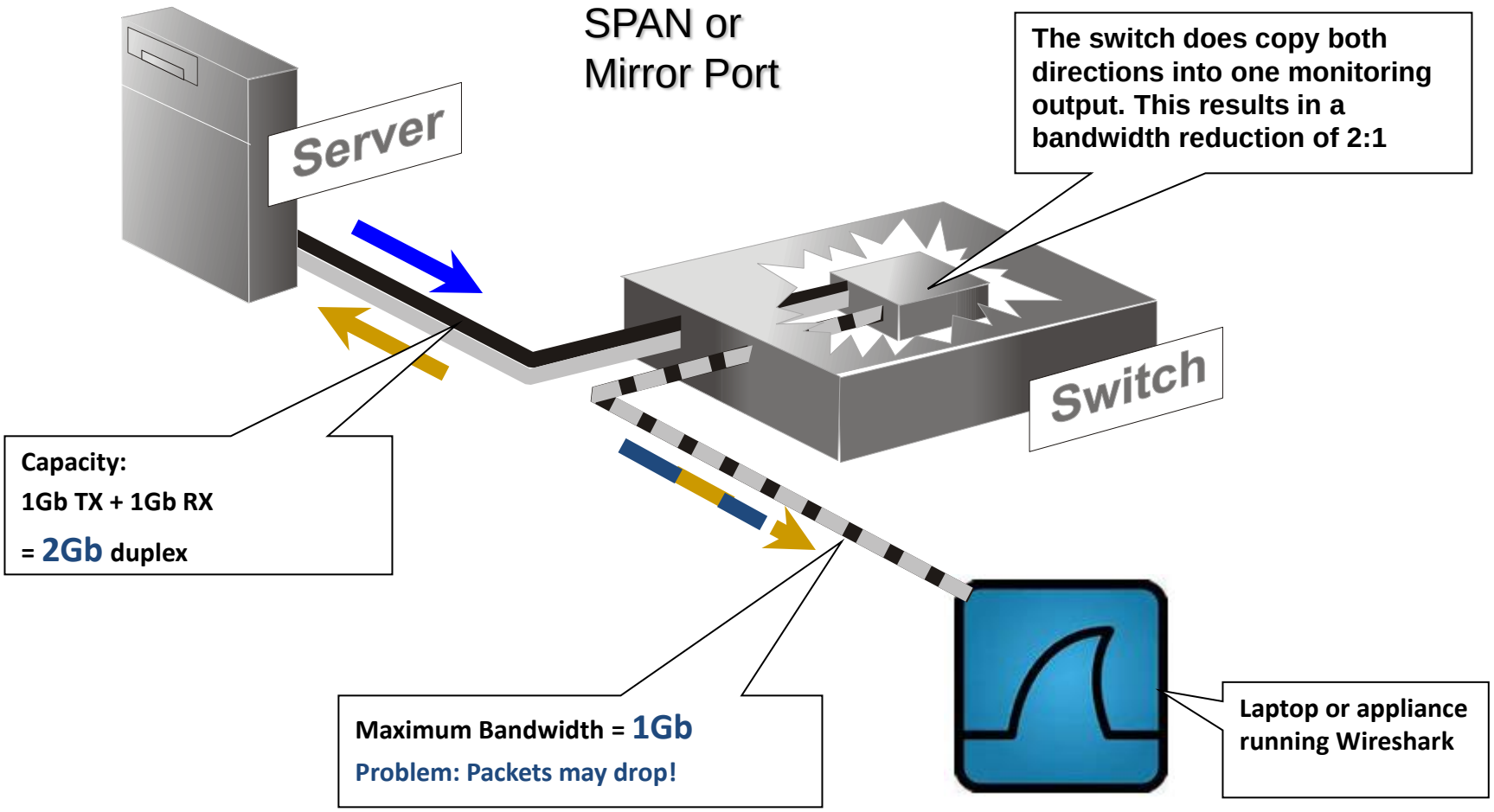
Wireshark Webinar September 2013

Wireshark direct attached to a SPAN Port

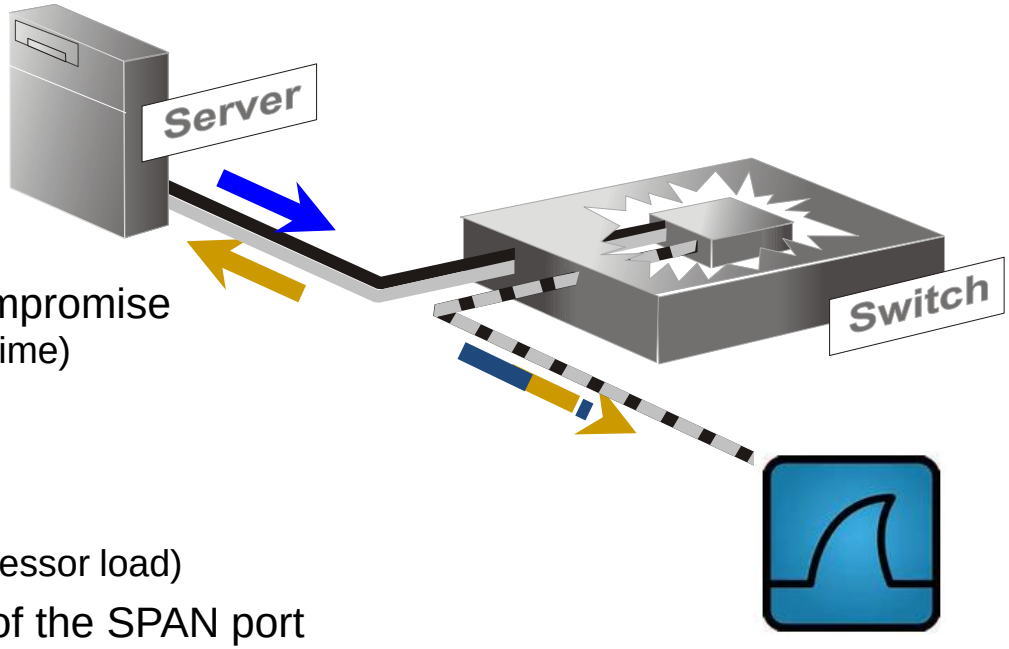
Usual way connecting Wireshark to the Network



tec4net

ixia

What are the imitating factors of a SPAN Port?



