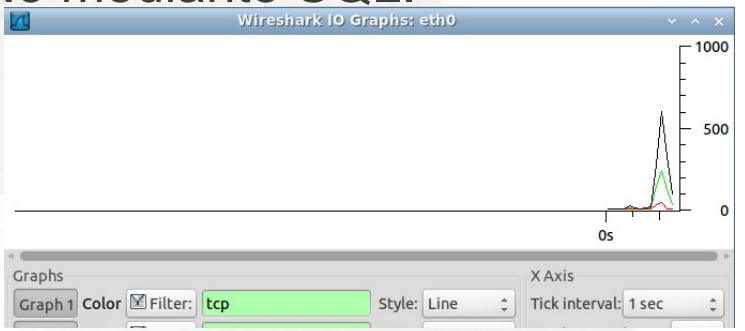
- Estadísticas básicas: Sí



Traffic	Captured	Displayed	Marked
Packets	1349	1243	0
Between first and last packet	12.407 sec	7.424 sec	
Avg. packets/sec	108.726	167.428	
Avg. packet size	732.737 bytes	785.953 bytes	
Bytes	988462	976939	
Avg. bytes/sec	79667.288	131590.562	
Avg. MBit/sec	0.637	1.053	

- Detalle de estadísticas: Sí utilizando filtros. No mediante SQL.





- Inyección de tráfico: No (futura línea trabajo)

NO ES NECESARIO NINGÚN DESARROLLO DE SOFTWARE ADICIONAL

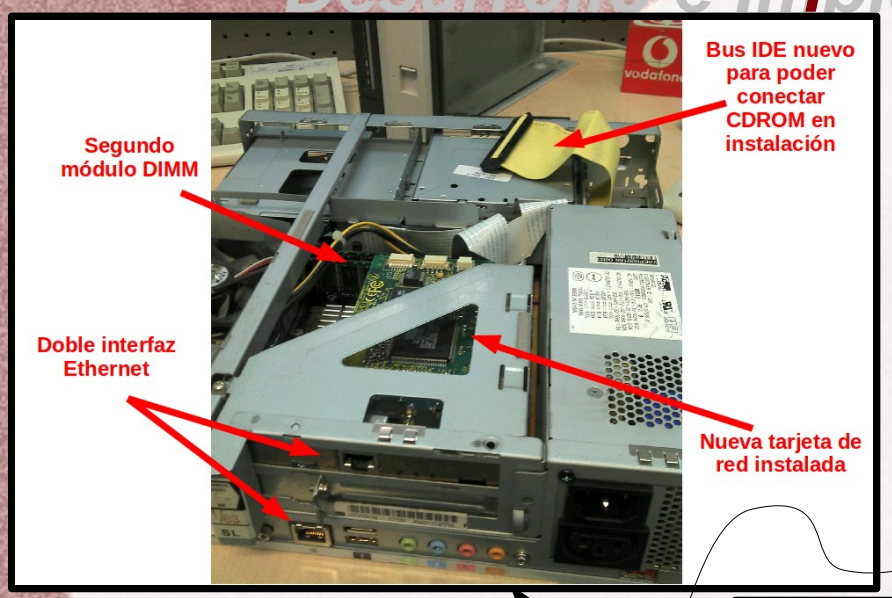
Diseño Prototipo. Máquina Anfitriona

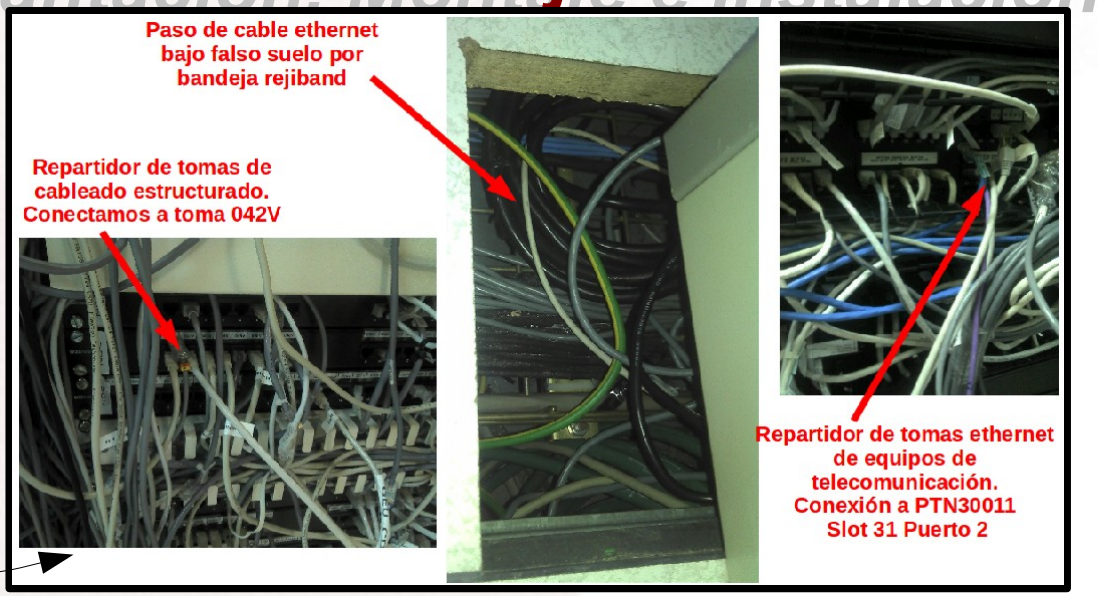
- Hardware reutilizado (obsoleto para Windows):
  - CPU: Pentium 4 (real 1,8 GHz) sin VT-x o AMD-V
  - RAM: 1GB
  - Disco Duro: Mínimo 10-20GB. Real 38GB IDE.
  - Tarjetas de Red: Al menos 2 interfaces de red: (corporativa y red analizada)
  - Resto de periféricos: gráfica simple (integrada). Durante la instalación monitor+teclado+ratón+unidad CDROM externa
- Sistema Base:
  - Lubuntu 10.10 (porque en la versión 11.10, los controladores de red virtual Virtualbox OSE provocaban “VLAN tag stripping”).
  - 1GB de swap.
  - IP fija para el interfaz conectado a intranet corporativa.
  - Un único usuario con shell “administrator” que es sudoer.
  - Protector de pantalla con contraseña.
  - Desactivado el permiso de apagado.
- Software:
  - Virtualbox OSE.
    - Modo headless.
    - Configurado como servicio autoarrancable.
    - Habilitado VNC a máquina virtual con password.
  - Vsftpd: sólo usuario “userftp” sin shell y enjaulado a carpeta compartida
  - SSH: para administración remota

