Sniffering and Captures in UC

Contenido

Packet Capture in UC 2

Captura en CUCM vía CLI (VMs de UC) 3

Recuperación de Sniffer Capture file en CUCM vía CLI 4

Recuperación de Sniffer Capture file en el CUCM vía RTMT 5

Embedded Packet Capture (IOS Routers) 8

SPAN a un PC Port en Cisco IP Phones 12

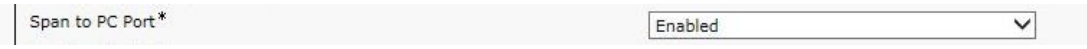
SPAN Simple o Local SPAN (IOS Switches) 13

Packet Capture in UC

A veces es necesario hacer capturas de tráfico tipo Sniffer para ver el comportamiento de un protocolo en específico o el cómo se está comportando el flujo de una aplicación hacia un dispositivo o ver su señalización a detalle.

Existe la posibilidad de hacer capturas de tipo Sniffer en los gateways de voz vía IOS CLI, donde esta característica se llama Embeddeb Packet Capture (**ECP**) así como también es posible hacerlo en los switches al momento de crear una sesión de captura llamada **SPAN** (Switched Port Analizer) .

Para el caso de necesitar una captura de tráfico en los servers de aplicativos como en el CUCM o CUPs que por lo general ya son maquina virtuales es posible ejecutar este tipo de capturas desde la consola de estas VMs vía CLI con el comando **"utils network monitor"**, o en caso de tener acceso al puerto de **"PC Port"** que se ubica detrás de un Cisco IP Phone es posible habilitar la captura al momento de habilitar el parámetro **"Span to PC Port"** en la configuración del CUCM en el menú de "Device > Phones".



Otro punto importante es la del manejo de la herramienta de Sniffer adecuadamente que para este caso usamos lo que es el software de Sniffer WireShark.

Por lo que este documento detalla las siguientes modalidades de capturas de tráfico:

1.- Captura en CUCM vía CLI (VMs de UC)
2.- Embedded Packet Capture (IOS Routers)
3.- SPAN to PC Port in Cisco IP Phones
4.- SPAN Simple o Local SPAN (IOS Switches)

Captura en CUCM vía CLI (VMs de UC)

Los CUCM tienen la capacidad de capturar tráfico de tipo Sniffer, lo cual ayuda a analizar cualquier tipo de protocolo o señalización. La captura se necesita hacer vía CLI desde la consola del CUCM. En caso de querer generar la captura en un CUCM que pertenezca a un Cluster debes de aplicar la captura en el CUCM en el cual este registrado el dispositivo Voip GW, IPPhone o Trunk que genera el tráfico que quieres analizar.

Para generar la captura se hace desde una sesión de CLI en la consola de un servidor de aplicaciones de colaboración, con el comando **"utils network capture"**, pero además se debe de indicar el nombre del archivo con el parámetro **"file <Nombre>"** que guardara la captura, la cantidad y el tamaño de los paquetes a capturar con los parámetros **"count <#> size all"**, lo que varía en los tipos de captura es el tipo de tráfico que quieras que se capture; ya sea aquel que tenga un numero de puerto en específico (**"port <Port_Number>"**) o una IP Address fuente en específico (**"ip <IP_address>"**) o simplemente pueden indicar que se capture todo el tráfico que entre por la interface Ethernet física del servidor con el parámetro **"eth0"**.

Estos son unos ejemplos de cómo se genera una captura desde la consola del CUCM vía CLI. El orden de los parámetros al parecer no es tan importante y puedes cambiar los parámetros que refieren al número de puerto, IP Address o interface en la ejecución de la instrucción de captura **"utils network capture"**:

```
admin: utils network capture eth0 file CUCM_Trace count 100000 size all

    o

admin: utils network capture host ip 10.253.0.54 port 389 size all count 10000 file ldap

    o

admin: utils network capture port 5061 file 851SIPTLS count 1000 size all
```

Aquí capturamos todo el tráfico de LDAP (Pto 389) que se hace desde el CUCM hacia un servidor de AD (10.253.0.54).

Este es un ejemplo de una captura que se aplicó desde un CUCM, para capturar todo el tráfico que entra o sale por la interface Eth0 del servidor CUCM.

```
admin: utils network capture  eth0  file packets   count 1000000 size all

    Warning: existing packets.cap was renamed packets_2.cap
    Executing command with options:
     size=ALL           count=100000       interface=eth0
     src=               dest=              port=
     ip=

Control-C pressed
```

Nota: Para detener la captura hay que presionar las teclas **"Ctrl-C"**.

La salida por default de la captura es enviada a la consola o a la sesión de SSH, pero únicamente envía un log de las conexiones como IPs, FQDNs y puertos de las conexiones generadas en tiempo real, por eso es importante aplicar el parámetro **"file <Nombre>"** para indicarle al CUCM que mande todo el tráfico de tipo captura (tipo Sniffer) a un archivo, al cual se le agrega la extensión **".cap"** automáticamente.

