Cisco Network Analysis Module
Overview Presentation
Agenda

- NAM Solution Overview
- NAM Hardware Overview
- NAM 4.1 Features and Functions
- NAM Use Cases
NAM Solution Overview
Cisco NAM: Functional Overview

- Application performance monitoring
  - Voice, Video and TCP-based applications
- End-to-End visibility into WAAS deployments
- Traffic Analysis
  - Applications, Host, Conversations
  - MPLS, DiffServ, URL, VLAN, ...
  - NetFlow collection
  - Per-application and per-user granularity
- Advanced Troubleshooting
  - Problem Isolation
  - Intelligent Packet Capture, Decodes, Filter
- Open Instrumentation

NAM delivers unparalleled visibility into application and network performance to help ensure the consistent and efficient delivery of applications and services to end users.
The unique design of the NAM combines a rich set of embedded data collection and performance analytics with a remotely accessible, Web-based management console, all on a single blade or appliance.
NAM Deployment
Where Does the Data Come From?

The collection point is dependent upon the collection purpose and source of data

- **Collection Purpose**: The location of where you gather the data depends on your collection purpose
  - Traffic Analysis (who, what, and how much)
  - Application Performance Analytics (Server Farm)
  - Voice / Video Analytics
  - Troubleshooting (Packet Capture / Decode)
  - Analyze QoS
  - WAAS Visibility

- **Data Sources**: Data can be gathered and analyzed from various data sources
  - Router and switch interfaces
  - Spanned traffic forwarded from ports and VLANs
  - NetFlow data exports
  - Wide area Application Engine (WAE) data exports
  - Packet headers (DiffServ and Type of Service (ToS) bits)
  - Network-Based Application Recognition (NBAR)
NAM Deployment

How does NAM Help?

- **Live Network Monitoring**
  (Utilization, Errors, Hosts, Conversations, Applications)

- **Historical Reporting & Trending**
  (Above statistics over time)

- **Troubleshooting**
  (Thresholds, Alarms, Packet Capture & Decode)

- **Performance Analytics**
  (Application Response Time, Voice/Video, URL, QoS Monitoring)

- **WAAS Visibility**
  (Identification for WAN Optimization, Impact of WAAS Deployment on Application Performance)
Places in Network where NAM is deployed

Data Center Edge: Visibility into business critical applications and transactions.

Server Farms: Monitor transactions and provide application performance analytics.

Campus Edge: voice quality of streams leaving the campus. Measure WAN utilizations and health metrics of branch routers using NetFlow.


Branch edge: visibility into all traffic crossing the branch boundary.

Distribution Layer: Troubleshooting issues related to one building or area of the network eg: voice calls.

Access Layer: Monitor access closet switch that serves critical company wide meetings, important conference rooms and IP phones.
NAM Appliance
## Cisco NAM 2220 Appliances

### High Performance, Scalability and Deployment Flexibility

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>2 Intel® Xeon® E5440 Quad core</td>
</tr>
<tr>
<td>RAM</td>
<td>16 GB SDRAM</td>
</tr>
<tr>
<td>Network Adaptor</td>
<td>2 x 10 Gb with options for optical XFP interfaces</td>
</tr>
<tr>
<td>Hard Disk</td>
<td>6 x 147 GB (~1 terrabyte) SAS hot swappable RAID1</td>
</tr>
<tr>
<td>Capture Buffer</td>
<td>10 GB</td>
</tr>
<tr>
<td>Form Factor</td>
<td>2RU</td>
</tr>
<tr>
<td>Performance</td>
<td>~ 9.7 Gbps monitoring throughput</td>
</tr>
<tr>
<td>Deployment</td>
<td>Data center, Server farm, Campus backbone, WAN edge/aggregation</td>
</tr>
</tbody>
</table>
# Cisco NAM 2204 Appliances

High Performance, Scalability and Deployment Flexibility

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel® E6400 Core2 Duo</td>
</tr>
<tr>
<td>RAM</td>
<td>8 GB SDRAM</td>
</tr>
<tr>
<td>Network Adaptor</td>
<td>4 x 1 Gb with options for <strong>optical SFP</strong> or <strong>1000BaseT</strong></td>
</tr>
<tr>
<td>Hard Disk</td>
<td>2 x 250 GB SATA server grade</td>
</tr>
<tr>
<td>Capture Buffer</td>
<td>2 GB</td>
</tr>
<tr>
<td>Form Factor</td>
<td>1RU</td>
</tr>
<tr>
<td>Performance</td>
<td>~ 1.9 Gbps monitoring throughput</td>
</tr>
<tr>
<td>Deployment</td>
<td>Data center, Campus, Distribution, Access, WAN, Edge/access</td>
</tr>
</tbody>
</table>