Diseño Prototipo. Máquina Huésped

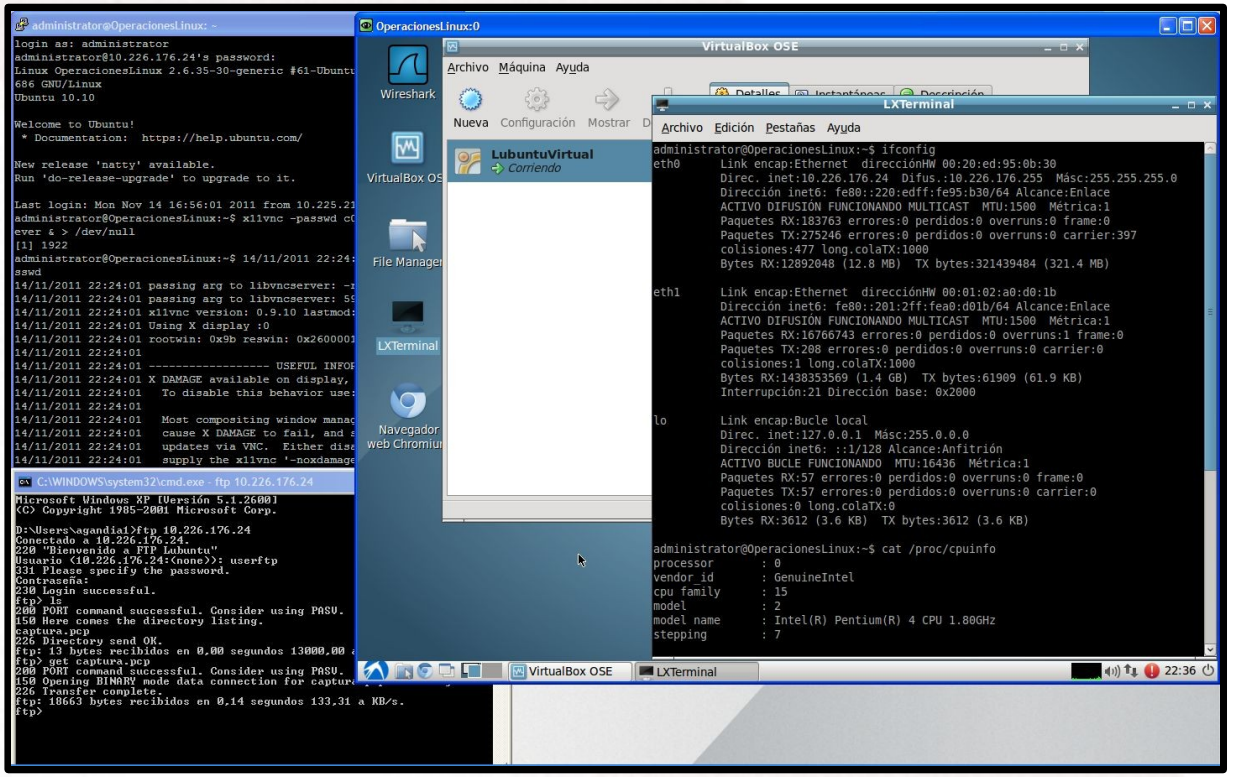
- Hardware virtual:
  - CPU: 1 Única CPU. No habilitado la extensión PAE/NX ni VT-x/AMD-V.
  - RAM: 512 Mbytes.
  - Placa Base: Deshabilitados IO APIC, EFI y dispositivo apuntador absoluto.
  - Tarjeta Gráfica: 12 Mbytes de memoria de video. Sin aceleración 3D.
  - Disco duro: Emulación de SATA, tipo AHCI. Está mapeado sobre un fichero portable (LubuntuVirtual.vdi) de tamaño 8Gbytes dinámico.
  - Red: Sólo 1 “adaptador puente” (promiscuo), sobre el interfaz que mira a la red analizada. Controlador Pcnet-FAST III (Am79C973) soporta VLAN.
  - Audio y Puerto Serie: Deshabilitado.
- Sistema Base:
  - Lubuntu 11.10 (sin swap).
  - 1GB de swap.
  - Un único usuario “user” conocido por todos los usuarios.
  - Protector de pantalla con contraseña.
  - Definición de carpeta compartida de Virtualbox en /etc/fstab.
- Software:
  - Wireshark.
    - Habilitado de captura sin ser root.
    - Desactivado “update list of packets in real time” por performance.

Desarrollo e Implantación. Montaje e Instalación





- Montaje Hardware
- Cableado en sala de equipos
- Instalación de paquetes de software y ejecución de pruebas de aceptación



Desarrollo e Implantación. Documentación y Formación

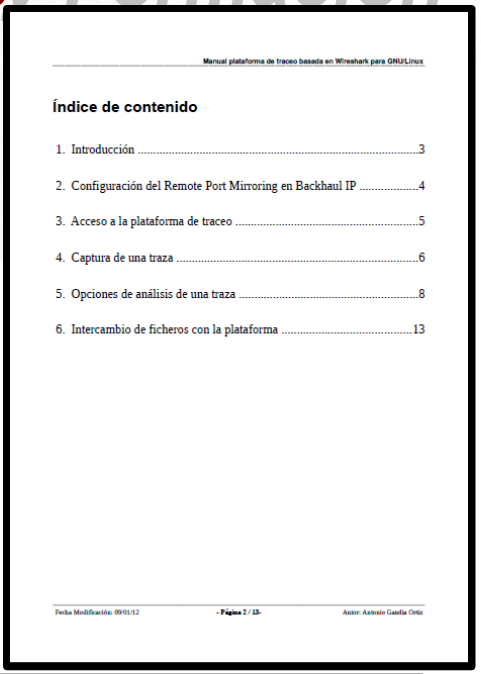
Manual de usuario
(anexado a la memoria)

Manual plataforma de traceo basada en Wireshark para GNU/Linux

Documento de uso interno nivel en la compañía.

