Introduction to Network Monitoring and Management

Network Startup Resource Center

www.ws.nsrc.org



These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license (http://creativecommons.org/licenses/by-nc/4.0/)

Objectives

Introducing Core Concepts and Terminology

- The NOC: Consolidating Systems
- Network Monitoring and Management
- What and Why we Monitor
- Uptime Expectations and Calculations
- Baseline Performance and Attack Detection
- What and Why we Manage
- Network Monitoring and Management Tools
- Network Monitoring and Management 2.0

NOC: Consolidating NMM Systems

NOC = Network Operations Center

- Coordination of tasks, handling of network related incidents (ticketing system)
- Status of network and services (monitoring tools)
- Where the tools are accessed
- Store of Documentation (wiki, database, repository ==> network documentation tool(s))

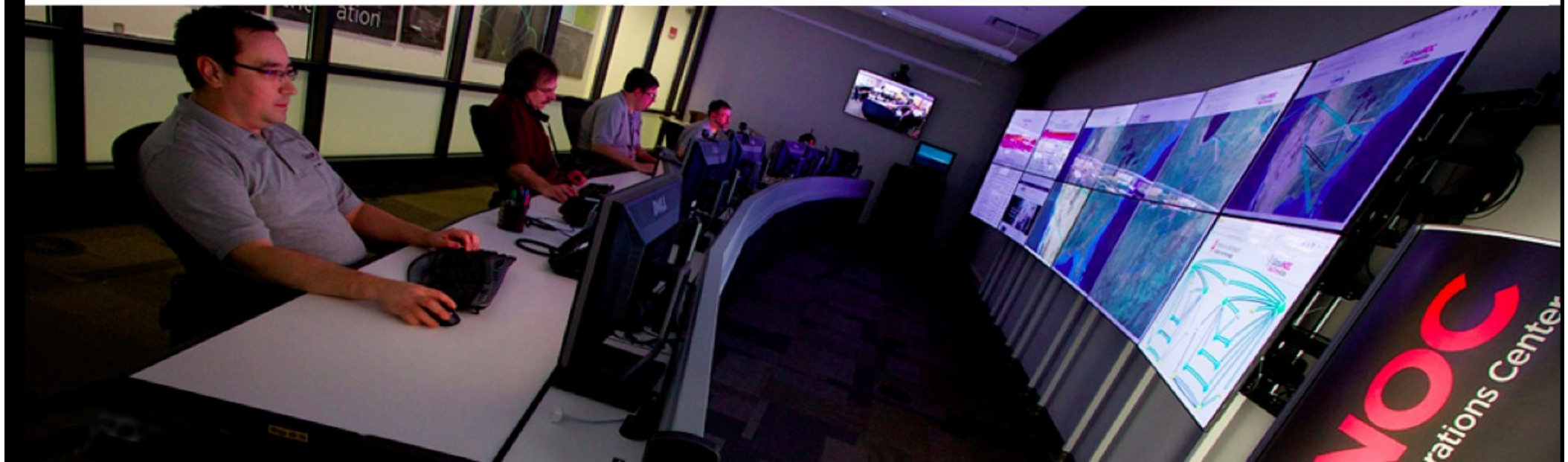
NOC: Consolidating NMM Systems

NOC Location

- NOC is an organizational concept
- Does not need to be a place, or even a single server
- Remote / Distributed NOC is valid with OOB Management







Network Monitoring & Management

Monitoring

- Check the status of a network

Management

- Processes for successfully operating a network

Monitoring Systems & Services

Systems

- Routers
- Switches
- Servers

Services

- DNS
- HTTP
- SMTP
- SNMP



What and why do we Monitor?

- Are Systems and Services Reachable?
- Are they Available?
- What's their Utilisation?
- What's their Performance
  - Round-trip times, throughput
  - Faults and Outages
- Have they been Configured or Changed?
- Are they under Attack?

What and why do we Monitor?