SPAN or Mirror Ports

- Limited number of SPANs leads to compromise
  (Multiple tools cannot be used at the same time)
- Have to be configured and maintained
  (Danger working on Production Network)
- Load depended behavior
  (tend to loose packets already at lower processor load)
- Speed of the Network dictates speed of the SPAN port
  (e.g. 10GE Network port ends up in 10GE SPAN port)
- Limited Filter functionality per SPAN port
  (difficult to setup via CLI, no complex filter algorithm)
- No Packet Processing possible
  > Packet Stripping (removing of MLPS, VLAN or GTP header)
  > Packet Trimming (removing of packet content for data protection or bandwidth reduction)
- rSPAN always copy the total load of the monitored link to the production link
  (Danger of overloading the Production Network with monitoring data)

tec4net

ixia

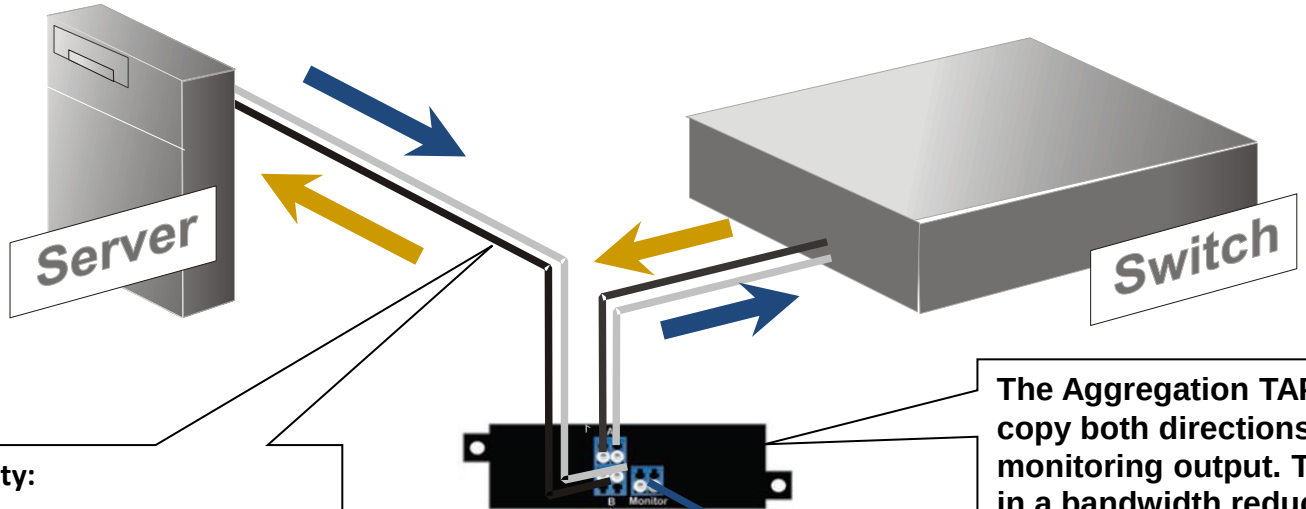
Is there something we could do better?

TAP is the solution

TAPs

- Part of the Network reduces the risk of impacts due to configuration mistakes
  (Once installed no need to touch anymore)
- No load depended behavior
- Many variants available
  (Copper, Fiber, Full-Duplex, Aggregation)
- Simplest optical TAPs are safe as houses
  and grow with the Network from GE to 10GE
- Copper TAPs are fail save when power is lost

Aggregation TAP



Capacity:
1Gb TX + 1Gb RX
= 2Gb duplex

The Aggregation TAP does copy both directions into one monitoring output. This results in a bandwidth reduction of 2:1