Autor: **Antonio Gandía Ortiz**

Enero 2012

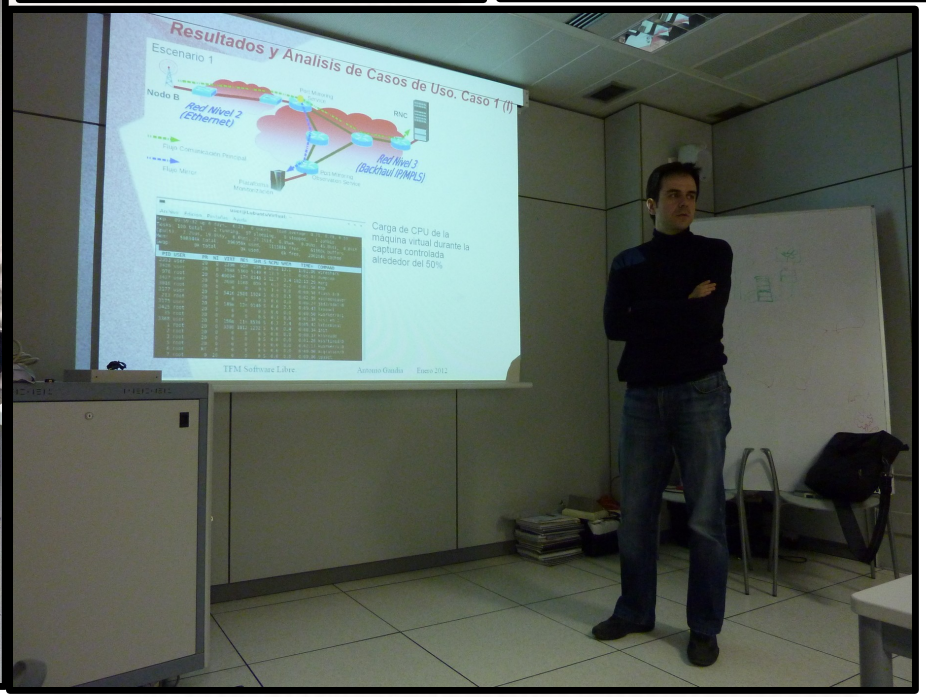


Manual plataforma de traceo basada en Wireshark para GNU/Linux

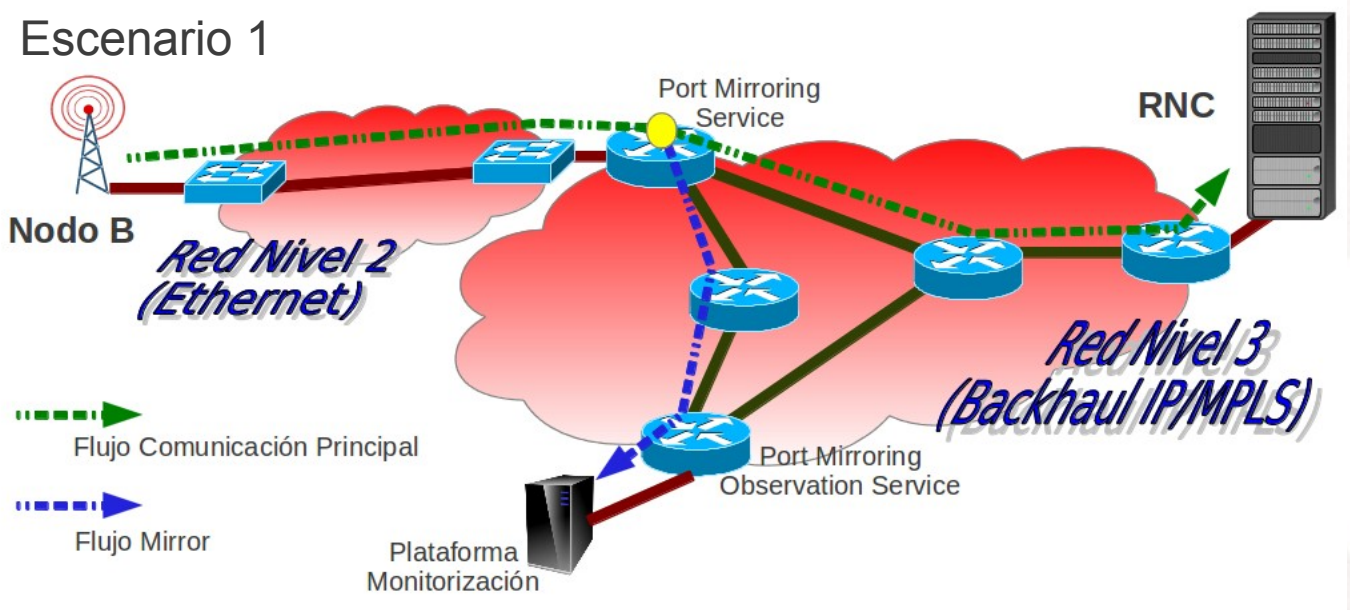
Índice de contenido

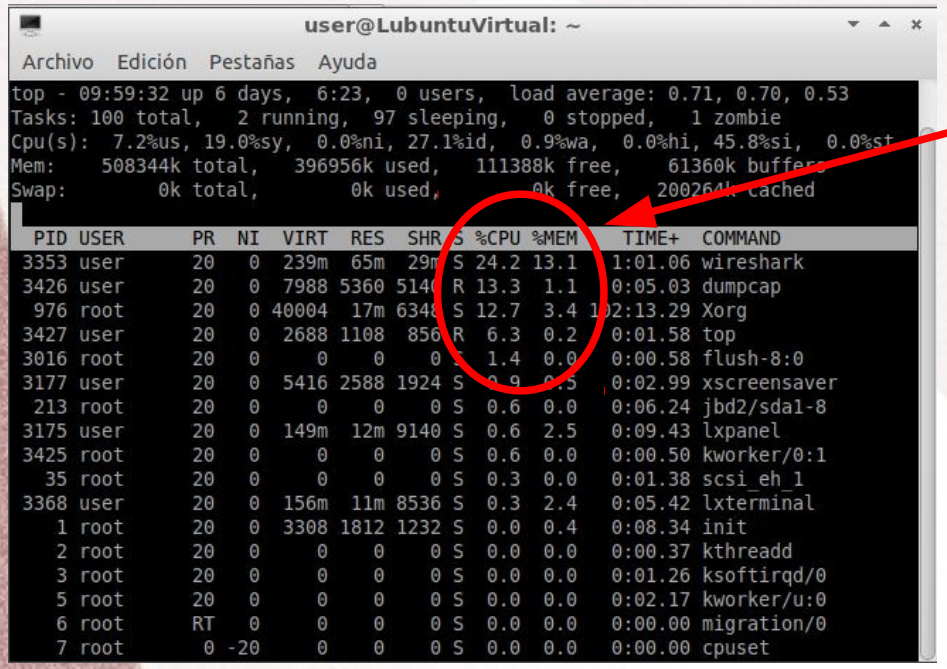
1. Introducción 3
2. Configuración del Remote Port Mirroring en Backhaul IP 4
3. Acceso a la plataforma de traceo 5
4. Captura de una traza 6
5. Opciones de análisis de una traza 8
6. Intercambio de ficheros con la plataforma 13

