Advanced diagnostics in a White Rabbit network

Greg Daniluk, Adam Wujek

1st White Rabbit Tutorial Workshop
7 October 2017
Barcelona, Spain

How to diagnose WR network

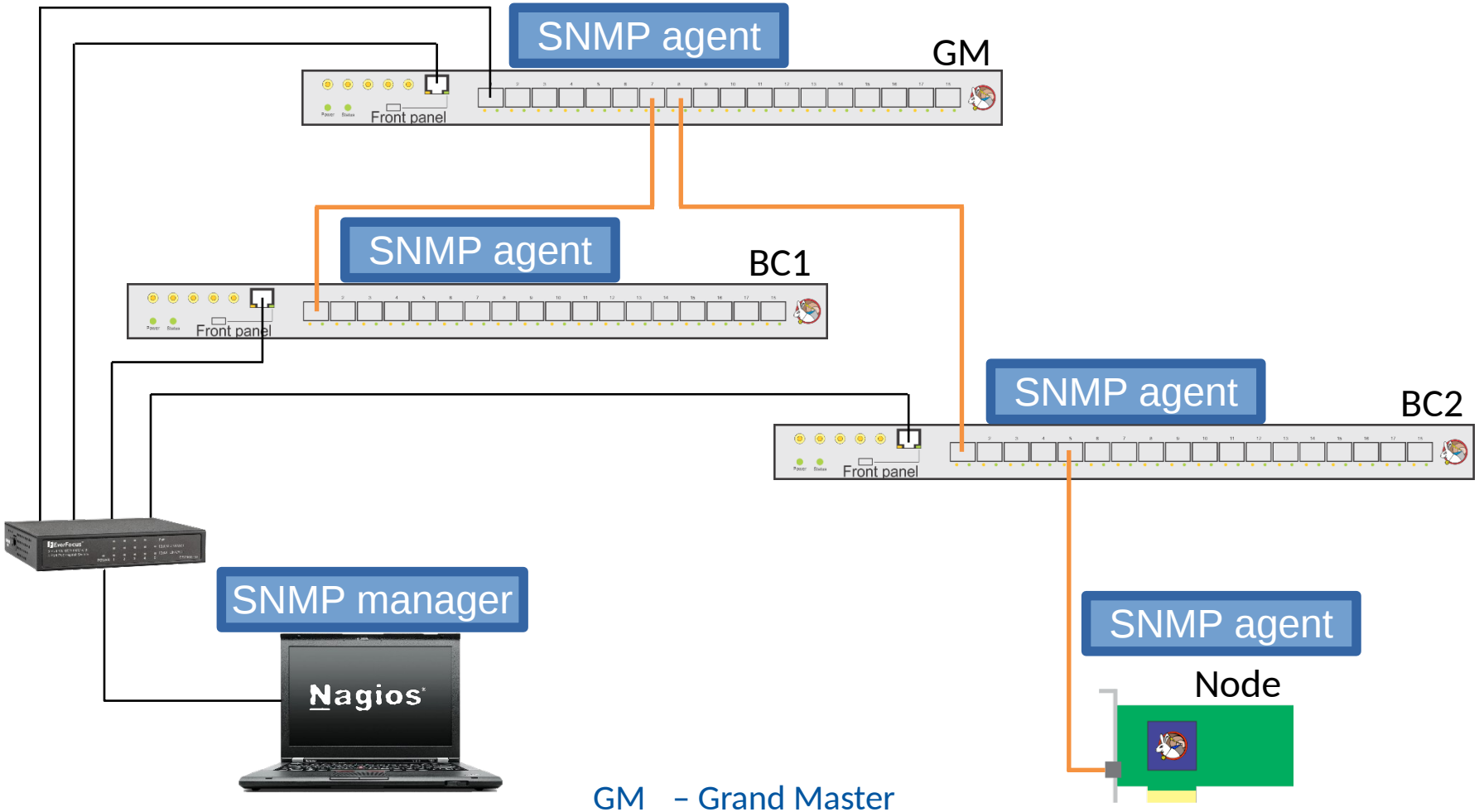
- White Rabbit is an extension of Ethernet
- It can be diagnosed using standard protocols and tools:
  - Simple Network Management Protocol (SNMP)
  - Syslog
  - Link Layer Discovery Protocol (LLDP)
  - Wireshark

What is SNMP

- Standard for monitoring off-the-shelf switches, routers, time servers, etc.
- Request-response architecture
- SNMP manager queries SNMP agents
- SNMP agents export information as Object IDs (OIDs)

- SNMP agents: WR Switches, WR Nodes
- SNMP manager: regular computer with monitoring software
  - e.g. open source Nagios or Icinga

