Problem Solving Via Network Packet Capture and Analysis

About Me

I work as an independent consultant performing system and small network administration, and writing specialized technical documentation.

I have used network packet capture and analysis for problem-solving since 1979.

Outline

Some History

Capturing Packets

Analyzing Captured Packets

Some History

- 1979: Serial Point-to-Point
- 1980: Ethernet Specification released (DIX)
- 1983: Ethernet products widespread
- 198x: Early Ethernet Capture Tools
- 1998: Ethereal/Wireshark
- 2005: 802.1Q VLAN tagging

circa 1979

- MOP
- DDCMP
- HP 1640B
- Distributed laboratory data acquisition and control system. Two semi-redundant hosts, 30 remote data concentrator systems

The HP 1640B


DISPLAY
FORMAT
MODE
LIST
EXECUTE
CURSOR
RUN
DEFAULT
STOP
PAUSE
ENTRY
CONT
INSERT
DELETE
SELF TEST COMPLETE
DATA CODE
MODE
BITS/SEC
ERROR CHECK
LINE
1640B SERIAL DATA ANALYZER
HEWLETT • PACKARD
OTHER = B = EBCDIC

circa 1988-89

- Ethernet is 8 years old
- 10Base2 (thinwire coax) becomes practical
- Network General Sniffer
- LBL tcpdump
- Meridian Technology Lanmon

1998 – Wireshark Begins

- Ethereal introduced
- Becomes WireShark in 2004

2005: 802.1Q VLAN tagging

32-bit field between addresses and Ethernet protocol type.

Usually used on trunk connections

802.1ad double tagging out of scope

Variable support in device drivers

Packet Capture

Same Device

Port Mirroring

Device Insertion

ARP Spoofing (IP Only)

Same Device

Wireshark if you have it

tcpdump

tshark

Any Wireshark compatible tool

Port Mirroring (Cisco SPAN)

Duplicates packets from one port to another

Any managed switch worth having

Some routers: RV320 ($120)