Sesión de formación a usuarios



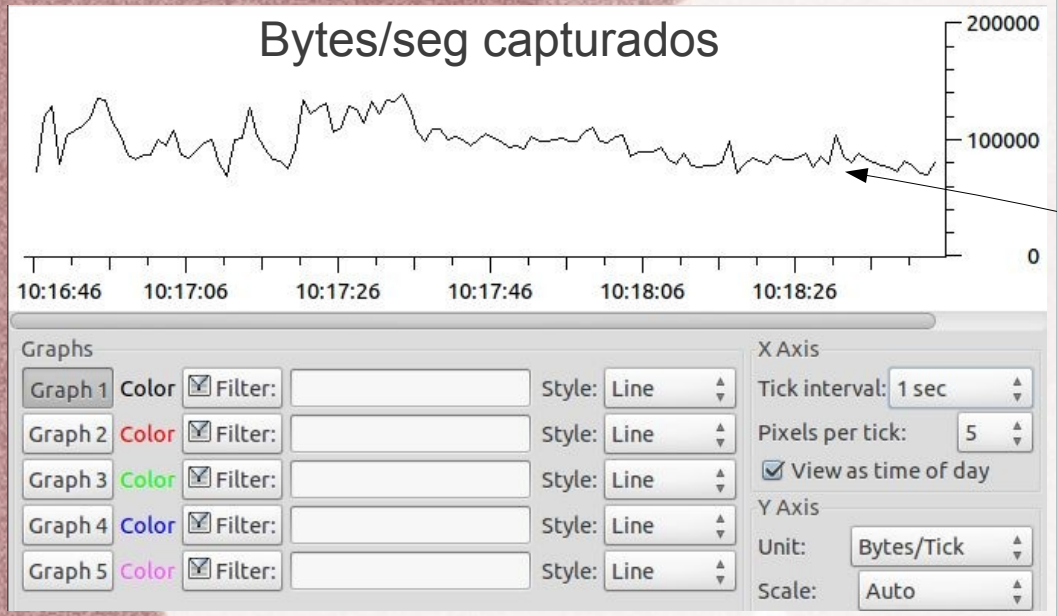
Resultados y Analisis de Casos de Uso. Caso 1 (I)

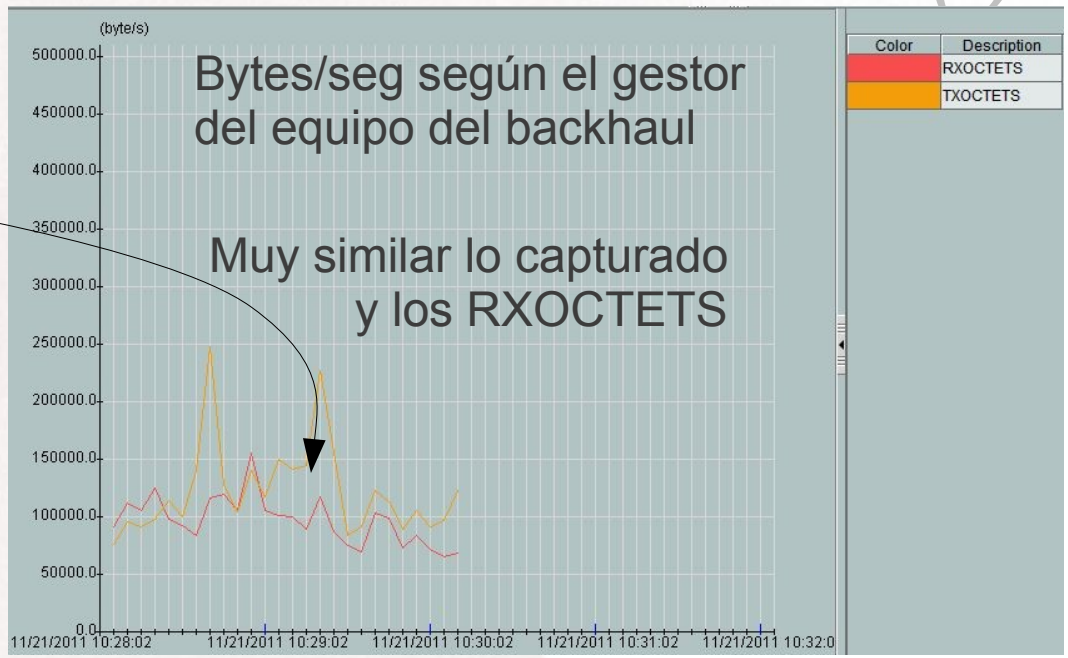




Carga de CPU de la máquina virtual durante la captura controlada alrededor del 50%

Resultados y Análisis de Casos de Uso. Caso 1 (II)





Son idénticos los capturados y el sentido ingress del Backhaul!!!

Ethernet: 2 | Fibre Channel | FDDI | IPv4: 4 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP: 2 | TCP: 1 | Token Ring | UDP: 639 | USB | WL

Ethernet Conversations

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B
00:18:82:88:31:31	00:25:9e:24:49:62	149 926	12 251 920	0	0	149 926	12 251 920
00:18:82:8a:aa:88	01:80:c2:00:00:02	130	7 800	130	7 800	0	0

Ethernet: 2 | Fibre Channel | FDDI | IPv4: 4 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP: 2 | TCP: 1 | Token Ring | UDP: 639

IPv4 Conversations

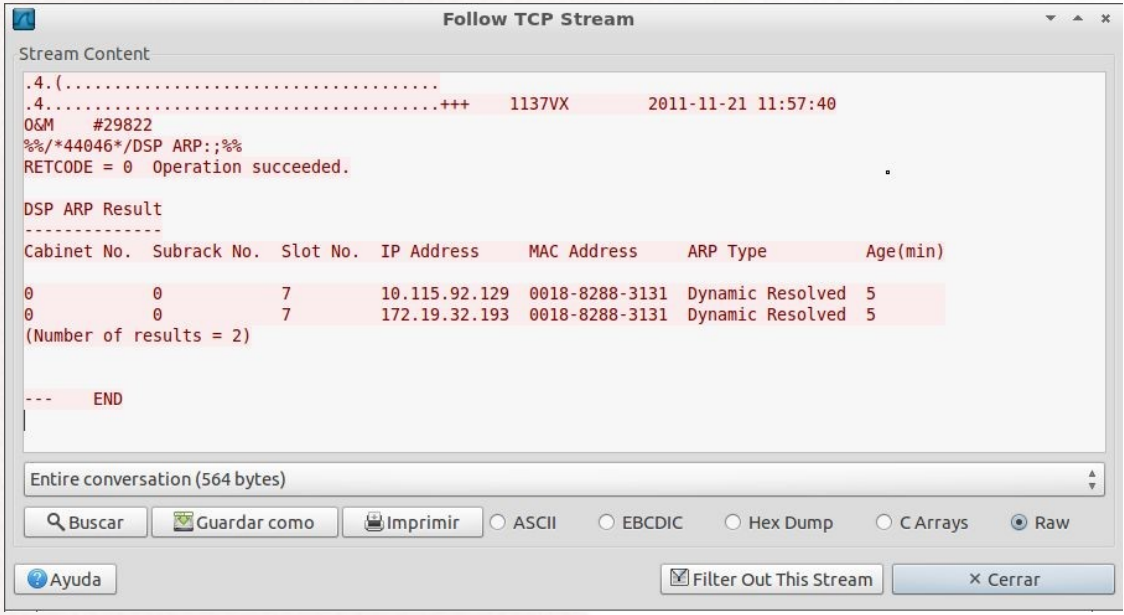
Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B
172.19.32.194	172.19.254.90	149 943	12 252 209	149 906	12 249 471	37	2 738
10.18.11.19	10.115.88.84	16	2 129	0	0	16	2 129
172.19.32.194	172.19.251.6	2	160	2	160	0	0
172.19.32.194	172.19.251.2	2	160	2	160	0	0

El backhaul no tiene bien implementado el Remote Port Mirroring para el sentido egress