White Rabbit test network



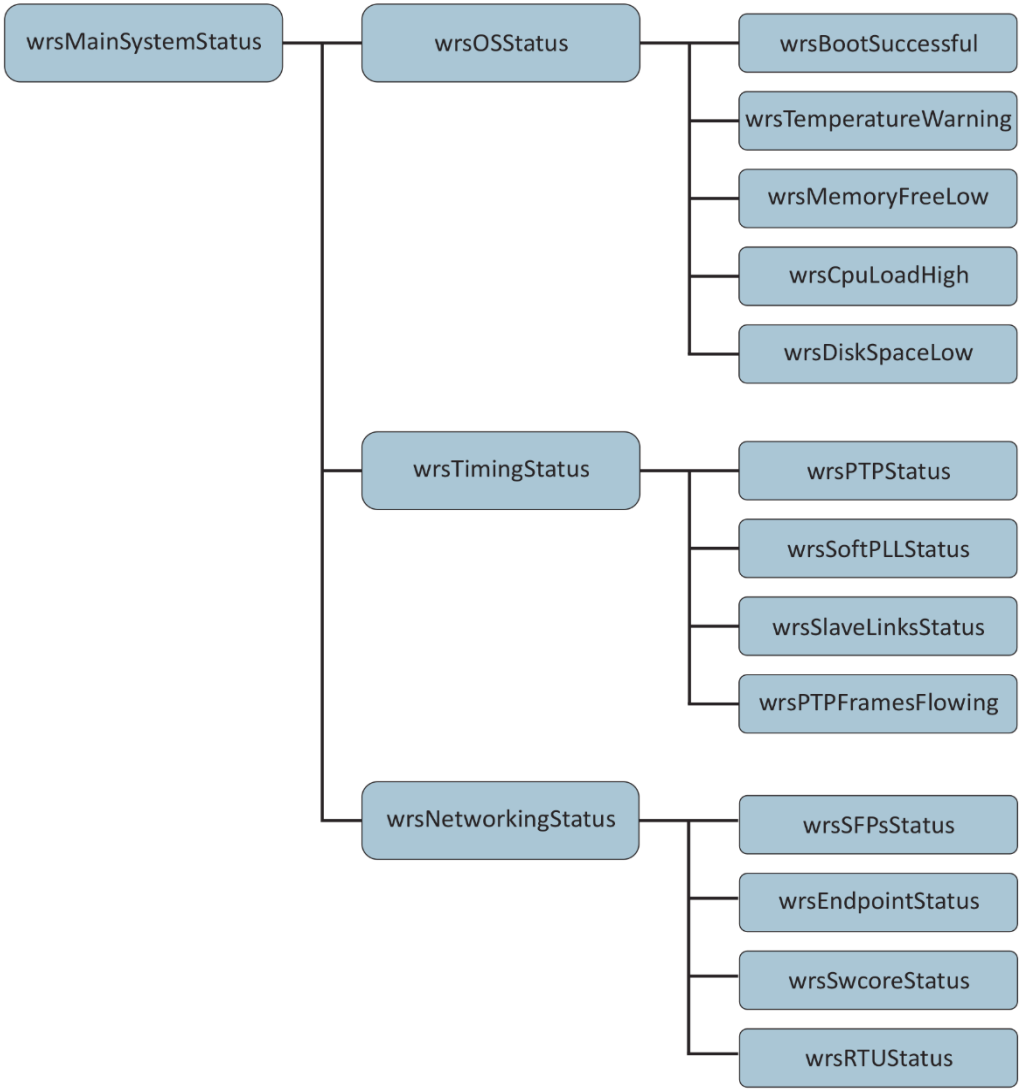
GM – Grand Master
BC – Boundary Clock

WR Switch agent

- Provides collective status for operators
- SNMP status tree

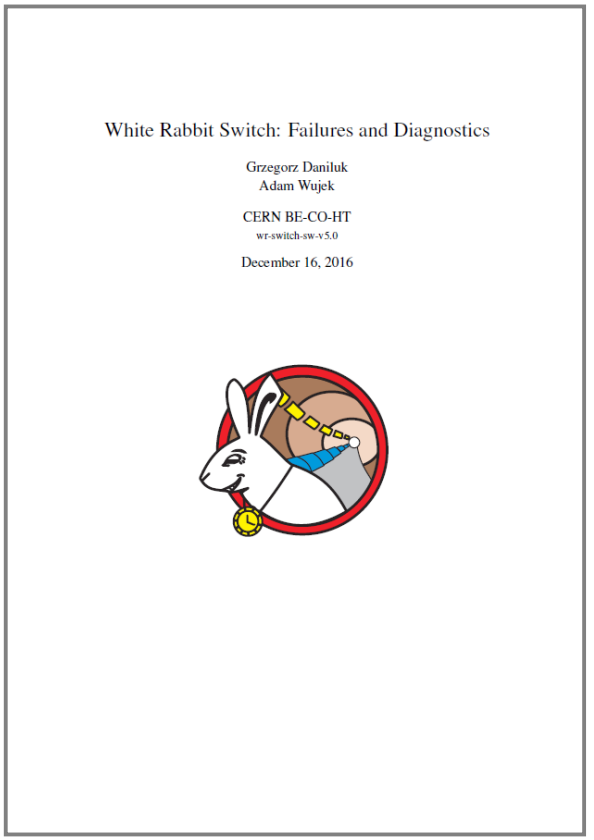
- Exports raw values for White Rabbit experts

WR Switch SNMP status tree



WR Switch: Failures and Diagnostics

- Document published with WR Switch firmware release
- Lists various errors reported by a switch
- Analyses problems that cause the error
- Proposes actions to mitigate problems


White Rabbit Switch: Failures and Diagnostics

Grzegorz Daniluk
Adam Wujek

CERN BE-CO-HT
wr-switch-sw-v5.0

December 16, 2016

WR Switch: Failures and Diagnostics

- Example:

* `wrsSFPsStatus`

Description: Reports the status of SFP transceivers inserted to the switch. `Error` when any of the SFPs reports an error. To find out which SFP caused the problem check `wrsPortStatusSfpError.<n>`.

On error:

1. Check `wrsPortStatusSfpError.<n>` SNMP objects or Syslog messages to determine the WR port on which the problem is reported. In case of Syslog, you should see a message similar to this one:
   `Unknown SFP vn="AVAGO" pn="ABCU-5710RZ" vs="AN1151PD8A" on port wri2`
2. If the reported port is intended to be used with WR not compatible equipment (e.g. using a copper SFP module), to avoid SNMP errors set this port to *non-wr*. To disable PTP traffic on this port set it to *none*.
3. Otherwise, you should use a WR-supported SFP module and make sure it is declared together with calibration values in the WRS configuration.

