
## Housekeeping

- **Attendees will be on mute during the presentation to prevent interruptions from feedback and background noise.**
- **If you wish to ask a question please use GoToWebinar's chat**
- **We will have a Q&A session at the end of the presentation**
- **A copy of this presentation is available in the GTW Handouts panel**
- **This session will be recorded and made available to all attendees**

## Topics for Today

During today's webinar you will learn how to…

- Remediate Network Events to reduce Background Noise and Load
- Focus Event Automation on Troubleshooting and Repair
- Leverage Trending Data to Reduce False Alerts
- Monitor Configuration Changes to Reduce Downtime

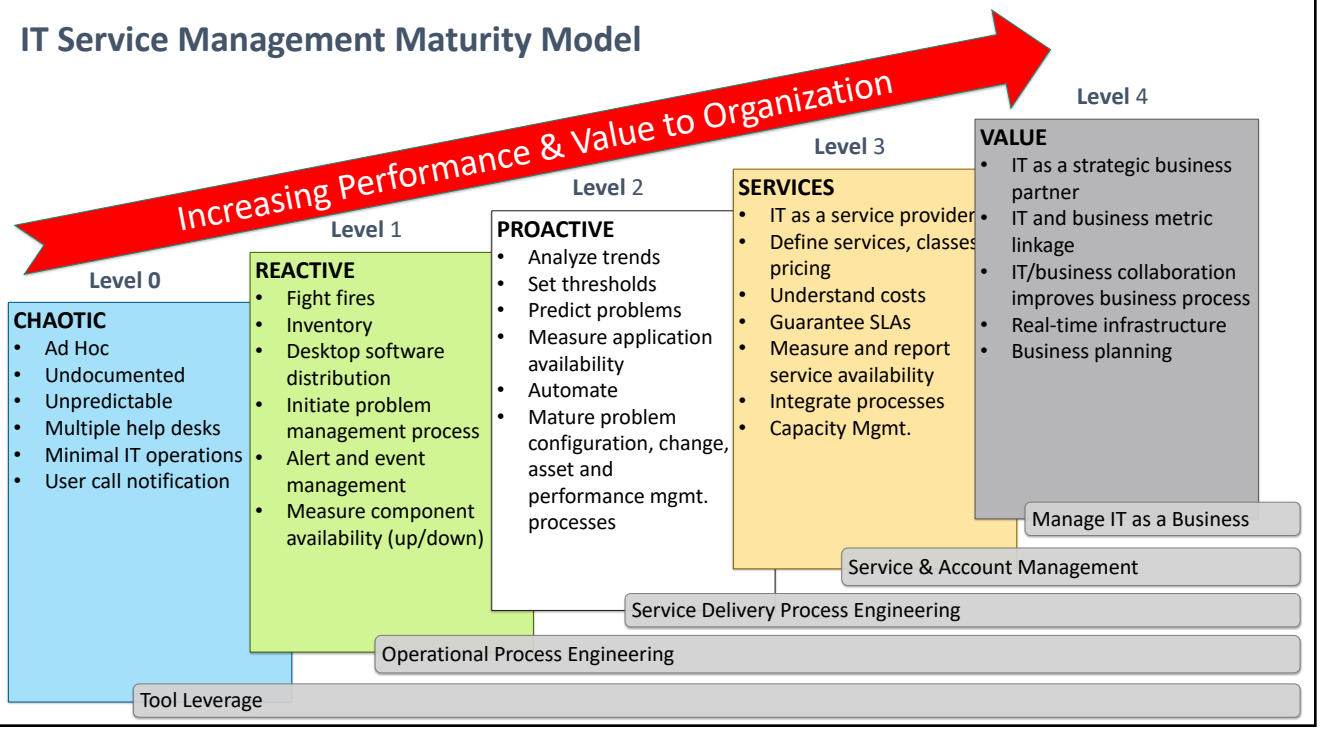
## WHY

## Leveraging Visibility to Improve Network Performance

Top Causes of Poor Network Performance ( a small sampling )

- Poor Network Design/Architecture Leads to Congestion
- Insufficient Hardware and Bandwidth Capacity as Usage Grows
- Poor Cable Selection/Installation Results in High Error Rates and Slow Data Transfer
- Unauthorized User Activity (Netflix, P2P, Facebook, etc.)

