A-7: SPAN Out of the Box

Wednesday June 16, 2010 1:15 pm – 2:45 pm

John HE, Hardware Engineer
Founder | Dualcomm Technology, Inc.

SHARKFEST **'10**
Stanford University
June 14-17, 2010

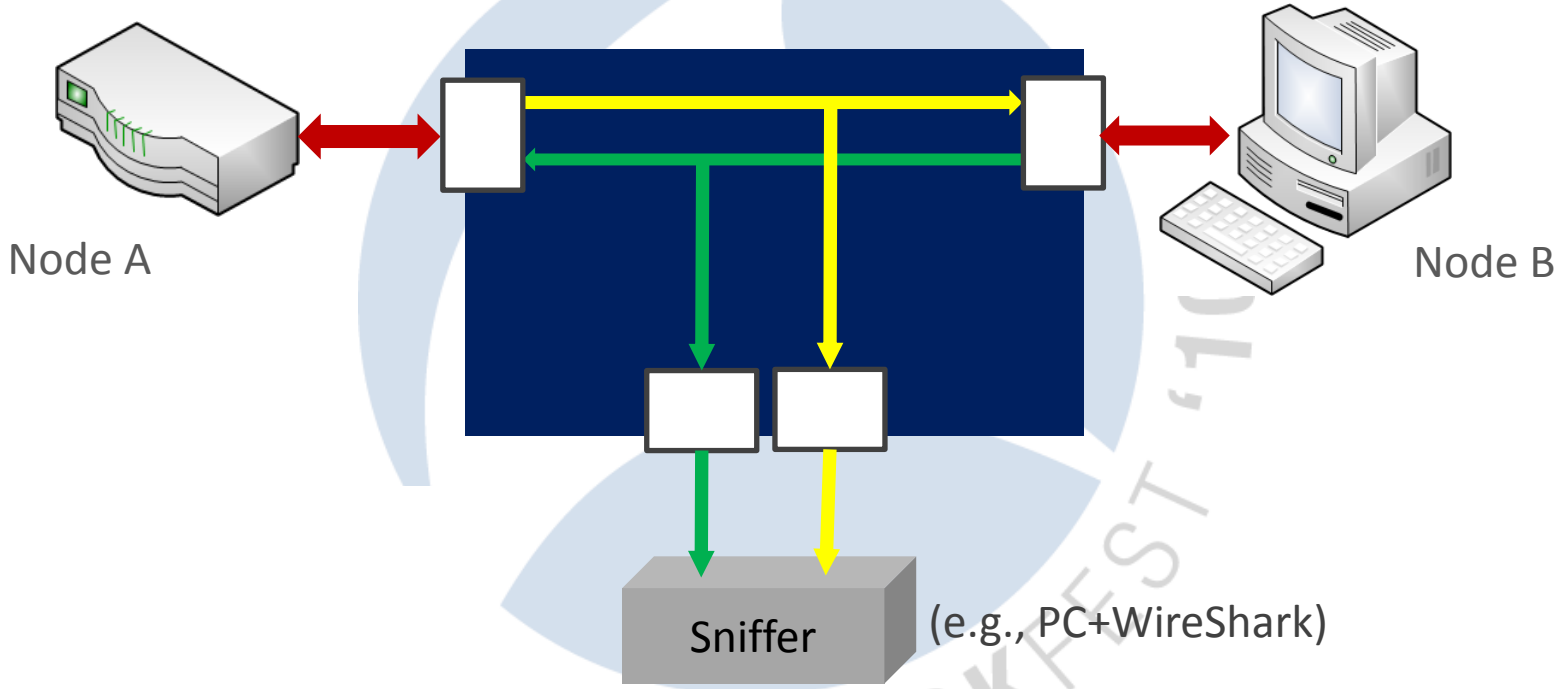
Outline

This presentation

- Relates to “TAP vs. SPAN”, a seemingly popular topic among TAP vendors,
- Examines what has been said about the “Cons” of using a SPAN port, and how real they are,
- Discusses the real headaches of using a SPAN port, and
- Introduces a “SPAN Out of the Box” solution to relief the headaches.

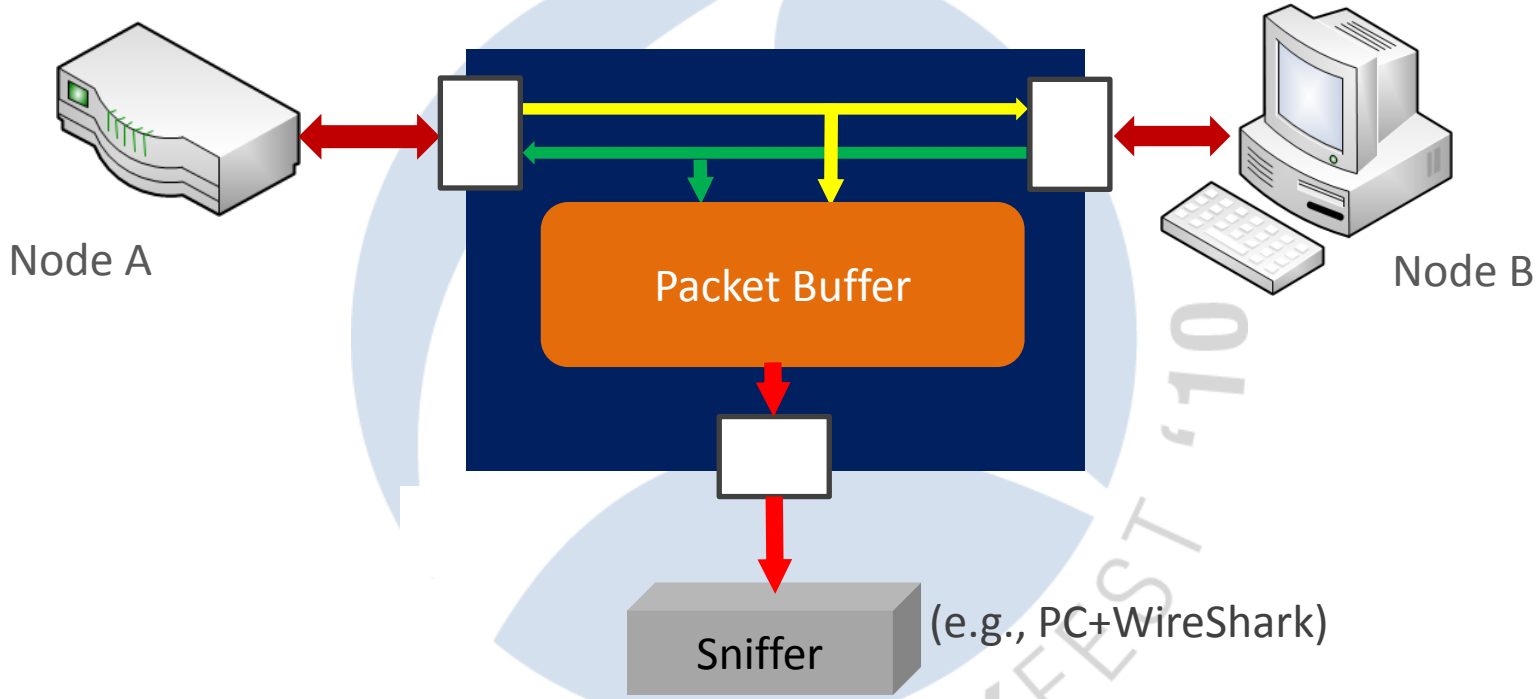
SHARKFEST '10

TAP = Test Access Point



Two NICs are needed!

