Wireshark & SPAN lab

Tom Cordemans

Wireshark & SPAN lab

Tom Cordemans

VIVES University College (Cisco Networking Academy)

tom.cordemans@vives.be

Odisee University College (Cisco Networking Academy)

tom.cordemans@odisee.be

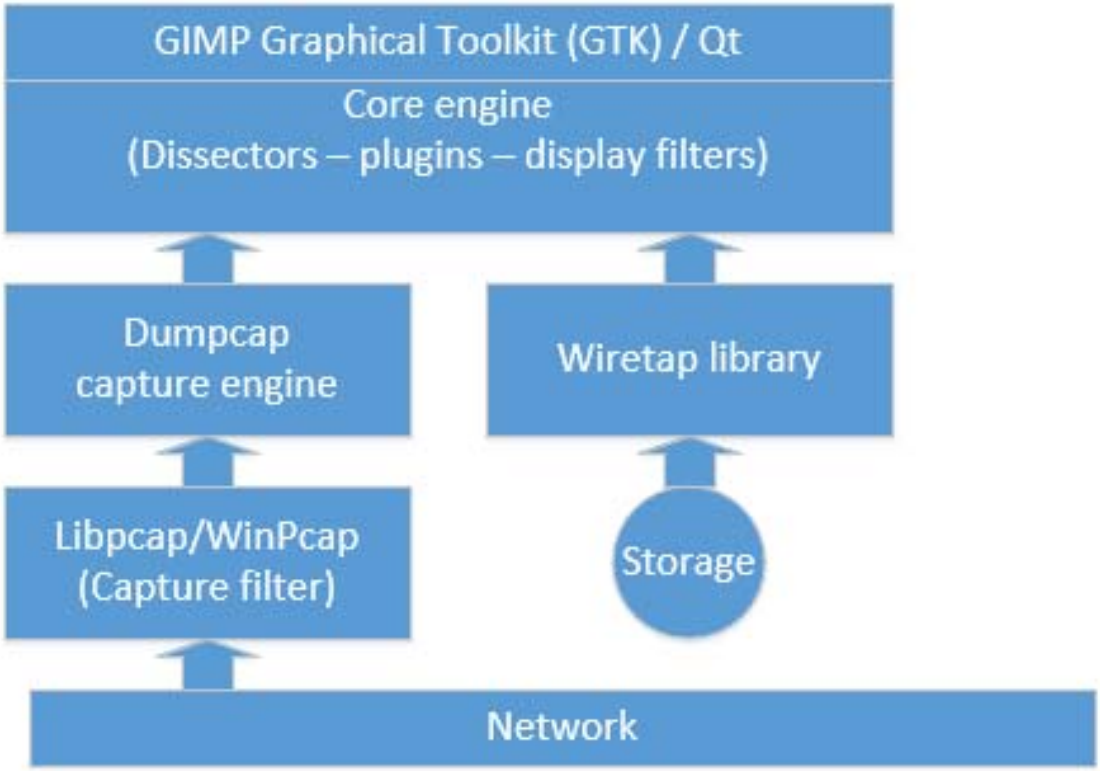
Wireshark & SPAN lab

- Introduction to Wireshark
- SPAN overview

Introduction to Wireshark

What is Wireshark?

Wireshark is a free and open source **packet sniffer** and **protocol analyzer**.



Introduction to Wireshark

What is Wireshark?

Wireshark is like an X-ray machine. It gives you a look at what's going on inside (the network), but you need to develop the skills to interpret what you see and know what to look for.

Anders Broman, Wireshark Core Developer and System Tester, Ericsson

Introduction to Wireshark

Wireshark dissectors

Each dissector decodes its part of the protocol, and then hands off decoding to subsequent dissectors for an encapsulated protocol.

```
> Frame 9: 493 bytes on wire (3944 bits), 493 bytes captured (3944 bits) on interface 0
> Ethernet II, Src: Dell_45:5b:92 (f8:ca:b8:45:5b:92), Dst: Sagemcom_8f:54:49 (00:1b:bf:8f:54:49)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 62.4.254.199
> Transmission Control Protocol, Src Port: 50193, Dst Port: 80, Seq: 1, Ack: 1, Len: 439
> Hypertext Transfer Protocol
```

Introduction to Wireshark

Important settings!