Related problems: 3.1.10, 3.3.9

WR PTP Core SNMP agent

- Very minimalistic SNMP implementation
- SNMP agent does not analyze errors
- There is no status tree like for the WR Switch

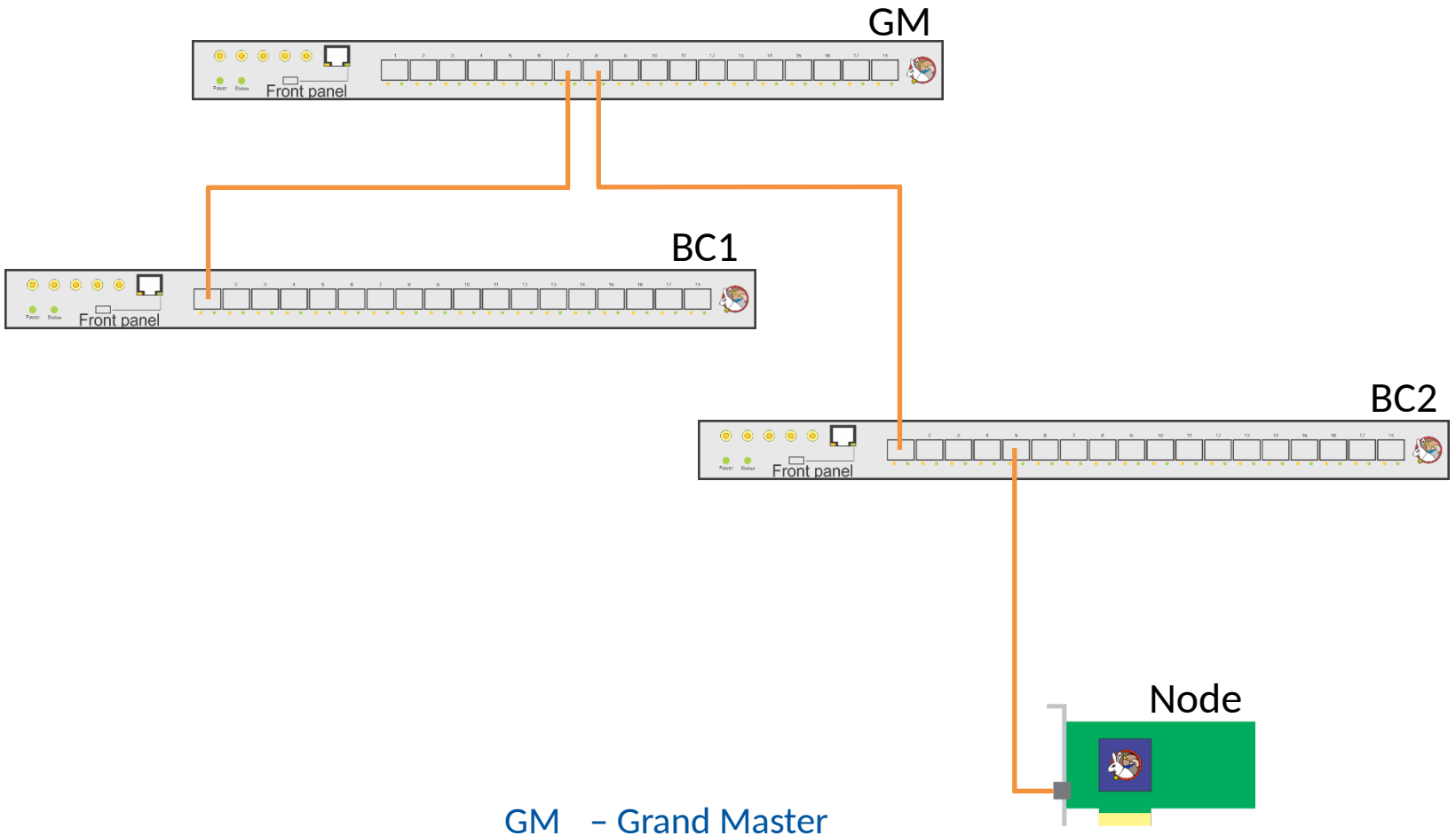
- Exports only raw values
- SNMP manager has to analyze errors according to the instructions in: *"WR PTP Core: Failures and Diagnostics"*

Syslog

- Computing standard for message logging
- WR devices send text messages to a configured server