Aggregation TAP

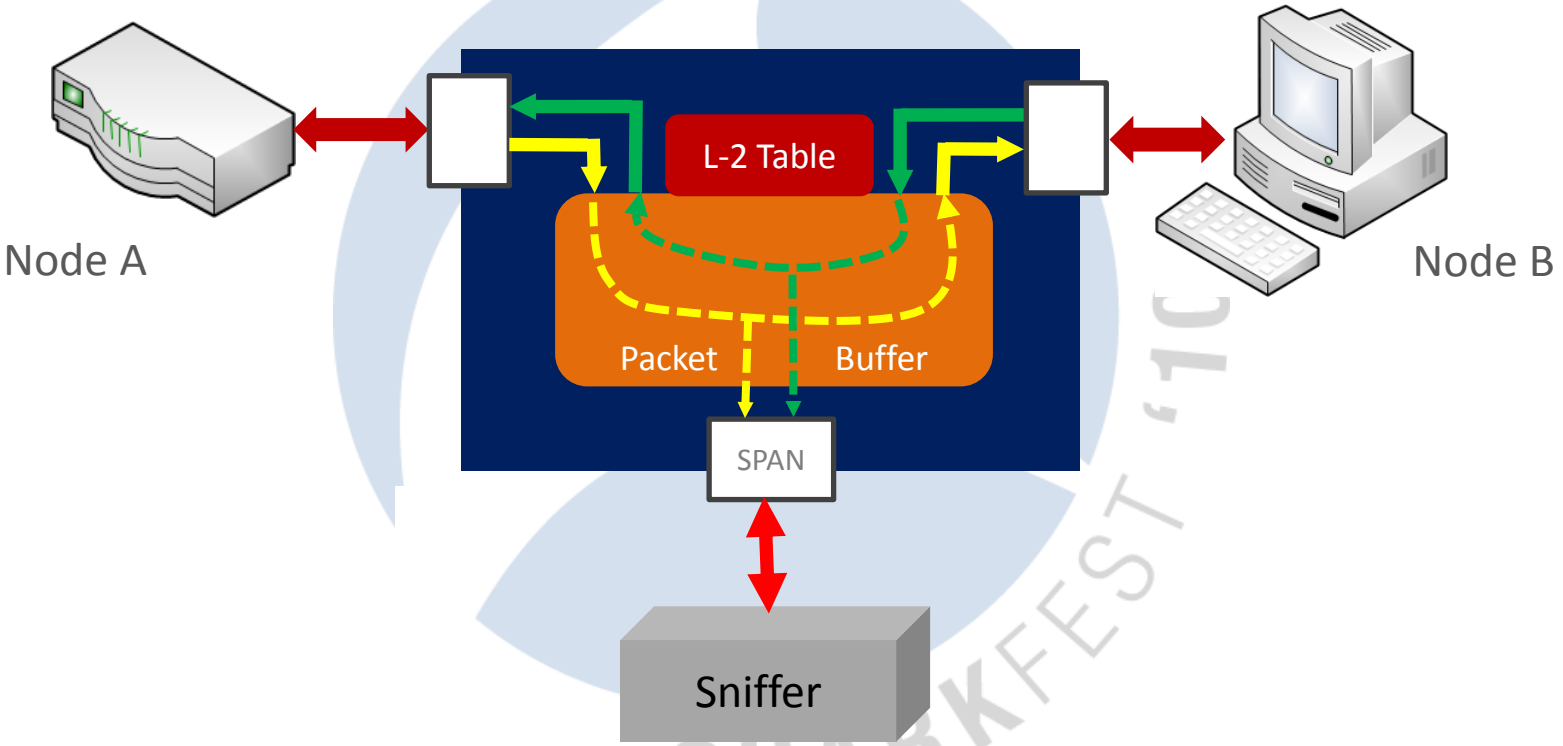


Only one NIC is needed!

SHARKFEST '10

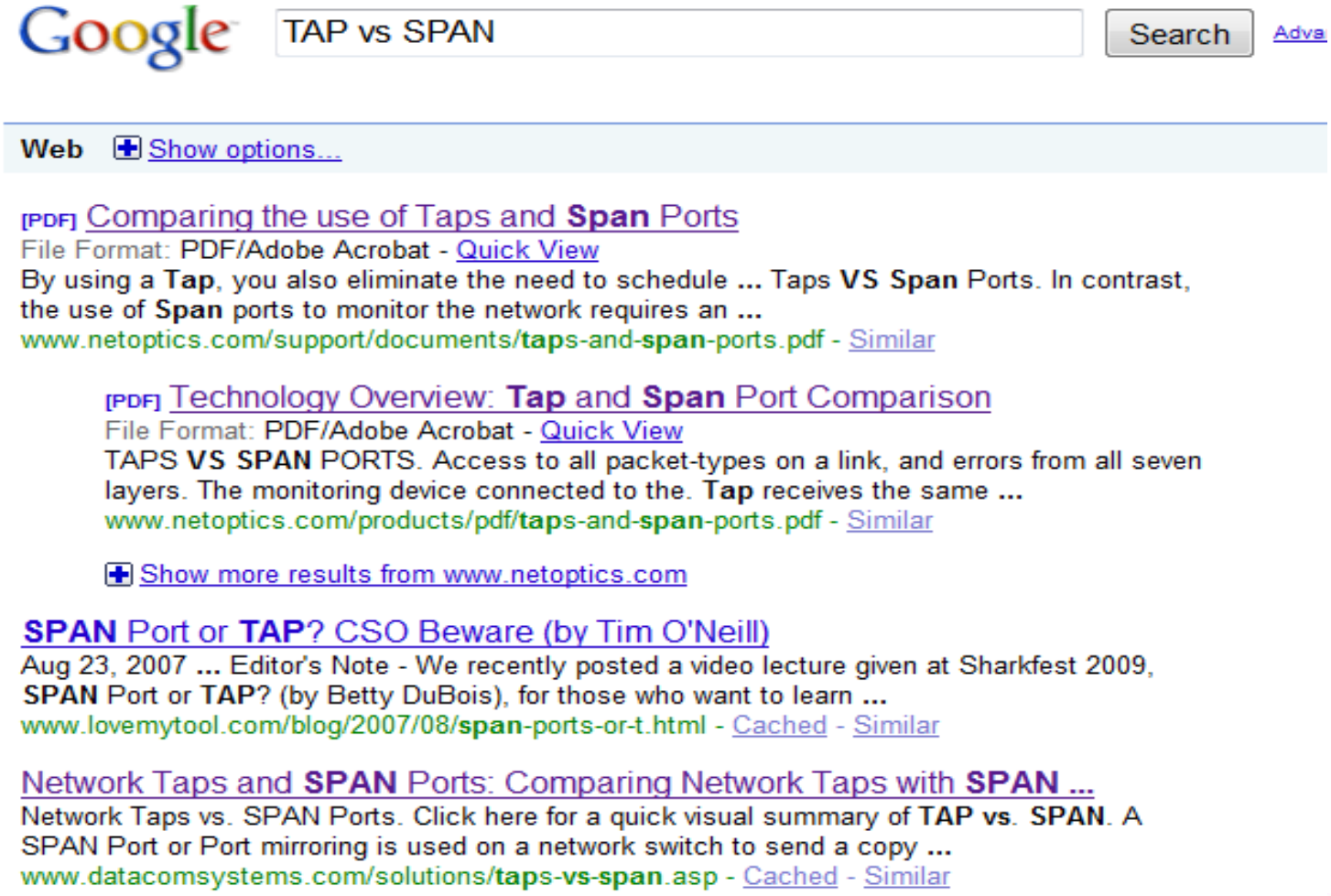
SPAN = Switched Port Analyzer

(Aka Port Mirroring)



SHARKFEST '10

TAP vs. SPAN – Google Search



TAP vs. SPAN – more….

[PDF] Data Monitoring Access
File Format: PDF/Adobe Acrobat - Quick View
Aug 29, 2007 **...** **SPAN** Port or Passive **TAP**? What's on your Network? Part 1. Is **SPAN** port a viable data access technology for today's business critical **...**
www.networkcritical.com/.../99cf06ab-87bd-454c-8be3-35e0b5b312ae.pdf

Network **tap** - Wikipedia, the free encyclopedia
A distributed **tap** is a set of network taps which report to a centralized **....** is to use port mirroring (called "**SPAN**", for Switched Port Analyzer, by Cisco, **...**
en.wikipedia.org/wiki/Network_**tap** - Cached - Similar

Network Instruments® | **Span vs TAP**
SPAN vs TAP. Most enterprise switches copy the activity of one or more ports through a Switch Port Analyzer (**SPAN**) port, also known as a mirror port. **...**
www.netinst.com/products/n**taps**/**span**_v_**tap**/index.html - Cached

[PDF] What is a **TAP**? Problems with **Span** Ports Benefits of TAPs Problems **...**
File Format: PDF/Adobe Acrobat - Quick View
A **Tap** provides a fail safe monitoring environment where if power is lost the network connection remains unaffected. Network TAPs **Vs**. **Span** Ports & Hubs.
www.vssmonitoring.co.jp/.../VSS%20monitoring%20-%20Network_**Taps**_**VS**_**Span**_ports.pdf - Similar

What Has Been Said about SPAN

- SPAN is not passive or fail-safe.
- SPAN drops packets when Oversubscription occurs.
- SPAN grooms packets and affects packet timing.
- Layer 2 errors are not visible. Corrupted packets are dropped.
- The performance of SPAN is not as reliable or predictable as TAP.
- SPAN is not always available or accessible operationally. Need permission to change switch configuration.

Reality Check

What Does It Mean by "Passive"?

- Interpretation #1: Having no power; not using power
- Interpretation #2: "Having no effect".