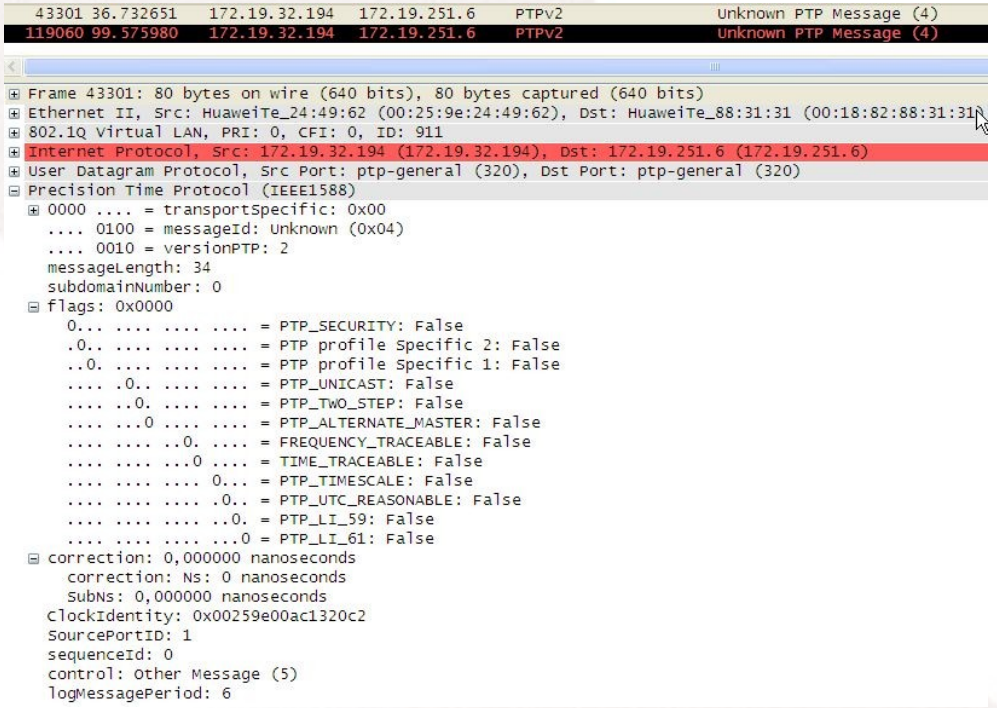
No se ven paquetes con destino al nodo B pero si originados en él!!!!

Resultados y Análisis de Casos de Uso. Caso 1 (III)

Análisis de Tráfico de gestión (O&M) del nodo B: Intercambio de paquetes TURN/STUN con el texto en plano de los comandos



Análisis de Tráfico de sincronismo: Intercambio de paquetes del protocolo PTP (Precission Time Protocol o IEEE 1588)



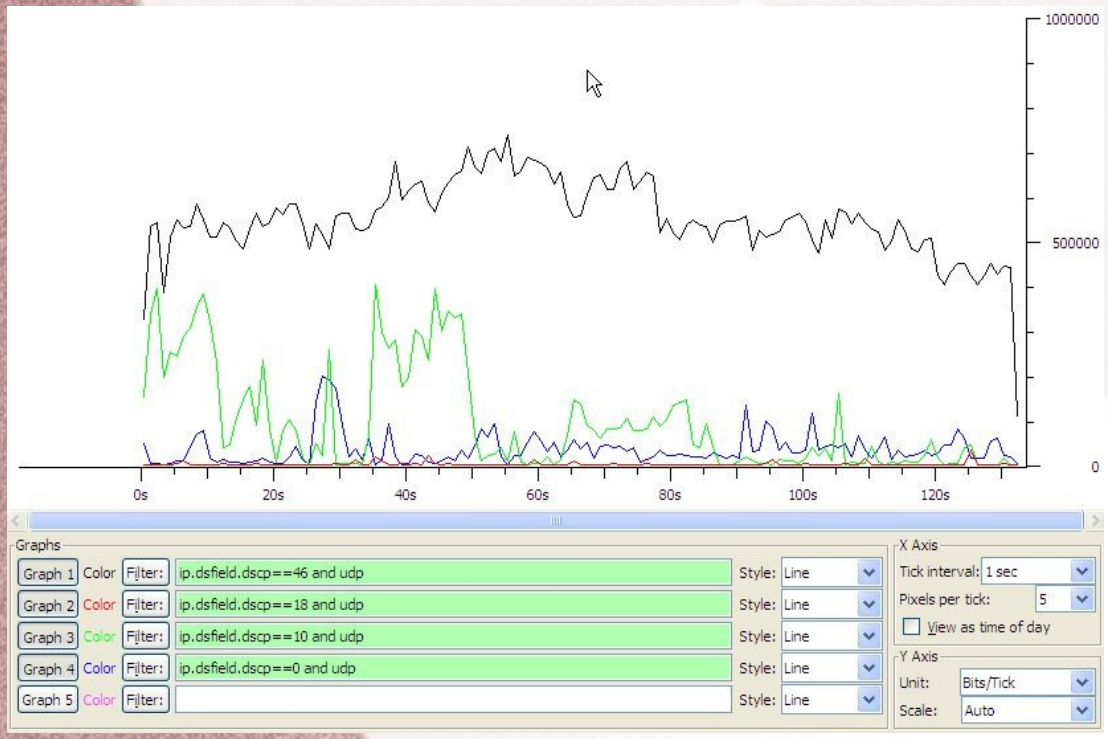
Resultados y Análisis de Casos de Uso. Caso 1 (IV)

Análisis de Tráfico de Señalización:

Se ven paquetes SCTP pero como nos falta un sentido de la comunicación (el egress) no tiene mucho sentido analizarlo aquí y lo analizaremos en profundidad en el Caso 2

