



# Overview Presentation: Cisco Branch Routers Series Network Analysis Module



November 2006

# Customer Challenges

- Networks have become increasingly complex
- It's no longer enough to ensure traffic flow from one point to another—now you must also ensure optimum performance
- Need clarity on how to tie user and business needs together
- Need to move beyond reactive management



# The Solution: Cisco Network Analysis Module (NAM)

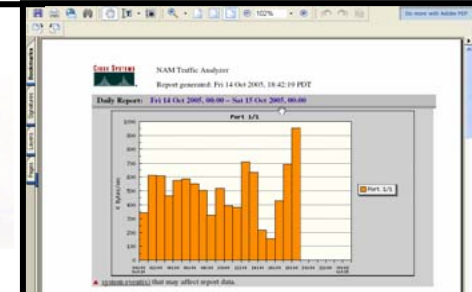
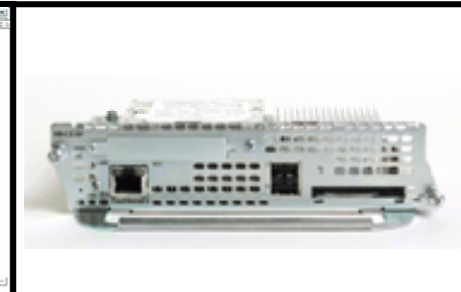
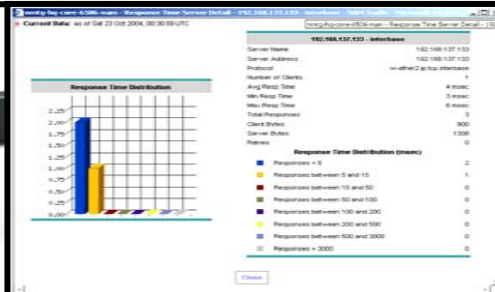
## Cisco® NAM Feature

- **Traffic analysis integrated in the network**  
Critical points, Web-based GUI
- **Real-time and historical monitoring**  
Applications, hosts, conversations
- **Application response time monitoring**  
User's experience of the network
- **Troubleshooting**  
Packet capture and decode



## Benefits

- **Eases deployment, management, and support**
- **Detects how applications and users use the network and receive services**
- **Reveals how applications are performing**
- **Isolates problems before they affect users**