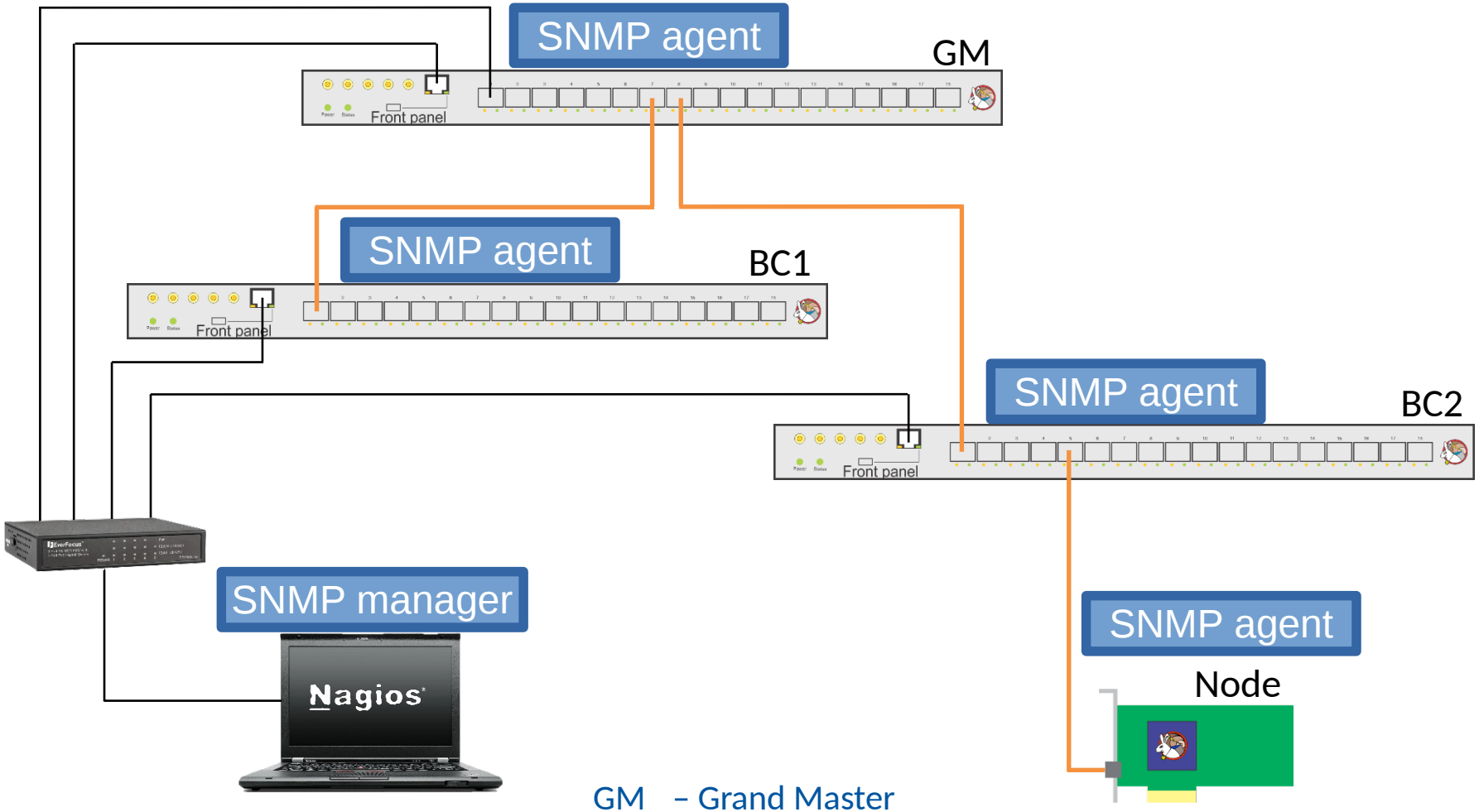
- Should be used with SNMP for WR network diagnostics
- Provides more information about the problem cause

