MCTSSA Cyber & Network Engineering Lab (MCNEL)

Industry Brief

Updated: January 2019

Capabilities

Deep Dive Packet Analysis for multiple purposes:

- Root cause analysis
- Network efficiency
- Application network profiles
- General network profiles/statistics

Capabilities

- Capture raw LAN-to-WAN traffic profiles for in-depth analysis (troubleshooting, optimization, forensics, baselining)
- Provide real-time analysis of aggregate flow to improve network efficiency
- Network health diagnostics and bandwidth consumption analysis
- Bandwidth over time (per enclave; aggregate and/or inbound vs outbound)
- DSCP/QoS markings
- Protocol distribution (e.g., TCP vs UDP, HTTP vs SMTP)
- Top ports (sources or destinations) and top IP talkers (clients/servers)
- TCP performance analysis (average round trip time, window size, errors

Facilities and Equipment

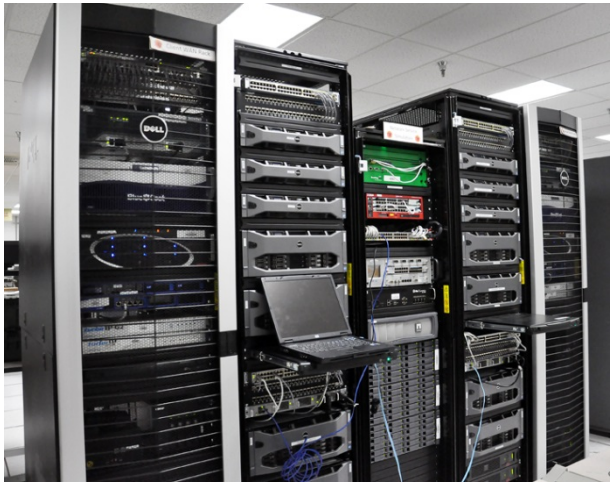
Network data capture and analysis

– nTAP

–Network Time Machine

– SteelCentral Packet Analyzer

– Wireshark



WAN link emulation

– Apposite Linktropy 7500 Pro

Test / Simulation tools (traffic generation)

– BreakingPoint Storm CTM

– Spirent SPT-3U

– Ixia Optixia XM2

Infrastructure as a Service (IaaS)

– OpenStack (private cloud)

MCNEL Problem

- Manipulating data captures is technically problematic
- Data captures or pcap merging has technical issues
- Resource intensive (commercial server capacity required)
- Time intensive (ties up personnel for long periods)
- Current vendor solutions are limited (HW/SW/Tools)
- Vendor solutions have a proprietary aspect (limits use)

Contact Information

MCNEL Team Lead

Billy Bertrand 760-725-2858 joseph.f.bertrand@usmc.mil

United States Marine Corps

0101010101101110011010010111010001100101011001000010000
0101001101110100011000010111010001100101011100110010000
0100110101100001011100100110100101101110011001010010000
0100001101101111011100100111000001110011000011010000101 0