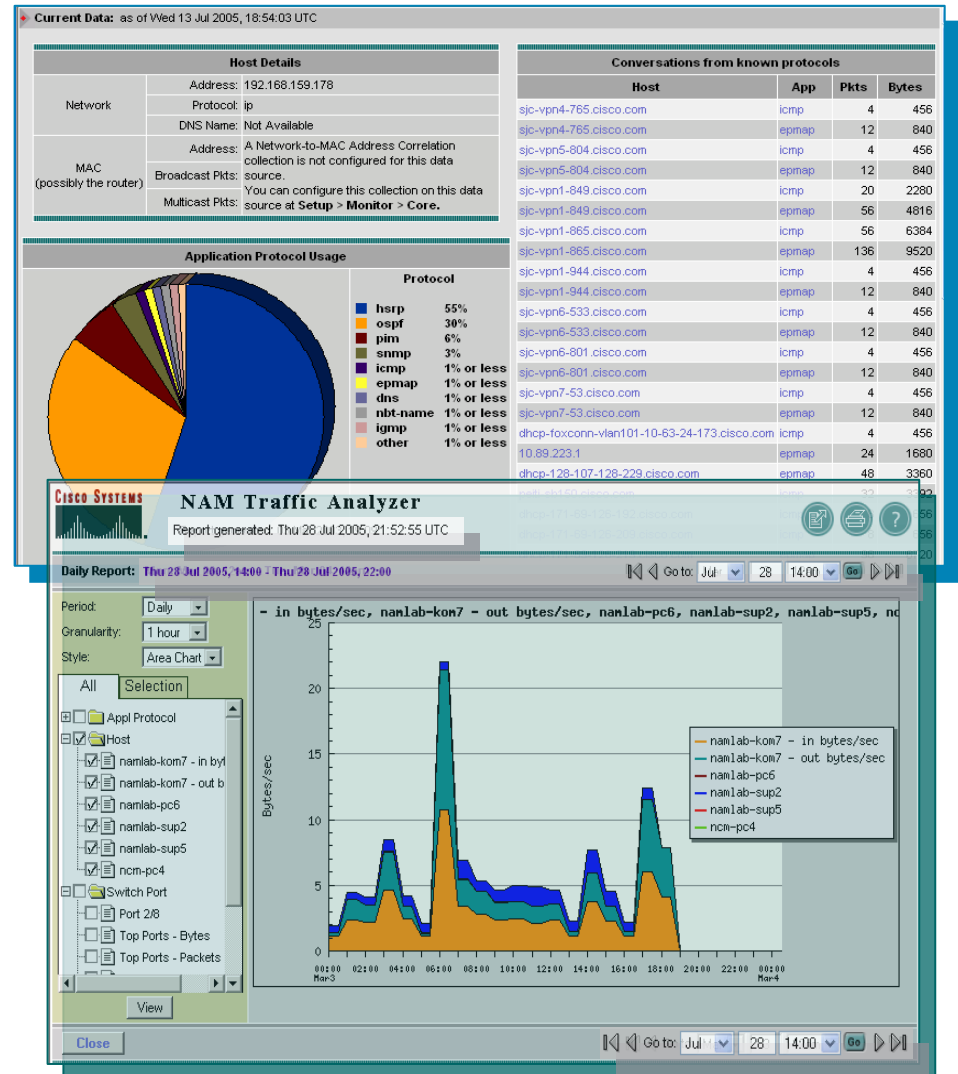
# Cisco Branch Routers Series NAM

- Features and Functions



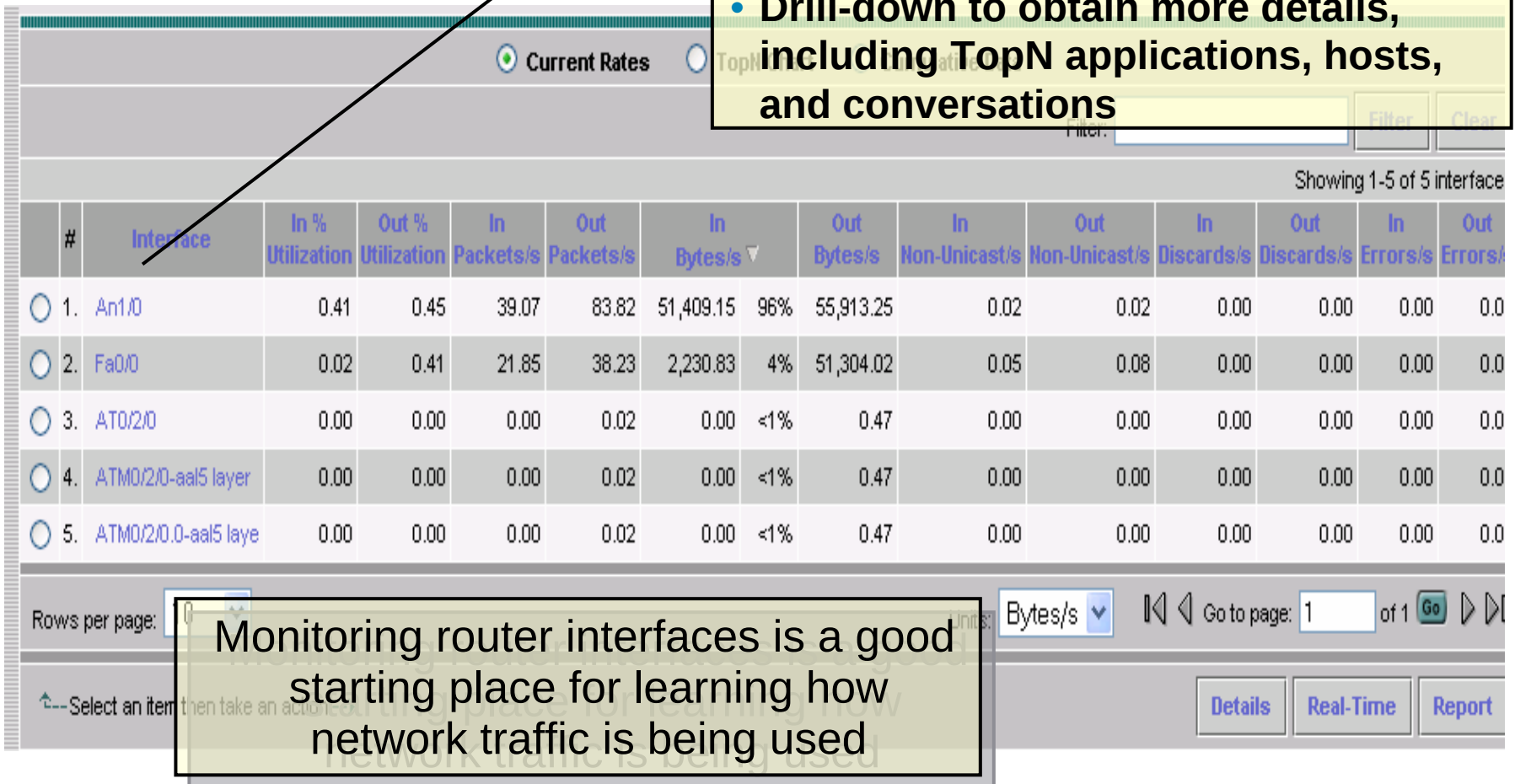
# Embedded Traffic Analyzer Software

- **Configuration of the NAM**
  - Network parameters
  - Selection of traffic to monitor
  - Types of statistics to gather
- **Real-time and historical reports**
  - MIB-II monitoring
  - Application, hosts, and conversation monitoring
  - Packet capture and decode
  - Application response time monitoring
  - Voice over IP (VoIP) and video monitoring
  - Differentiated Services (DiffServ) monitoring