SNMP and Syslog demo



GM – Grand Master
BC – Boundary Clock

SNMP and Syslog demo

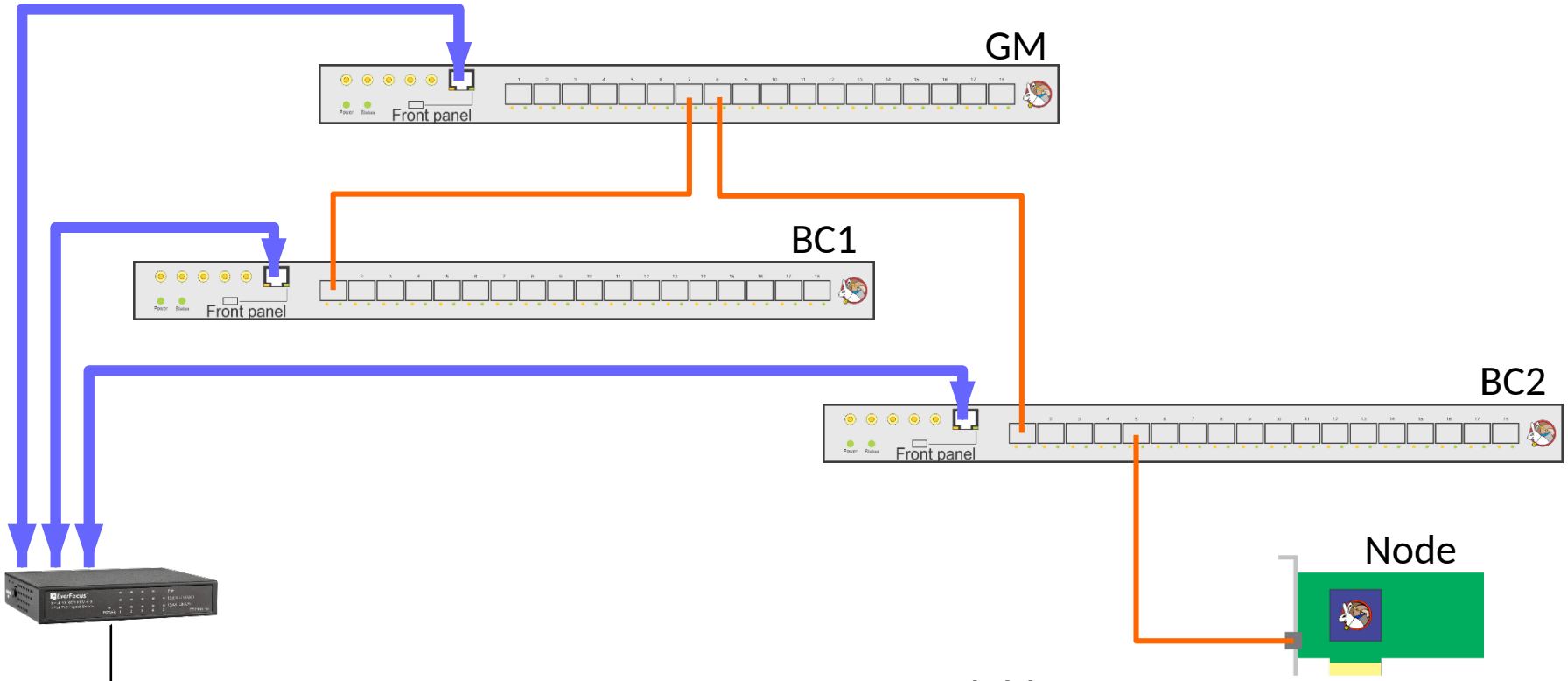


GM – Grand Master
BC – Boundary Clock

Link Layer Discovery Protocol (LLDP)

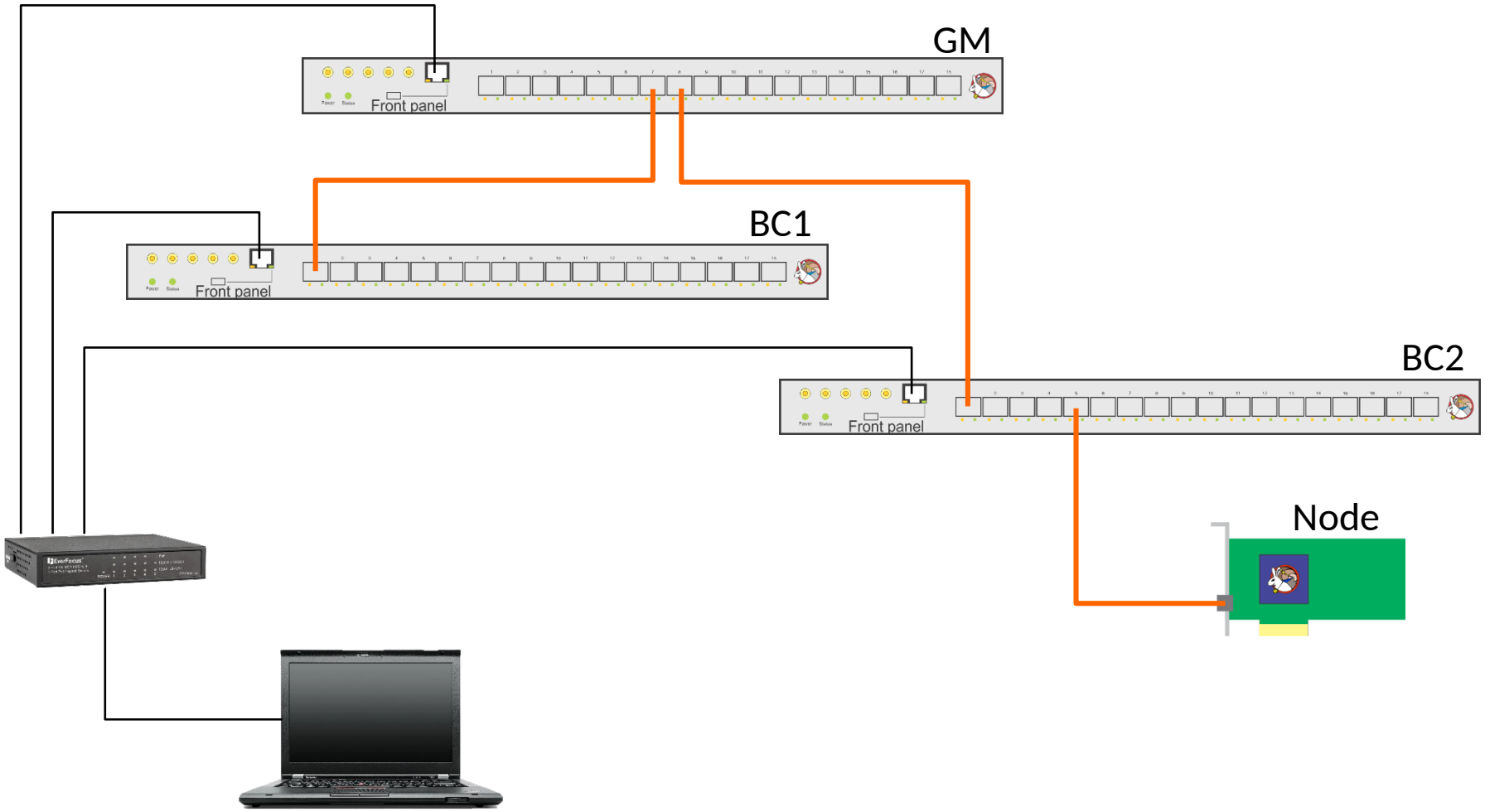
- Layer 2 protocol defined in IEEE 802.1ab
- Used to discover neighbors
  - Only directly connected
- All information is sent in one packet with information like:
  - System name
  - Chassis ID and description
  - Port ID and description
  - Time To Live
- Possible to discover a network topology
  - Starting from a device/switch
  - Traverse a network via SNMP to get all LLDP stored data

Link Layer Discovery Protocol (LLDP)



MON: GM, Any Neighbors?
GM: Yes, BC1 on port 7 and BC2 on port 8
MON: BC1, Any Neighbors?
BC1: Yes, GM on port 1
MON: BC2, Any Neighbors?
BC2: Yes, GM on port 1 and Node on port 5

