

**APNIC**



# Introduction to NMM

Further information | 00 Example 2020

Trainer Name

# Table of Content



- Basics of Network Monitoring
- Network Monitoring and Management
- Monitoring – Why, What and How
- Management – Why, What and How
- Network Monitoring and Management best practices
- Out Of Band (OOB) Management
- Techniques and Tools
- SaaS (Software as a Service) based Monitoring and Management service

# Basics of Network Monitoring



- Network have evolved from being a flat to a complex network with lot more technologies:
  - Cloud
  - Wireless
  - Remote Users and VPN
  - Mobile Devices
  - IoT
  - VOIP
- Simple networks don't meet the requirements of modern infrastructure anymore

# Basics of Network Monitoring



- In spite of all the evolution that has occurred, one factor that has been constant is the need for network monitoring
- For effective monitoring solution it's critical to understand the
  - Major network components → Router, Switch, Firewall, Load Balancer, Server & Services
  - Protocols → SNMP, ICMP, gRPC, Netflow
  - Monitoring Tools → LibreNMS, Nagios, Cacti etc

# Network Monitoring and Management



- **Monitoring**
  - Constantly checks/scans the status of a network
  - Collect statistics and performance metrics
  - Checking for error conditions notifies the network administrator for slow or failing components
- **Network Monitoring involves**
  - What we should be looking for → Throughput, Latency, Packet loss, Bandwidth
  - How to find it → Ping, SNMP Trap, SNMP Poll, API
  - Where and how to store the values → Cloud, On-prem, RRD, Time Series Data
  - What thresholds indicate a problem situation → Performance metrics
  - How to notify → Email, SMS, Webhook

# Network Monitoring and Management



- **Management**
  - The processes, tools and applications used to administer, operate and maintain a network infrastructure
- **Network Management involves**
  - Administration → Tracking network resources
  - Operation → Network functions well
  - Maintenance → Upgrades and fixes to network resources
  - Provisioning → Network resource configuration



Every Network is different

And

No single system will solve all your problems

Or

Meet all your requirements



# Network Monitoring

# WHY do we Monitor



- Track resource utilization and get historical data
- Establish a baseline (what's normal for the network)
- Understand the performance matrices and do capacity planning
- Helps network and systems administrators identify possible issues before they affect business continuity
- Find the root cause of problems when something goes wrong in the network
- Track configuration changes
- Identify security threats

# WHAT do we Monitor



- All the resources vs Critical resources
  - Hardware → Network Devices & Servers
  - Services → DNS, DHCP, HTTP/HTTPS, SMTP
  - Application → On-prem and Cloud
- Underlay vs Overlay
  - IGP (OSPF, ISIS)
  - OMP
  - EVPN & VXLAN