- Disable IP, UDP en TCP checksum validations
- Enable TCP Calculate conversation
- Enable TCP track number of bytes in flight
- Disable TCP Allow subdissector to reassemble stream

Introduction to Wireshark

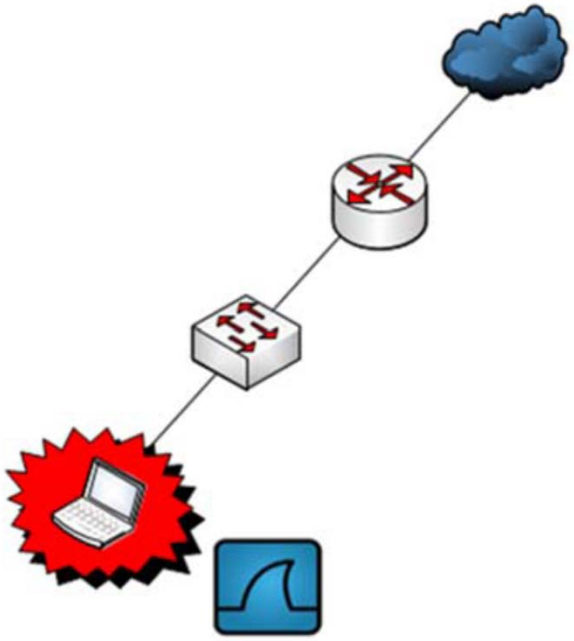
Where to capture?

Always as close as possible to the problem or the complainer.

Introduction to Wireshark

How to capture?

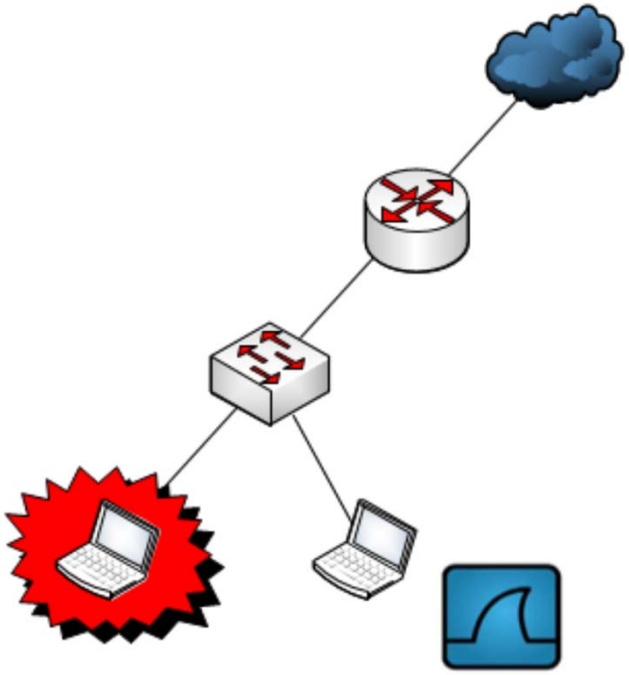
<u>Method 1:</u>



Introduction to Wireshark

How to capture?