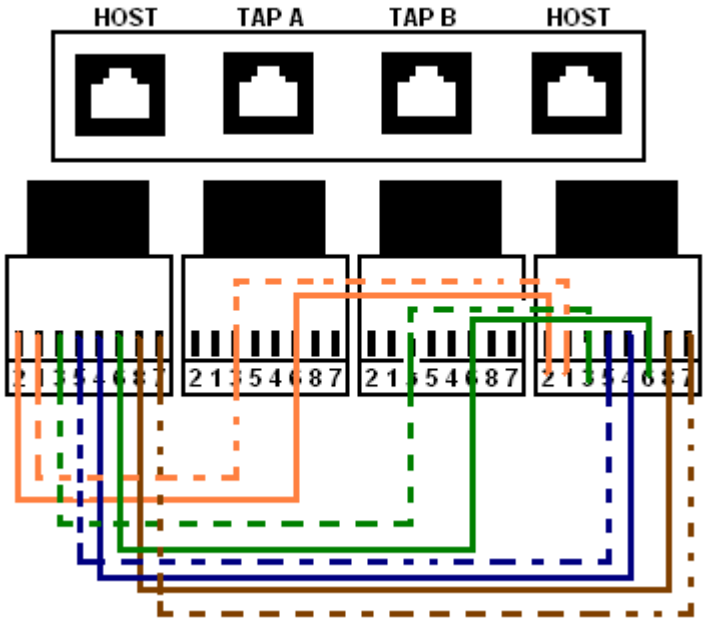
Is SPAN port a passive technology – No!

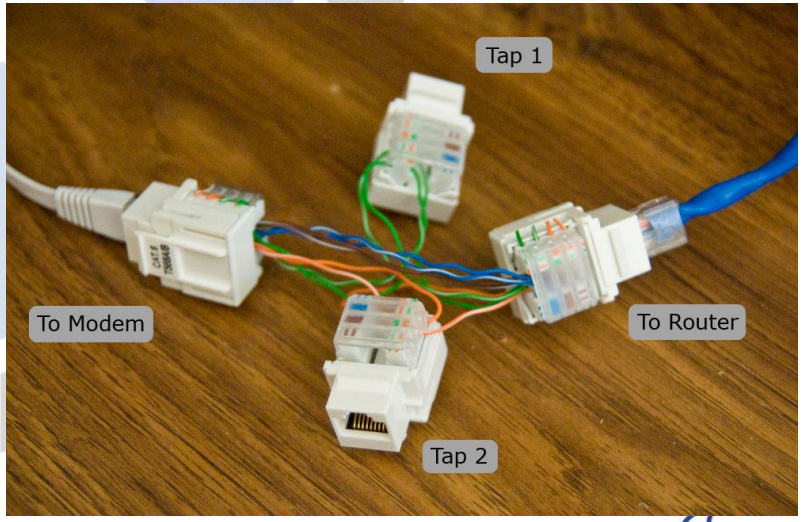
Some call SPAN port a passive data access solution – but passive means "having no effect" and spanning (mirroring) does have measurable effect on the data.

http://www.lovemytool.com/blog/2007/08/span-ports-or-t.html

Is TAP a Passive Technique? (1)

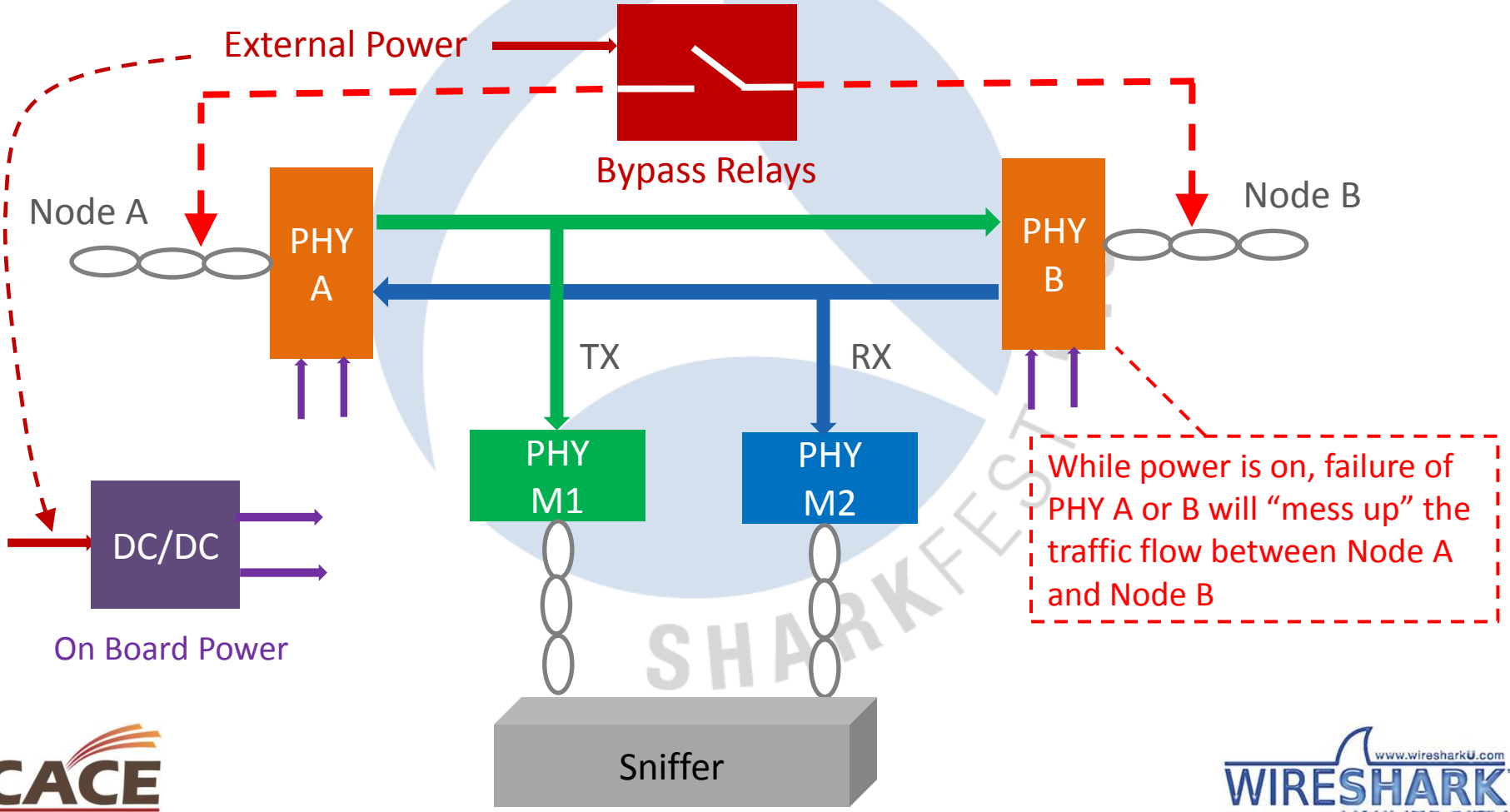
- As to this $20 DIY TAP, the answer is “YES”, Maybe?
- However, it does not have much practical use.
  - Must use short cables for TAP ports to avoid severe signal. reflection and corruption.
  - No support for Auto-Negotiation.
  - 10/100M only, but not recommended for 100M.