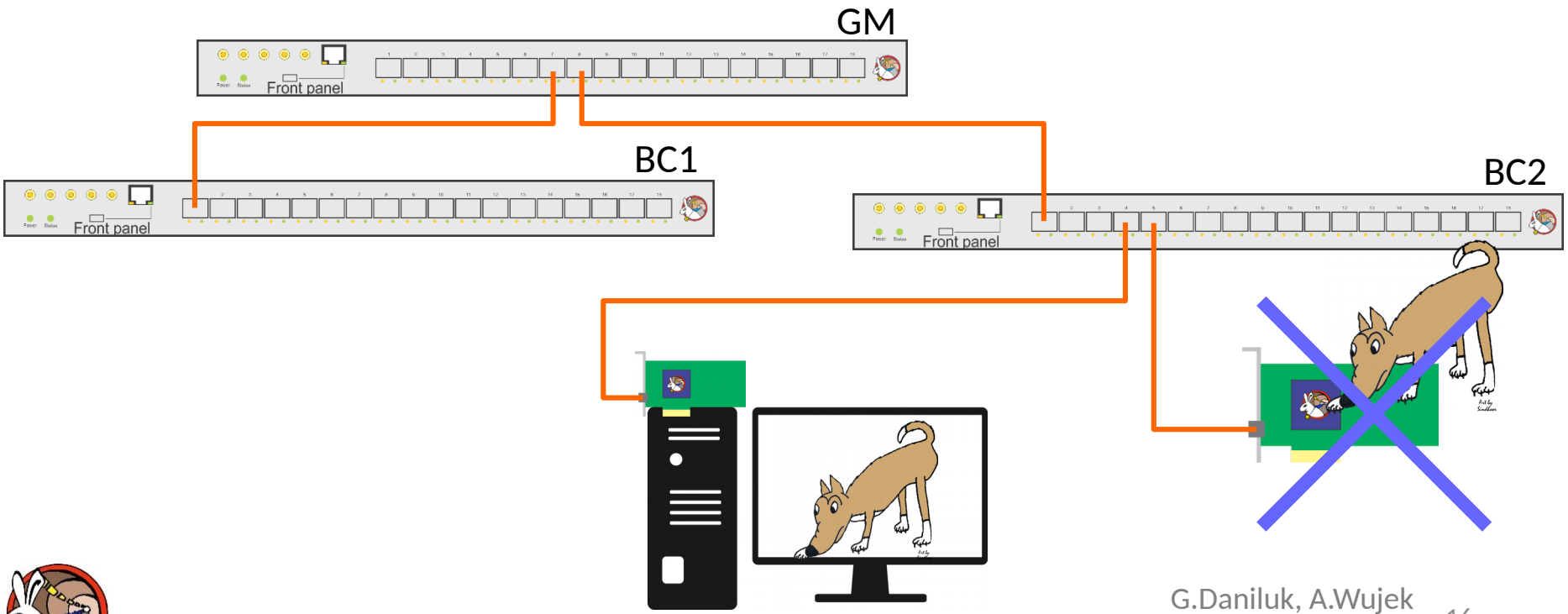
Demo network topology



Analyzing a traffic in a WR network

Running sniffer on a WR node

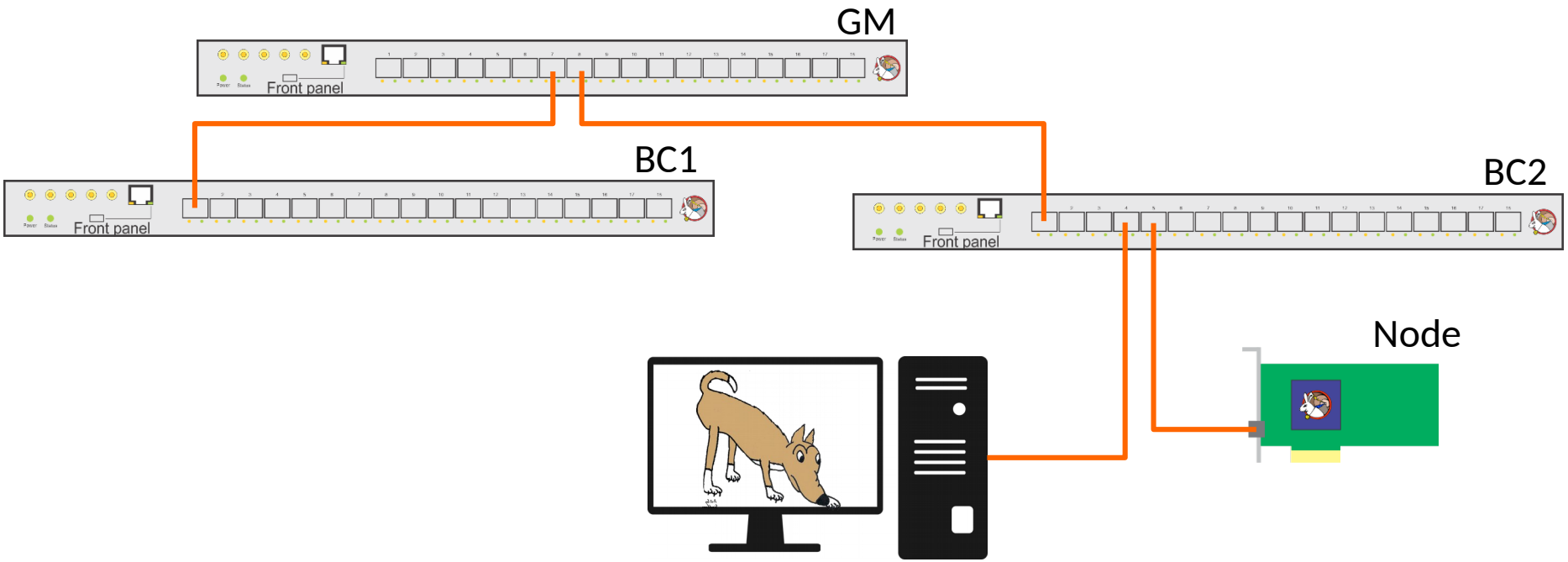
- Not enough resources on WRPC
- Possible to forward traffic to the host
  (refer to the WR-NIC project)
  - But not possible to mirror WR and SNMP traffic to the host