# Interface Monitoring

- View traffic statistics for all interfaces
- Drill-down to obtain more details, including TopN applications, hosts, and conversations



Showing 1-5 of 5 interface

| #  | Interface             | In % Utilization | Out % Utilization | In Packets/s | Out Packets/s | In Bytes/s | Out Bytes/s | In Non-Unicast/s | Out Non-Unicast/s | In Discards/s | Out Discards/s | In Errors/s | Out Errors/s |
|----|-----------------------|------------------|-------------------|--------------|---------------|------------|-------------|------------------|-------------------|---------------|----------------|-------------|--------------|
| 1. | An1/0                 | 0.41             | 0.45              | 39.07        | 83.82         | 51,409.15  | 96%         | 55,913.25        | 0.02              | 0.02          | 0.00           | 0.00        | 0.00         |
| 2. | Fa0/0                 | 0.02             | 0.41              | 21.85        | 38.23         | 2,230.83   | 4%          | 51,304.02        | 0.05              | 0.08          | 0.00           | 0.00        | 0.00         |
| 3. | AT0/2/0               | 0.00             | 0.00              | 0.00         | 0.02          | 0.00       | <1%         | 0.47             | 0.00              | 0.00          | 0.00           | 0.00        | 0.00         |
| 4. | ATM0/2/0-aal5 layer   | 0.00             | 0.00              | 0.00         | 0.02          | 0.00       | <1%         | 0.47             | 0.00              | 0.00          | 0.00           | 0.00        | 0.00         |
| 5. | ATM0/2/0.0-aal5 layer | 0.00             | 0.00              | 0.00         | 0.02          | 0.00       | <1%         | 0.47             | 0.00              | 0.00          | 0.00           | 0.00        | 0.00         |

Rows per page: 0

Units: Bytes/s

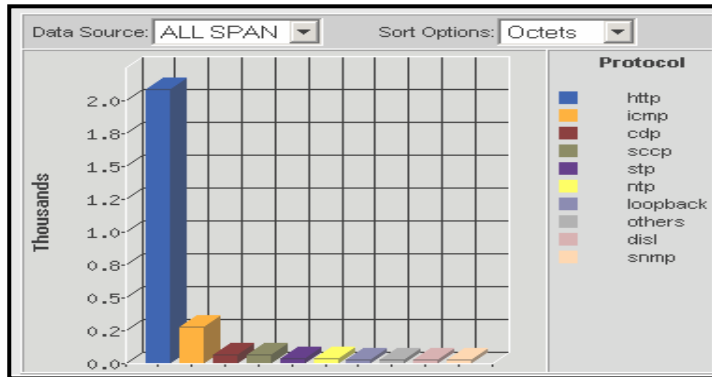
Go to page: 1 of 1

Details Real-Time Report

Monitoring router interfaces is a good starting place for learning how network traffic is being used