Prepare in advance -

- Every connection via managed switch
- Extra line from mirror port to your desk

Device Insertion

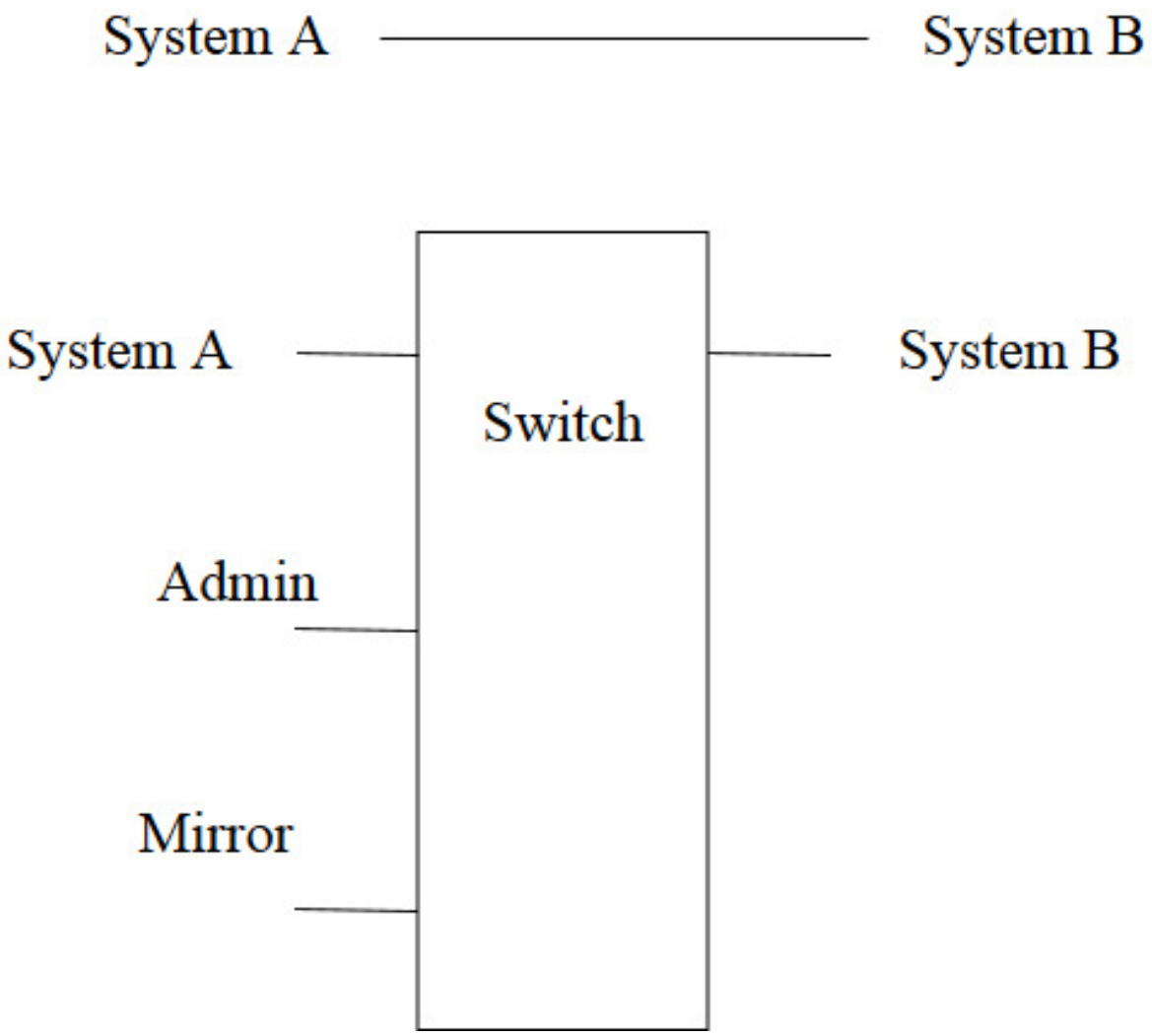
10 Mb Hub – old, old school

Purpose-made Tap – Expensive

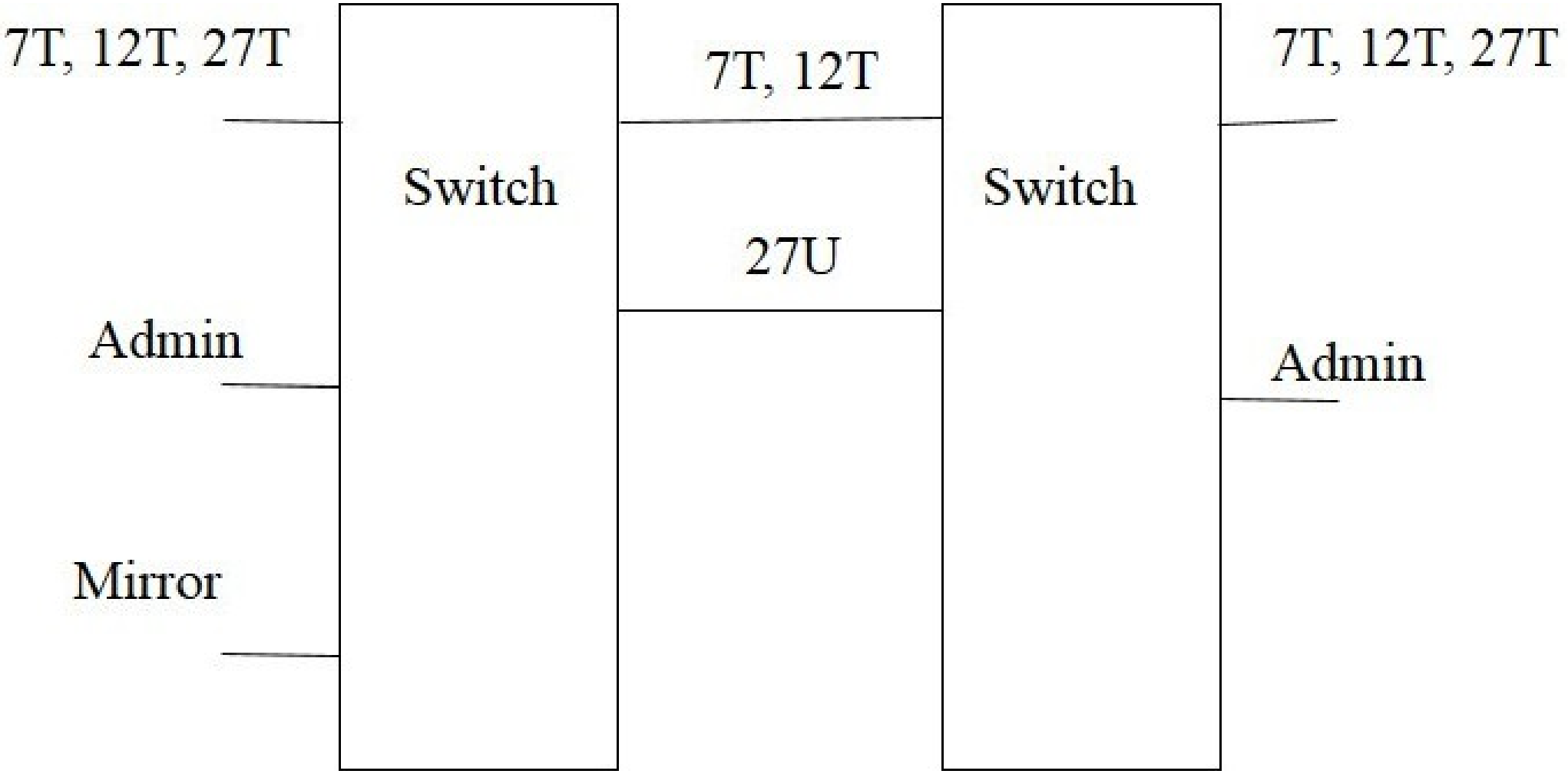
A small managed switch -- or two

Netgear GS305E < $40

One Switch



Two Switches



Packet Analysis

Use Wireshark

Get it from your distribution package

Exception: when tcpdump one-liner is enough

Packet Analysis

No free Lunch …

- Need some knowledge
- Research sometimes required

But Wireshark does the grunt work.

Some problems are easy.

Examples

Ping

Email submission

ARP Spoofing (if time permits)

Questions?

Problem Solving Via Network Packet Capture and Analysis