Analyzing a traffic in a WR network

Connect a host with a sniffer to another WR port

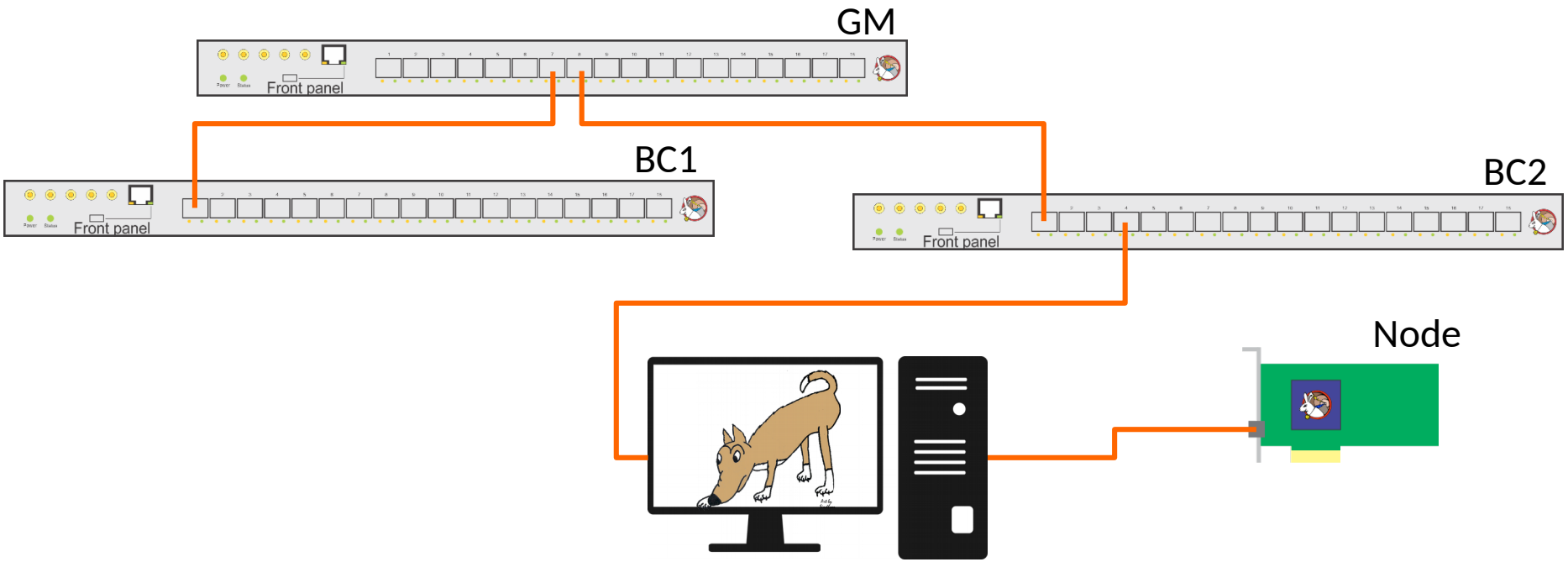
- Good for broadcast traffic
- … but not for WR traffic (which is link local)
- … or requires port mirroring on a switch
  (not implemented yet)



Analyzing a traffic in a WR network

"Men in the middle" sniffing

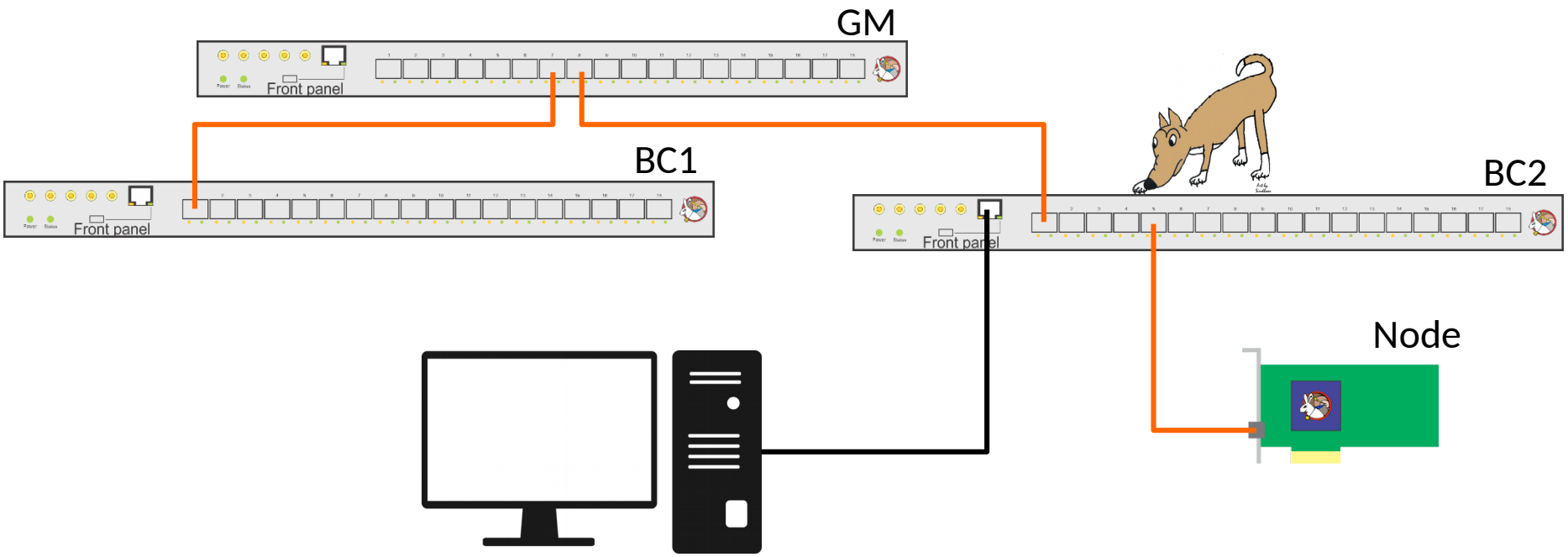
- Good for sniffing data streams
- WR synchronization disturbed