Recuperación de Sniffer Capture file en CUCM vía CLI

Ya que se generaron las capturas en el CUCM hay que bajar los archivos que tienen la extensión **".cap"** al escritorio de tu PC o Lap-top para analizar esta captura con la herramienta Wireshark. Esto se puede hacer utilizando la herramienta del RTMT o también lo puedes bajar vía línea de comandos utilizando un servidor de SFTP que este corriendo en tu PC o Lap-top.

Para bajar el archivo vía CLI lo que tienes que hacer es ejecutar una aplicación de SFTP en tu PC o Lap-top (para volver este dispositivo en un servidor de SFTP) y después vía la sesión abierta de CLI en el CUCM utilizas el comando **"file get activelog platform/cli/<file_name>.cap"** para iniciar la transferencia del archivo capturado.

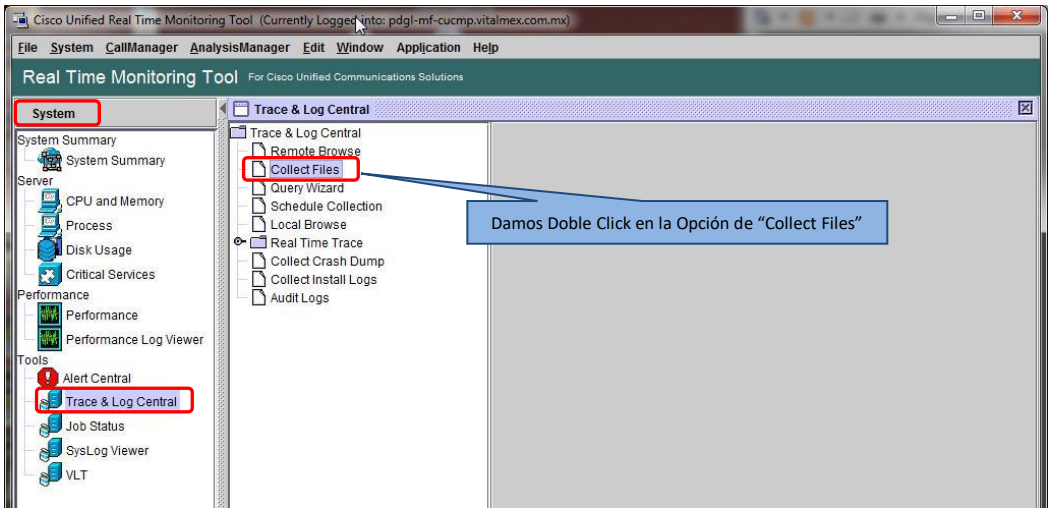
```
admin: file get activelog platform/cli/851SIPTLS.cap
Please wait while the system is gathering files info ...done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 24
Total size in Kbytes: 0.0234375
Would you like to proceed [y/n]? y
SFTP server IP: 172.17.19.8
SFTP server port [22]:
User ID: cisco
Password: *****

Download directory: /

The authenticity of host '172.17.19.8 (172.17.19.8)' can't be established.
RSA key fingerprint is 65:06:99:05:ac:40:19:06:7c:43:2a:e6:9b:73:2a:00.
Are you sure you want to continue connecting (yes/no)? yes
.
Transfer completed.
```

Nota: Para verificar que existe el archivo capturado **".cap"** en el CUCM es con el comando **"file list activelog platform/cli/"** y presionamos lo que es la tecla **"Enter"** para de esta manera poder visualizar que archivos o files existen en el directorio **"platform/cli/"**.

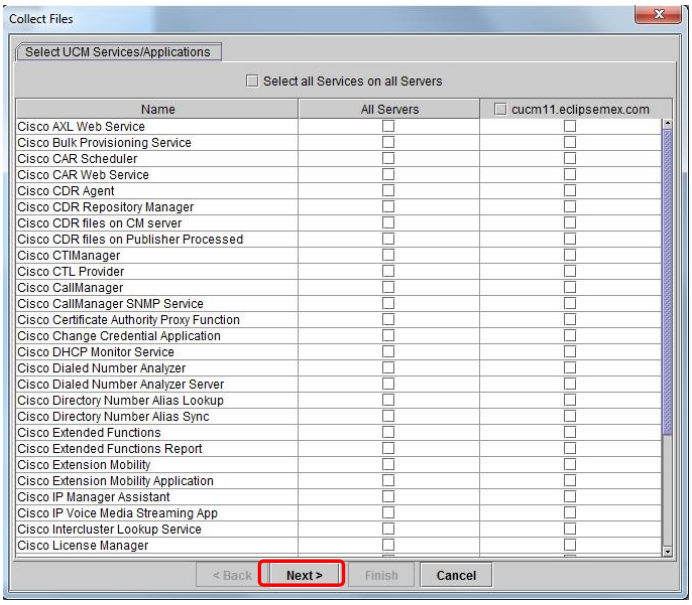
```
admin:file list activelog platform/cli/
  test01.cap                    test02.cap
  851SIPTLS.cap
  dir count = 0, file count = 3
```