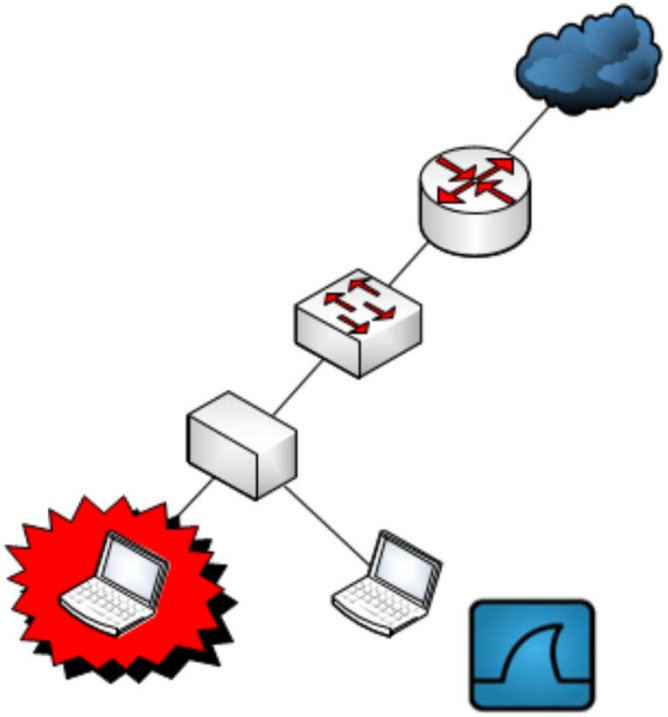
<u>Method 2:</u>



Introduction to Wireshark

How to capture?

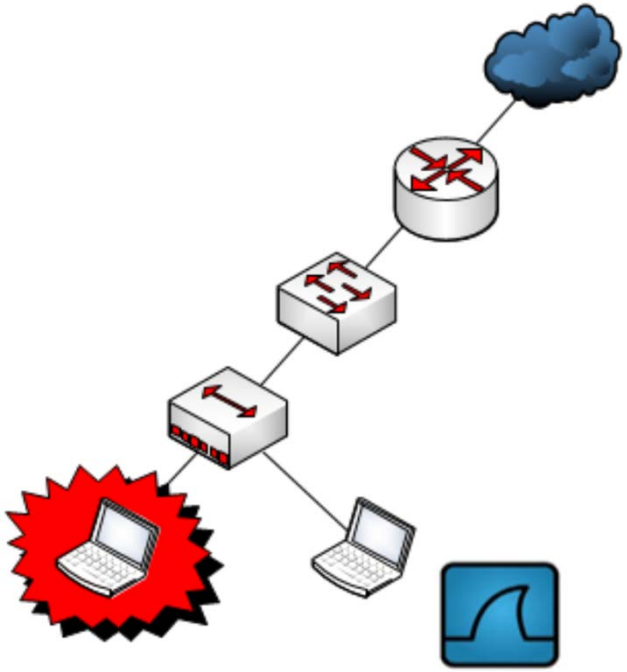
<u>Method 3:</u>



Introduction to Wireshark

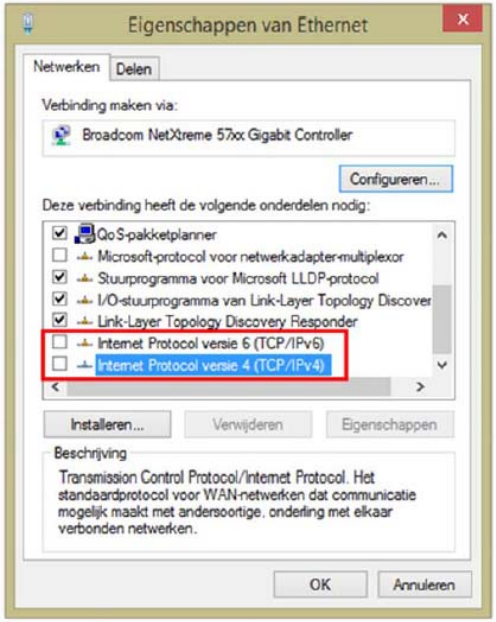
How to capture?

<u>Method 4:</u>



Introduction to Wireshark

How to capture without being found?