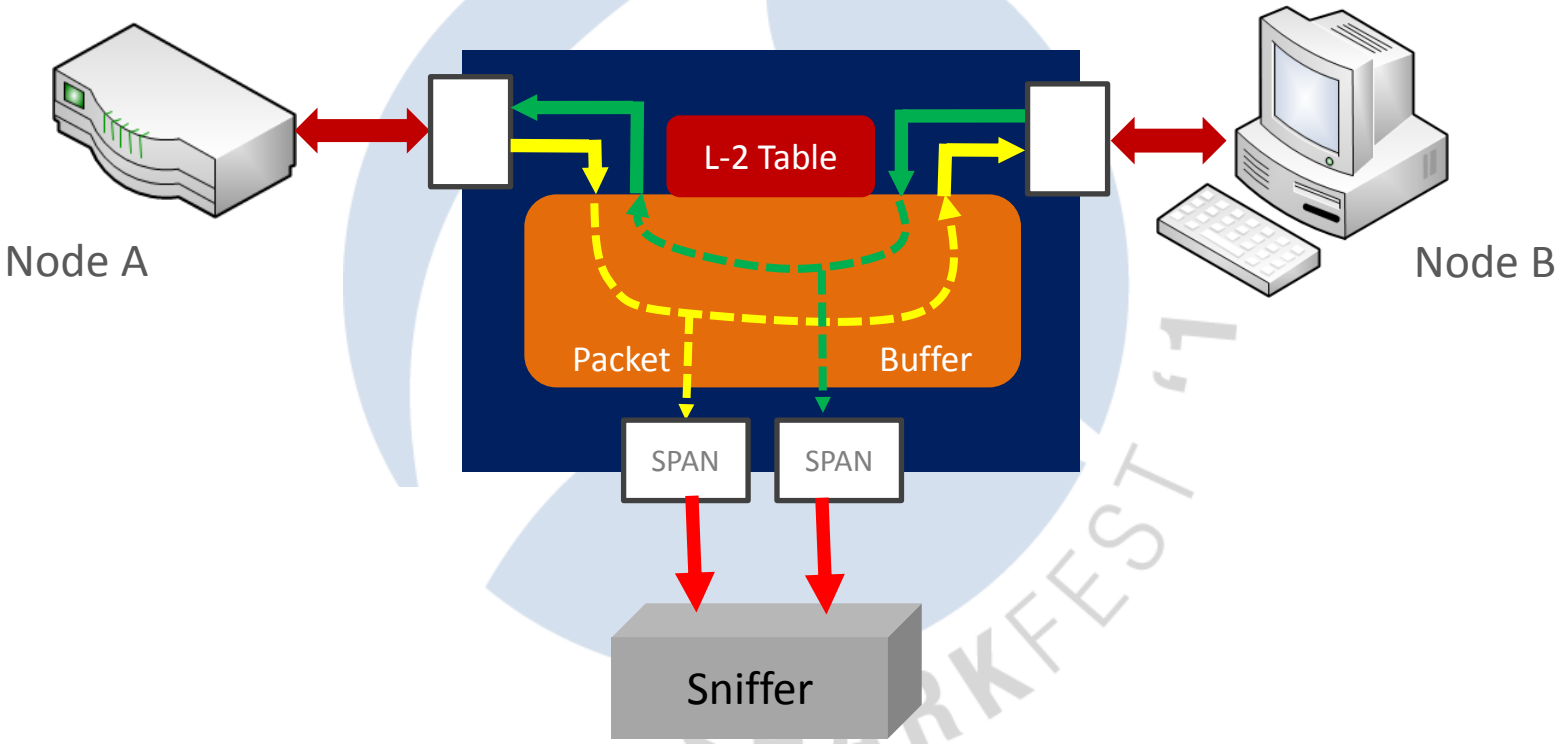
Is TAP a Passive Technique? (2)

This TAP supports Auto-Negotiation, but it is not a passive device any more and it also becomes a single point of failure.



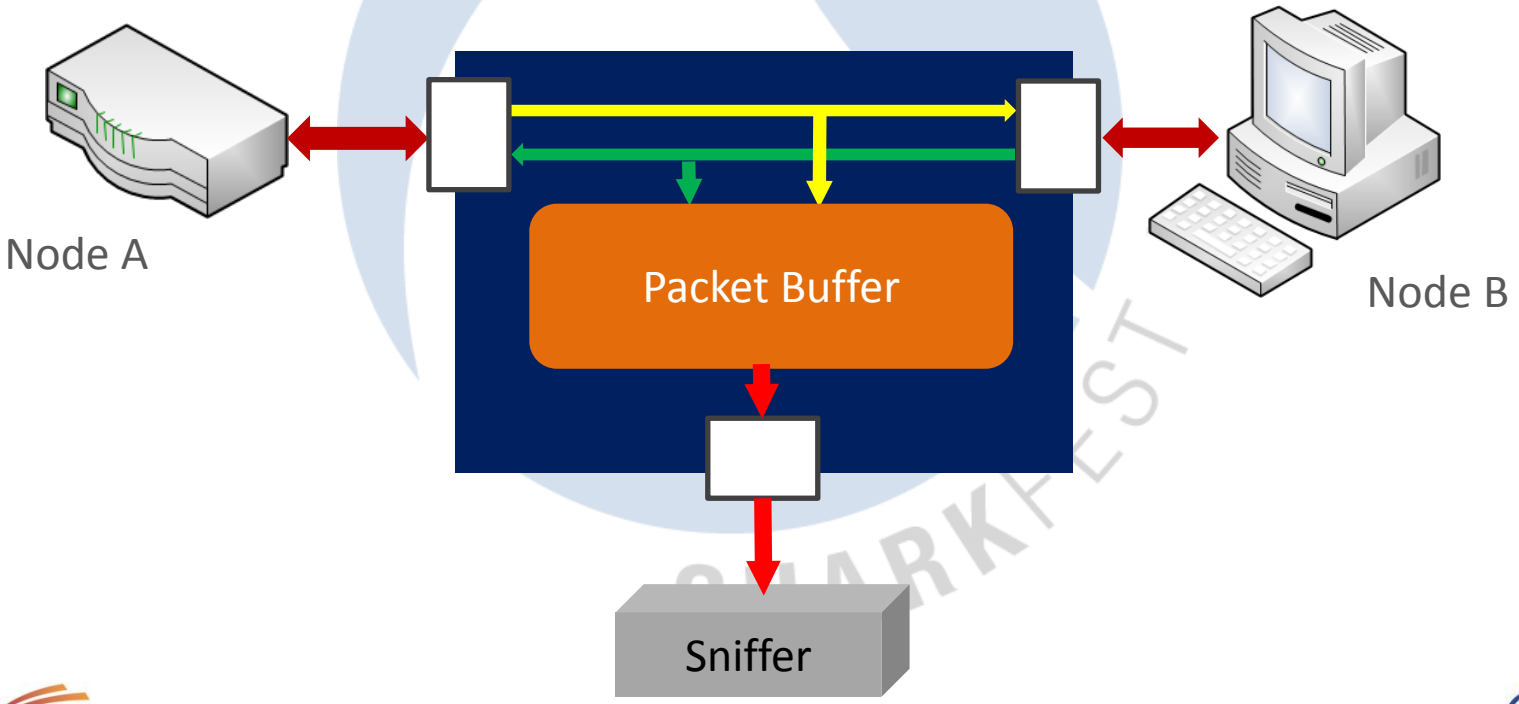
Can SPAN be Made Free of Over-Subscription?

- SPAN can be implemented as shown below to avoid dropping packets.



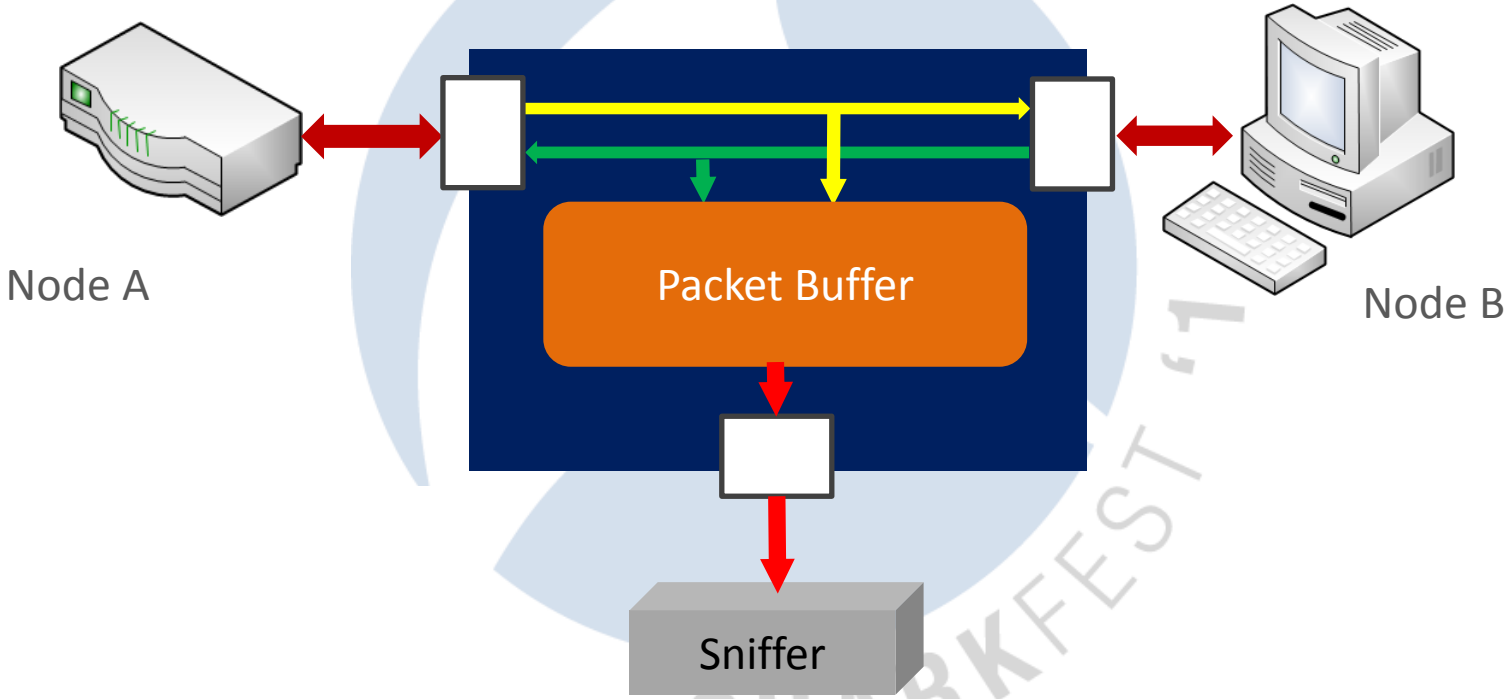
Does TAP Drop Packets?