- Know when there are problems – before our customers!
- Track resource utilisation, and bill our customers
- To Deliver on Service Level Agreements (SLAs)
  - What does management expect?
  - What do customers expect?
  - What does the rest of the Internet expect?
- To prove we're delivering
  - Have we achieved Five Nines? 99.999%
- To ensure we meet SLAs in the future
  - Is our network about to fail? Become congested?

Uptime Expectations

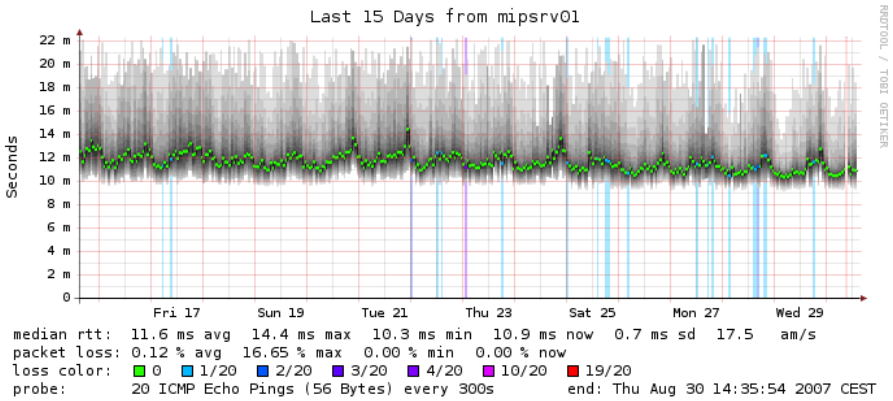
- What does it take to deliver 99.9% uptime?
  - Only 44 minutes of downtime a month!
- Need to shut down one hour a week?
  - That's only 99.4% uptime ((732-4)/732 = .9945355...)
- Maintenance might be negotiated in SLAs
- What does it mean that the network is up?
  - Does it work at every location? Every host?
  - Is the network up if it works at the Boss's desk?
  - Should the network be reachable from the Internet?

Establishing a Baseline

Monitoring can be used to **Establish a Baseline**

Baseline = What's normal for your network?

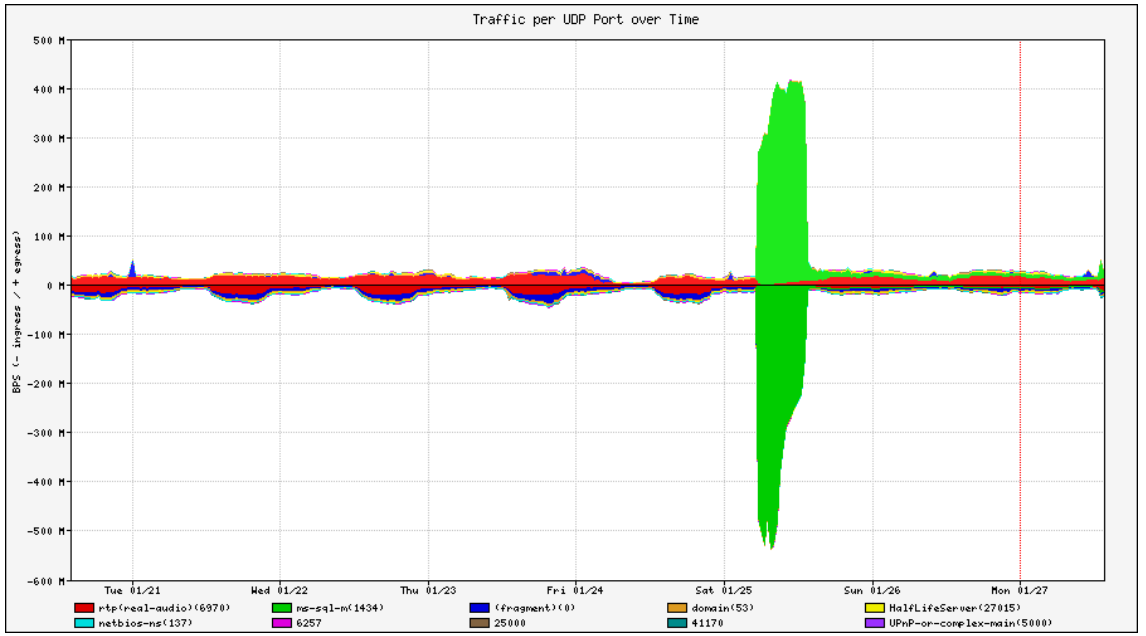
- Typical latency across paths
- **Jitter across paths**
- Load on links
- Percent Resource Utilisation
- Typical amounts of noise
  - Network scans & random attacks from the Internet
  - Dropped packets
  - Reported errors or failures