Introduction to Wireshark

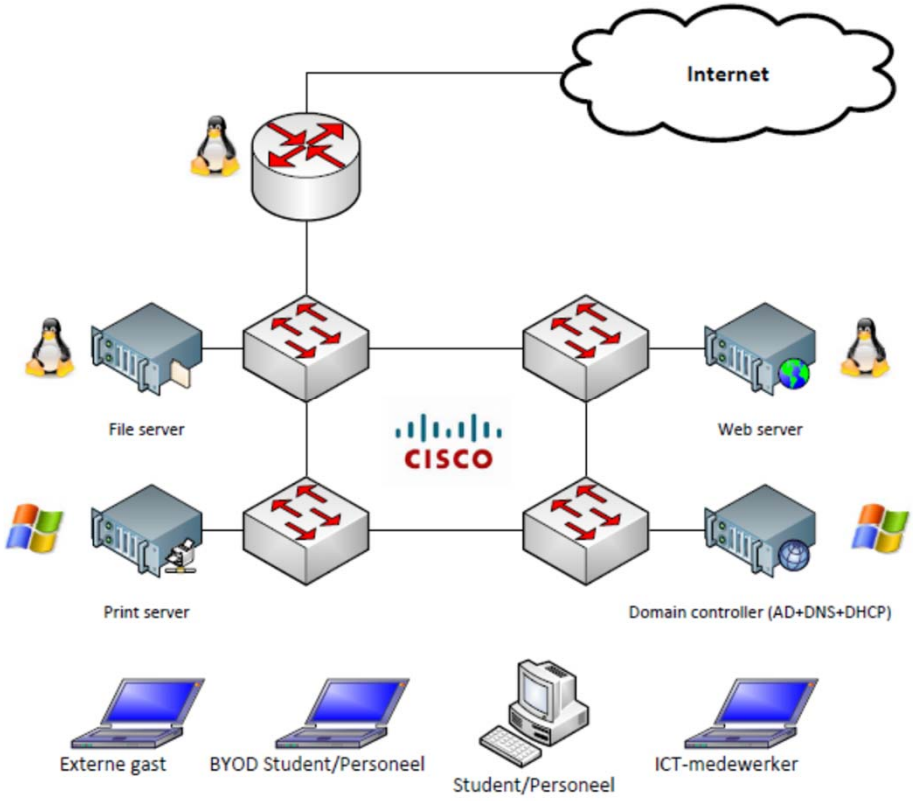
Capture filters versus display filters

Capture filters are placed on incoming traffic to reduce the amount of traffic that flows into the buffer.

Display filters are placed on traffic in the trace buffer so that you can view specific types of packets as a subset of the buffer.

Introduction to Wireshark

Capture a trunk link.



Introduction to Wireshark

Capture a trunk link.

```
> Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
> Ethernet II, Src: Dell_5e:02:11 (00:23:ae:5e:02:11), Dst: IntelCor_bb:97:dd (00:d0:b7:bb:97:dd)
> Internet Protocol Version 4, Src: 192.168.1.73, Dst: 202.12.27.33
> User Datagram Protocol, Src Port: 52719, Dst Port: 53
> Domain Name System (query)
```

Introduction to Wireshark

Capture a trunk link.

```
> Frame 1: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
> Ethernet II, Src: AsustekC_00:e6:30 (10:bf:48:00:e6:30), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 40
> Internet Protocol Version 4, Src: 192.168.1.90, Dst: 192.168.1.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service
```