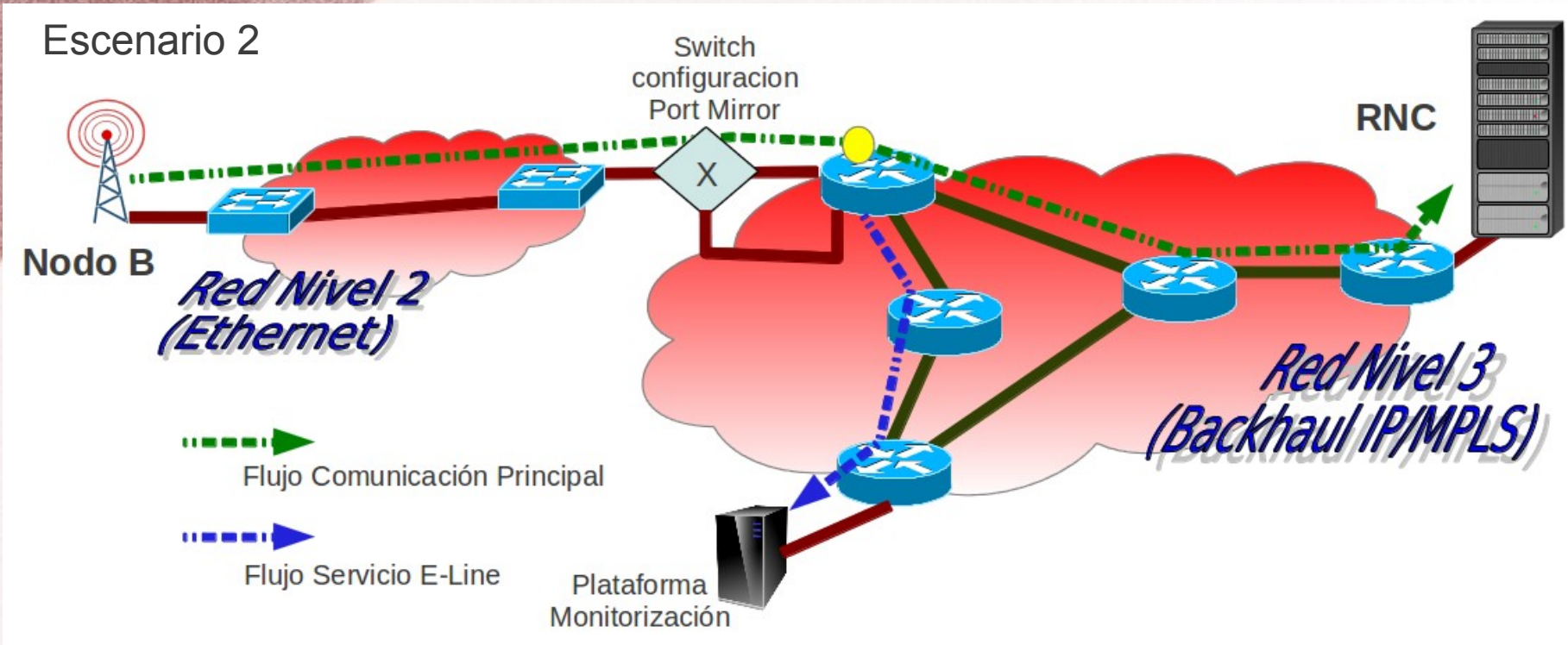
Análisis de Tráfico de Usuario:

- Tráfico encriptado para proteger la privacidad de las comunicaciones de usuario.
- Se puede hacer un análisis estadístico por QoS (DSCP), ya que los tráficos con mayor prioridad (p.e. Expedited Forward) suele utilizarse para voz y los de menor prioridad (p.e. Best Effort) para datos de internet.
- Tráfico de voz = bastante constante en tiempo y paquetes pequeños
- Tráfico de datos = a ráfagas y paquetes algo mayores



		DSCP=46 (EF, Expedited Forward)	DSCP=18 (AF21, Assured Forward 21)	DSCP=10 (AF11, Assured Forward 11)	DSCP=0 (BE,Best Effort)
Convesaciones UDP		509	8	97	61
Rango puertos RNC		29122-64896	29758-57818	30310-64856	29714-64946
Rango puertos NodoB		1024-5822	2174-4590	1086-5794	1130-5773
Paquetes		123053	287	12381	5156
%Paquetes		*82,0%*	*0,2%*	*8,3%*	*3,4%*
Bytes		9170000	30704	1568966	603691
%Bytes		*74,8%*	*0,3%*	*12,8%*	*4,9%*
Histograma Longitud Paquetes	0-19	*0,0%*	*0,0%*	*0,0%*	*0,0%*
	20-39	*0,0%*	*0,0%*	*0,0%*	*0,0%*
	40-79	*49,9%*	*5,9%*	*0,6%*	*1,2%*
	80-159	*50,1%*	*90,2%*	*82,0%*	*88,0%*
	160-319	*0,0%*	*3,8%*	*16,3%*	*10,2%*
	320-639	*0,0%*	*0,0%*	*1,1%*	*0,6%*
	640-1279	*0,0%*	*0,0%*	*0,0%*	*0,0%*
	1280-2559	*0,0%*	*0,0%*	*0,0%*	*0,0%*
	2560-5119	*0,0%*	*0,0%*	*0,0%*	*0,0%*
	>5120	*0,0%*	*0,0%*	*0,0%*	*0,0%*

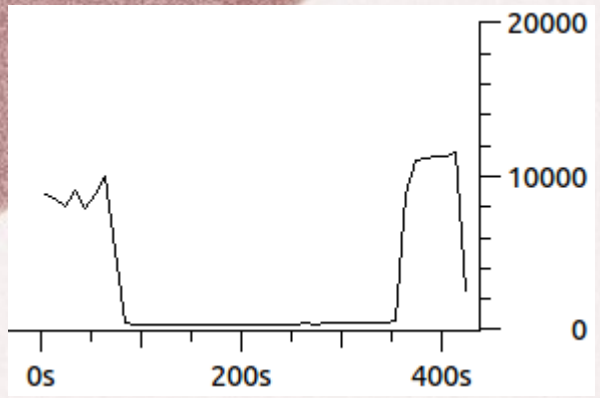
Resultados y Análisis de Casos de Uso. Caso 2 (I)



- Para poder capturar el sentido egress del Backhaul, se compró e instaló un switch con capacidades de Port Mirror. El intercalado del switch provoca un corte de servicio y se ha de hacer en horas de bajo tráfico (madrugada).
- La captura completa se envía al puerto donde está la plataforma mediante un servicio E-Line del Backhaul.
- El objetivo es capturar la señalización bidireccional.
- Como el trabajo se hizo de noche, capturamos un reinicio del nodo para capturar la señalización de un proceso de establecimiento de celdas radio.

Resultados y Análisis de Casos de Uso. Caso 2 (II)

Ancho de banda capturado (reinicio de nodo B)



Capturas bidireccionales

IPv4 Conversations: 8

Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B
129 176	10 386 325	44 540	3 578 592	84 636	6 807 733
6 765	608 952	5	420	6 760	608 532
344	71 377	153	12 869	191	58 508
2 274	204 804	6	520	2 268	204 284
30	3 504	30	3 504	0	0
6	564	3	282	3	282
9	3 264	9	3 264	0	0
399	25 536	0	0	399	25 536

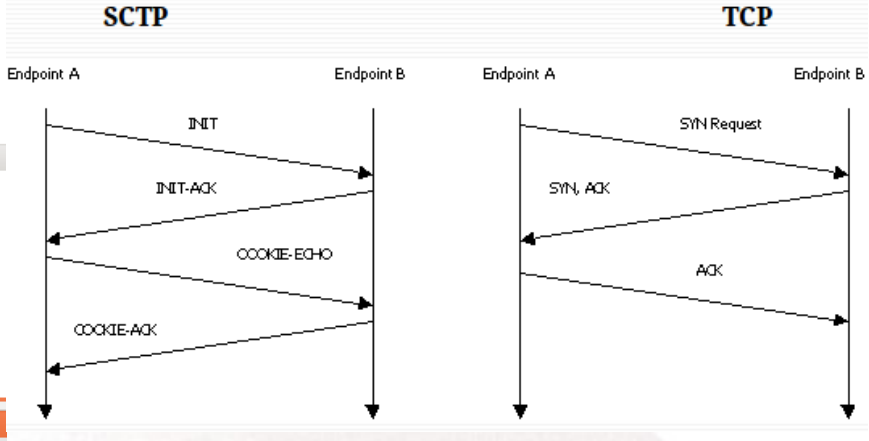
Análisis del protocolo de establecimiento conexiones SCTP (a 4 bandas) tras reinicio. Son 2 porque NBAP monta 2 (NCP y CCP)

