Packet-Foo Network Capture Equipment Checklist

This checklist should be used before deploying a capture device in a reactive network capture situation. See the Packet Capture Playbook blog post series at https://blog.packet-foo.com for more information.

Pos.	Activity / Test	Pass/Fail/not appl.
1	Check device network card setup to match the capture plan (fiber, copper, link speeds, number of ports) for each capture device	☐ pass ☐ fail ☐ n/a
2	Check all SFPs are the right type and speed (if any)	☐ pass ☐ fail ☐ n/a
3	Check additional cabling present for each capture device (power cord, management network)	☐ pass ☐ fail ☐ n/a
4	Check that all required TAPs are available with the correct link speeds and physical connectors, including power supplies (if any)	☐ pass ☐ fail ☐ n/a
5	Check all additional cables are available to insert the TAPs and connect them to the capture device (usually 3: 1 for insertion, 2 for full duplex towards the capture)	☐ pass ☐ fail ☐ n/a
6	Start each capture system to verify if it boots correctly	☐ pass ☐ fail ☐ n/a
7	Check system clock to match current date and time	☐ pass ☐ fail ☐ n/a
8	Verify that the management IP is correct and working and RDP, SSH or VNC can be used to remote control the device (if required)	☐ pass ☐ fail ☐ n/a
9	Check that old PCAP/PCAPng files have been backed up and removed, freeing as much disk space as possible	☐ pass ☐ fail ☐ n/a
10	Run a test capture to see if the capture cards are identified correctly and work in the capture mode required for the task (e.g. link aggregation for full duplex TAP captures).	☐ pass ☐ fail ☐ n/a
11	Make sure all sleep/standby functionality is disabled (BIOS and OS) and that the system runs on maximum performance settings	☐ pass ☐ fail ☐ n/a
12	Verify that you have a working restore CD / USB device to recover each capture device OS onsite without Internet access in case of trouble	☐ pass ☐ fail ☐ n/a
13		☐ pass ☐ fail ☐ n/a
14		☐ pass ☐ fail ☐ n/a
15		☐ pass ☐ fail ☐ n/a

Additional comments: _____

_____

_____

_____

Tests performed by: _____ Date & Time: _____

Signature _____