**Cisco NAM 2204**
NAM 2200 Appliance
Internal Architecture

- Cisco Managed Device
- SNMP Agent
  - Mini RMON per interface
- Management Interface for NDE and ERSPAN
- Monitor Interface for SPAN/VACL/Wire Tap
  - Data from SPAN, VACL or Wire Tap Sources
- Data from ERSPAN
- Data from NDE
- Data from WAE Flow Agent

- Supported MIBs:
  - RMON I, II
  - HCRMON
  - SMON
  - DSMON
  - ART

- Web Server
  - HTTP/S
  - Poll Process
  - Metric Engine
  - Sensor

- Note: The NAM 2204 can support four simultaneous SPAN/VACL/Tap sessions
Packet Processing Engine
Heart of the NAM appliance
High speed, high precision, efficient traffic filtering

Full-line speed (2x10Gbps) raw traffic processing

Large onboard buffer to handle traffic bursts

High-precision time-stamping (10 nanoseconds)

Efficient data transfer to NAM application

High-speed filtering, i.e., addresses, protocols, encapsulations...
Hardware Assisted Capture

Hardware Filters Improve Capture Performance of NAM 2220

Only one Hardware Assisted Capture session at a time

Can be used in conjunction with other software based capture sessions.

For best performance narrow down the amount of captured traffic as much as possible with very specific hardware filters

Software filters also available for added flexibility
Cat65xx/C76xx NAM
## NAM-1/2 Hardware Overview

### Specifications

<table>
<thead>
<tr>
<th></th>
<th>NAM-1 (WS-SVC-NAM-1-250S)</th>
<th>NAM-2 (WS-SVC-NAM-2-250S)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fabric and Bus Support</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>Dual PIII</td>
<td>Dual PIII + Acceleration</td>
</tr>
<tr>
<td><strong>RAM</strong></td>
<td>2 GB</td>
<td>2 GB</td>
</tr>
<tr>
<td><strong>Hard Disk</strong></td>
<td>250 GB</td>
<td>250 GB</td>
</tr>
<tr>
<td><strong>Capture Buffer</strong></td>
<td>200 MB</td>
<td>500 MB</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td>Sub-gigabit</td>
<td>Gigabit</td>
</tr>
<tr>
<td><strong>No. of SPAN / VACL Session</strong></td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td><strong>No. of NetFlow Sessions</strong></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Deployment Scenarios</strong></td>
<td>Distribution, Access, small core, Branch office</td>
<td>Server Farm, Data Center, Distribution, WAN Edge</td>
</tr>
</tbody>
</table>

### Monitoring Applications

- Fast Ethernet, Low capacity GE
- Gigabit

- Server Farm, Data Center, Distribution, WAN Edge
Detailed Port Monitoring
Spanning Traffic to the NAM for Detailed Analysis

Packets from Ports, VLANs, or EtherChannels Can Be Analyzed in Detail by Spanning (Copying) the Packets to the NAM’s DataPort Interface

SPAN Session #1 Copies Critical Gigabit Port to DataPort-1 on the NAM for Detailed Analysis

SPAN Session #2 Copies a Voice VLAN to DataPort-2 on the NAM for Detailed Analysis
NAM-1/2 VLAN ACLs (VACL) Data Sources

- Multiple Uses of VLAN ACLs for Traffic Analysis
  - Use a VACL to analyze WAN interfaces that can not be spanned
  - Use a VACL if no more SPAN sessions are available for use
  - Use a VACL to pre-filter specific types of traffic for analysis

- VACL traffic sent to NAM data port looks just like SPAN data to the NAM

Example: A VLAN ACL can be used to capture WAN traffic and forward to the NAM as an Ethernet frame