- TAP with two separate receive channels: No
- Aggregation TAP: YES.



Does TAP Cause Packet Delay?

- Aggregation TAP: YES .
- An aggregation TAP causes even longer delay than a switch does as its packet buffer is usually much larger in size (e.g., >512MBytes) than that of a switch.



[Example] (worst case estimate)

For an Aggregation Tap with a 512MByte buffer at 100Mbps, the delay could be: 512M*8/ 100M = 40.96 seconds

Does SPAN affect timing?

- Does It Matter? Probably not.
- Ethernet is NOT a TDM based technology.
- Ethernet is still a best-effort delivery technology.
- Latency and jittering introduced by SPAN is negligible compared to the overall delay budget.

[Example]

Voice: A 150~200 ms one-way (mouth-to-ear) delay budget is acceptable for high voice quality.

Delay/Jittering caused by a switch: < 8 ms (worst case @ 100M)

Is TAP Useful in Troubleshooting L-2 Errors?

- Probably not much.
- TAP does pass L-2 Error packets, but it can not tell who causes the problem.
- Even if TAP passes L-2 error packets, most packet analysis tools (e.g., WireShark) may not able to see them. (more on next slide).
- Tapping is intrusive. Inserting a TAP may make otherwise real L-2 errors "disappear", or may cause L-2 errors by itself.
- A more straightforward approach is to read error counters from two end devices to identify and understand the nature of root causes.
- Conclusion: TAP is not meant to be a tool for capturing and trouble-shooting L-2 errors.

Can WireShark Capture L-2 Errors?

Q 7.9: How can I capture packets with CRC errors?

A: Wireshark can capture only the packets that the packet capture library - libpcap on UNIX-flavored OSes, and the WinPcap port to Windows of libpcap on Windows - can capture, and libpcap/WinPcap can

configured, configure it if necessary and possible, and make whatever changes to libpcap and the packet capture program you're using are necessary, if any, to support capturing those packets.

Most OSes probably do **not** support capturing packets with invalid CRCs on Ethernet, and probably do not support it on most other link-layer types. Some drivers on some OSes do support it, such as some Ethernet drivers on FreeBSD; in those OSes, you might always get those packets, or you might only get them if you capture in promiscuous mode (you'd have to determine which is the case).

http://www.wireshark.org/faq.html#q7.9

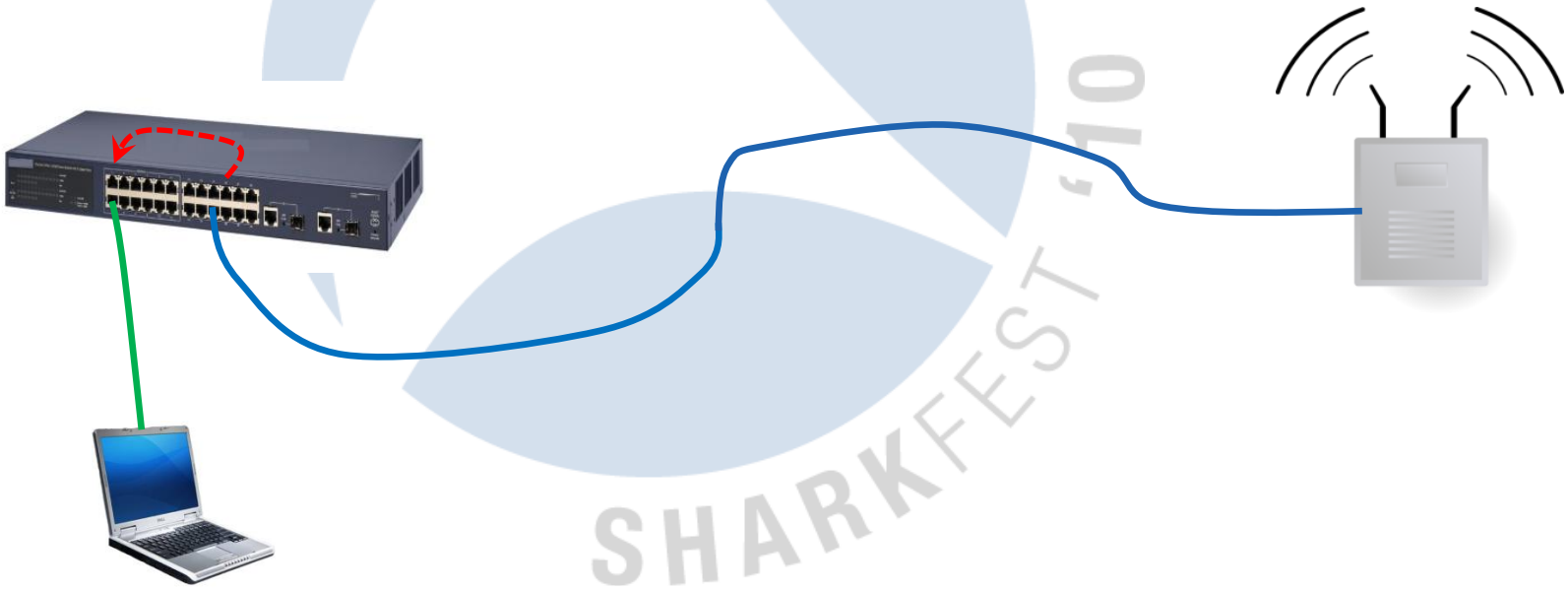
Is SPAN Not as Reliable/Predictable as TAP?

- Most switch vendors implemented SPAN in their switches more as a “nice to have” feature. Its priority is lower than forwarding “revenue” packets.
- What people complained about SPAN are just “bad” implementations of SPAN, not the theory of operation of SPAN.
- SPAN can be technically implemented as reliable and predicable as TAP in mirroring packets.

SHARKFEST '10

The Real Headaches of SPAN

- Therefore, merely comparing TAP with SPAN on technical aspects would not reveal the real headaches of SPAN.



SHARKFEST '10

Headaches of Using a SPAN Port?

The headaches of using a SPAN port come from the operational aspects.

- ☒ It need authorization/approval to change configuration.
- ☒ There are risks that a switch may be mistakenly configured, and things are messed up.
- ☒ It may be hard or not convenient to access the switch.
- ☒ No spare port is available as a mirroring port.
- ☒ You don't know what you will get as each switch is vendor dependent.