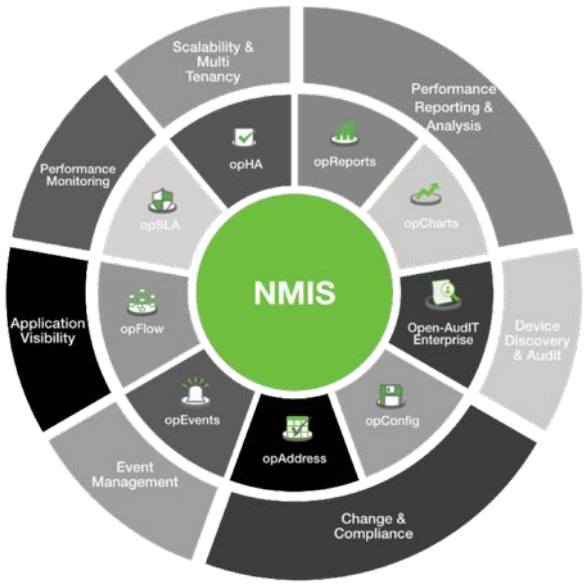
## IT Service Management Maturity Model



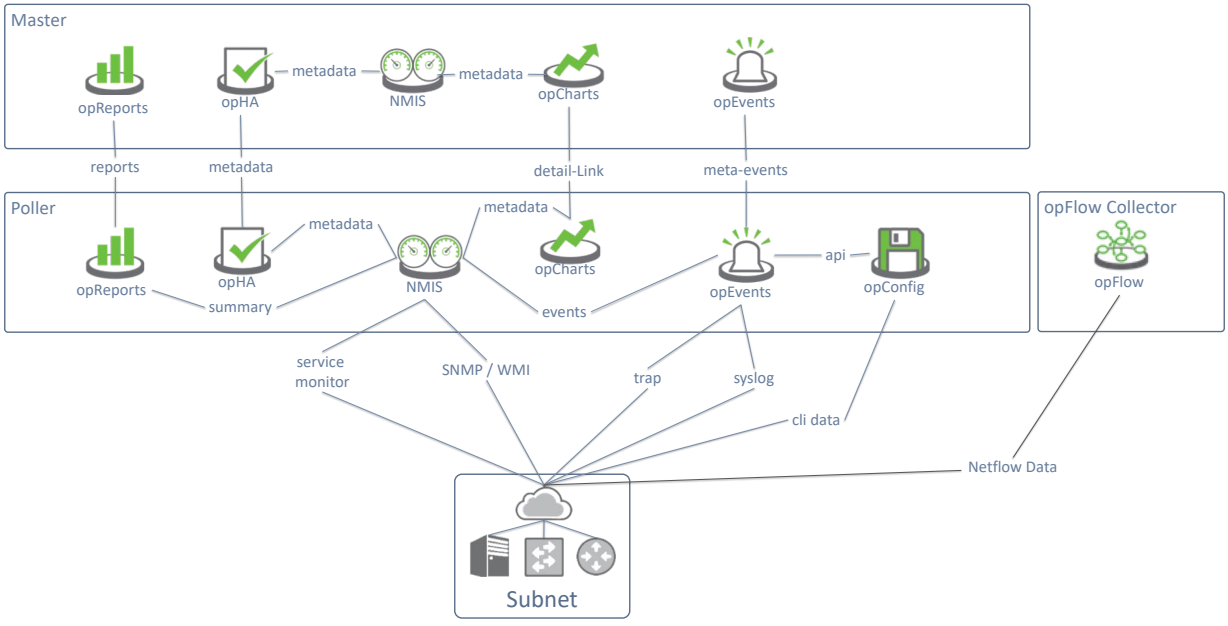
# MULTILAYERED APPROACH

Solutions Covered Today:

NMIS: Performance and Fault Monitoring
opEvents: Operational Automation
opTrend: Predictive analytics engine
opConfig: Configuration and compliance management




# OPMANTEK APPLICATION FLOW



## How

## Process

Follow this basic process daily for 1-month; network performance will improve 50%

HOW – Task a single responsible individual, or small team, to follow this process and invest 3hrs/day, every day. Track repeat issues, use ticketing systems to task other resources.

1. Remediate top 2-3 devices with performance issues out of acceptable norm (i.e. high CPU, low memory, low drive space, etc.). Should thresholds be adjusted or device reconfigured/replaced?
2. Remediate top 2-3 events every day; what devices are creating them, what are they, why are they happening, can they be stopped or should they be silenced?
3. Enable opTrend to augment/replace static thresholds; is there enough data to enable yet?
4. Check device configuration collection, determine if any changes need to be addressed/alerted on, build-out as needed (i.e. add new devices, create support/rules for devices, etc.)

## NMIS

Open Source Performance and Fault Management

WHY – Proactive remediation results is less load on equipment and background noise that distracts the engineering team(s)

- Reports -> Current -> Top 10
- Network Performance -> Top 10 (subtly different from the Reports version)
- Service Desk -> Alerts -> Events
- Reports -> Current -> Collect/Update Time
- System -> Configuration Check -> Node Admin Summary (Only Exceptions)
- System -> Host Diagnostics -> NMIS Runtime Graph

## opEvents

Advanced Fault Management and Operational Automation

WHY – Expands on efforts already done through NMIS, and scientifically improves automated response thereby decreasing workload and improving operational efficiency

- Configure Daily Summary Reports in opCommon.nmis
- Views -> Summary Reports
- Process - Daily Summary Reports
    - Work Top 3 Events and Devices every day (see: Top 10 nodes and events by event count)
    - Compare to NMIS Top 10 list (or opCharts TopN if available)
    - Identify troubleshooting procedures that could be automated

## opTrend

Leverage Trending Data to Reduce False Alerts

WHY – Reduces false alerts by understanding what is normal operation for a given day and window of time

- Start Trending with Core Devices
- After 45-60 days Enable Trended Thresholding (opCommon.nmis)
- Adjust what you respond to with opEvents and EventActions.nmis

## opConfig

Monitor Configuration Changes to Reduce Downtime

WHY – Proactively monitoring devices for unauthorized changes reduces potential downtime and impact.

- Start Collecting on Core devices, expand collection over time ensuring all relevant commands are being collected and backed up
- Use detect_change to control when a new version of a collected command should be stored
- Use raise_change to raise an event in NMIS if a change is detected for a particular command
- If you're using opEvents you could automate the response to a change detection – even going so far as to call opConfig to roll back the device change to a known good configuration

NEXT

## Next Steps

Look into bandwidth users, performance bottlenecks, shape traffic

WHY – After you've adopted all the previous recommendations expand into…

- opReports; traffic reports, device performance, WAN and LAN reports
- opFlow; identify top-talkers and noisy applications. Who is using the bandwidth on what?
- opSLA; uses Cisco IP-SLA to generate mesh traffic, removes load from poller
- CBQoS; Monitored through NMIS as part of Performance Monitoring

## CONTACT FOR FOLLOW UP

Commercial enquiries:

**Tom Wiri**
Account Executive
+1 (512) 430-4450
usa@opmantek.com

Technical enquiries:

**Mark Henry**
Senior Engineer
+1 (207) 951-2428
markh@opmantek.com

OPMANTEK