VACL traffic sent to NAM Data Port
ISR NME-NAM
# The NME-NAM-120S

## Specifications

<table>
<thead>
<tr>
<th>Hardware Feature</th>
<th>NM-NAM</th>
<th>NME-NAM-120S</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>500 MHz Intel Pentium III CPU</td>
<td>1.0 GHz Intel Celeron M CPU</td>
</tr>
<tr>
<td>SDRAM</td>
<td>256MB</td>
<td>1 GB</td>
</tr>
<tr>
<td>Internal Disk Storage</td>
<td>20GB IDE</td>
<td>120GB 24x7 SATA</td>
</tr>
<tr>
<td>Flash Memory</td>
<td>16MB</td>
<td>24MB</td>
</tr>
<tr>
<td>Interfaces</td>
<td>2 FE</td>
<td>2 GE</td>
</tr>
</tbody>
</table>
NME-NAM: Hardware and Software Requirements

- Routers supported:
  - **Cisco 2800**: 2811, 2821, and 2851
  - **Cisco 3700**: 3725 and 3745
  - **Cisco 3800**: 3825 and 3845

  Note: Cisco 3745 and 3845 support hot swap. NAM must be shut-down prior to removal from the router

- IOS supported: 12.4(9)T or later

- Browsers supported: IE 6.0 or later; Firefox 2.0 or later
NME-NAM Interfaces

WAN traffic monitoring using Cisco Express Forwarding (CEF) to copy packets to the NAM internal interface.

LAN traffic monitoring by connecting external NAM interface to a Gigabit Ethernet source.

Branch Router

MIB-II / NBAR-PD

CEF Copied Traffic

Router Internal GE Interface

Internal GE Interface

External GE Interface

OR

Switch Device

SPAN
NME-NAM
NetFlow & Management Traffic

NAM Management traffic - HTTP(S), telnet, SSH, SNMP, NetFlow, etc – user’s choice to use internal or external GE

Internal Interface for Management traffic uses router CPU, RAM, and backplane resources

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential
Cisco WAAS NAM Virtual Blade
Cisco WAAS NAM Virtual Blade

Key highlights

- First NAM software offering
- Available on WAAS 574 and 674 appliances
- NAM software resides in a virtual environment within WAAS
- 60 day fully functional evaluation license
- WAAS Flow Agent flows and Netflow available as data sources
- Sized for small data centers and proof-of-concept environments
- Facilitates rapid roll-out of WAAS solution.
Cisco WAAS NAM Virtual Blade

Typical Deployment

- NAM Virtual Blade software resides in a Virtual Environment within WAAS appliances
- WAAS Embedded instrumentation is a data source for NAM Virtual Blade
- NAM GUI accessible via web based browsers
Installation Workflow

- WAAS Central Manager provisions Virtual Environment on WAAS appliances
- WAAS CM installs NAM ISO from FTP server to Physical disk on Host WAAS Appliance
- User logs onto NAM VB GUI via Web Browser
NAM 4.1
Features and Functions
NAM 4.0 Feature Highlights

High-Performance Appliances
- Multi-Gigabit performance and large onboard storage
- Deployment flexibility extending the reach of NAM blades

Intelligent Application Performance (IAP)
- Reflects True End-User Quality of Experience
- Transaction-Aware performance metrics accurately characterize end-to-end application performance

Superior Voice Quality Monitoring
- Standards-based Voice Quality (MOS) Measurements
- Integration with Cisco Unified Communication Management Suite (CUCMS) for Enterprise-wide monitoring

Visibility into WAN-optimized Networks
- Identification of opportunities for WAN optimization
- Impact of WAAS deployment on application performance
- Real-time troubleshooting
NAM 4.1 Feature Highlights

**WAAS NAM Virtual Blade**
- Zero Hardware footprint based NAM offering
- Targeted for Proof of Concept (PoC) and Small Data Center deployments

**Enhanced Appliance performance**
- Appliance performance improvements increased by 50%
- Hardware based packet capture filtering for targeted troubleshooting

**Improved Visibility into WAN-optimized Networks**
- Support for WAAS Passthrough traffic
- Multi-segment display for visual correlation of Server/WAN/Client segments
- Server filters for IAP based analytics

**Better Support for Mobility environments**
- Application Visibility with GPRS Tunneling Protocol (GTP)
- Troubleshooting with targeted packet captures
Feature Summary

- Traffic monitoring
  - Applications
  - Hosts
  - Conversations
  - Top N
  - VLANs
- Packet capture and decode
- Intelligent Application Performance Analytics
- Voice quality analytics
- QoS (DiffServ) monitoring
- Port and Switch monitoring
- MPLS monitoring
Traffic Monitoring: Real-Time & Historical