SPAN: Root Cause of the Headaches

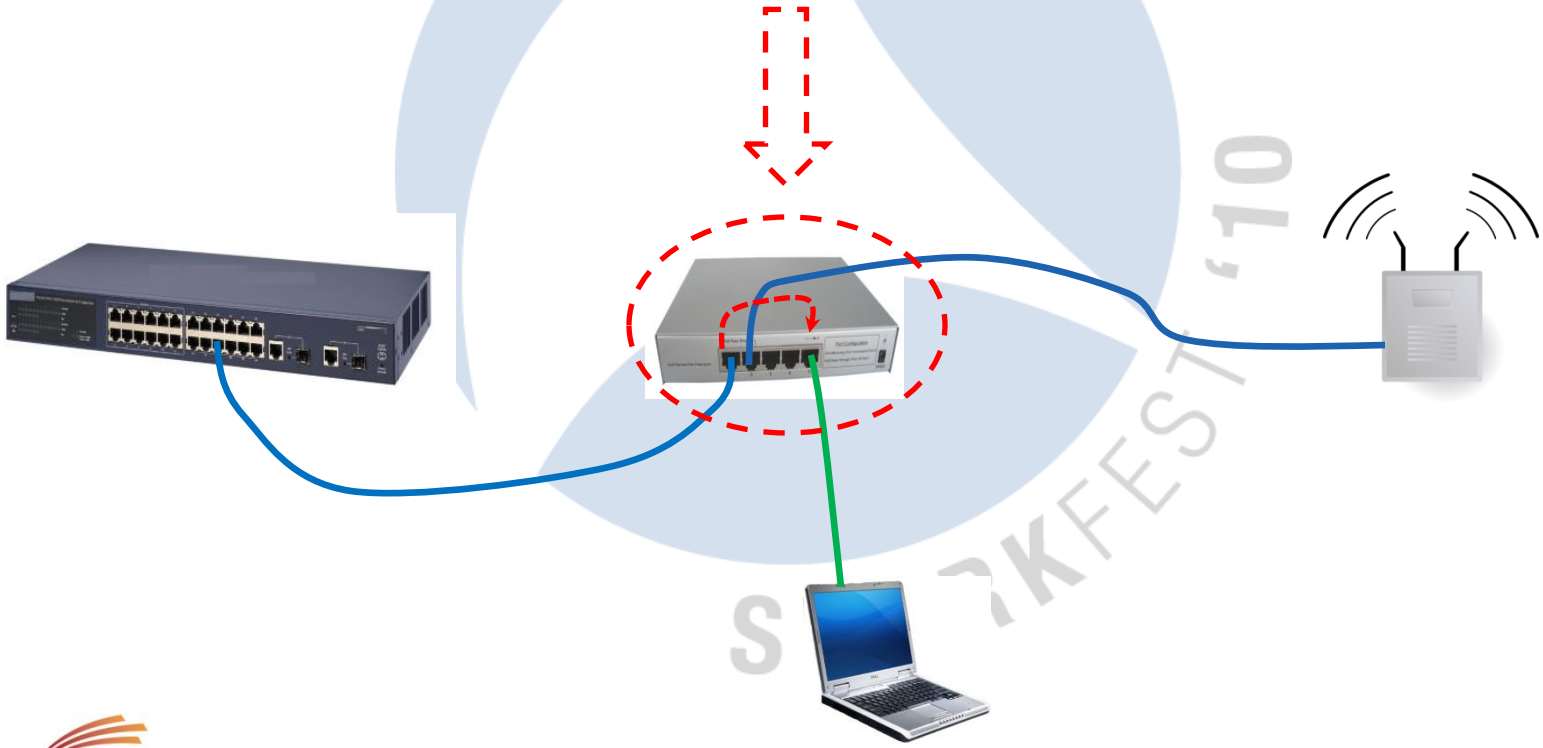
- TAP does not have such operational headaches that SPAN does.
- A simple fact: TAP operates outside a switch box, and SPAN is conducted inside a switch box
- The headaches are not what SPAN does, but where it does.

SHARKFEST '10

Thinking Out of the Box!!!

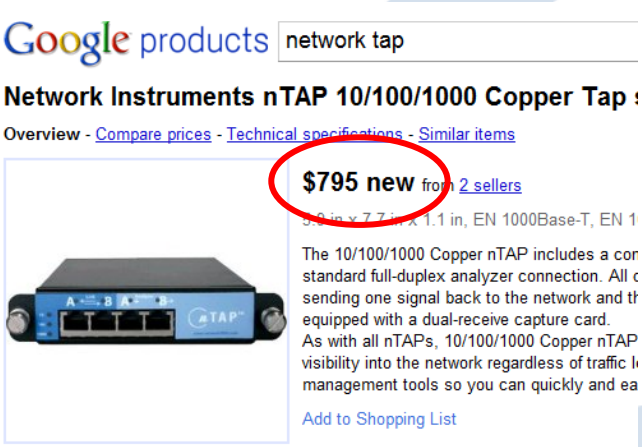
Solution: SPAN Out of the Box (SOB)

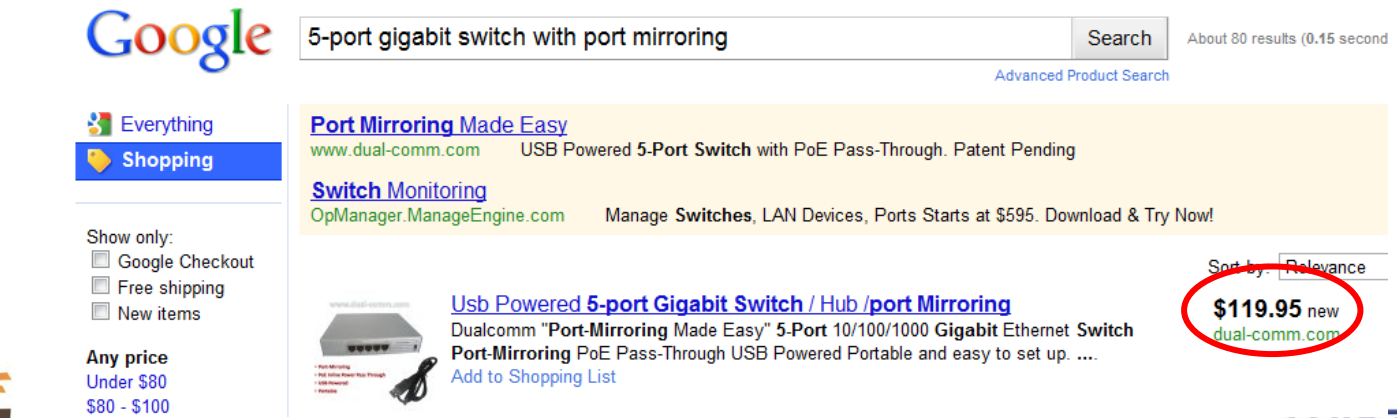
- Use an eternal switch device to do SPAN outside the main switch box, just like using a TAP.



Why Not Just Use a TAP instead? (1)

- Price, Price and Price.





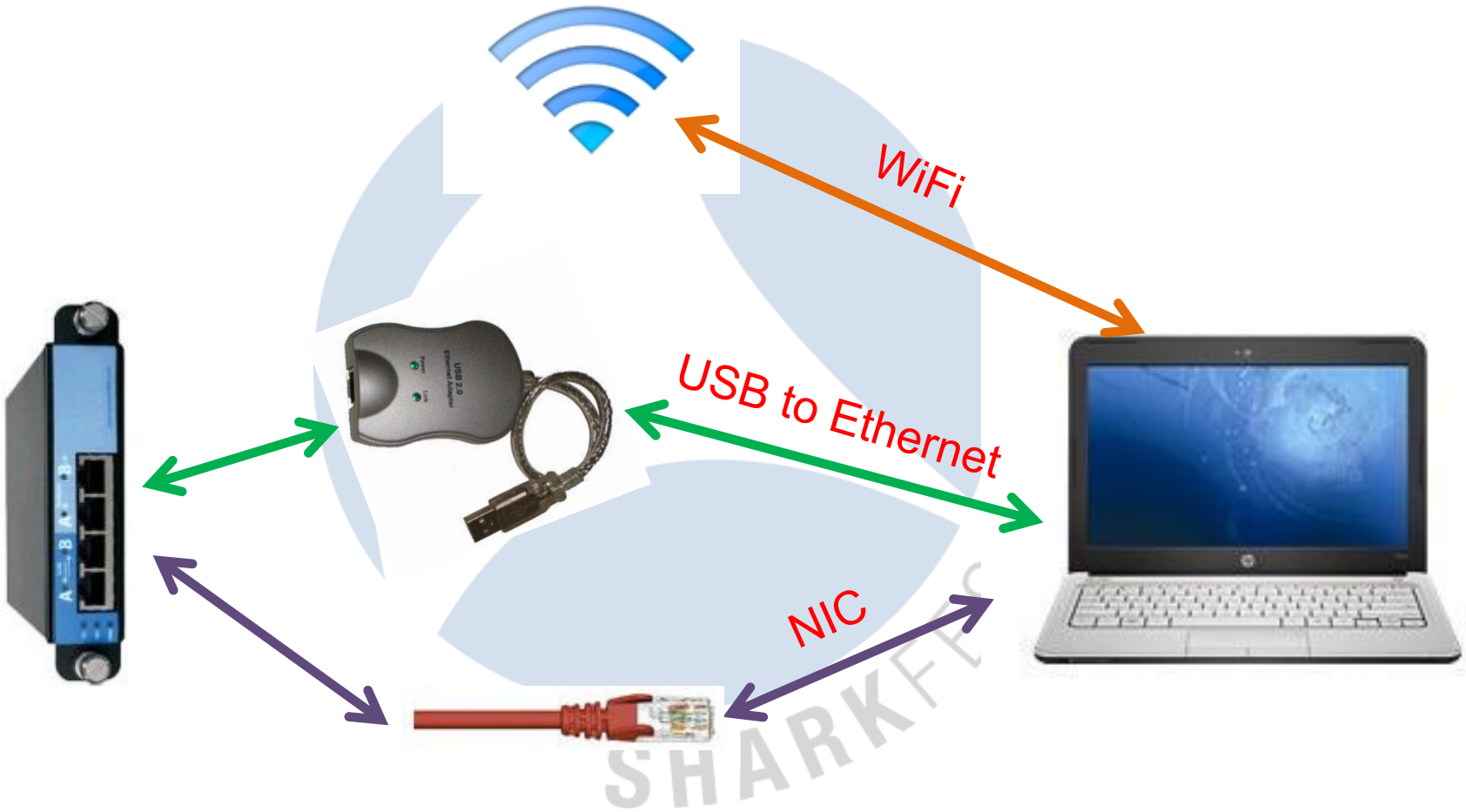
Why Not Just Use TAP instead? (2)

- Usability, Usability, Usability.