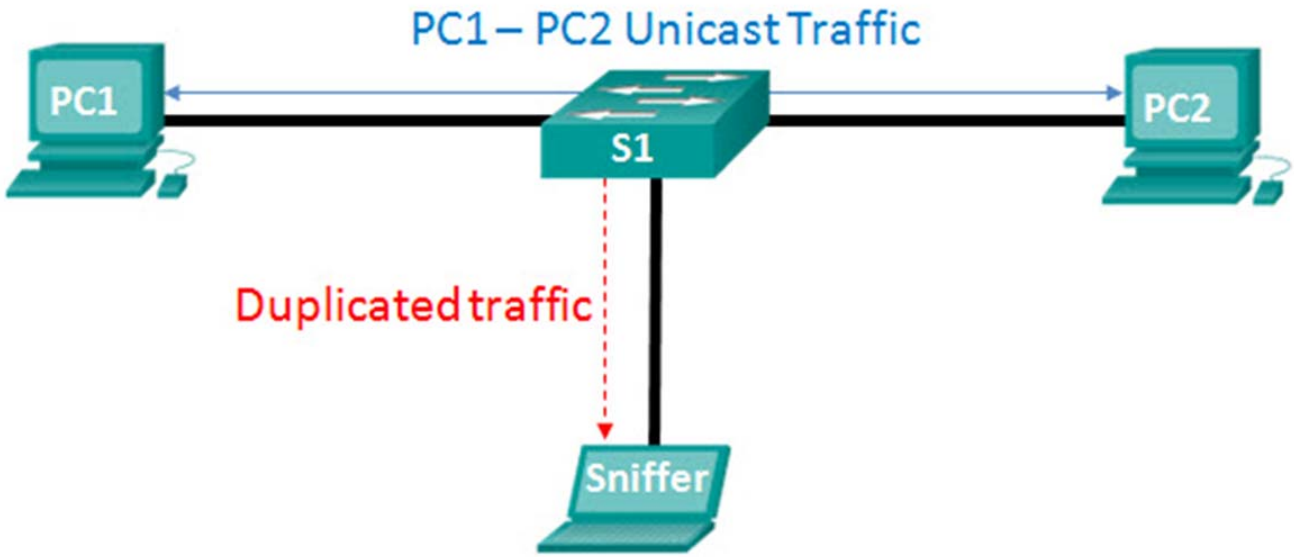
Introduction to Wireshark

Capture a trunk link. Reason? Microsoft!

https://wiki.wireshark.org/CaptureSetup/VLAN

SPAN Overview

SPAN = Switch Port Analyzer



vzw BiASC asbl
Belgian IT Academy Support Center
Improving the way people learn

SPAN Overview

SPAN terminology

Term	Definition
Ingress traffic	This is traffic that enters the switch.
Egress traffic	This is traffic that leaves the switch.
Source (SPAN) port	This is a port that is monitored with use of the SPAN feature.
Destination (SPAN) port	This is a port that monitors source ports, usually where a packet analyzer, IDS or IPS is connected. This port is also called the monitor port.
SPAN session	This is an association of a destination port with one or more source ports.
Source VLAN	This is the VLAN monitored for traffic analysis.

SPAN Overview

There are three important things to consider when configuring SPAN:

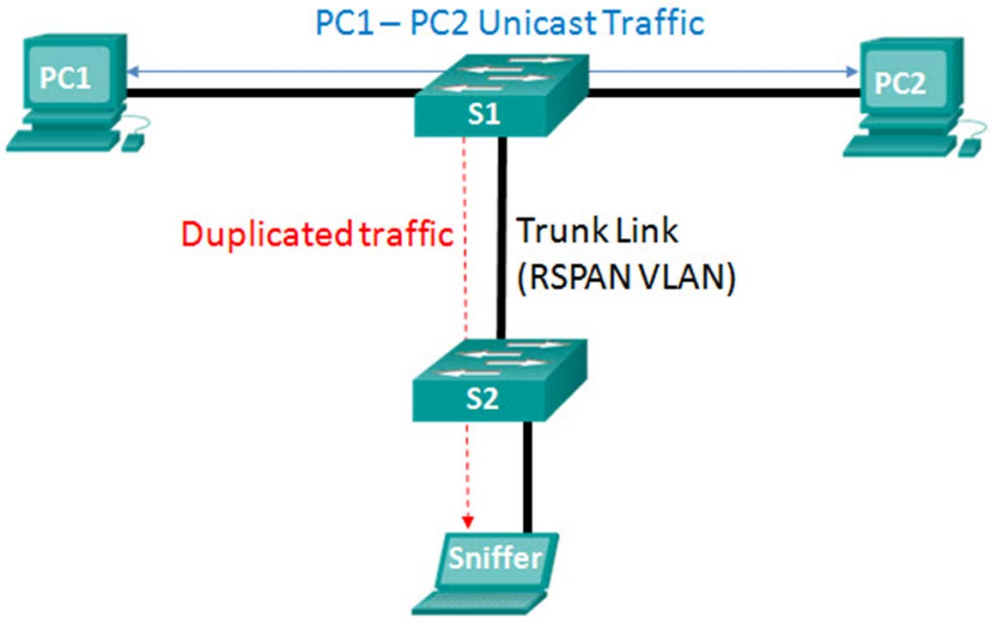
1) The destination port cannot be a source port, and the source port cannot be a destination port.