- Learn what applications are running on the network, who’s using them, and how much bandwidth they’re consuming
- Proactively spot bottlenecks before your network suffers blows to performance
- Define and improve the consistency and quality of both individual and overall network services
- Understand network behavior before and after a business change
Real-Time Monitoring
Live traffic visibility and rapid troubleshooting

1. Examine real-time traffic flow
2. Drill down into actual conversations
3. Sniff packet flow to eliminate suspicion

![Diagram showing real-time traffic monitoring and analysis tools.](image-url)
Historical Reporting
Analyzing trends for network planning

1. Create a report to view traffic from branch to HQ. The Daily report is showing an increasing traffic pattern.
2. Drill down to 1 min granularity to determine how bursty the traffic is.
3. Monthly view shows a consistent traffic pattern. This information can be used to replicate a branch setup.
Historical Reporting
Visibility via Top N Reports

1. Top Conversations (App-Layer) report for SPAN, Netflow, WAE data sources shows top 50 flows at the DC and branch with 15 min granularity for up to 100 days.

2. Top Applications report shows traffic mix profile over time.

3. Top N response time report from Netflow and WAE data sources show worst performing applications at a branch.
Packet Capture and Decode

- Resolve problems before they affect users
- View decodes while the data is still being captured
- Use triggers, filters, and a capture analysis toolkit to identify and resolve transient problems
- Perform continuous captures and save capture onboard or remotely (NFS, iSCSI)
- Download capture files from the NAM in PCAP or ENC format

Support Troubleshooting Efforts
Intelligent Application Performance Analytics
Intelligent Application Performance Analytics

Overview

Is It the Network or the Application?

- Total Time
- Server Latency
- Application Server
- The Network
- NAM ART Analyzer
- Application Clients
- Network Flight Time
- Total Time - Server Latency

Network Flight Time

Server Latency

Application Server

The Network

NAM ART Analyzer

Application Clients

Total Time

Is It the Network or the Application?
Intelligent Application Performance Analytics

- Measure application response time delays
- Troubleshoot application performance problems
- Perform pre- and post-deployment monitoring of application optimization & acceleration services
- Analyze application behavior and trends for capacity planning
Intelligent Application Performance Analytics
Extends NAM’s Transaction-Aware Response Time Functionality

Includes additional transaction-based stats (45 total) and offers improved response time granularity

- Data Transfer Time
- Connection duration
- Number of bytes/packets transmitted
- Transaction Time
- Client Network Delay
- Server Network Delay
- Number of refused connections
- Application Delay
- And more…

Unifies application performance with end user experience
Available Performance Metrics in NAM 4.1

- Response time (avg, min, max)
- Application Delay (avg, min, max)
- Network Delay (avg, min, max)
- Client Network Delay (avg, min, max)
- Server Network Delay (avg, min, max)
- Total Transaction time (avg, min, max)
- Retransmission Delay (avg)
- Data Transfer Time (avg)
- Connection (Session) Duration

- Number of Responses
- Number of Late Responses
- Number of Responses by Response time
- Client Bytes and Packets
- Server Bytes and Packets
- Number of Connections (Sessions)
- Number of Closed Connections
- Number of Refused Connections
- Number of Unresponsive Connections
- Number of Transactions
- Number of Lost/Retransmitted Bytes and Packets

* New in NAM 4.0
Application Performance Metrics

![Diagram showing the sequence of events and metrics in an application performance measurement.](image)

- **Client**: SYN, ACK 1, Request, ACK 3, ACK 6, ACK 8, Request.
- **Server**: SYN-ACK, SEQ 1, SEQ 2, SEQ 4, SEQ 5, SEQ 3, SEQ 6, SEQ 7, SEQ 8.
- **Metrics**:
  - Connection Setup
  - Server Response
  - Data Transfer
  - Retransmission
  - Network RTT
  - Request Data
  - Response Data
  - Non-data
  - Transaction Time
  - Session Time

- **Events**:
  - Packet Loss
  - Retransmission

---

*Presentation_ID* 42

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential
Use Case: Response Time Analytics

2. Examine historic report for response time pattern
3. Examine packet decodes to detect unusual activity
Visibility Into WAN-Optimized Networks

- NAM measures and reports on application response time, WAN bandwidth utilization, LAN/WAN data throughput, and other application performance metrics
- Identify application optimization opportunities
- Analyze impact of Cisco WAAS implementation
- Leverage visibility for ongoing optimization improvements and troubleshooting
Identify Business Critical Applications