Maximum Bandwidth = 1Gb

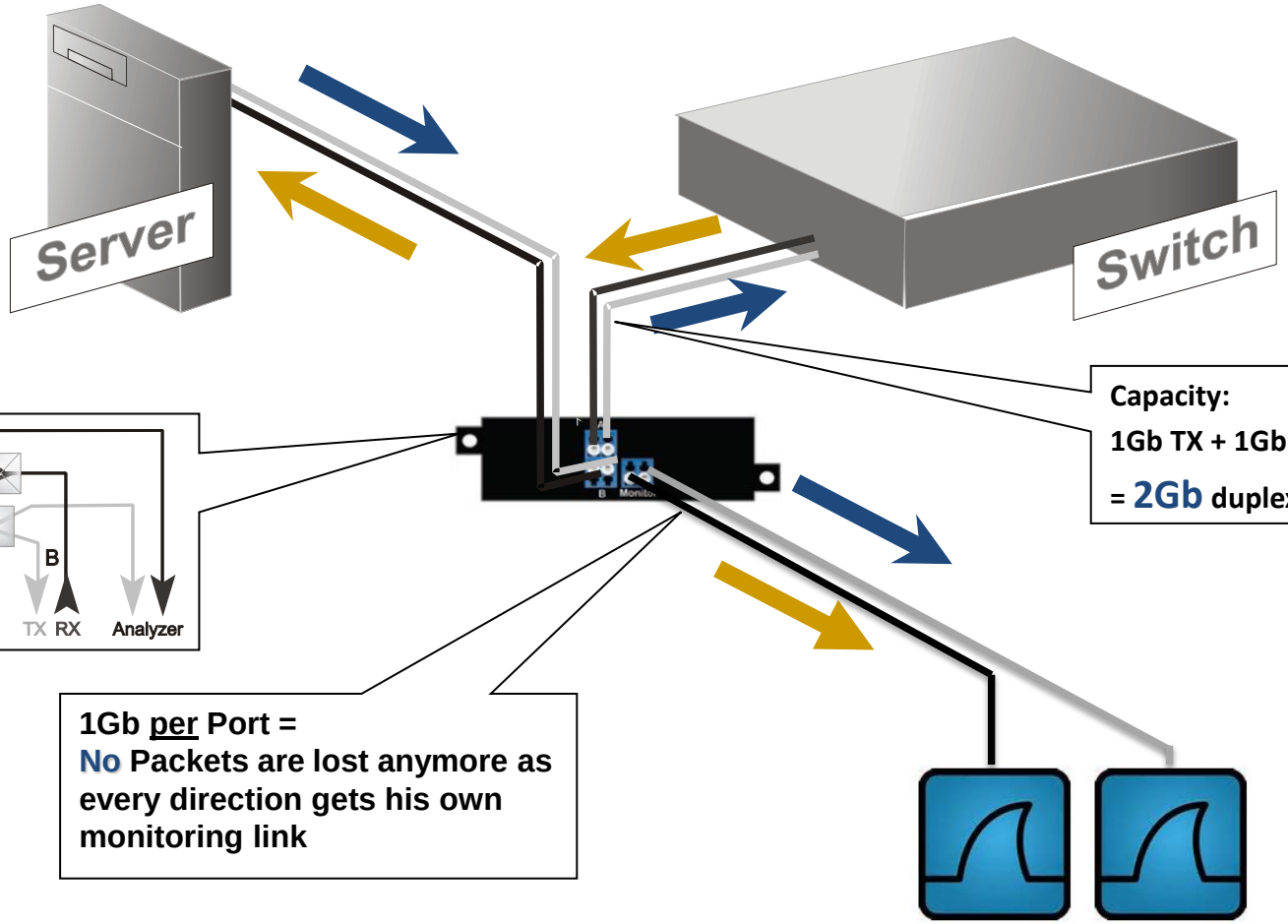
Problem: Packets will be dropped if the bandwidth in both directions is overstepping the GE capacity.
The advantage against a SPAN Port is that the TAP does not show a load dependent behavior and need to be configured

Wireshark can be directly connected to the TAP but what if the monitored link runs on 10GE instead of on GE only? What bandwidth is on the aggregated link? Is Wireshark able to handle the total capacity and are all packets of interest?

tec4net

ixia

Full-duplex TAP



Capacity:
1Gb TX + 1Gb RX
= 2Gb duplex

1Gb per Port =
No Packets are lost anymore as every direction gets his own monitoring link

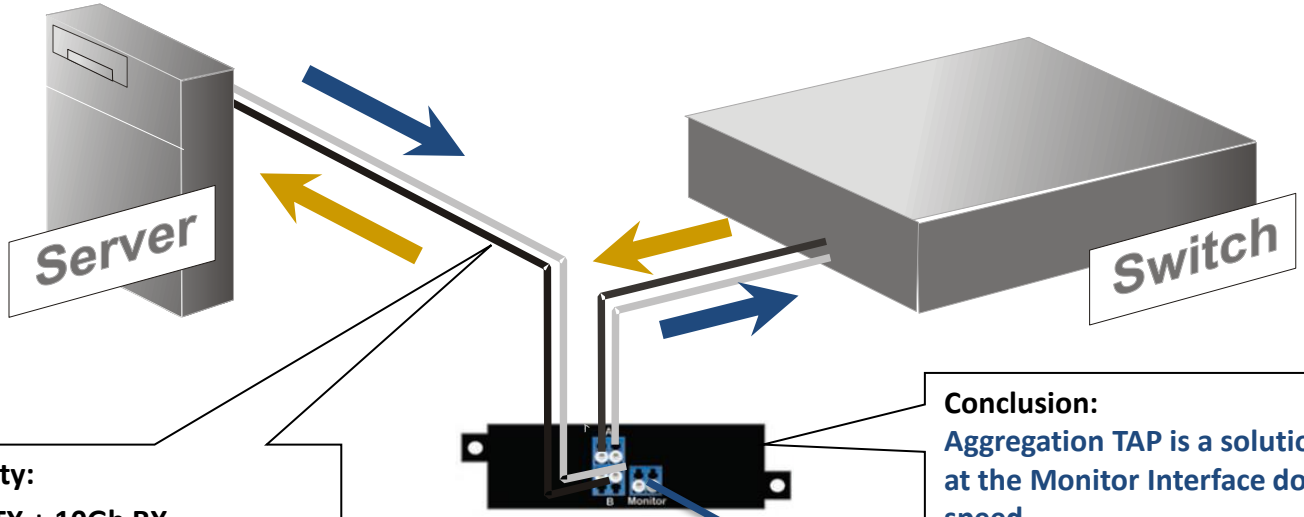
With a full Duplex TAP no packets are lost anymore as the TAP can handle Line Rate in both directions. But now we do have two links and would need 2 Wireshark appliance. In addition we still have not sold the matter what bandwidth is at the link? Is Wireshark able to handle the total capacity and are all packets of interest?

tec4net

ixia

Again, can we do better?