Analyzing a traffic in a WR network

Intercept WR traffic on a switch

- Good for WR traffic
- Not for sniffing data streams

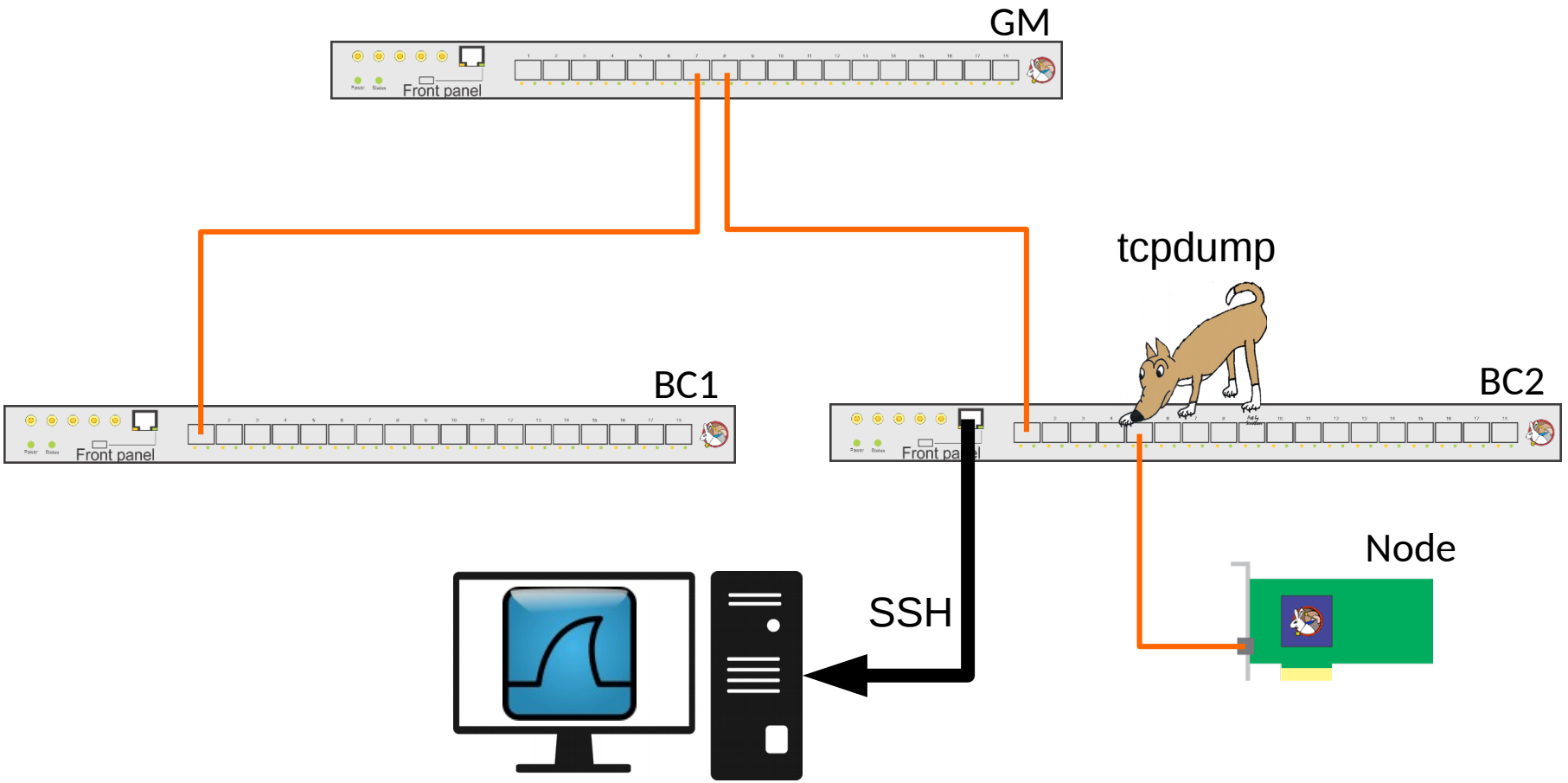


Wireshark

- Wireshark is the world's foremost and widely-used network protocol analyzer since 1998
- It lets you see what’s happening on your network at a microscopic level
- Live capture and offline analysis
- Deep inspection of hundreds of protocols, with more being added all the time
- Capable to dissect WR messages (not official)
- Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others

https://www.wireshark.org/

Wireshark Demo



Summary

- White Rabbit is an extension of Ethernet
- … thus can benefit from many existing standard tools
- WR network can be managed by an IT department
- Using standard protocols like SNMP and LLDP reduces new developments and the risk of vendor lock-in
- Introducing new users to WR network technology is much easier