1. Real-time overview of applications, hosts, protocols and server performance
2. Real-time drill down into active applications
3. Historical Top N applications reports (by traffic volume)
Measure baseline application performance and bandwidth usage

1. Monitor real-time Application Response Time (server & client-server)
2. Review server details for detailed response time breakdown
3. Monitor Bandwidth Usage (per host/server)
4. Review historical trend of Application response time
Configuring WAAS – NAM Integration

1. Export flows from WAAS to NAM.
2. Add the WAE Data Source in NAM.
3. Inform the WAE Flow Agent which servers to monitor (can be imported from NetQoS).
4. Setup historical reports for response time.
WAAS Before and After Report(s)

Avg transaction time seen from the DC SPAN data source before WAAS, compared to avg transaction time from the branch side WAE

Comparison of test client experience for same file transfer before and after WAAS with respect to bandwidth utilization and transaction time

Note: Impact of WAAS on a test client at the site can be performed from a NAM in the Data Center
WAAS Before and After Report(s)

Average transaction time from the internal data source before and after WAAS

60% increase in the branch LAN traffic after WAN optimization enabled

Note: Site level reports can be created by placing a NAM at the site.
Visibility into Pass-Through Traffic

- Identify if the traffic marked for optimization appears in pass-through stream
- Drill-down to individual conversation within the pass-through stream
- Filter by individual source or destination

<table>
<thead>
<tr>
<th>#</th>
<th>Protocol</th>
<th>Packets/s</th>
<th>Bits/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>http</td>
<td>9.63</td>
<td>48,011.15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Protocol</th>
<th>Packets/s</th>
<th>Bits/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>http</td>
<td>0.05</td>
<td>13.95</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Source</th>
<th>Via</th>
<th>Destination</th>
<th>Packets/s</th>
<th>Bits/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>perf-ny-branch-client.cisco.com</td>
<td></td>
<td>hq-cat6k-gw-nam2.cisco.com</td>
<td>0.10</td>
<td>27.78</td>
</tr>
<tr>
<td>2</td>
<td>perf-ny-branch-client.cisco.com</td>
<td></td>
<td>perf-na-hq-access.cisco.com</td>
<td>0.05</td>
<td>13.89</td>
</tr>
<tr>
<td>3</td>
<td>hq-cat6k-gw-nam2.cisco.com</td>
<td>perf-na-hq-access.cisco.com</td>
<td>perf-ny-branch-client.cisco.com</td>
<td>0.03</td>
<td>6.94</td>
</tr>
<tr>
<td>4</td>
<td>perf-na-hq-access.cisco.com</td>
<td>perf-ny-branch-client.cisco.com</td>
<td>perf-ny-branch-client.cisco.com</td>
<td>0.03</td>
<td>6.94</td>
</tr>
</tbody>
</table>
Visibility into Optimized Traffic

1. View optimized streams at each WAE
2. Correlated 3 segment response-time view for optimized streams.
3. Drill down to details 45 metric view for individual streams at each WAE data source
Proactive Troubleshooting of Optimized and Pass-through streams

1. Setup Alarm Threshold to trigger a packet capture if Pass-Through traffic increases for optimized applications at a particular branch.

2. Setup a capture session on the SPAN data-source to capture all traffic for that application going to the branch in question when triggered.
Upgraded IAP capabilities
Reporting enhancements, server filtering, Extended WAAS visibility

- Create transaction reports directly from the real-time monitoring function without having to switch to the reports function

- View Top N historical reports for response time, transactions, and network delay

- Create new Response Time reports for Client and Server bit/byte volume

- Filter Response time for specific servers through the Monitored Server list

- Observe response time data based on information from multiple WAAS devices and segments in a new multi-segment window to provide a big picture view of application performance optimization

- Obtain critical performance analytics on pass-through traffic to provide a comprehensive view of both optimized and non-optimized traffic in WAAS environments
Enterprise-wide Performance Visibility with Third-party Reporting Application
Application Response Time Data Export to NetQoS

- Application profiling and trending
- Baseline performance for each application by location
- Monitor performance policies and SLOs
- Alert when performance thresholds are violated
- Seamless drill-down to NAM 4.x

- Comprehensive Application-aware performance analytics
  - Transaction-based statistics: Transaction Time, Data Transfer Time, etc.
  - Connection-based statistics: Open, Close, Refused, Unresponsive, etc.
  - And more…

- Web-based UI optimized for advanced troubleshooting
  - Deeper level of visibility (host vs. subnet, few seconds vs. ~15 min, and supporting packet-level analysis)

