How to validate proper SPAN configuration

created by: Rainer Bemsel – **Version** 1.1 – **Dated**: Feb/19/2012

The purpose of this document is to provide you with a best practice guideline to validate a proper SPAN port configuration and the health of that port. I've used it as a cheat sheet in many proof-of-concept scenarios with PacketShaper, NetQoS SuperAgent & Network Instruments GigaStor. Especially when asymmetric traffic exists in your network, this would cause faulty results or even no results.

There are a few Cisco commands; you can use to verify the health of a SPAN port. First you need to know, which port is being used for spanning and what ports are being spanned.

Search for the Span Port Interface

```
csco-2950-1#show monitor session all
Session 1
---------
Type               : Local Session
Source Ports       :
    Both           : Fa0/1
Destination Ports  : Fa0/24
    Encapsulation  : Native
          Ingress: Disabled
csco-2950-1#
```

Verify Span Port Speed and Connection

```
csco-2950-1#show interface fast 0/24 status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/24    MONITOR            monitoring   1          a-full  a-100 10/100BaseTX
csco-2950-1#
```

Search for Errors on SPAN Port Interface

```
csco-2950-1#sho int fa0/24
FastEthernet0/24 is up, line protocol is down (monitoring)
  Hardware is Fast Ethernet, address is 0019.2ffb.6d98 (bia 0019.2ffb.6d98)
  Description: MONITOR
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 100BaseTX
  input flow-control is unsupported output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:37:53, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1000 bits/sec, 2 packets/sec
```

```
5 minute output rate 36000 bits/sec, 15 packets/sec
      2334 packets input, 380136 bytes, 0 no buffer
      Received 2240 broadcasts (0 multicast)
      0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 567 multicast, 0 pause input
      0 input packets with dribble condition detected
86773 packets output, 42350594 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
csco-2950-1#
```

FastEthernet0/15 is up	Tells the status of the hardware interface. Administratively Down would mean it has been disabled in the configuration with “shutdown”
line protocol is up	Status of the line protocol.
MTU	Maximum Transmission Unit. By default, this is 1500 bytes, which describes the largest packet that can be sent through the interface before the packet is fragmented.
BW 100000 Kbit, DLY 100 usec	Bandwidth (BW) simply a descriptive value. Does not have an effect on the bandwidth Delay (DLY) is the amount of micro seconds of delay.
reliability 255/255, txload 1/255, rxload 1/255	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over five minutes (default). Load Average. Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over five minutes (default).
Encapsulation ARPA	Encapsulation is the type of Data-Link encapsulation. ARPA is Cisco‘s term for Ethernet Version II (aka DIX).
Last input, output	Number of hours, minutes, and seconds since the last packet was successfully received or transmitted by an interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process switched, not when packets are fast switched.
Output queue, input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped due to a full queue.
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
2334 packets input, 380136 bytes	Total number of error-free packets received by the system.
Received 2240 broadcasts	Total number of broadcast or multicast packets received by the interface
Runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Number of packets that are discarded because they exceed the medium's maximum packet size. For example, any Ethernet packet that is greater than 1,518 bytes is considered a giant.
Throttles	This counter indicates the number of times (0) the input buffers of an interface have been cleaned because they have not been serviced fast enough or they are overwhelmed. Typically, an explorer storm can cause the throttles counter to increment. It's important to note that every time you have a throttle; all the packets in the input queue get dropped. This causes very slow performance and may also disrupt existing sessions.

Input Errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
Frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
Overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
Ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
Dribble Condition	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
86773 packets output, 42350594 bytes	Total number of messages transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.
Output Errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
Collisions	Number of messages transmitted due to an Ethernet collision. A packet that collides is counted only once in output packets.
Interface Resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down or cable was loose.
Late Collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble. The most common cause of late collisions is that your Ethernet cable segments are too long for the speed at which you are transmitting.
Deferred	Deferred indicates that the chip had to defer while ready to transmit a frame because the carrier was asserted.

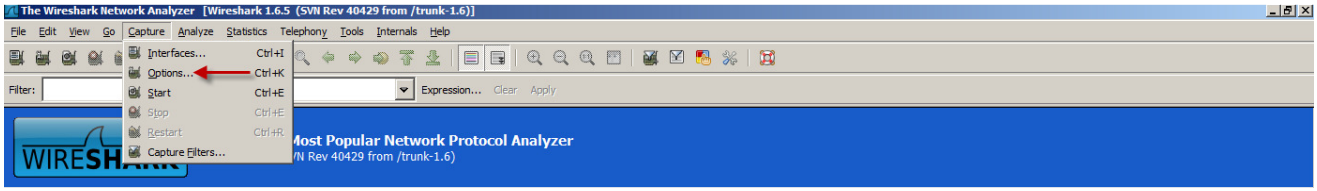
A great reference can be found:
http://www.cisco.com/en/US/docs/switches/lan/catalyst2940/software/release/12.1_19_ea1/configuration/guide/swspan.html

SPAN Port seems to be fine and no drops or other errors had been shown, Next would be to verify, if data of interest is being seen. Most engineers have WireShark or another Packet Capture possibility in their tool-box. Let's assume you want to capture and analyze data from a specific host.