Availability

Uptime

Reliability

Jitter, Latency, RTT

Capacity

Traffic, Port Utilization

Performance

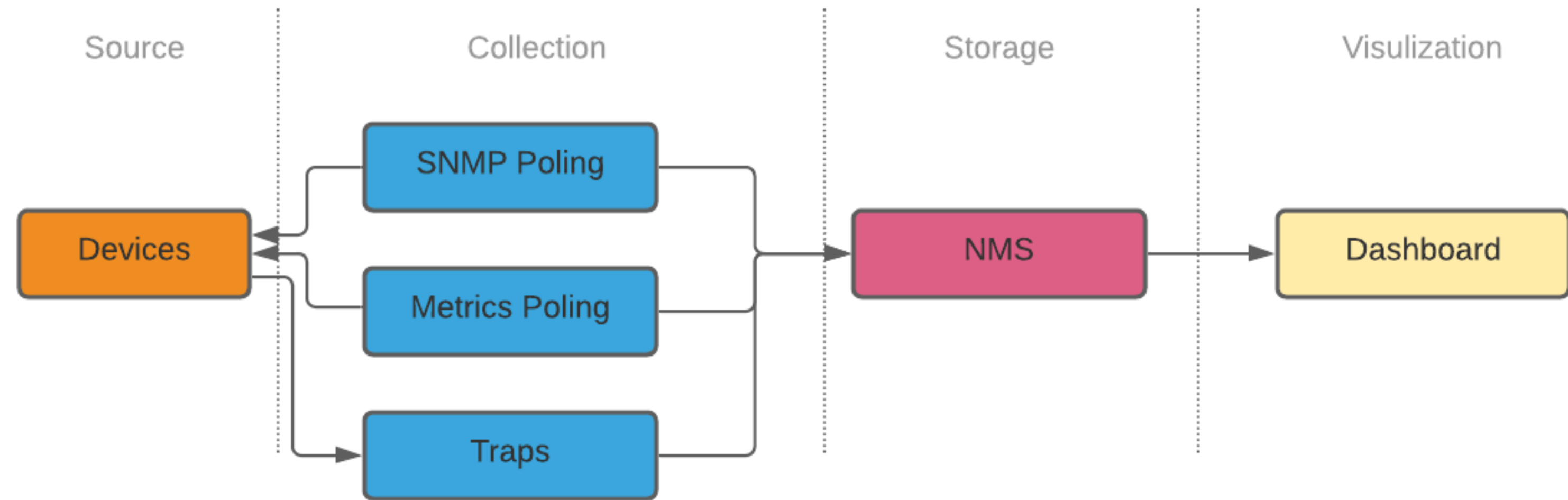
CPU, Memory, Disk, Processes

# HOW to Monitor



- Commonly used technologies:

- Ping
  - SNMP Trap
  - SNMP Poll
- SNMP
- Syslog
- CDP/LLDP
- Netflow
- API



- There are tools which leverages these features to monitor network

Title of course/ webinar

# Network Management

# WHY do we Manage



- Maximum efficiency and improve IT productivity
- Security and Threat detection
- Network upgrade and visibility

# WHAT do we Manage



- Network resources (routers, switches, Firewall, Load Balancer)
- Systems (Servers, Applications)
- Power system devices
- Customer Premises Equipment (CPE)
- Storage



# HOW to Manage



- Agent based – reside on manage network/system element
- Most common protocol is SNMP SET
- Few new protocols include NETCONF and RESTCONF

	<b>SNMP</b>	<b>NETCONF</b>	<b>SOAP</b>	<b>RESTCONF</b>
Standard	IETF	IETF	W3C	IETF
Resources	OIDs	Paths		URLs
Data Models	Defined in MIBs	YANG		YANG
Management Operations	SNMP	NETCONF	XML	HTTP Operations
Encoding	BER	XML	XML	XML, JSON
Transport Stack	UDP	SSH TCP	SSL HTTP TCP	SSL HTTP TCP



- Baseline network behaviour
- Escalation matrix
- Layered breakdowns
- Implement High Availability with failover options
- Capacity planning and growth

# OOB (Out Of Band)



- Out-of-band management uses a completely separate network that's dedicated strictly to managing infrastructure.
- If we need to reboot a router, collect data for regulatory compliance, or adjust QoS settings due to traffic changes, OOB makes it possible - even if our production network is down.
- Reasons to have out-of-band management:
  - Restore uptime fast from anywhere
  - Get unified control of our network