Recuperación de Sniffer Capture file en el CUCM vía RTMT

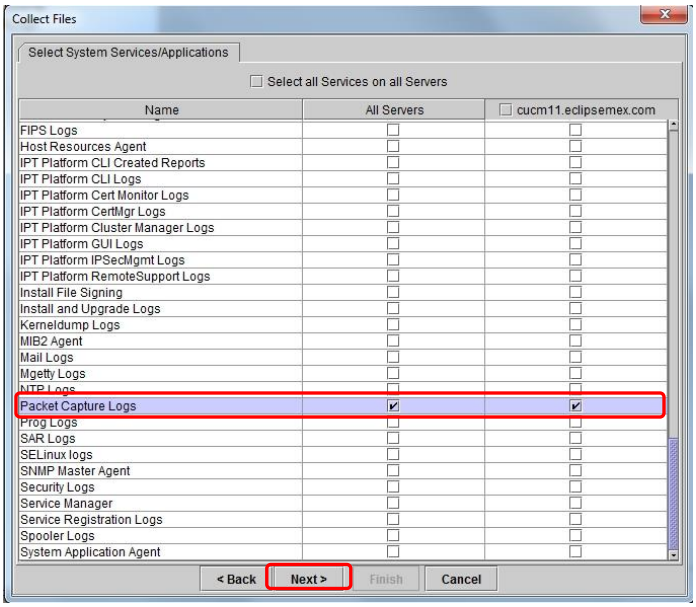
Para bajar el archivo **".cap"** usando la herramienta RTMT, se hace entrando a las siguientes opciones **"System >Trace & Log Central > Collect Files"** y damos doble click sobre la opción de Collect Files. Esto hace que el RTMT abra una nueva ventana, la cual lista los servicios que deseamos seleccionar, así como en que servidor CUCM miembro del Cluster queremos seleccionar.



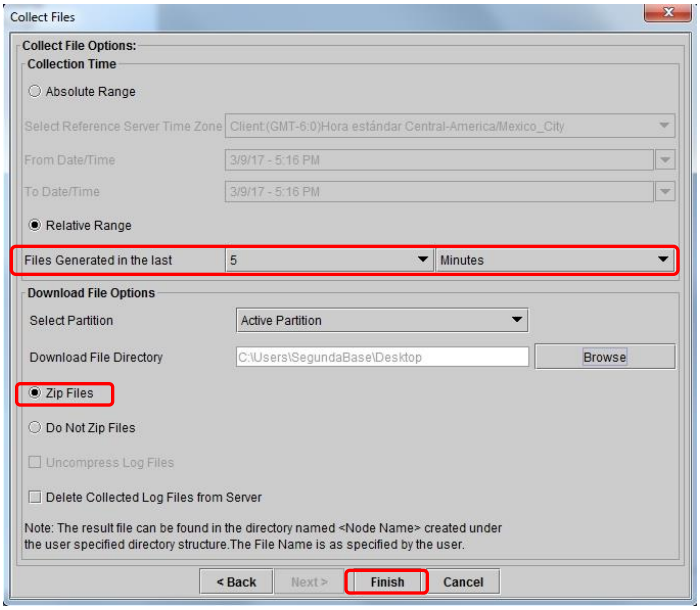
Para bajar el archivo **".cap"** que acabamos de generar con la captura, el servicio que necesitamos seleccionar se llama **"Packet Capture Logs"**. Por default la primera ventana que se muestra no contiene el servicio que estamos buscando (**"Packet Capture Logs"**) por lo que damos click en el botón de **"Next".**



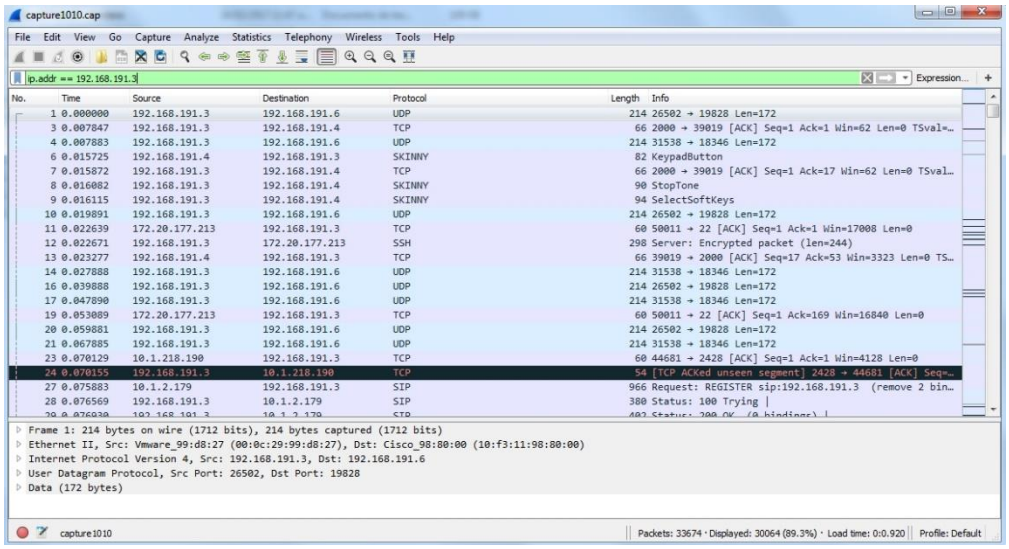
A continuación nos aparece la siguiente ventana. Por comodidad podemos indicar que deseamos acceder a este tipo de servicio en todos los miembros del Cluster y esto lo indicamos cuando le damos click al Check Box que se ubica en la columna de "All Servers" y después damos click en el botón de **"Next"**.