You may need a computer with three network ports (NICs) in order to use a TAP to capture packets.

1x for TX channel from the TAP
1x for RX channel from the TAP
1x for accessing the network.

Tapping with Laptop



Using a Managed Switch for SOB?

- For a web managed switch, you have to figure out what the IP address the switch is assigned dynamically (DHCP) in order to configure and enable a SPAN port.
- Hard to find a managed switch that is small and portable.

SHARKFEST '10

“Port Mirroring Made Easy” Ethernet Switch for SOB

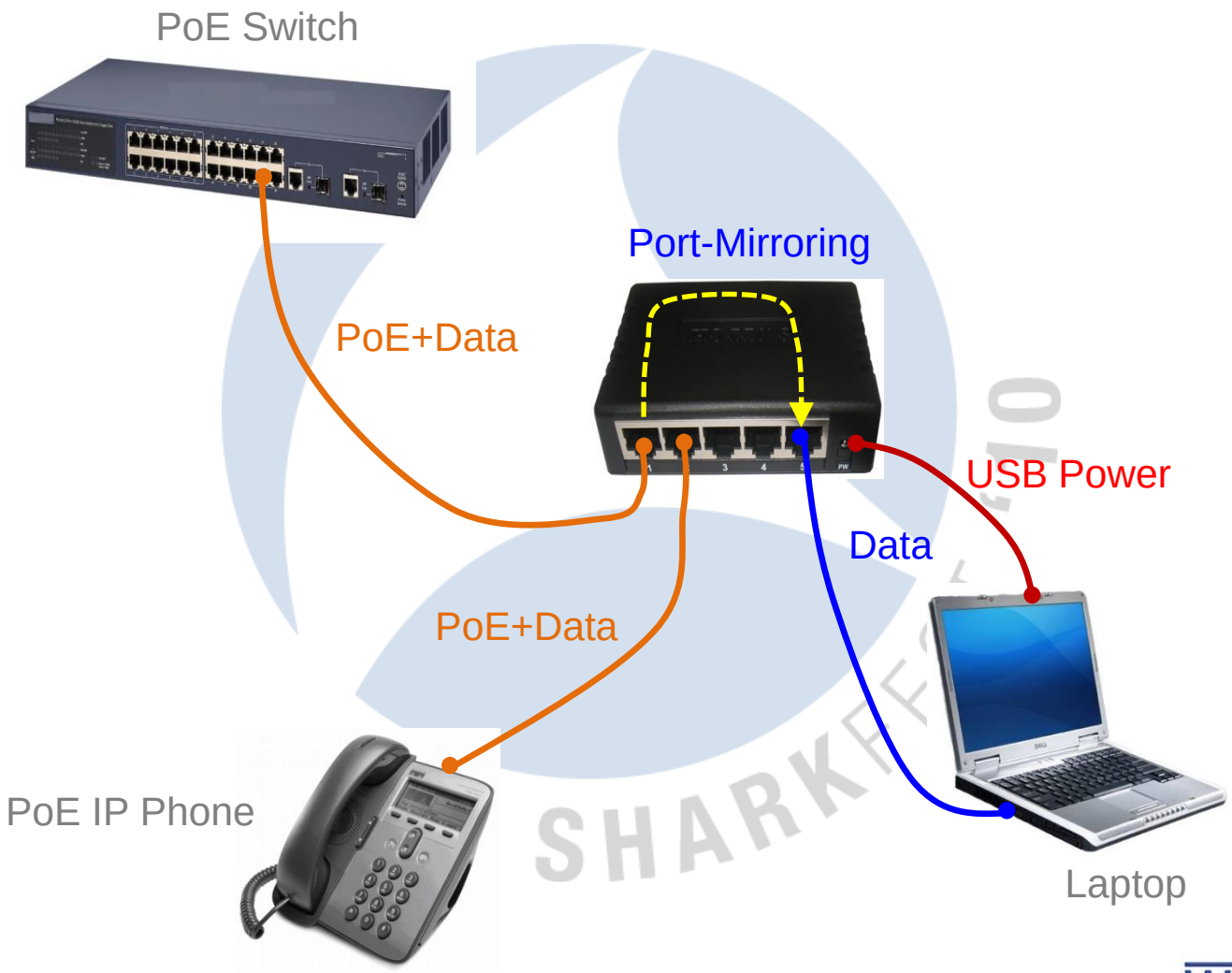
- A small portable 5-port Ethernet Switch.
- “Hard-wired” mirroring port. Plug & Play. No software configuration is needed.
- IP address-less. Non-addressable network device.
- USB powered.
- Support PoE inline power pass-though.