Aggregation TAP plus Monitoring Switch



Capacity:

10Gb TX + 10Gb RX

= 20Gb duplex

Conclusion:

Aggregation TAP is a solution as long as the bandwidth at the Monitor Interface does not overstep the physical speed

Maximum Bandwidth = 10Gb

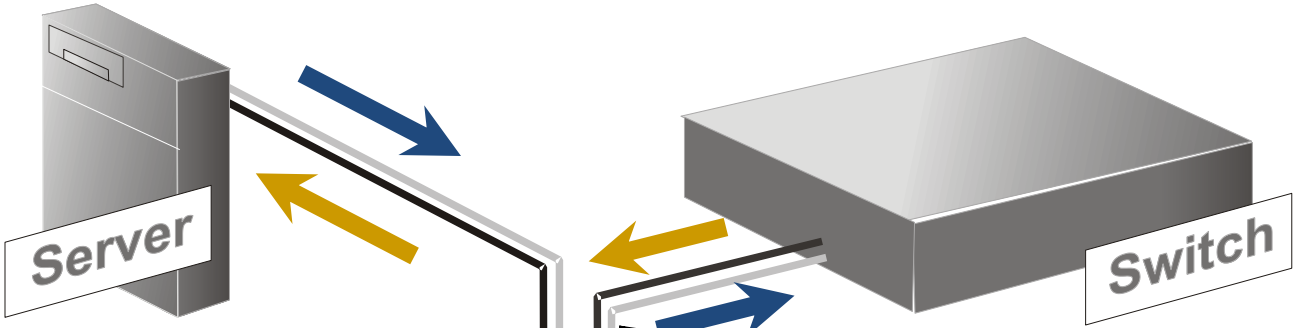
Problem: Packets will be dropped if the bandwidth in both directions is overstepping the 10GE capacity

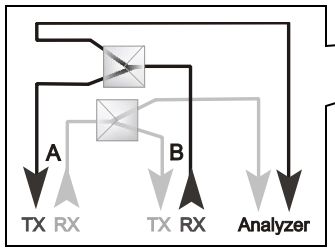
By aggregating and filtering on the relevant Packets, no Packets are lost at the Monitoring Switch even it the link towards Wireshark is only a single GE link.

tec4net

ixia

Full-duplex TAP plus Monitoring Switch





Capacity:
10Gb TX + 10Gb RX
= 20Gb duplex

10Gb per Monitor Port =
No Packets are lost

By aggregating and filtering on the relevant Packets, no Packets are lost even on a single GE link.

Conclusion:
Full Duplex together with a Monitoring Switch is the best fit for Wireshark Application

tec4net

ixia

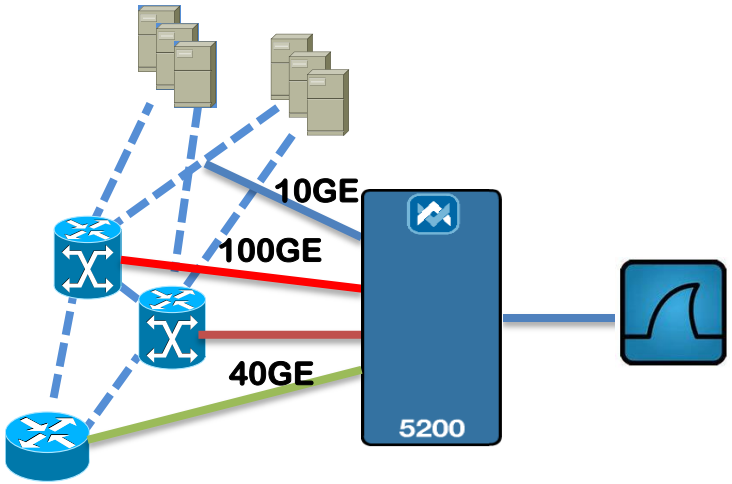
What benefits does a Monitor Switch provide when using it together with Wireshark?

Problem:

The same amount of Wireshark probes are needed as TAPs deployed in the network. In addition The physical speed of the network dictates the probe being used, even if the bandwidth in a 10GE is just 500MB.

Solution:

A Network Monitoring Switch does aggregate various TAP ports and decouple the physical speed of the network from Wireshark.



Filtering on the relevant data does reduce the bandwidth and allows using a single Wireshark probe without loosing any packets.