Detecting Attacks

- Deviation from baseline can mean an attack
- Are there more flows than usual?
- Is the load higher on some servers or services?
- Have there been multiple service failures?

Example of Anomaly-Based DDoS Detection Using NetFlow and Arbor Networks



https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/white_paper_c11_556320.html

These things could mean an attack

What do we Manage?

- Asset management: What equipment have we deployed?
  - What software is it running
  - What's its configuration (hardware & software)
  - Where is it installed
  - Do we have spares?
- Incident management: fault tracking and resolution
- Change management: Are we satisfying user requests?
  - Installing, moving, adding, or changing things
- Staff management

Why do we Manage?

- To ensure we meet business requirements for service level, incident response times etc
- To make efficient use of our resources (including staff)
- To learn from problems and make improvements to reduce future problems
- To plan for upgrades, and make purchasing decisions with sufficient lead time

Network Monitoring Tools*

- **Availability**: Nagios
  - for servers, services, routers, switches, environment
- **Reliability**: Smokeping
  - connection health, rtt, service response time, jitter
- **Performance**: LibreNMS
  - traffic, port utilisation, cpu, RAM, disk, processes

Integration & overlap exists between these programs!

**Each tool noted is just one example of several available tools*

Network Management Tools*

- **Ticket Systems**: RT
  - Manage provisioning & support
- **Configuration Management**: RANCID, Oxidized
  - Track router configurations
- **Network Documentation**: Netbox, GLPI
  - Inventory, Location, Ownership of Network Assets

Integration & overlap exists between these programs!

**Each tool noted is just one example of several available tools*

NET MANAGEMENT	NETFLOW / IPFIX / SFLOW	LOGS / SIEM	DOCUMENTATION
Cacti	ElastiFlow	Beats	diagrams.net
LibreNMS	Filebeat	Elasticsearch	GLPI
Nagios/Icinga	NfSen	Fluentd/fluent-bit	InvenTree
Netdata	ntop	Loki	IPplan
OpenNMS	pmacct	OSSEC/Wazuh	Netbox
Prometheus	**SECURITY / NIDS**	Sagan	Netdisco
Sensu	Nessus	**TICKETING**	phpIPAM
Zabbix	Prelude	OSticket	Snipe-IT
PERFORMANCE	Snort	OTRS	**CHANGE MGMT**
perfSONAR	Suricata	RT	Oxidized
Smokeping	Zeek	Trac	RANCID

What about “NMM 2.0?”

Older practices:

- Classic polling model using snmp, service query or pings
- Coarse data collection (5 minute intervals typically)

Newer practices include:

- “Streaming Telemetry” (network data)
- Pull methodology using http(s), agent-based or map to snmp
- Time series databases (large) often NoSQL based
- Collectors and parsers using metrics, gauges and counters

Some tools you may have heard mentioned:

- ELK, TICK, Kafka, Prometheus Stacks
- Grafana, InfluxDB, MongoDB
- Beats, Elasticsearch, fluentd, Kibana, Loki, etc…

One example in use

Netdata

- https://github.com/netdata/netdata/wiki
- Real-time, fine-grained, detailed host monitoring.
- http://www.ws.nsrc.org:19999/
- Don’t all go at once! ☺