# Application, Host, and Conversation Monitoring

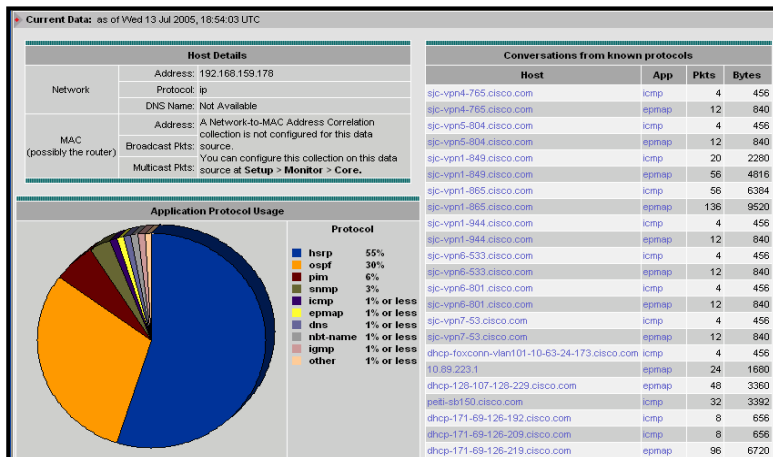
## Protocol Distribution



## Conversation Pair Statistics

| #  | Source                       | Via | Destination                  | Pkts | Octets |
|----|------------------------------|-----|------------------------------|------|--------|
| 1  | namlab-pik2.cisco.com        | ip  | static-10-24-2-108.cisco.com | 1    | 1510   |
| 2  | dhcp-171-69-69-92.cisco.com  | ip  | namlab-shared.cisco.com      | 1    | 424    |
| 3  | static-10-24-2-108.cisco.com | ip  | namlab-pik2.cisco.com        | 1    | 273    |
| 4  | 10.0.0.22                    | ip  | namlab-pc5.cisco.com         | 1    | 102    |
| 5  | namlab-pc5.cisco.com         | ip  | 10.0.0.22                    | 1    | 102    |
| 6  | namlab-sup1.cisco.com        | ip  | cbucci-uf10.cisco.com        | < 1  | 9      |
| 7  | cbucci-uf10.cisco.com        | ip  | namlab-sup1.cisco.com        | < 1  | 8      |
| 8  | 172.20.98.129                | ip  | namlab-sup1.cisco.com        | < 1  | 7      |
| 9  | 172.20.98.129                | ip  | namlab-sup2.cisco.com        | < 1  | 7      |
| 10 | 172.20.98.129                | ip  | namlab-sup3.cisco.com        | < 1  | 7      |

Go To Entry: of 62 Go Prev Next

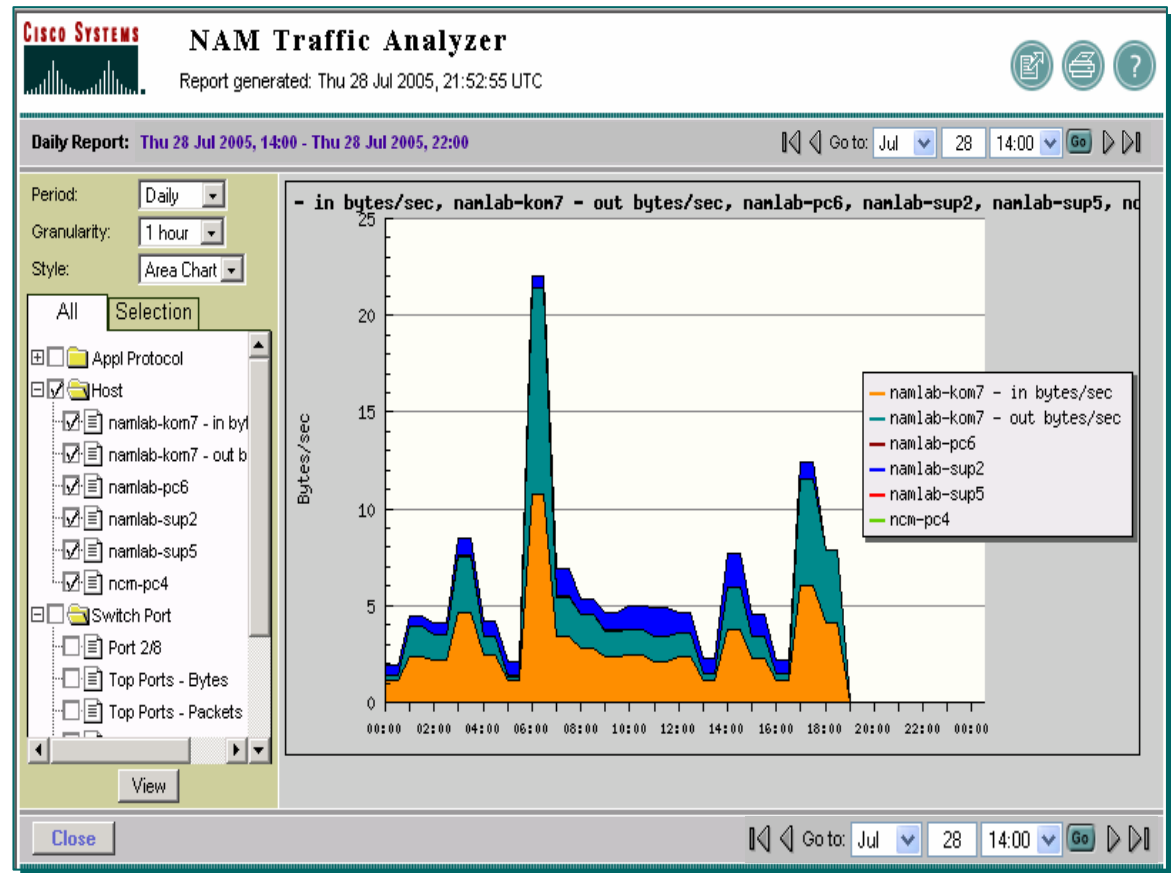


NAM detects the applications, the bandwidth they consume, and the hosts using costly WAN resources

## Detailed Host and Conversation Statistics

# Historical Reporting

- Select and monitor network performance over time
- 100-day historical reports for preselected variables
- Detailed information to support planning activities and to aid postevent troubleshooting