# Techniques and Tools

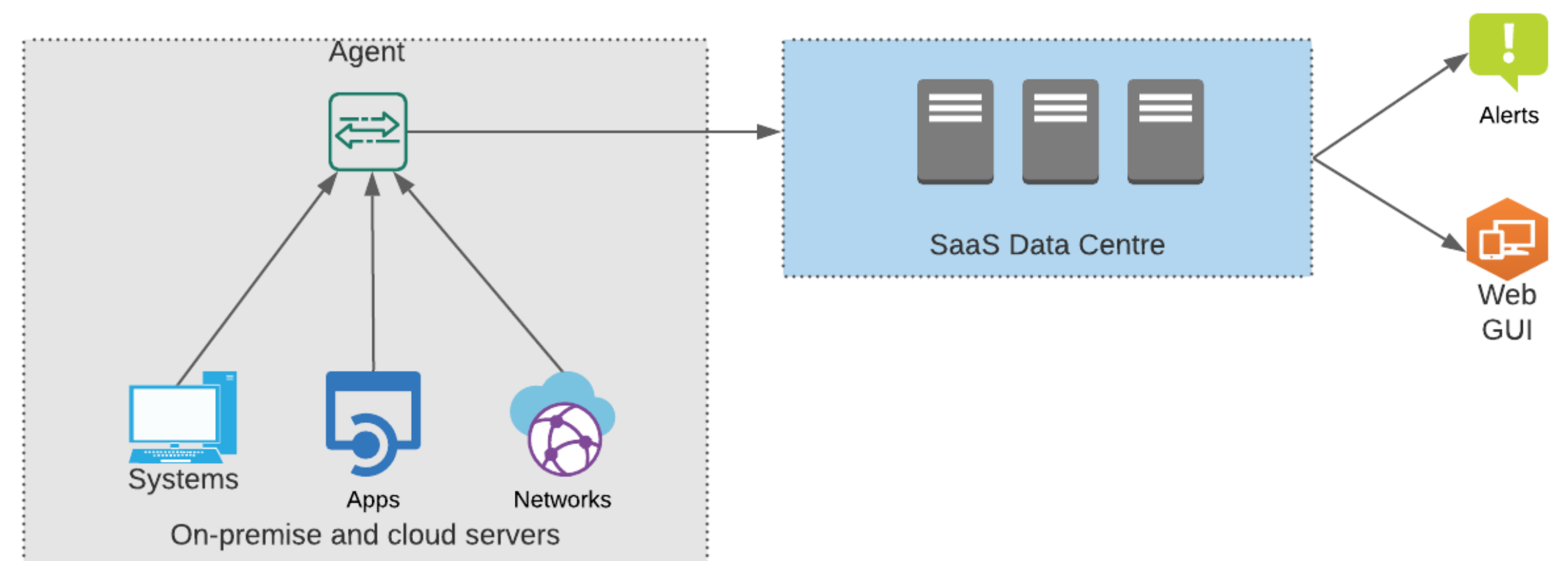


- Agent-based and Agentless Monitoring
- Internal and External Monitoring
- Centralized vs Decentralized Network Management

# SaaS based Monitoring and Management



- SaaS based monitoring and management tools
- Scalability, accessibility, upgradability, resilience and pay-as-you-go pricing options
- Work for both on-prem and cloud infrastructure
- Few SaaS based Monitoring tools
  - LogicMonitor
  - New Relic
  - Auvik
  - StatusCake



- Few Network Monitoring & Management tools

Tool	Function	Link
Icinga	Availability, Performance, Monitoring	<a href="https://icinga.com/">https://icinga.com/</a>
Nagios	Availability, Performance, Monitoring	<a href="https://www.nagios.org/">https://www.nagios.org/</a>
LibreNMS	Availability, Capacity, Discovery, Performance, Monitoring	<a href="https://www.librenms.org/">https://www.librenms.org/</a>
Zabbix	Availability, Capacity, Discovery, Performance, Monitoring	<a href="https://www.zabbix.com/">https://www.zabbix.com/</a>
Smokeping	Availability, Latency, Monitoring	<a href="https://oss.oetiker.ch/smokeping/">https://oss.oetiker.ch/smokeping/</a>
Nfsen/Nfdump	Traffic Analysis, Monitoring, Flow Collection	<a href="http://nfsen.sourceforge.net/">http://nfsen.sourceforge.net/</a> <a href="https://github.com/phaag/nfdump">https://github.com/phaag/nfdump</a>
AS-Stats	Traffic Analysis, Monitoring, Flow Collection	<a href="https://github.com/manuelkasper/AS-Stats">https://github.com/manuelkasper/AS-Stats</a>
Rancid	Backup, Monitoring, Management	<a href="https://shrubbery.net/rancid/">https://shrubbery.net/rancid/</a>
Oxidized	Backup, Monitoring, Management	<a href="https://github.com/ytti/oxidized">https://github.com/ytti/oxidized</a>
RT/OSTicket	Ticketing System	<a href="https://osticket.com/">https://osticket.com/</a>
NetDisco	Discovery, Inventory, IPAM	<a href="http://netdisco.org/">http://netdisco.org/</a>
Syslog-ng	Log Management	<a href="https://github.com/syslog-ng/syslog-ng">https://github.com/syslog-ng/syslog-ng</a>
Graylog	Log Management	<a href="https://www.graylog.org/products/open-source">https://www.graylog.org/products/open-source</a>
Netdot	Documentation	<a href="https://github.com/cvicente/Netdot/">https://github.com/cvicente/Netdot/</a>
Nipap	IPAM	<a href="https://spritelink.github.io/NIPAP/">https://spritelink.github.io/NIPAP/</a>



# Network Monitoring and Management – What Next?



	Legacy Way	Modern Way
Network Monitoring	SNMP Get SNMP Trap RRD	API (Webhook) Model Driven Telemetry (gRPC) Time Series Database (TSD)
Network Management	SNMP Set	NetConf RestConf OpenConfig



# Thank You!