2) The number of destination ports is platform-dependent. Some platforms allow for more than one destination port.

3) The destination port is no longer a normal switch port. Only monitored traffic passes through that port.

SPAN Overview

RSPAN = Remote SPAN



vzw BiASC asbl
Belgian IT Academy Support Center
Improving the way people learn

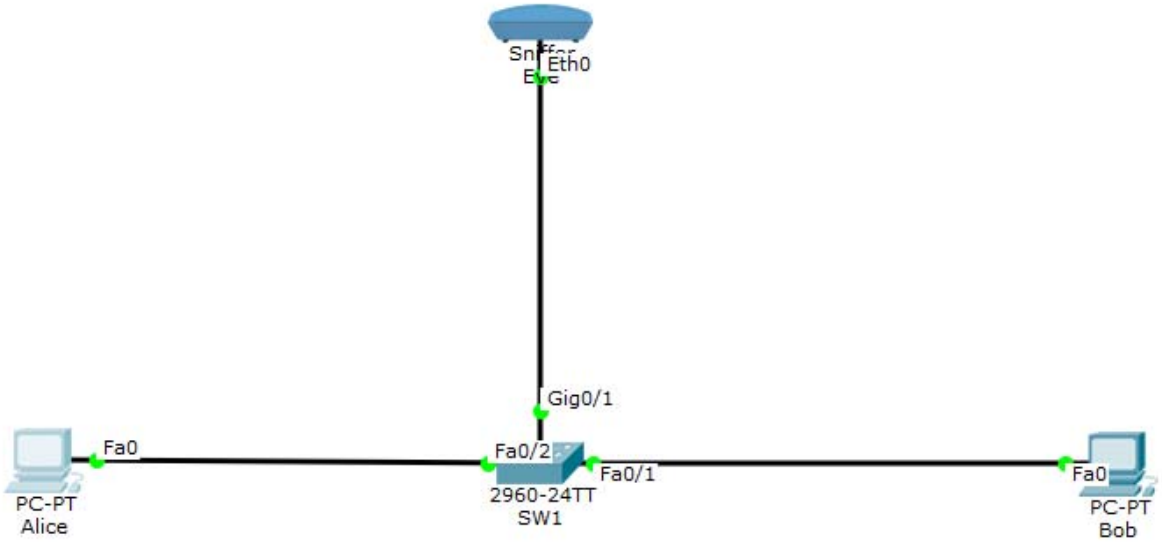
SPAN Overview

RSPAN terminology

Term	Definition
RSPAN source session	· This is the source port / VLAN to copy traffic from.
RSPAN destination session	· This is the destination VLAN / port to send the traffic to.
RSPAN VLAN	· A unique VLAN is required to transport the traffic from one switch to another. · VLAN is configured with the **remote-span** vlan configuration command. · This VLAN must be defined on all switches in the path and must also be allowed on trunk ports between the source and destination..

SPAN Overview

Basic configuration of SPAN




```
Switch#show run | begin monitor
monitor session 1 source interface Fa0/2
monitor session 1 destination interface Gig0/1
!
end


Switch#show monitor
Session 1
---------
Type                   : Local Session
Description            : -
Source Ports           :
    Both               : Fa0/2
Destination Ports      : Gig0/1
    Encapsulation      : Native
          Ingress      : Disabled


Switch#
```

SPAN Overview

Attention!

The port speed of the destination should be at least 2 times higher than the port speed of the source (Why? Ingress and egress traffic).

Capturing a trunk port?

monitor session 1 source interface Gi0/1

monitor session 1 destination interface Gi0/2 ***encapsulation replicate***

SPAN Overview

Labs delivered by Cisco NetAcad

4.8.2.2 Lab - Implement Local SPAN

4.8.3.2 Lab - Troubleshoot LAN Traffic Using SPAN

SPAN Overview

Todays lab