# Packet Capture and Decode

The screenshot displays a network packet capture tool interface. At the top, there are tabs for Setup, Monitor, Reports, Capture, Alarms, and Admin. Below these is a breadcrumb trail: Settings > Decode > Download > Custom Filters > . The main area shows 'Packets: 1-1000 of 1756' with navigation buttons (Stop, Prev, Next, Go to) and a search filter. A table lists the first four packets, showing details like time, size, source, destination, protocol, and info. Packet 1 is selected, and its details are expanded in the lower section, showing the protocol stack (Ethernet II, VLAN, IP, TCP, HTTP) and the raw packet data in hexadecimal and ASCII.

| Pkt | Time(s) | Size | Source                 | Destination           | Protocol | Info                                           |
|-----|---------|------|------------------------|-----------------------|----------|------------------------------------------------|
| 1   | 0.000   | 387  | sjc-vpn3-255.cisco.com | nam-6506.embu-mlab... | HTTP     | GET /capture/getstatus.php HTTP/1.1            |
| 2   | 0.367   | 68   | sjc-vpn3-255.cisco.com | nam-6506.embu-mlab... | TCP      | 1157 > http [ACK] Seq=31746281 Ack=14166704... |
| 3   | 10.227  | 387  | sjc-vpn3-255.cisco.com | nam-6506.embu-mlab... | HTTP     | GET /capture/getstatus.php HTTP/1.1            |
| 4   | 10.703  | 68   | sjc-vpn3-255.cisco.com | nam-6506.embu-mlab... | TCP      | 1157 > http [ACK] Seq=31746606 Ack=14166708... |

**Packet** Number: 1 - Time: Jul 27, 2005 18:26:20.153 - Packet Length: 387 bytes - Capture Length: 387 bytes

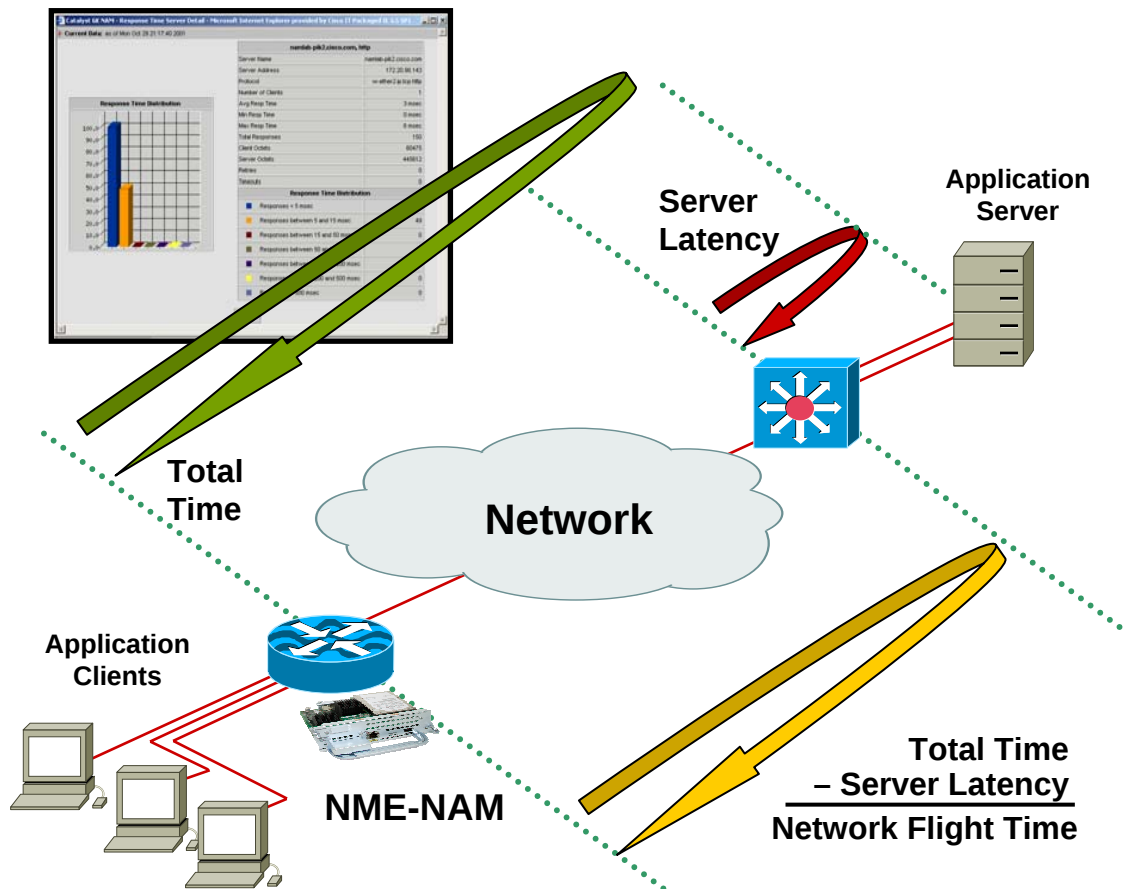
- ETH** Ethernet II, Src: 00:d0:bc:f4:8f:08, Dst: 00:e0:b0:ff:39:78
- VLAN** 802.1q Virtual LAN
- IP** Internet Protocol, Src Addr: sjc-vpn3-255.cisco.com (10.21.64.255), Dst Addr: nam-6509.embu-mlab.cisco.com (192.168.76.12)
- TCP** Transmission Control Protocol, Src Port: 1157 (1157), Dst Port: http (80), Seq: 31745956, Ack: 1416670066, Len: 325
- HTTP** Hypertext Transfer Protocol
  - GET /capture/getstatus.php HTTP/1.1\r\n
  - Accept-Language: en\r\n
  - Accept: text/html, image/gif, image/jpeg, \*, q=.2, \*