- Problems isolation across silos: Network, Server and Application

- Problem resolution with traffic capture/decode, comprehensive traffic analysis and intelligent use of multiple data-sources (NetFlow, SPAN, etc)

- Performance threshold-based proactive alerts

- Deployment versatility with multiple form-factors (blades and appliances) offer flexibility for end-to-end network coverage
NetQoS + NAM Integration provides end-to-end workflows

1. Identify incidents and application performance at a site/subnet level using the NetQoS SuperAgent Management Console
2. Identify reporting NAM devices
3. Drill down into the NAM for per conversation response time and troubleshooting with packet capture, port stats and traffic analysis
Benefits of Combining NAM with NetQoS

**NetQoS Customer: “Why do I need NAM?”**

- When troubleshooting is required, drill-in from SuperAgent to the NAM
  - 30 second granularity for response-time metrics
  - Host level granularity for user centric troubleshooting
  - Intelligent packet capture and decode
- Embedded instrumentation in the CAT6K eliminates the need for additional hardware
  - Less hardware and easier administration
  - Leverage integrated blade paradigm
  - Eliminate need for both SuperAgent collectors and aggregations
- Support for multi-gigabit rates
- Platform Richness (ISR, Cat65xx, 7600, Appliances)
- Higher Scalability with local analytics

**NAM Customer: “Why do I need NetQoS?”**

- Enterprise-wide reporting
  - Complement real time analytics troubleshooting with exception-based, proactive network management
  - Multi NAM reporting solution to scale to the largest enterprise networks
  - Incidents, automated investigations, SLAs, and subnet reporting
- NetQoS is the recognized platform within Cisco for reporting and analysis (e.g. WAAS, ACE, CAT6K, NAM, NetFlow, IP SLA, CBQoS, NBAR)
- Application Performance troubleshooting from SuperAgent Management Console to the high granularity NAM real time analytics
Compuware Vantage-NAM Integration

- Vantage collects Intelligent Application Performance (IAP) metrics from multiple NAMs
- The Vantage Analysis Server (VAS) builds an enterprise view of application usage and performance for all users
- NAMs are installed at locations strategic to specific traffic monitoring and analysis requirements
  - Data centers, branch offices, etc.
- All NAM platforms are supported
  - Version 4.1 is required
### Compuware Complements Cisco’s NAM Offering

<table>
<thead>
<tr>
<th>Cisco NAM</th>
<th>Compuware Supporting Value</th>
<th>Customer Advantage</th>
</tr>
</thead>
</table>
| Application performance monitoring | ▪ Multiple NAM reporting  
▪ Quantify affected users by business applications and locations  
▪ Business transaction monitoring for web and non-web applications (e.g. web page load) | ▪ Comprehensive network visibility  
▪ Fault domain isolation across the client, network, server and application  
▪ Business impact quantification and enhanced problem resolution  
▪ Application performance as seen from the end user transaction perspective |
| Real-time and historical reporting | ▪ Baselines  
▪ Historical trending across applications and locations | ▪ Real-time problem identification  
▪ Cisco architecture and capacity planning decisions based on business demand |
| Problem resolution | ▪ Navigate from enterprise wide reports to NAM for advanced troubleshooting | ▪ Reduced MTTR to effectively identify the fault domain between the client, network, and data center tiers |
| End-to-end visibility into WAAS deployments | ▪ WAAS reporting from the client, optimized link and data center perspectives across the enterprise | ▪ Quantification of the response time and capacity improvements |
Voice Quality Analytics
Voice Quality Analytics
Assure the Effective Delivery of Voice Services

- Gain visibility into how users experience voice services
  - Obtain real-time quality metrics on voice performance using standards-based MOS
- Improve voice performance with intelligent troubleshooting
  - Use indicators such as jitter and packet loss to pinpoint and correct poor performance
- View voice quality enterprise-wide
  - Get the big picture with consolidated end-to-end monitoring, troubleshooting, and reporting – NAM as a key component of the UC suite of management solutions
Standards-based Voice Quality Monitoring

- Reports MOS every 1-min based on 3-sec data-points, for each active RTP stream
- Calculates MOS based on ITU-T Recommendations G.107
- Analyze voice quality trends over time

Pinpoint the individual RTP stream experiencing degraded voice quality

Investigate network performance indicators (Jitter, Packet Loss, SoC, SSC)
Integration with Cisco Unified Communication Management Suite