NMM 2.0: **ElastiFlow**

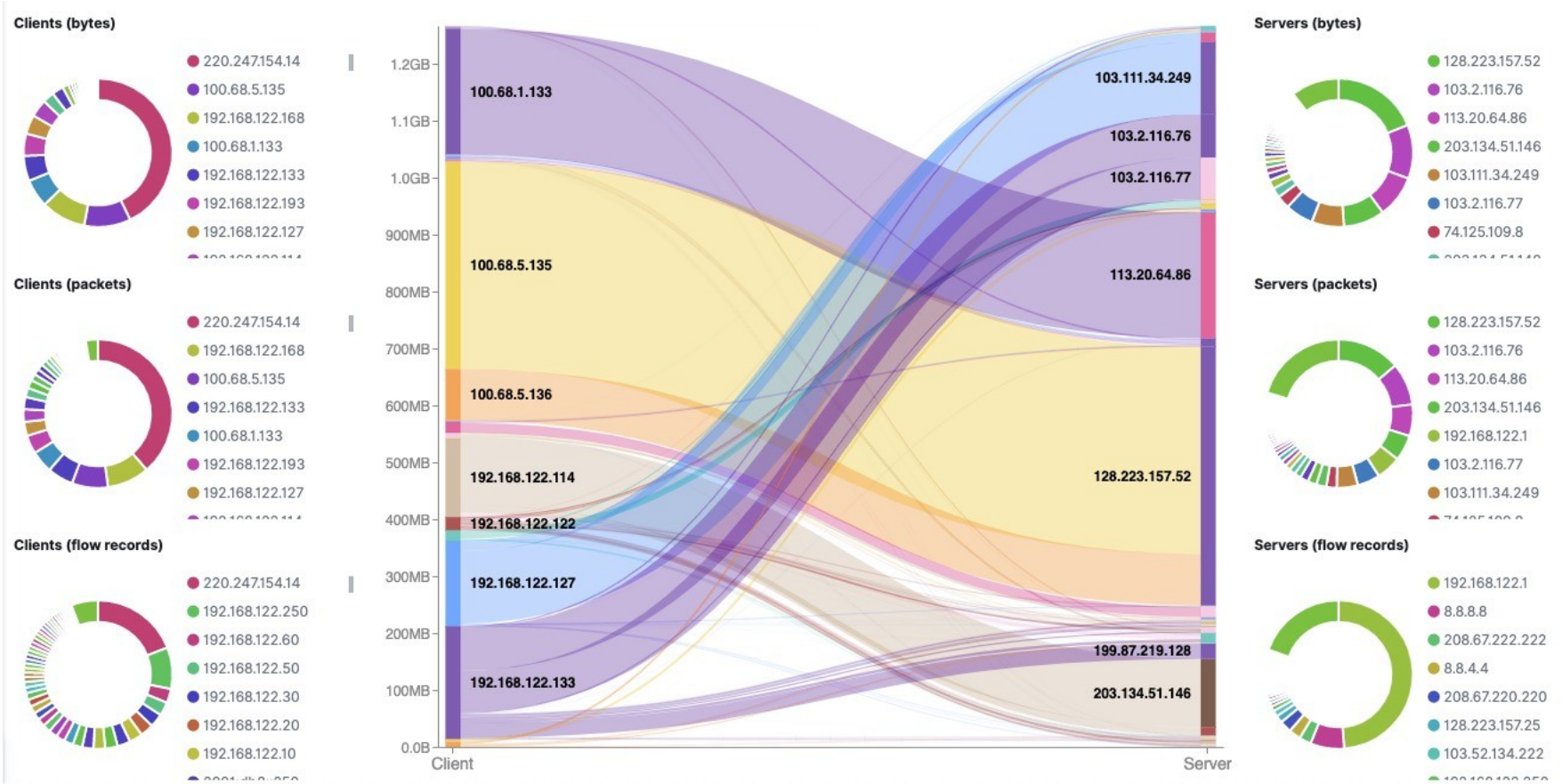






Takes the following flow protocols

- Netflow – IPFix – Sflow
- Instead of NfSen
- https://github.com/robcowart/elastiflow



NMM Review

- Network Monitoring & Management
- What & Why we Monitor
- Uptime Expectations & Calculations
- Baseline Performance & Attack Detection
- Network Attack Detection
- What & Why we Manage
- Network Monitoring & Management Tools
- The NOC: Consolidating Systems
- NMM 2.0

Questions?