Al mostramos la siguiente ventana el asistente del RTMT, se nos indica en que formato podemos bajar el contenido de los servicios que seleccionamos, en este caso son los archivos de captura. Los formatos son en **".zip"** o NO **".zip"** (no compactados), también es necesario especificar una fecha determinada o un rango de tiempo en la que fueron creados estos archivos.



Ya que bajamos el archivo **".cap"** o el archivo **".zip"** dependiendo del formato que seleccionamos, lo guardamos sobre escritorio de nuestra PC o Lap-top, después lo abrimos con la herramienta de Wireshark.


capture1010.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.191.3
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.191.3 192.168.191.6 UDP 214 26502 → 19828 Len=172
3 0.007847 192.168.191.3 192.168.191.4 TCP 66 2000 → 39019 [ACK] Seq=1 Ack=1 Win=62 Len=0 TSval=…
4 0.007883 192.168.191.3 192.168.191.6 UDP 214 31538 → 18346 Len=172
6 0.015725 192.168.191.4 192.168.191.3 SKINNY 82 KeypadButton
7 0.015872 192.168.191.3 192.168.191.4 TCP 66 2000 → 39019 [ACK] Seq=1 Ack=17 Win=62 Len=0 TSval…
8 0.016082 192.168.191.3 192.168.191.4 SKINNY 90 StopTone
9 0.016115 192.168.191.3 192.168.191.4 SKINNY 94 SelectSoftKeys
10 0.019891 192.168.191.3 192.168.191.6 UDP 214 26502 → 19828 Len=172
11 0.022639 172.20.177.213 192.168.191.3 TCP 60 50011 → 22 [ACK] Seq=1 Ack=1 Win=17008 Len=0
12 0.022671 192.168.191.3 172.20.177.213 SSH 298 Server: Encrypted packet (len=244)
13 0.023277 192.168.191.4 192.168.191.3 TCP 66 39019 → 2000 [ACK] Seq=17 Ack=53 Win=3323 Len=0 TS…
14 0.027888 192.168.191.3 192.168.191.6 UDP 214 31538 → 18346 Len=172
16 0.039888 192.168.191.3 192.168.191.6 UDP 214 26502 → 19828 Len=172
17 0.047890 192.168.191.3 192.168.191.6 UDP 214 31538 → 18346 Len=172
19 0.053089 172.20.177.213 192.168.191.3 TCP 60 50011 → 22 [ACK] Seq=1 Ack=169 Win=16840 Len=0
20 0.059881 192.168.191.3 192.168.191.6 UDP 214 26502 → 19828 Len=172
21 0.067885 192.168.191.3 192.168.191.6 UDP 214 31538 → 18346 Len=172
23 0.070129 10.1.218.190 192.168.191.3 TCP 60 44681 → 2428 [ACK] Seq=1 Ack=1 Win=4128 Len=0
24 0.070155 192.168.191.3 10.1.218.190 TCP 54 [TCP ACKed unseen segment] 2428 → 44681 [ACK] Seq=…
27 0.075883 10.1.2.179 192.168.191.3 SIP 966 Request: REGISTER sip:192.168.191.3 (remove 2 bin…
28 0.076569 192.168.191.3 10.1.2.179 SIP 380 Status: 100 Trying |
Frame 1: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
Ethernet II, Src: Vmware_99:d8:27 (00:0c:29:99:d8:27), Dst: Cisco_98:80:00 (10:f3:11:98:80:00)
Internet Protocol Version 4, Src: 192.168.191.3, Dst: 192.168.191.6
User Datagram Protocol, Src Port: 26502, Dst Port: 19828
Data (172 bytes)
capture1010
Packets: 33674 · Displayed: 30064 (89.3%) · Load time: 0:0.920
Profile: Default

Embedded Packet Capture (IOS Routers)

EPC (Embedded Packet Capture) es una característica que te permite hacer capturas tipo Sniffers sobre un Cisco Router series 890, 1900, 2900. 3900, 7200. Esta funcionalidad fue incluida a partir de la versión de IOS 12.4 (20T).

Lo que hace esta caracteristica, es capturar el tráfico dirigido a la IP Address de una interface especificada en la configuración de la sesión de EPC, la cual se le llama **"Capture Point"**. La captura la guarda en un área de memoria **"Buffer"** creada de manera temporal en la DRAM del Cisco Router. Posteriormente se tiene que iniciar la sesión de captura y detenerla, para después bajar el archivo con el trafico ya capturado a una PC y analizarlo con la una herramienta tipo Sniffer.

Nota: Esta funcionalidad no está habilitada en todas las versiones de IOS posteriores, ya que fue eliminada o restringida por que bloquea los equipos y los hace inestables.

Para configurar este servicio de captura se hace en cuatro pasos básicamente:

1.- Creación del **"Buffer"** de la captura: Definir el nombre, tamaño y tipo de operación del **"Buffer"**, así como el tamaño máximo de los packets que se aceptaran en la captura.
2.- Creación del **"Capture Point"** : Definir el nombre, tipo, número de interface del **"Capture Point"** y el tipo de tráfico a capturar (in, out o both).
3.- Generar la asociación entre el **"Capture Point"** y el **"Buffer"**.
4.- Iniciar la captura y detener la captura.