- NAM complements CUCMS with network visibility and advanced troubleshooting
- NAM offers scalable and flexible deployment options (Wiring Closet, Access, Distribution, Campus Edge)
- CUSM rolls-up voice metrics to deliver enterprise-wide service quality view
- CUSM generates alerts on service quality degradations
- CUOM allows drill-down to NAM for near real-time views and advanced troubleshooting

Cisco NAM complements with CUCMS to deliver an enterprise-wide voice management solution

<table>
<thead>
<tr>
<th>Sensor 1040</th>
<th>NME-NAM</th>
<th>NAM-2</th>
<th>NAM 2204 Appliance</th>
<th>NAM 2220 Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>100</td>
<td>400</td>
<td>1500</td>
<td>4000</td>
</tr>
</tbody>
</table>
Troubleshooting Voice Quality

- Assess MOS distribution to detect poor quality calls
- Troubleshoot by Worst-N calls, Known Phones or RTP streams
- Pinpoint to individual call or RTP stream experiencing degraded voice quality
- Investigate the root-cause
  - Assess network performance indicators (Jitter, Packet Loss, SoC, SSC)
  - View VoIP traffic by DSCP values
  - Analyze interface statistics
  - Monitor Cisco Communication Manager response time using IAP analytics
Use Case: Voice Quality Analytics

1. Monitor Active Calls MOS Quality
   Number of poor calls increase
2. Drill down into the RTP Stream, observe an increase in Packet loss.
3. Drill down to interface utilization/QoS parameter

Note: Reports related to Worst Phones, Worst Calls, Call Volume, Top RTP Streams help in identifying call patterns and transient quality problems.
Video (RTP) Quality Monitoring

- Provides real-time video packet loss statistics
- Includes src/dest address filter to monitor key RTP streams of interest
- Key data includes RTP packet count, packet loss, and packet loss rate
- Enables alarm thresholds to be set on packet loss variables
- Logs RTP packet loss events as syslog

<table>
<thead>
<tr>
<th>RTP Stream Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Address (Port): 16.26.3.143 / 22335</td>
</tr>
<tr>
<td>Destination IP Address (Port): 16.21.3.143 / 5064</td>
</tr>
<tr>
<td>Payload Type: G711 U-law/8k</td>
</tr>
<tr>
<td>SSRC: 113</td>
</tr>
<tr>
<td>Total Duration Monitored (seconds): 70</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stream Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worst / Avg / Max MOS: 4.05 / 4.37 / 4.30</td>
</tr>
<tr>
<td>Worst / Avg / Min Inter Packet Loss (ms): 1.58 / 2.81 / 1.58</td>
</tr>
<tr>
<td>Worst / Avg / Min Adjusted Packet Loss (%): 0.18 / 0.45 / 0.00</td>
</tr>
<tr>
<td>Worst / Avg / Min Actual Packet Loss (%): 0.00 / 0.00 / 0.00</td>
</tr>
<tr>
<td>Worst / Avg / Min Seconds of Concealment: 2.0 / 0.0 / 0.0</td>
</tr>
<tr>
<td>Worst / Avg / Min Seconds of Severe Concealment: 1.0 / 0.0 / 0.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Last N Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Timestamp</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>18-17-19 09:49:06 America/Los_Angeles</td>
</tr>
<tr>
<td>18-17-19 09:48:40 America/Los_Angeles</td>
</tr>
</tbody>
</table>
QoS Monitoring (DSMON)

- Validate planning assumptions and QoS allocations
- Detect incorrectly marked or unauthorized traffic
- View VoIP traffic by DSCP values
Support for Mobility Environments
GTP (GPRS Tunneling Protocol)

NAM enables:
- Visibility into GTP Traffic between Mobile station and the GGSN
- Targeted packet capture
- Manageable packet capture files

Benefits include:
- Management simplicity avoiding wrongly routed traffic & application outage
- Avoid “looking for a needle in a haystack”

Gateway GPRS Support Node (GGSN): Converts GPRS packets from SGSN to IP traffic

Serving GPRS Support Node (SGSN): Serves mobile ‘stations’ and interfaces with GGSN
**NetFlow and RMON Monitoring**

- **NetFlow** provides application-level visibility
  - NAM both collects and analyzes NetFlow
- **NAM** monitors NetFlow on an aggregate basis
  - Applications, Hosts, Conversations
  - Can monitor more traffic as the NAM analyzes flows not actual packets
- **NAM** can process NetFlow data from remote switch and routers
- **RMON** packet monitoring provides detailed analysis of traffic of interest (Additional visibility over NetFlow)
  - Voice, ART, QoS, packet decode