10/100 Model

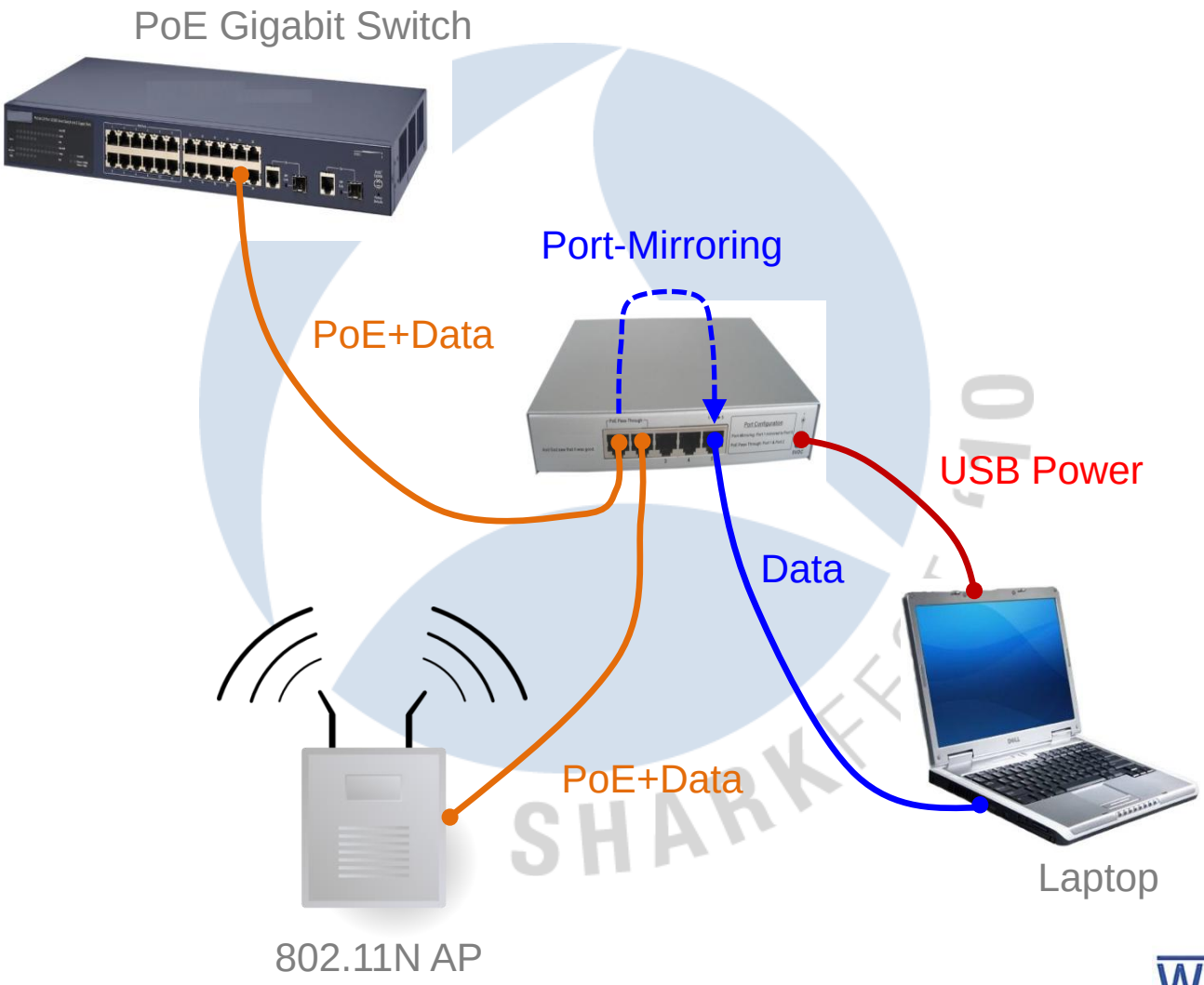
10/100/Gigabit Model

SHARKFEST ‘10

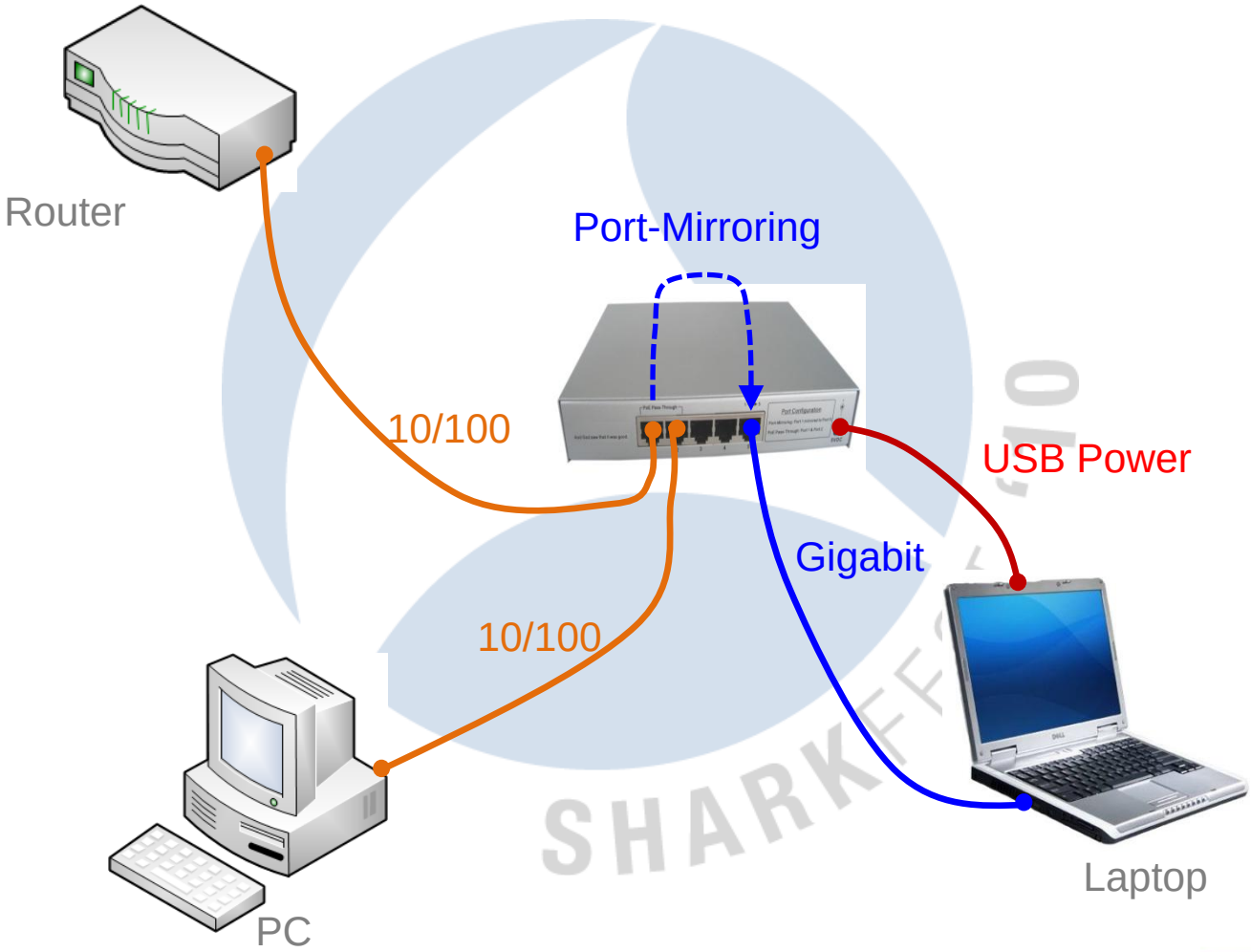
Use Case Example: Probing IP Phone Traffic



Use Case Example: Probing Wire Side Traffic of AP



Use Case Example: Avoiding Port Oversubscription

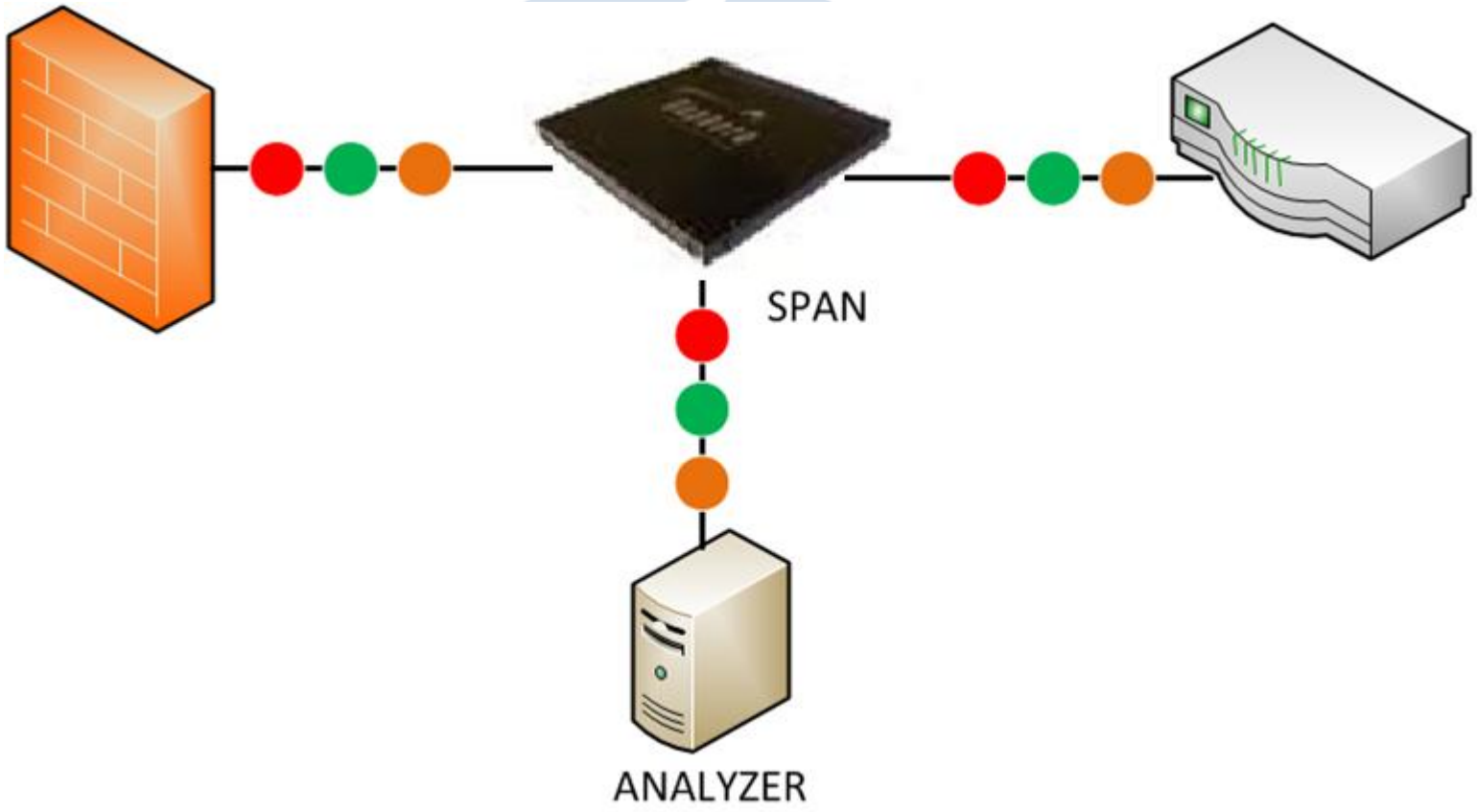


SOB for 10G Systems (1)

- The “SPAN Out of the Box” approach can be applied to 10G systems.
- Converting a 10G Ethernet switch dedicated for capturing traffic applications is becoming cost-effective because of the availability of low-cost 10G switching SOC.
- For example, a Sub-$10K multi-port SFP+ 10G Ethernet Switch is currently available that can be converted to a 10G traffic monitoring TAP switch.

SHARKFEST '10

SOB for 10G Systems (2)



Summary

- The headaches of SPAN are not what SPAN does, but where SPAN does.
- Comparison of TAP vs. SPAN merely on technical aspects does not reveal real headaches of SPAN.
- “SPAN Out of the Box” is best used as a portable packet sniffing solution for troubleshooting. It can alleviate most of operational pains of using SPAN.

SHARKFEST '10

Contact Us

Please contact us by email or phone if you need more information or have any questions.

Dualcomm Technology, Inc
Email: info@dual-comm.com
Phone: (925) 658-4824

Thank You

SHARKFEST '10