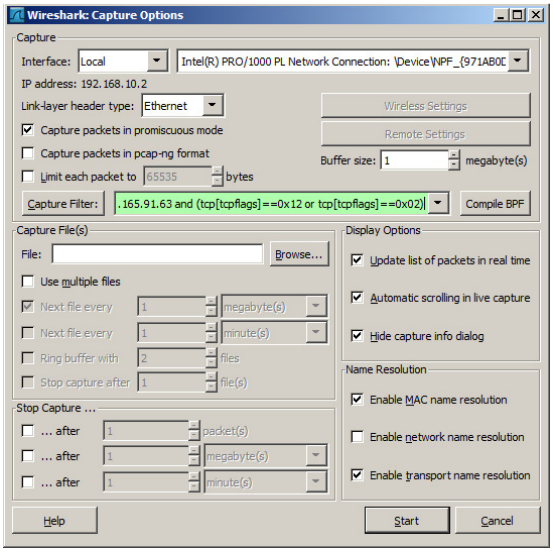
Is the host of interest being spanned?

I've attached a WireShark laptop on the SPAN port and filtering on the Webserver (82.165.91.63) and I'm only interested in SYN and SYN-ACK packets. That would confirm, for seeing the complete session and no asymmetric routing is in place (at least not for that communication)

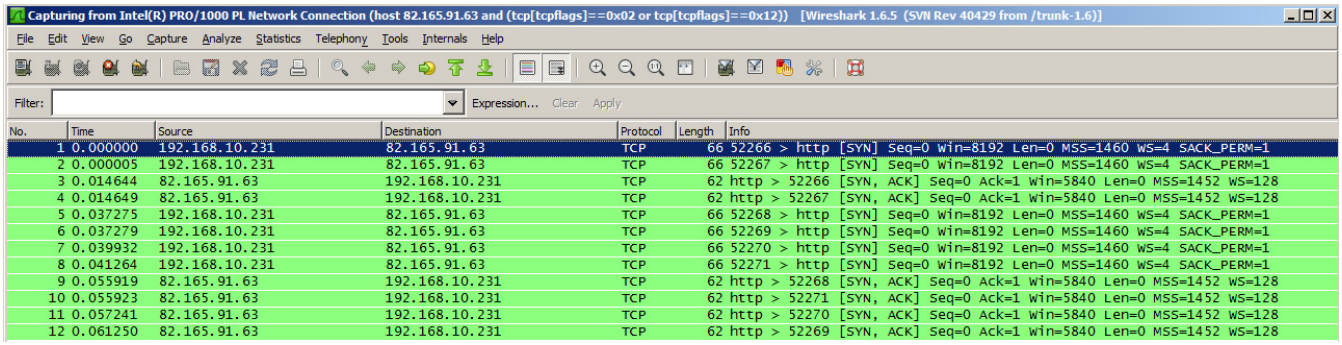
To use the same setup, make sure packet capture is stopped. Next, click on Capture and Options.



Capture Filter: host 82.165.91.63 and (tcp[tcpflags]==0x02 or tcp[tcpflags]==0x12)



host 82.165.91.63 -> Source or Destination
tcp[tcpflags]==0x02 -> SYN Packet
tcp[tcpflags]==0x12 -> SYN ACK Packet

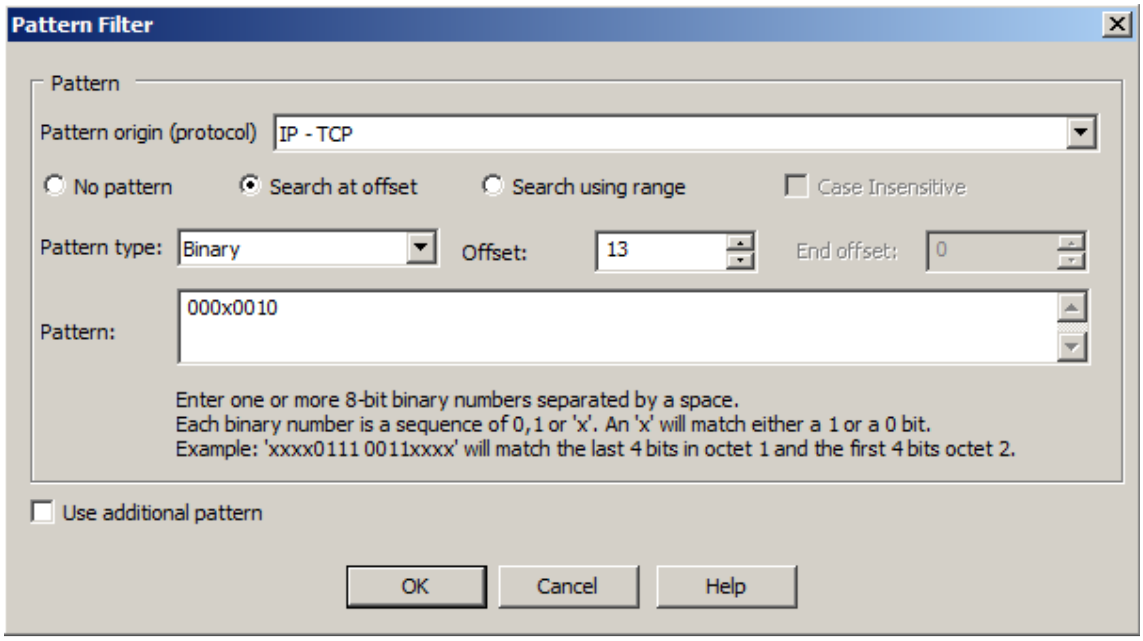


My favorite Wireshark Capture Filter:

Note: WireShark parameters are case sensitive. **H**ost would not work, **h**ost is required

host 192.168.10.231 and host 82.165.91.63
host 82.165.91.63 and (tcp[tcpflags]==0x02 or tcp[tcpflags]==0x12)

My favorite Network Instrument Observer Capture Filter:



How to setup this Observer Capture Filter, check out:
http://www.bemsel.com/TechTip/techiestuff/RBE-NI-SYN-FILTER.pdf