0000 00 e0 b0 ff 39 78 00 d0 bc f4 8f 08 81 00 00 00 ...X.....C  
 0010 08 00 45 00 01 6d 63 b7 40 00 77 06 47 0b 0a 15 ..E..mc.@.w.G...  
 0020 40 ff c0 a8 4c 0c 04 85 00 50 01 e4 67 a4 54 70 @...L....P..g.Tp  
 0030 ab 72 50 18 22 45 52 f4 00 00 47 45 54 20 2f 63 .rP."ER...GET /c  
 0040 61 70 74 75 72 65 2f 67 65 74 73 74 61 74 75 73 apture/getstatus  
 0050 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 41 .php HTTP/1.1..A  
 0060 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 ccent-Language:

**Support troubleshooting efforts with trigger-based captures, filters, decodes, and a capture-analysis toolset**

# Application Response Time (ART) Monitoring

Learn how users experience application performance



- Statistics include Client-Server Network Round Trip Time, Application Response Time, Total Transaction Time
- Displays the data in intuitive tables and graphs
- Historical viewing and reporting

# Voice Monitoring

- Active IP telephony monitoring
  - Track active call attributes
  - Identify call quality degradation via packet loss and jitter statistics
  - See call details for individual phones
- Voice-application monitoring
  - View distribution of VoIP protocols
- Application response time (ART)
  - Measure Cisco® CallManager response times
- QoS
  - Monitor voice traffic for QoS violations
  - Verify that voice traffic is receiving the appropriate priority
- Video telephony
  - Identify active video calls

Anticipate infrastructure improvements needed to support increased demand in voice services

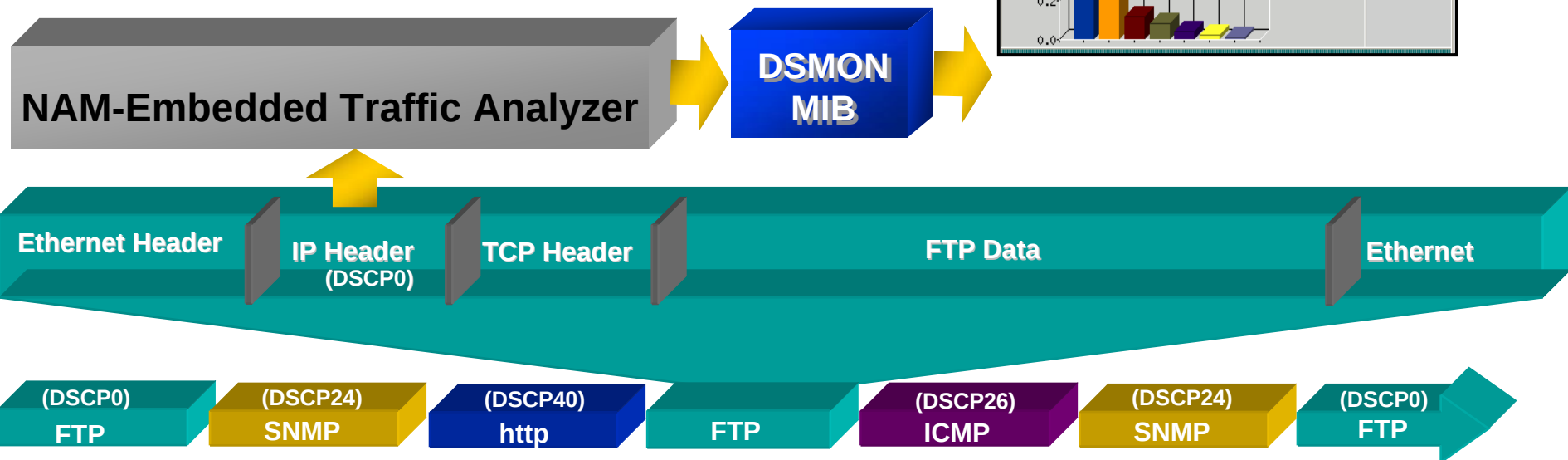
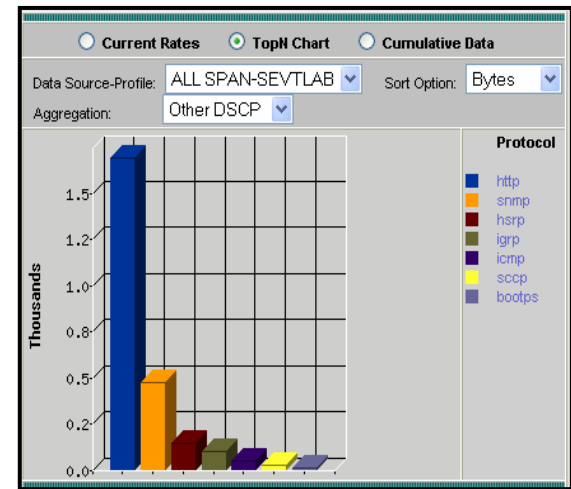