Antes de configurar una captura de tipo Sniffer en un Cisco Router debemos verificar si existen **"Buffers"** y **"Capture Points"** configurados previamente y esto se hace con los comandos **"show monitor capture buffer all parameters"** y **"show monitor capture point all"** respectivamente.

```
C2911-HQ-Lab#show monitor capture buffer all parameters

  Capture buffer cap-01 (linear buffer)
  Buffer Size : 1048576 bytes, Max Element Size : 5000 bytes, Packets : 3
  Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
  Associated Capture Points:
  Name : CP, Status : Inactive

  Configuration:
  monitor capture buffer cap-01 max-size 5000 linear
  monitor capture point associate CP cap-01
```

La salida de este comando nos indica que existe un **"Buffer"** llamado **"cap-01"**.

```
C2911-HQ-Lab#show monitor capture point all

  Status Information for Capture Point POINT
  IPv4 Process
  Switch Path: IPv4 Process       , Capture Buffer: None
  Status : Inactive

 Configuration:
 monitor capture point ip process-switched POINT both
```

El caso del Capture Point el tipo de tráfico puede ser dos opciones **"process-switched"** o **"CEF"**.

En el caso de existir **"Buffers"** y **"Capture Points"** configurados previamente se borran con los comandos : **"no monitor capture buffer <Cap_Point_Name>"** y **"no monitor capture point ip <Tipo_Trafico> <Cap_Point_Name>"** respectivamente.

```
C2911-HQ-Lab#no monitor capture buffer cap-01

  Capture Buffer deleted

C2911-HQ-Lab#no monitor capture point ip process-switched POINT
```

1. Creación del **"Buffer"** de la captura.

En la creación del **"Buffer"** para captura tenemos diversas opciones que pueden ser seleccionadas cuando se define; por ejemplo el tamaño del buffer (en Kbytes), el tamaño máximo del paquete a capturar (en bytes), forma de operar ya sea Circular o Lineal. Para la creación del **"Buffer"** usamos el comando **"monitor captura buffer <Buffer_Name> <size> <Circular|linear>"**.

```
C2911-HQ-Lab# monitor capture buffer MYBUFFER size 90000 max-size 2000 linear
```

Con este comando estas definiendo el tamaño del buffer de 9000 Kbytes y tamaño máximo de los paquetes a capturar es 2000 Bytes y el buffer es va operar de tipo lineal.

Nota: El tamaño por default del **"buffer"** de captura es de 1024 k y del paquete es de 68 bytes.

2. Creación del **"Capture Point"**.

El **"Capture Point"** define la ubicación en donde ocurre la captura. Se puede definir si el **"Capture Point"** ocurre en una interface con una dirección IPv4 o el IPv6 o se puede llegar a definir una ACL para especificar exactamente que trafico capturar. El comando que se utiliza es **"monitor captura point <ip|ipv6> <cef|process-switched> <Capture_Point_Name> <Interface_Type> <X/Y> <in|out|both>"**.

```
C2911-HQ-Lab# monitor capture point ip cef POINT gigabitEthernet 0/1 both
```

3. Generar la asociación entre el **"Capture Point"** y el **"Buffer"**.

Ya que se crearon tanto el **"Capture Point"** y el **"Buffer"** se tienen que asociar ambas entidades con el comando **"monitor captura point associate <Capture_Point_Name> <Buffer_Name>"**.

```
C2911-HQ-Lab# monitor capture point associate POINT MYBUFFER
```

Si en este punto de la configuración de la sesión de EPC llegamos a monitorear el **"Capture Point"** y el **"Buffer"** debemos de ver que están asociados pero inactivos. Esto se hace con los comandos **"show monitor capture buffer all parameters"** y **"show monitor capture point all"**.

```
C2911-HQ-Lab#show monitor capture point POINT

Status Information for Capture Point POINT
IPv4 CEF
Switch Path: IPv4 CEF , Capture Buffer: MYBUFFER
Status : Inactive

Configuration:
monitor capture point ip cef POINT GigabitEthernet0/1 both

C2911-HQ-Lab#show monitor capture buffer all parameters

Capture buffer MYBUFFER (linear buffer)
Buffer Size : 9216000 bytes, Max Element Size : 2000 bytes, Packets : 0
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Name : POINT, Status : Inactive

Configuration:
monitor capture buffer MYBUFFER size 9000 max-size 2000 linear
monitor capture point associate POINT MYBUFFER
```

Nota: Un **"Buffer"** puede estar asociado a varios **"Capture Point"**, pero un **"Capture Point"** solo puede tener un **"Buffer"**.

