Network Capture Preparation Questionaire

	Location 1	Location 2	Location 3
General			
What is the purpose of the network capture? (e.g. cable test/bit error analysis/fault check, troubleshooting, performance analysis, baselining, creating a QoS profile,...)			
What is the target date deadline for the oral/written report?			
Who is the main project contact at the customer?			
Who is the main technical contact at the costumer?			
Who are the administrative contacts at the customer/3rd parties (e.g. for gaining access to data centers, configuring switches, etc.)			
Building/Site Access			
Which standards & regulations exist when trying to bring in capture equipment? (e.g. notification of plant/building security staff)			
What are the limitations when trying to get access to the data center?			
Are there any special security & accident prevention guidelines that need to be followed?			
Documentation			
Are there up-to-date network diagrams (physical, logical)?			
if not: is there someone available to explain the network infrastructure?			
if not: does the customer accept the risk of reduced quality caused by suboptimal capture location selection in the analysis report?			
What performance metrics of the network are documented (e.g. Round Trip Times, Protocol Distribution, Top Talker, Top Listener,...)			
Network topology			
What are the topologies that need to be captured? Fiber, Copper, 10/100/1000/10G/...			
if Fiber: what kind of connectors (LC, SC, ...) and what wave lengths are used (SX, LX,...)			
Capture locations			
How many capture locations are planned?			
How will the packets be captured (SPAN, TAP)?			
Is there enough resources at each capture location to deploy a capture system (rack space, power sockets with 24/7 power, what kind of voltage, what kind of power socket connectors)?			
What locations will be captured (Workstation, Router, LAN/WAN side of a firewall, server, loadbalancer,...)			
Are there NAT gateways or loadbalancers involved?			
Are there any QoS solutions, packet shapers or WAN accelerators involved?			
If using SPAN			
Is there anyone who can configure SPAN ports at all planned locations?			
If not: which switch types are being used (Vendor, model, firmware version)? Can anyone provide the administrative credentials?			
if credentials are unknown: at which date & time can a password recovery process be performed (Warning: this may lead to the device becoming temporarily unavailable)?			
if our analysts have to configure the SPAN port: is the customer accepting the risk of something going wrong (wrong port information given to analysts, switch misbehaving)?			

	Location 1	Location 2	Location 3
If using TAPs			
In case of fiber: what cable type is used (MultiMode, SingleMode)			
Where can the TAP be deployed? Is there enough power sockets (for copper TAPs) and room for the TAP to be placed into the rack?			
When can the TAPs be inserted and removed? Is a maintenance window required?			
Does the customer wish to buy the TAPs once inserted, to avoid having to remove them again?			
Project duration			
What is the time frame to capture & monitor the network (One time for a reproducable error/until a sporadic error occurs/long term network planning)			
for long term captures: how can the capture device be monitored during operation (e.g. remote access, manual local inspection)? Who will perform the monitoring?			
What amount of data is expected to be captured?			
How can the data be copied from the capture device while continuing the capture?			
Confidentiality of recorded data			
Do the captured packets contain sensitive information (personally identifiable information, classified information)			
Are there any rules & regulations that need to be followed (e.g. when analyzing email traffic)?			
What kind of information can only be kept in anonymized form in the analysis report (e.g. User IDs, IP addresses, workstation names,...)			
Is it possible to perform the analysis off-site? If not, additional travel costs may apply.			
if not: where and when can the analysis be performed?			
Does the customer wish to buy the hard drives with the packet captures after the analysis is complete?			
if not: what wiping procedures are required to deleted the packet data?			

Hint: The idea of this questionnaire is to have a guildeline of questions to ask the customer. It is not supposed to be handed over to the customer to be filled out. It should be used by the analysts during in an on-site meeting or in a conference call while planning the capture with the customer.