| SCCP call detail for called party |                               |                 |
|-----------------------------------|-------------------------------|-----------------|
|                                   | Calling Party                 | Called Party    |
| Phone Number:                     | 1101                          | 1001            |
| IP Address:                       | 191.167.138.42                | 192.168.159.203 |
| Call Reference:                   | 16784794                      |                 |
| Owner:                            | -                             | -               |
| Call State:                       | On Hook                       |                 |
| RTP Port:                         | 65535                         | -               |
| Line Instance:                    | 1                             |                 |
| Conference Id:                    | 16784794                      |                 |
| Pass Thru Party Id:               | 16898465                      |                 |
| RTP Sampling Period:              | 20                            |                 |
| Payload Type:                     | G.711 ulaw 64k                |                 |
| RTP Pre Value:                    | 184                           |                 |
| Silence Suppression:              | Off                           |                 |
| Max Frames per Pkt:               | 0                             |                 |
| G.723 Bit Rate:                   | -                             |                 |
| Start Time:                       | Thu 28 Jul 2005, 22:36:43 UTC |                 |
| End Time:                         | Thu 28 Jul 2005, 22:36:43 UTC |                 |
| Packets Sent:                     | 0                             |                 |
| Packets Received:                 | 0                             |                 |
| Octets Sent:                      | 0                             |                 |
| Octets Received:                  | 0                             |                 |
| Packet Loss (%):                  | 0.00                          |                 |
| Jitter (msec):                    | 0                             |                 |
| Switch Port:                      | -                             |                 |

# Differentiated Services Monitoring (DSMON)

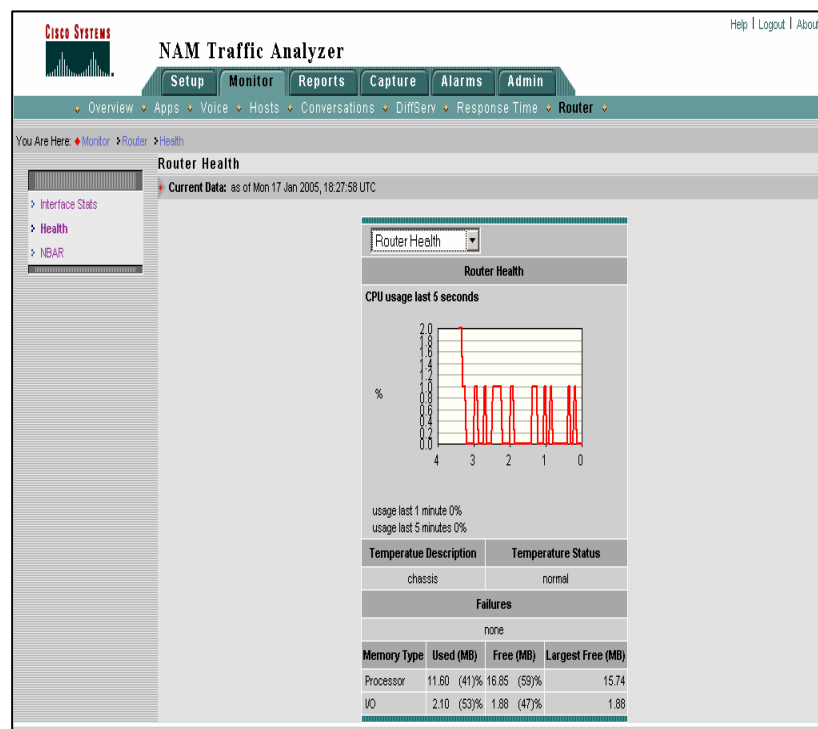
DiffServ monitoring can be used to:

- Validate planning assumptions and QoS allocations
- Detect incorrectly marked or unauthorized traffic



# Router Health Monitoring

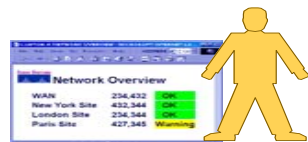
- Monitor vital router resources such as CPU usage, memory usage, temperature and fan status, sysUpTime, hardware revisions, and power-supply status
- Provides the network manager with immediate information on the health of critical network devices