4. Iniciar la captura y detener la captura.

Después necesitamos iniciar el proceso de la captura

```
C2911-HQ-Lab# monitor capture point start POINT
```

Después monitoreamos que tanto el "Capture Point" y el "Buffer".

```
C2911-HQ-Lab# show monitor capture point POINT

Status Information for Capture Point POINT
IPv4 CEF
Switch Path: IPv4 CEF          , Capture Buffer: MYBUFFER
Status : Active

Configuration:
monitor capture point ip cef POINT GigabitEthernet0/1 both

C2911-HQ-Lab#show monitor capture buffer all parameters

Capture buffer MYBUFFER (linear buffer)
Buffer Size : 9216000 bytes, Max Element Size : 2000 bytes, Packets : 0
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Name : POINT, Status : Active

Configuration:
monitor capture buffer MYBUFFER size 9000 max-size 2000 linear
monitor capture point associate POINT MYBUFFER
```

Generamos tráfico a capturar hacia la IP de la interface para este ejemplo mediante un ping, y monitoreamos que la cantidad de packets se incremente con el comando "show monitor captura buffer all parameters".

```
C2911-HQ-Lab#show monitor capture buffer all parameters

Capture buffer MYBUFFER (linear buffer)
Buffer Size : 9216000 bytes, Max Element Size : 2000 bytes, Packets : 47
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Name : POINT, Status : Active

Configuration:
monitor capture buffer MYBUFFER size 9000 max-size 2000 linear
monitor capture point associate POINT MYBUFFER
```

Para detener la captura es con el comando "monitor captura point stop <Capture_Point>".

```
C2911-HQ-Lab#monitor capture point stop POINT
```

Se puede examinar la captura del tráfico desde el mismo IOS del equipo con el comando "show monitor capture buffer <Buffer_Name> dump", solo que la salida muestra la información en hexadecimal.

```
C2911-HQ-Lab#show monitor capture buffer MYBUFFER dump

19:38:44.250 GMT Dec 28 2017 : IPv4 LES CEF    : Gi0/0.2 Gi0/1

3DB4BC20: 28940FA3 E4C0E8B7 48882719 08004500  (..#d@h7H.'...E.
3DB4BC30: 00E5192B 00007F11 0C670A0A 00640A0A  .e.+.....g...d..
3DB4BC40: 00FF008A 008A00D1 195A1102 83D90A0A  .......Q.Z...Y..
3DB4BC50: 0064008A 00BB0000 20464845 4A454F43  .d...;.. FHEJEOC
3DB4BC60: 4E444944 48454B45 4A455045 46464544  NDIDHEKEJEPEFFED
3DB4BC70: 48444446 43464743 41002045 46454445  HDDFCFGCA. EFEDE
```

```
3DB4BC80: 4D454A46 41464445 46454E45 46464943  MEJFAFDEFENEFFIC
3DB4BC90: 41434143 41434143 41424E00 FF534D42  ACACACACABN..SMB
3DB4BCA0: 25000000 00000000 00000000 00000000  %...............
3DB4BCB0: 00000000 00000000 00000000 11000021  ...............!
3DB4BCC0: 00000000 00000000 00E80300 00000000  .........h......
3DB4BCD0: 00000021 00560003 00010000 00020032  ...!.V.........2
3DB4BCE0: 005C4D41 494C534C 4F545C42 524F5753  .\MAILSLOT\BROWS
3DB4BCF0: 45000100 80FC0A00 57494E2D 38374A49  E....|..WIN-87JI
3DB4BD00: 4F455437 33525600 06012B10 80000F01  OET73RV...+.....
3DB4BD10: 55AA0000                             U*..

19:40:44.730 GMT Dec 28 2017 : IPv4 LES CEF    : Gi0/0.3 Gi0/1

3DB4BC20: 28940FA3 E4C0E8B7 48882719 08004500  (..#d@h7H.'...E.
3DB4BC30: 00520045 00007F11 5D5F0A0A 0364D054  .R.E....]_...dPT
```

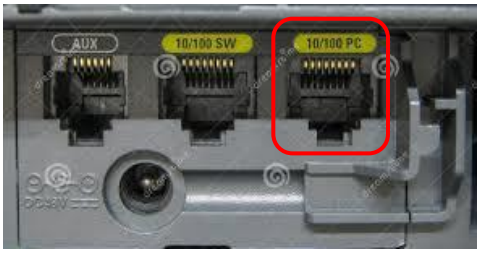
Para exportar la información almacenada en el **"Buffer"** del router para analizarla por medio de un Sniffer en una PC, es hace via TFTP con el comando **"monitor capture buffer <Buffer_Name" export tftp://<IP_TFTP>/<Nombre_Archivo.cap>"**. A veces el método anterior no es posible o el acceso vía TFTP al dispositivos IOS NO es opción, se puede tomar una copia del vaciado hexadecimal y utilizar cualquier convertidor en línea del hex.-pcap para ver los archivos.

```
C2911-HQ-Lab#monitor capture buffer MYBUFFER export tftp://10.10.99.15/POINT.cap

!!!!!
```

Nota: Una vez que se han obtenido las capturas hay que borrar el **"Buffer"** y **"Capture Point".**