Filter: sctp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.19.254.90	172.19.32.194	SCTP	142	HEARTBEAT
146	8.000056	172.19.254.90	172.19.32.194	SCTP	142	HEARTBEAT
291	16.000284	172.19.254.90	172.19.32.194	SCTP	142	HEARTBEAT
344	19.000273	172.19.254.90	172.19.32.194	SCTP	60	ABORT
772	42.782643	172.19.32.194	172.19.254.90	SCTP	82	INIT
773	42.784422	172.19.254.90	172.19.32.194	SCTP	798	INIT_ACK
774	42.786716	172.19.32.194	172.19.254.90	SCTP	766	COOKIE_ECHO
775	42.788758	172.19.254.90	172.19.32.194	SCTP	60	COOKIE_ACK
776	42.790398	172.19.254.90	172.19.32.194	DUA	82	UNKNOWN [Malformed Packet]
777	42.792521	172.19.32.194	172.19.254.90	SCTP	66	SACK
842	45.830618	172.19.32.194	172.19.254.90	SCTP	82	INIT
843	45.832738	172.19.254.90	172.19.32.194	SCTP	798	INIT_ACK
844	45.834730	172.19.32.194	172.19.254.90	SCTP	766	COOKIE_ECHO
845	45.836262	172.19.254.90	172.19.32.194	SCTP	60	COOKIE_ACK
846	45.837088	172.19.254.90	172.19.32.194	DUA	90	UNKNOWN [Malformed Packet]
847	45.850616	172.19.32.194	172.19.254.90	SCTP	142	HEARTBEAT
848	45.852180	172.19.254.90	172.19.32.194	SCTP	142	HEARTBEAT_ACK
853	46.070654	172.19.32.194	172.19.254.90	SCTP	66	SACK
901	48.824955	172.19.254.90	172.19.32.194	DUA	82	UNKNOWN [Malformed Packet]
902	48.824967	172.19.254.90	172.19.32.194	DUA	90	UNKNOWN [Malformed Packet]

```
▸ Frame 842: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
▸ Ethernet II (VLAN tagged), Src: HuaweiTe_24:49:62 (00:25:9e:24:49:62), Dst: HuaweiTe_88:31:31 (00:18:82:88:31:31)
▸ Internet Protocol Version 4, Src: 172.19.32.194 (172.19.32.194), Dst: 172.19.254.90 (172.19.254.90)
▸ Stream Control Transmission Protocol, Src Port: 1025 (1025), Dst Port: 58080 (58080)
```

Comparativa SCTP (4 bandas) y TCP (3 bandas)



Resultados y Análisis de Casos de Uso. Caso 2 (III)

Los chunks de datos (chunk type DATA), se decodificaban como protocolo DUA (Payload Id=10) pero Malformados!!!

```
▼ Stream Control Transmission Protocol, Src Port: 58080 (58080), Dst Port: 1024 (1024)
    Source port: 58080
    Destination port: 1024
    Verification tag: 0x63682d43
    Checksum: 0xd7370f0d (not verified)
  ▼ DATA chunk(ordered, complete segment, TSN: 447948207, SID: 0, SSN: 0, PPID: 10, payload length: 14 bytes)
    ▶ Chunk type: DATA (0)
    ▶ Chunk flags: 0x03
      Chunk length: 30
      TSN: 447948207
      Stream Identifier: 0x0000
      Stream sequence number: 0
      Payload protocol identifier: DUA (10)
      Chunk padding: 0000
▶ DPNSS/DASS2-User Adaptation Layer
▶ [Malformed Packet: DUA]
```

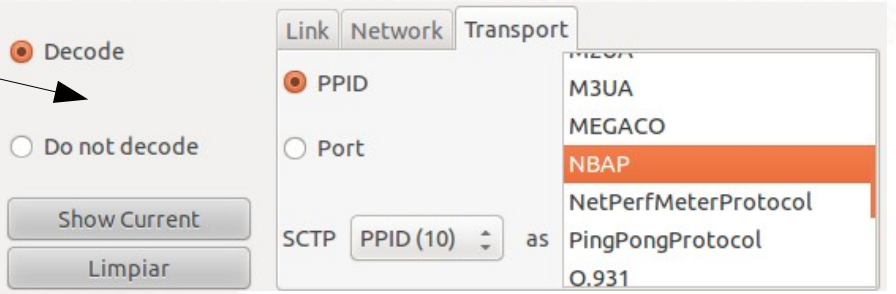
Según el estándar para el SCTP, el payload para NBAP (el protocolo de señalización para nodos B UTRAN) debería tener un Payload Id=25 en vez de 10 (el fabricante no está siguiendo el estándar!!)

Payload Protocol Identifiers.

Identifier	
0	
1	IUA, ISDN Q.921-User Adaptation.
2	M2UA, MTP2-User Adaptation.
3	M3UA, MTP3-User Adaptation.
4	SUA, Signalling Connection Control Part User Adaptation Layer.
5	M2PA, MTP2 User Peer-to-peer Adaptation Layer.
6	V5UA, V5.2-User Adaptation.
7	H.248.
8	BICC / Q.2150.3.
9	TALI, Transport Adapter Layer Interface.
10	DUA.
11	ASAP, Aggregate Server Access Protocol.
12	ENRP, Enpoint Name Resolution Protocol.
13	H.323.
14	Q.IPC / Q.2150.3.
15	SIMCO.
16	DDP Segment Chunk.
17	DDP Stream Session Control.
18	S1AP, S1 Application Protocol.
19	RUA.
20	HNBAP.
21	ForCES-HP.
22	ForCES-MP.
23	ForCES-LP.
24	SBc-AP.
25	NBAP.