**Tight integration with the router permits the NAM to monitor and track important infrastructure health diagnostics**

# Managing NAM— Cisco Performance Visibility Manager (PVM)

Available Now



Reports

API

- Data collection, aggregation, correlation
- Application response time correlation
- Traffic analysis
- Bandwidth utilization
- Baselining
- Monitoring based on policy and thresholds
- History and trending

RMON  
ART MIB  
DSMON  
SMON  
Mini-RMON

Cisco® NAMs

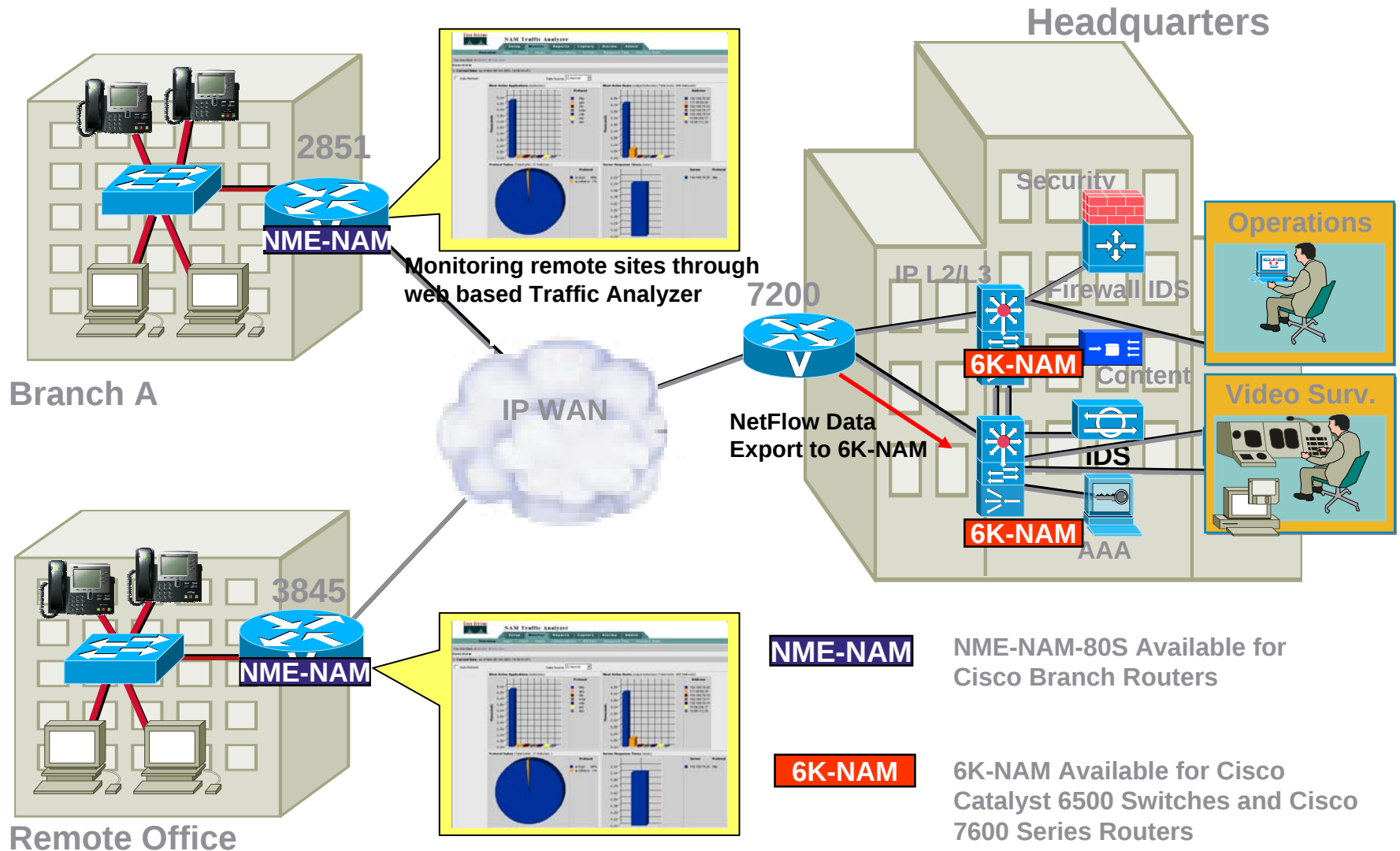


NetFlow



Cisco Confidential – NDA Use Only

# Deployment Scenario: NAMs in LAN and WAN



# Business Benefits

- **Gain visibility into the network services and applications that make up the business**

**Monitor how applications and users utilize the network and receive services**

**Improve network performance**

- **Better visibility enables enterprises and service providers to optimize IT investments and enhance network security**

**Prevent unauthorized or frivolous use of network resources**

**Reduce downtime and failures**

- **“Right-size” the network to reduce network spending**

**Determine services trends to anticipate infrastructure improvements that will be needed to support increased demand**

**Tie network usage to business need**