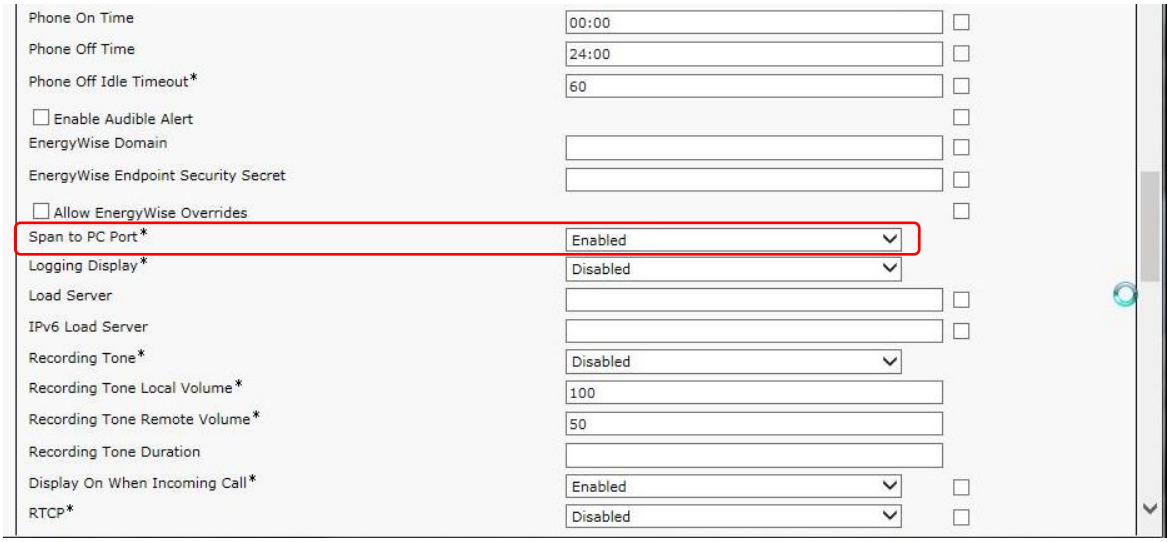
SPAN a un PC Port en Cisco IP Phones

Una manera de poder capturar el tráfico que genera un Cisco IP Phone hacia el puerto del Switch, es conectando una PC en el puerto marcado como "10/100 PC" que se ubica detrás del Cisco IP Phone con la finalidad de capturar trafico espejo generado por el micro-switch del Cisco IP Phone hacia ese puerto. Esta característica se llama **"Span to PC Port"**.



Una vez que tengamos conectado una PC en dicho puerto, procedemos a realizar una configuración dentro del CUCM a nivel de Device, para especificarle al Micro-Switch del Cisco IP Phone que todo tráfico que genere envié tráfico espejo hacia el puerto "10/100PC".

El servicio de **"Span to PC Port"** se configura entrando a "Cisco Unified CM Administration > Device > Phone > <IP Phone>" dentro de la configuración general del Cisco IP Phone buscamos el campo **"Span to PC Port"** y del lado derecho seleccionamos el valor de **"Enable"**.



Una vez que tenemos habilitado la característica de **"Span to PC Port"**. Se conecta en el puerto del IP Phone "10/100 PC" la PC que va capturar el tráfico.

Es importante tener el Sniffer (WireShark) corriendo en la PC que conectamos en el puerto del Cisco IP Phone **"10/100 PC"** para que capture el tráfico espejo que se genera por parte del Micro-Switch.

En el WireSharck lo que se tiene que configurar son las opciones de "Capture > Option > Local Conection > Start ".

SPAN Simple o Local SPAN (IOS Switches)

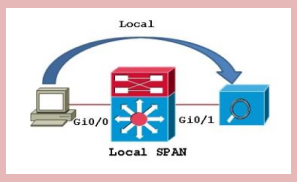
Es posible capturar el tráfico de red que pasa a través de un puerto o grupo de puertos de un Switch o incluso una de sus SVI mediante la creación de una sesión SPAN (Switched Port Analizer).

Lo que hace este feature de SPAN es generar una copia del tráfico de los puertos definidos como puertos origen que puede ser una interfaz o un grupo de interfaces desde las cuales se originara el tráfico ya sea de entrada, salida o ambos que se van a capturar, esta copia de tráfico se envía a un puerto del Switch definido como puerto destino. En este puerto destino se debe de conectar un analizador de tráfico de red o Sniffer.

Existen tres diferentes tipos de modalidades de captura de tráfico en un Switch. Estas modalidades son:

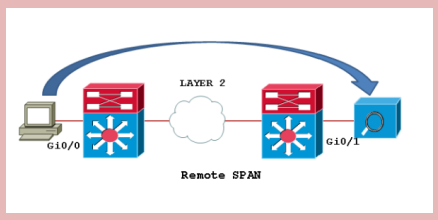
Switched Port Analizer (SPAN)
Remote Switched Port Analizer (RSPAN)
Encapsulated Remote Switched Port Analizer (ERSPAN)

Switched Port Analizer (SPAN) – Es la versión básica de **SPAN** y se ejecuta solo a nivel de caja dentro del mismo Switch, esta sesión también es conocida como **Local SPAN**. En este tipo de sesión los puertos de origen y destino se encuentran físicamente en la misma caja o Switch.