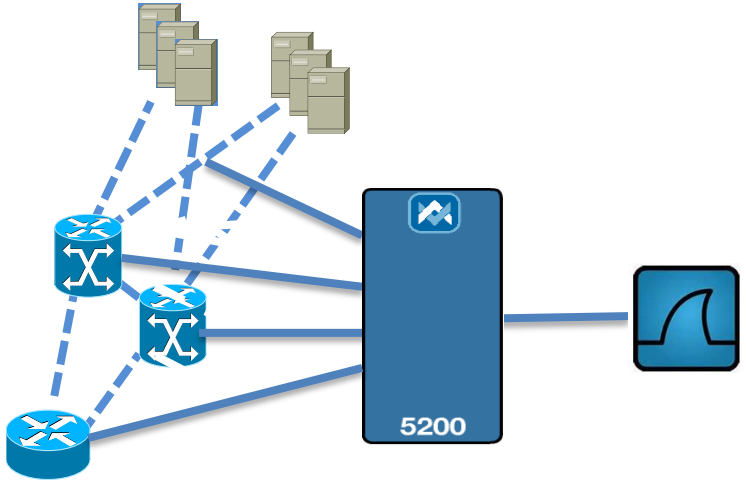
Duplicated Packets

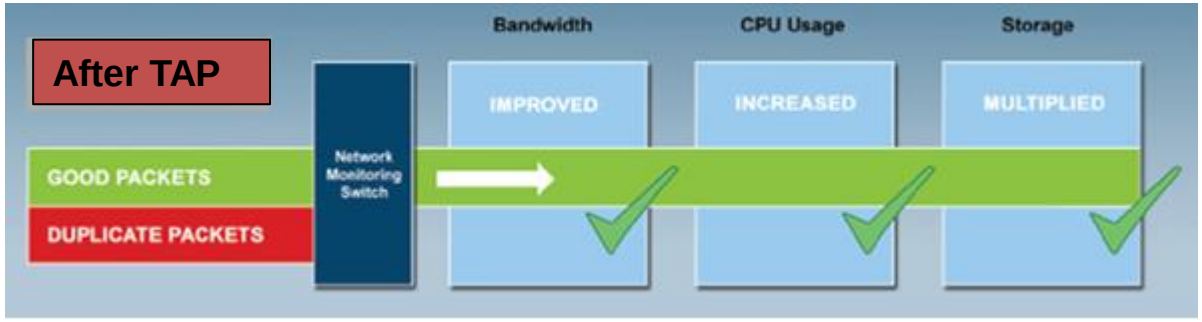
Problem:

- 50-80% of the Network load my result out of duplicated packets
- Wireshark link performance is blocked by duplicated packets
- Storage capacity is wasted due to duplicated packets

Solution:

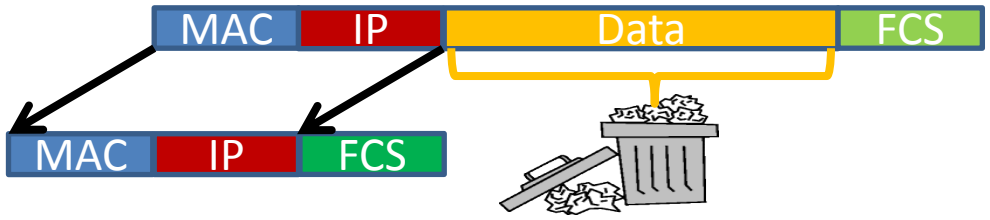
The Network Monitoring Switch
De-Duplication function
does remove duplicated packets





tec4net

ixia

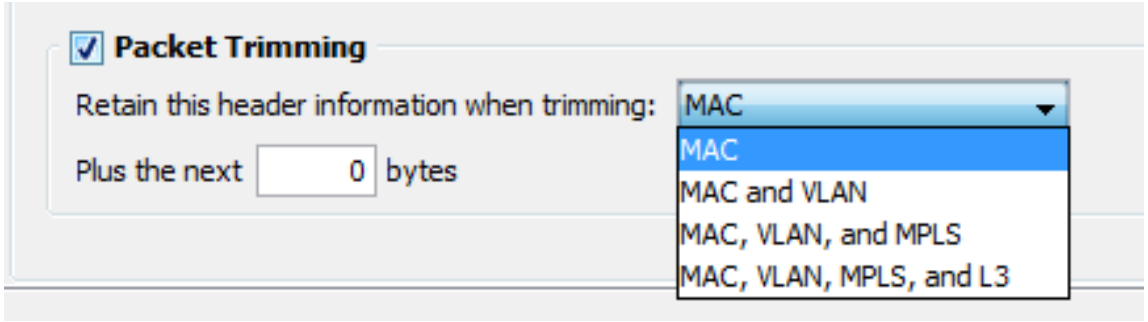


Problem:

In many cases only the header is needed for analyzing. Forwarding e.g. a 1500byte packet to Wireshark does consume more memory at the disk than a 64byte packet.
If the data content is not needed this would be wasting recourses beside that it does consume bandwidth on the link to Wireshark.

Solution:

A Network Monitoring Switch does remove the data content of a packet before the packet will be forwarded to Wireshark.
The user can define by the GUI what header information will retrain after trimming.

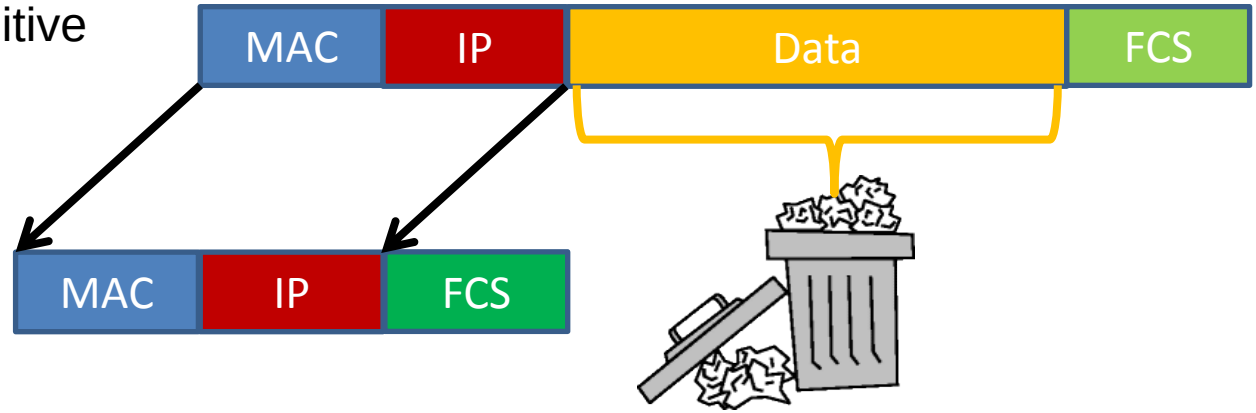


tec4net

ixia

Scenario:

Packets may content sensitive data



Problem:

Security issues

Data Protection

Solution:

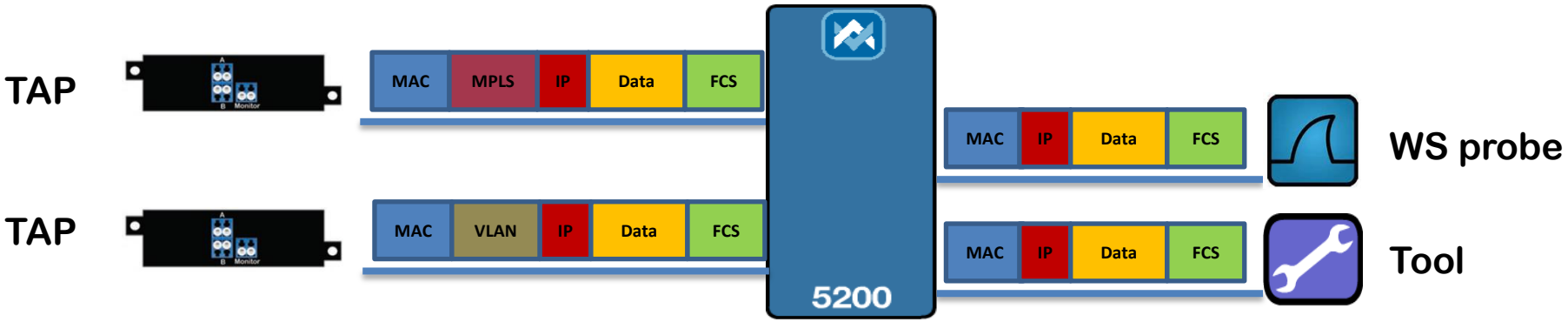
A Network Monitoring Switch
does remove the sensitive content of a packet
before it will be forwarded to Wireshark

tec4net

ixia

Problem:

In many cases additional header information such as VLAN, MPLS, VN-Tag or GTP-tunnel is not needed or would prevent analyzing the data.
In addition when using other tools in parallel these tools may not be able handling packets that does content these additional header information.



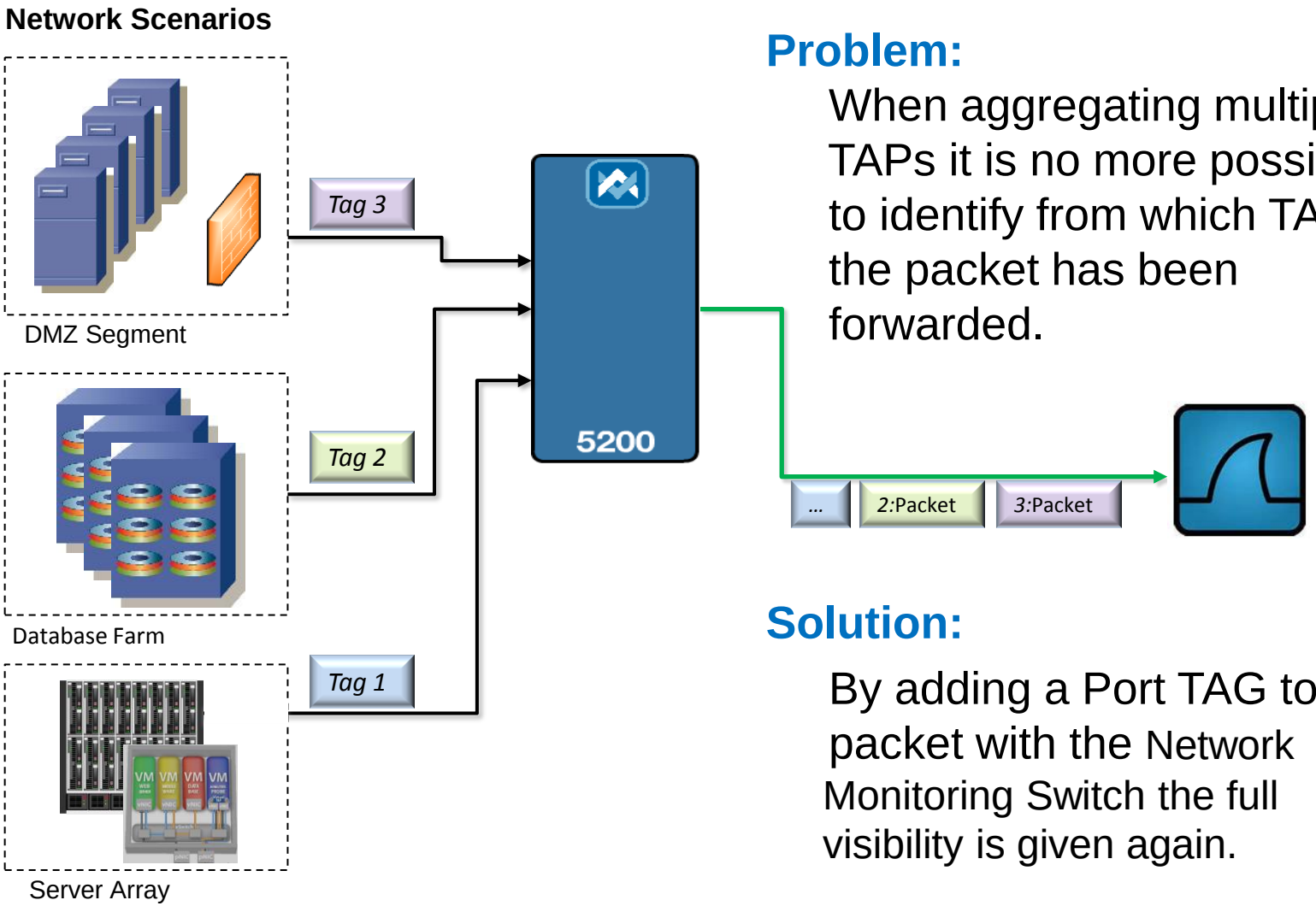
Solution:

Network Monitoring Switch does remove MPLS, VLAN, VN-Tag or GTP header information.

tec4net

ixia

Port Tagging



Problem:

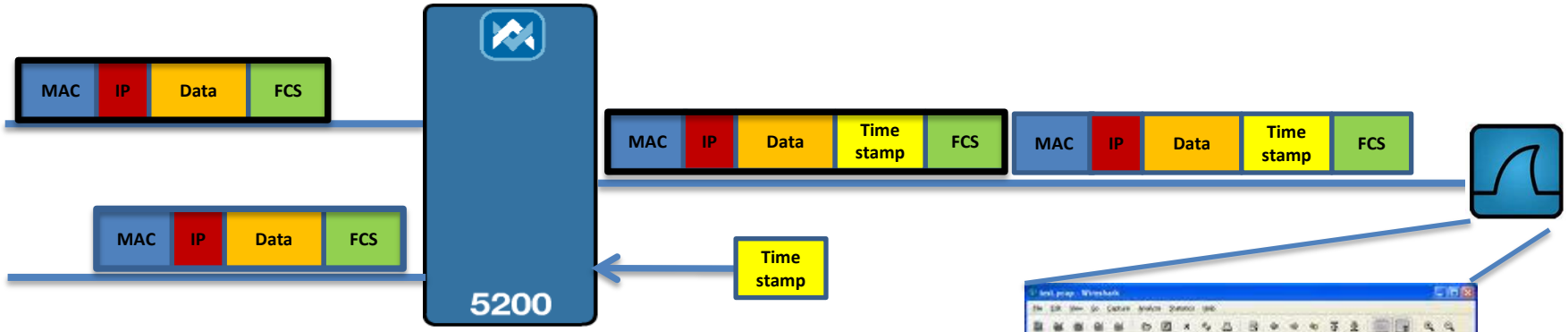
When aggregating multiple TAPs it is no more possible to identify from which TAP the packet has been forwarded.

Solution:

By adding a Port TAG to the packet with the Network Monitoring Switch the full visibility is given again.

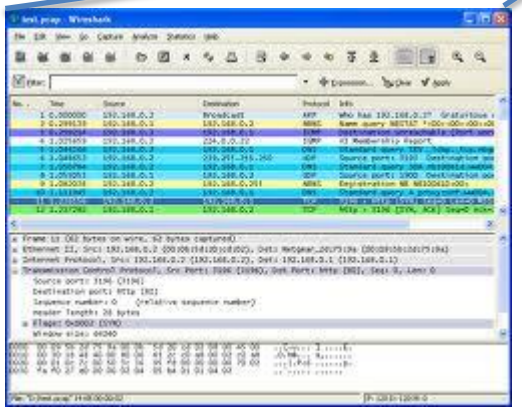
Problem:

In applications like high frequency trading or routing the monitoring data over a long distance to Wireshark it is on interest when the packet has arrived at the monitoring switch.



Solution:

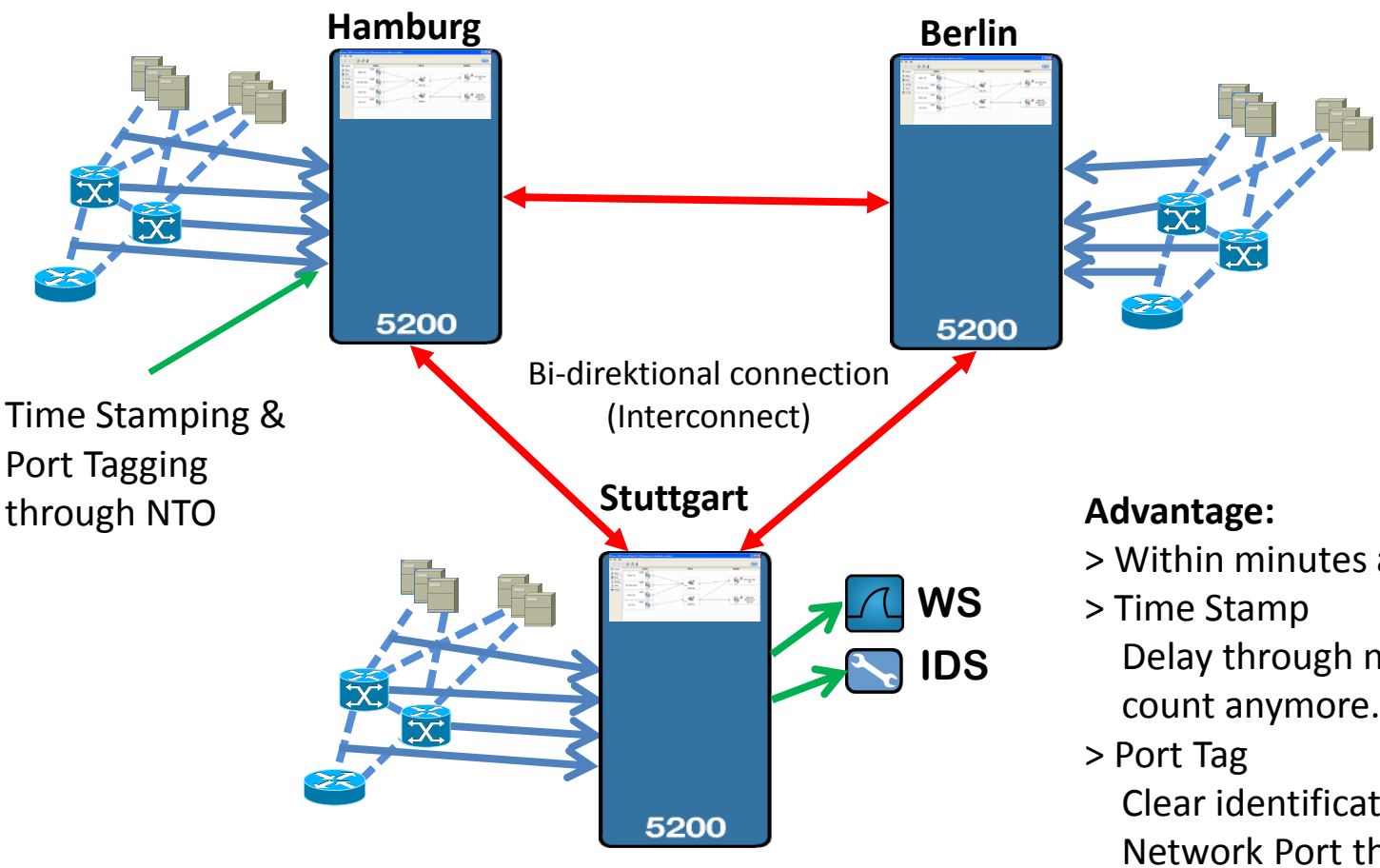
An external Timestamp synchronized over NTP or GPS will provide this information. Wireshark is able decoding this Timestamp.