<table>
<thead>
<tr>
<th>RMON/NetFlow support in NAM</th>
<th>Applications</th>
<th>RMON and NetFlow</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hosts</td>
<td>RMON and NetFlow</td>
</tr>
<tr>
<td></td>
<td>Conversations</td>
<td>RMON and NetFlow</td>
</tr>
<tr>
<td></td>
<td>Voice</td>
<td>RMON</td>
</tr>
<tr>
<td></td>
<td>VLAN</td>
<td>RMON</td>
</tr>
<tr>
<td></td>
<td>ART</td>
<td>RMON</td>
</tr>
<tr>
<td></td>
<td>DiffServ</td>
<td>RMON</td>
</tr>
<tr>
<td></td>
<td>PortStats</td>
<td>RMON</td>
</tr>
</tbody>
</table>
Port Monitoring

- View traffic statistics on all ports
- Traffic statistics include utilization, bytes, packets, broadcasts, multicasts, and errors
- Drill-down on a particular port to obtain more granular details
Switch/Router Health Monitoring

- Monitor vital switch/router resources such as CPU usage, backplane bandwidth, memory usage, temperature and fan status, sysUpTime, and power supply status
- Provides immediate information on the health of critical network devices

Tight integration with the switch/router permits the NAM to monitor and track important infrastructure health diagnostics.
Other NAM Use Cases
Troubleshoot Intermittent Branch Connectivity

Challenges
- Lack of end-to-end visibility and centralized manageability in a large network with 500+ sites

Solution
- NAM aggregates/analyzes traffic from multiple data sources to troubleshoot the problem:
  - NetFlow from remote router
  - SPAN data from the host switch
  - Local switch information on the host switch
- NAM offers embedded Traffic Analyzer web interface that can be accessed remotely eliminating the need to send personnel to remote sites or haul large amounts of data over WAN links to the central site.

Conclusion
- Problem isolated to a faulty network interface card on the switch. NAM provided both local and remote visibility to quickly troubleshoot the problem
Deliver LAN-like application performance levels to remote users
-WAN bandwidth bottlenecks cause application performance issues
-Loss of visibility due to application traffic intercepted by WAN optimization technologies

NAM Solution Facilitates Data Center Consolidation
-Offers end-to-end application performance visibility from branch to data center
-Integrates with WAAS to accurately characterize the performance of optimized applications
-Combines performance monitoring, traffic analysis and advanced troubleshooting to help ensure the consistent and efficient delivery of applications to end users.
-Helps sell more Cat6K switches in the data center, and
-Positions WAAS as a complete solution for application delivery
Understand Impact of Infrastructure Upgrades

- Insurance company in the midst of network infrastructure refresh is concerned about the impact of the refresh on application performance across various sites

- They deploy NAM-2 on Cat6500 in all data centers to obtain application visibility and monitor application response times
  
  Baseline network and application performance at all branch sites before the upgrade

  Monitor the application response time during the upgrade using threshold-based alarms to proactively detect any deviation from baseline

  Proactively fix performance degradations detected during the transition

- Improvement in application response time justified the infrastructure upgrade
Monitor Load Balancer Effectiveness

- Healthcare provider is in the midst of data center consolidation, deploying business-critical Siebel CRM application supporting more than 3500 customer service representatives.

- Load balancer service module is deployed on Cat6500 switch to ensure effective distribution of load across the server farm.

- Traffic from both WAN and server side of the load balancer is directed to NAM (service module on Cat6500) for analysis. NAM monitors the traffic distribution across servers by measuring the number of packets being sent to each server.
  - Top N Host report displays the servers (hosts) and their "bytes/packets in/out" statistics.
  - A detailed report including all servers in the farm will indicate whether the load is fairly distributed across all servers (load balancer is doing its job), or whether it is skewed towards 1 or 2 servers (load balancer is not effective).

- NAM reports validate the impact of the load balancer service module by showing pre- and post-deployment traffic reports. This allows IT to justify the investment.
Additional Resources

- Questions:
  ask-c6500-pm@cisco.com, ask-nam-pm@cisco.com

- Cat6500 NAM Collateral (internal)

- Cisco ISR NAM Collateral (internal)

- NAM Training

- NAM Tech Docs

- NAM Online Demo
Q and A