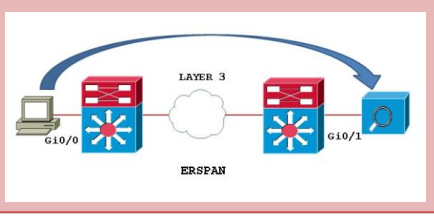
Cuando el origen es una SVI (VLAN) en una sesión de **SPAN** a esta modalidad se le determina **VSPAN**.

Remote Switched Port Analizer (RSPAN) – Esta modalidad tiene la ventaja que se pueden generar capturas de trafico de puertos origen distribuidos entre diferentes cajas o Switches. Este tráfico origen es trasportados a través de una VLAN dedicada llevar este tráfico espejo de la sesión de **RSPAN** al puerto destino que puede estar en un punto central de la red LAN u en otro Switch.



En la configuración **RSPAN** es importante verificar que el dominio de VTP no esté podado (pruning) y que el filtrado de los UP links o TRUNKs hacia el Switsh donde se ubica el puerto destino se permite la VLAN de **RSPAN**.

Emcapsulated Remote Switched Port Analizer (ERSPAN) – Esta modalidad lo que hace es encapsular el trafico en un túnel de GRE y transportar el trafico espejo a través de un enlace de capa 3.



Nota: La sesión de **SPAN** no afecta a la operación o funcionamiento en los puertos de origen o interfaz SVI. Pero en el caso del puerto destino, su uso es únicamente para recibir el tráfico espejo generado de la captura de los puertos origen de la sesión de **SPAN**.

Para la configuración de una sesión de **SPAN** en un switch cisco se hace en dos partes:

1.- Primero se debe definir el origen de tráfico a capturar; esto puede ser un puerto, grupo de puertos o una SVI y además definir el tipo tráfico a capturar, esto es de entrada, salida o ambos.
2.- Definir el puerto destino a donde se enviará el tráfico espejo capturado desde el origen.

Antes de configurar una sesión de **SPAN** es importante verificar si existe una sesión de **SPAN** en el Switch, para no generar algún conflicto. Para verificar si existen sesiones activas de **SPAN** en el Switch se hace aplicando el comando **"show monitor"** o de lo contrario si lo que se quiere es borrarla esto es con el comando **"no monitor session <# session>"** a nivel de configuración de terminal.

```
Switch# show  monitor
   No SPAN configuration is present in the system.
```

O

```
Switch(config)# no monitor session 1
```

Para la configuración de o de los puertos origen se hace con el comando **"monitor session <#Session> source interface <interface type> <Num Interfaz> <in/out/both> "**.

```
Switch#configure terminal
Switch(config)#monitor session 1 source interface fastethernet 0/4 - 5 both
```

En este ejemplo lo que se creó fue una sesión de **SPAN** con el número de identificación "1" y se está definiendo dos puertos origen que son las interfaces de tipo fastethernet "0/4" a la "0/5", el tráfico que se va a capturar es tanto el de entrada como el de salida ya que se aplicó el parámetro **"both"**.

Para la configuración el destino o más bien el puerto destino se hace con el comando **"monitor session <#Session> destination interface <interface type> <#Interfaz> <in/out/both> "**.

```
Switch#configure terminal
Switch(config)#monitor session 1 destination interface fastethernet 0/6
```

Aquí se definió el puerto destino o el puerto a donde se enviará el tráfico espejo capturado de la sesión de **SPAN** 1 al puerto fastehernet 0/6.

Por default una sesión de **SPAN** envía hacia el puerto destino únicamente el tráfico untagged, incluso la sesión de **SPAN** NO envía tráfico de **BPDUs**, **CDP**, **VTP**, **DTP**, **PAgP**, **802.1q**, **ISL**. En caso de querer capturar tráfico de origen de un puerto que este etiquetando con 802.1q los frames (puerto en modo Trunk), es necesario aplicar los parámetros **"encapsulated replicate"** en la configuración del puerto destino de la sesión de **SPAN**.

```
Switch#configure terminal
Switch(config)#monitor session 1 destination interface fastethernet 0/5 encapsulated replicated
```

En caso de querer el trafico de una VLAN en específico cuando se está definiendo un puerto de tipo Trunk como origen para la sesión de **SPAN** se puede aplicar el parámetro **"filter vlan <#Vlan>"**.

```
Switch#configure terminal
Switch(config)#monitor session 1 filter vlan 1 - 5, 9
```

Filtra la captura de tráfico para desde la Vlan 1 a la Vlan 5 e incluyendo a la Vlan 9.

Se puede revisar el estado de la sesión de SPAN con los comandos "show monitor session <#sesion>" o "show monitor detail" o revisar la configuración con "show running-config | include monitor".El siguiente ejemplo tenemos configurada la siguiente sesión:

```
Switch#show running-config | include monitor
monitor session 1 source interface Fa0/4 – 5
monitor session 1 destination interface Fa0/6 encapsulation replicate

Switch#show monitor session 1
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Fa0/4-5
Destination Ports      : Fa0/6
    Encapsulation      : Replicate
        Ingress        : Disabled

Switch#show monitor detail
Session 1
-------------------------
Type                   : Local Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : Fa0/4-5
Source VLANs           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : None
Destination Ports      : Fa0/6
    Encapsulation      : Replicate
        Ingress        : Disabled
Filter VLANs           : None
Dest RSPAN VLAN        : None
```