tec4net

ixia

Independent Monitoring Network



Advantage:

> Within minutes access to all data

> Time Stamp

Delay through network does not count anymore.

> Port Tag

Clear identification from which Network Port the packet is coming from.

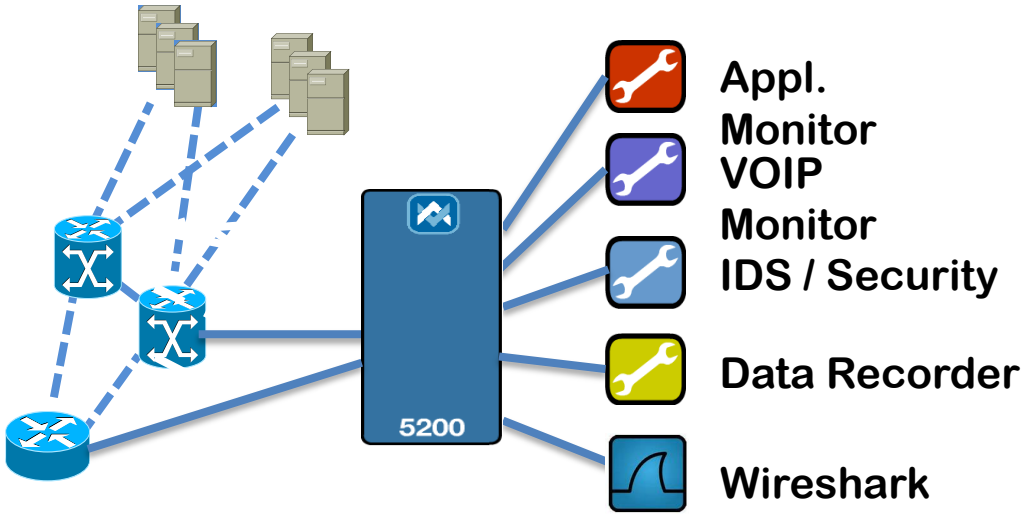
tec4net

ixia

Not enough Monitoring Points

Problem:

Not enough Monitoring Points are available connecting all required tools at the same time



Solution:

A Network Monitoring Switch does collect the data from SPAN or/and TAPs

Individual Filter settings does provide each tool the data required.

Multi User Access with different access rights protects each departments configuration.

tec4net

ixia

Ixia Portfolio: A Solution for Every Need

Monitoring Switches

High Performance 1/10/40/100G

5288

- **Flexible, scalable, high density**
- **16 x 40G, 64 x 1/10G or 4x 100G**

Advanced Functionality 1/10G

5236

- **Versatile, robust**
- **24 x 10G & 4 x 1G**

Entry

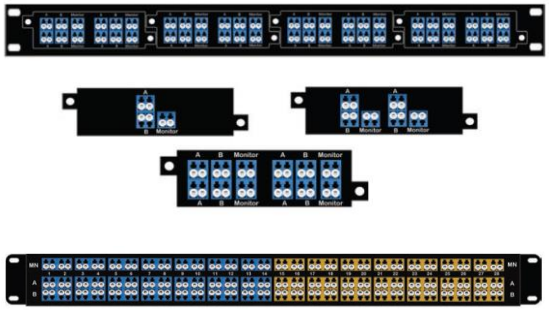
5204 NTO

- **Copper**
- **4x10G + 24x1G**

TAPs

Copper TAPs

Optical TAPs



Inline Monitoring

Bypass TAPS (1/10G)

tec4net

ixia

Q & A

tec4net IT-Solutions
Flunkgasse 22
81245 München

www.tec4net.com
info@tec4net.com

Tel.: +49 (89) 54043630
Fax: +49 (89) 54043631