Resultados y Análisis de Casos de Uso. Caso 2 (IV)

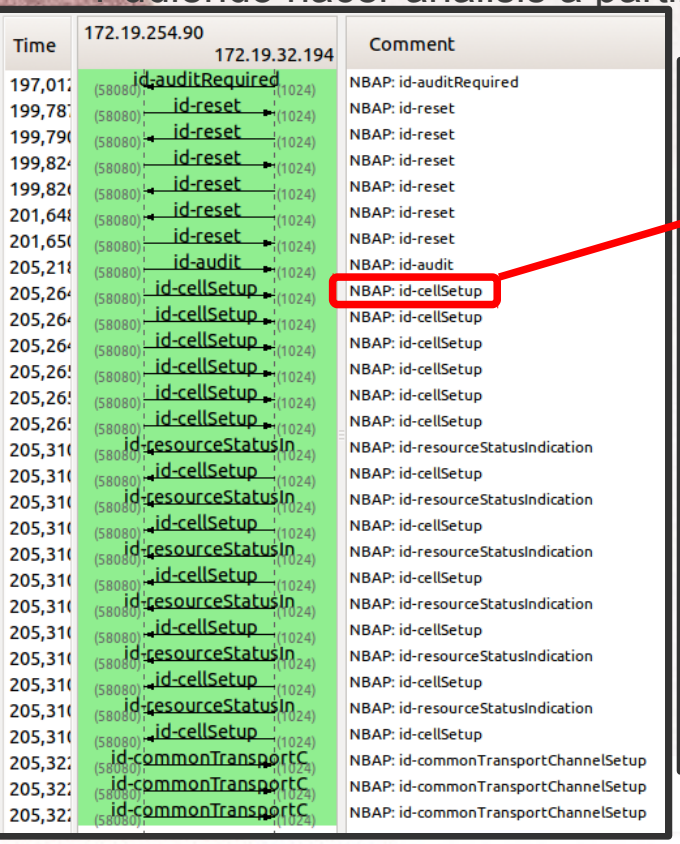
En Wireshark, configuramos para que el Payload Id=10 lo interprete como NBAP



Y decodificamos correctamente la señalización

```
▸ Frame 846: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
▸ Ethernet II (VLAN tagged), Src: HuaweiTe_88:31:31 (00:18:82:88:31:31), Dst: HuaweiTe_24:49:62 (00:25:9e:24:49:62)
▸ Internet Protocol Version 4, Src: 172.19.254.90 (172.19.254.90), Dst: 172.19.32.194 (172.19.32.194)
▸ Stream Control Transmission Protocol, Src Port: 58080 (58080), Dst Port: 1024 (1024)
▾ UTRAN Iub interface NBAP signalling
```

Pudiendo hacer análisis a partir de ahora del protocolo de aplicación de señalización con todos sus mensajes y campos decodificados correctamente:




```
UTRAN Iub interface NBAP signalling
    NBAP-PDU: initiatingMessage (0)
        initiatingMessage
            procedureID
                procedureCode: id-cellSetup (5)
                ddMode: fdd (1)
            criticality: reject (0)
            messageDiscriminator: common (0)
            transactionID: longTransActionId (1)
                longTransActionId: 1600
            value
                CellSetupRequestFDD
                    protocolIEs: 16 items
                        Item 0: id-Local-Cell-ID
                            ProtocolIE-Field
                                id: id-Local-Cell-ID (124)
                                criticality: reject (0)
                                value
                                    Local-Cell-ID: XXXXXXXXXX
                        Item 1: id-C-ID
                            ProtocolIE-Field
                                id: id-C-ID (25)
                                criticality: reject (0)
                                value
                                    C-ID: XXXXXXXXXX
                        ...
                        Item 4: id-UARFCNforNu
                            ProtocolIE-Field
                                id: id-UARFCNforNu (282)
                                criticality: reject (0)
                                value
                                    UARFCN: XXXXXXXXXX
                        Item 5: id-UARFCNforNd
                            ProtocolIE-Field
                                id: id-UARFCNforNd (281)
                                criticality: reject (0)
                                value
                                    UARFCN: XXXXXXXXXX
                        Item 6: id-MaximumTransmissionPower
                            ProtocolIE-Field
                                id: id-MaximumTransmissionPower (131)
                                criticality: XXXXXXXXXX
                                value
                                    MaximumTransmissionPower: XXXXXXXXXX
                        Item 7: id-Closed-Loop-Timing-Adjustment-Mode
                            ProtocolIE-Field
                                id: id-Closed-Loop-Timing-Adjustment-Mode (333)
                                criticality: reject (0)
                                value
                                    Closedlooptimingadjustmentmode: XXXXXXXXXX
                        Item 8: id-PrimaryScramblingCode
                            ProtocolIE-Field
                                id: id-PrimaryScramblingCode (181)
                                criticality: reject (0)
                                value
                                    PrimaryScramblingCode: XXXXXXXXXX
```

Valoración y Conclusiones

Cumplimiento de requisitos mínimos:

- *Grabar y Analizar Trazas*. Cumplido.
- *Analizar cualquier interfaz del Backhaul IP.* Cumplido en ingress en Remote Port Mirroring
- *Operación remota.* Cumplido.
- *Estadísticas Básicas.* Cumplido.
- *Coste económico próximo a cero.* Cumplido.
- *Separación de tráfico de telecomunicaciones y tráfico de la red corporativa.* Cumplido.
- *Seguridad.* Cumplido

Cumplimiento de requisitos deseables:

- *Analizar cualquier interfaz*. Probado Port Mirroring (futuro estudio acceso remoto).
- Detalle de *desglose/segmentación de estadísticas:* Cumplido pero mejorable
- *Filtros de tráfico* para que la traza sólo sea del tráfico deseado. Cumplido.
- *Inyección de tráfico.* No considerado, pero posible en futuros trabajos.
- *Sin desplazamientos.* Cumplido para interfaces de Backhaul.
- *Operación remota encriptada.* Cumplido para la administración.

Objetivos adicionales cumplidos:

- *Profundización de conocimientos:* herramientas de monitorización de red, técnicas de captura, puesta en producción de sistemas de virtualización, acceso remoto, administración de máquinas GNU/Linux, análisis de bajo nivel de protocolos UTRAN.
- *Aplicación de una metodología de desarrollo de proyectos* (clásica en cascada) tanto desde el punto de vista teórico, como en el sentido práctico de abordar problemáticas compleja.
- Conocimiento, difusión y uso dentro de la empresa de herramientas de Software Libre.

La valoración global del presente proyecto ha sido de un grado muy satisfactorio, tanto desde el punto de vista práctico de la empresa como del crecimiento personal y académico.

Líneas Futuras de Trabajo

- Seguimiento de implementación del fabricante de Backhaul, de captura “Egress”. Este punto es básico para el éxito futuro del sistema.
- Extensión más allá del Backhaul (instalación de la virtualización en ordenadores de técnicos de campo). Aunque probada y operativa se deberá estudiar:
  - Conexionado local para capturar (switches con Mirroring para personal de campo).
  - Configurar Windows para acceso remoto seguro por conexión de internet móvil.
- Extensión de la plataforma a una máquina de mayores prestaciones (mayor capacidad de proceso, instrucciones de virtualización AMD-V/VT-x, más interfaces de red pinchados).
- Difusión del conocimiento y uso a toda la compañía.
- Si crece estudiar la dinámica de su mantenimiento.
- Ampliación de funcionalidades: sonda activa (p.e. pruebas de medición de ancho de banda end-to-end mediante inyección de tráfico), procesado de estadísticas de capturas mediante base de datos relacionales (p.e. usando C5 Sigma), programado temporal y automático de capturas de forma desatendida (p.e. administrado desde un servidor web),...