Understanding Service Level and Traffic Management

Session NCM-208

Performance vs. Fault Management

Service Level Management

Users

Fault Management

Performance Management

Devices & Software
Session Focus

• This presentation looks at some tools available for traffic and service level management—it is by no means an exhaustive review
• It also focuses primarily on the monitoring component of management—leaving provisioning as a separate exercise

Agenda

• Traffic Management
• Service Level Management
• Tools and Technologies
• Case Studies
Traffic Management

Traffic Management in a Multiservice Network

Network Must Provide Each Application With Different Service Level Characteristics Simultaneously
Traffic Management Challenges

• Planning
  Verify application impact on the network and vice-versa
  Deployment of new applications and services
  Gain understanding of traffic flows
  Utilization and latency dependent on application mix

• Troubleshooting
  Bursts in traffic load caused by applications
  Service degradation
  Rogue applications that hijack the network
  Misconfigured applications

Performance Measurement Strategies

<table>
<thead>
<tr>
<th>Synthetic</th>
<th>Observed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Agents</td>
<td>External Probes</td>
</tr>
<tr>
<td>Device/Link</td>
<td>End-to-End/Path</td>
</tr>
<tr>
<td>User</td>
<td>Network</td>
</tr>
</tbody>
</table>
## Sampling Method

<table>
<thead>
<tr>
<th>Observed</th>
<th>Synthetic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong></td>
<td>Actual end-user network traffic where performance is measured by timing specific application traffic flows</td>
</tr>
<tr>
<td><strong>Advantages</strong></td>
<td>Most accurate for live application traffic on a specified link</td>
</tr>
<tr>
<td><strong>Disadvantages</strong></td>
<td>Limited to measuring: Existing traffic types, which may not be present on the network at all times Existing traffic patterns, which may not reflect patterns for new or future applications</td>
</tr>
</tbody>
</table>

| **Definition** | Network traffic generated strictly for the purpose of measuring a network performance characteristic |
| **Advantages** | Measures performance: Between any two points in the network Controllable, on a continuous basis By traffic class based on IP Precedence marking |
| **Disadvantages** | Only an approximation for performance of live traffic |

## Collection Method

<table>
<thead>
<tr>
<th>Embedded</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong></td>
<td>Mechanisms for collection of network statistics are integrated into the network communication device (e.g., router or switch), itself</td>
</tr>
<tr>
<td><strong>Advantages</strong></td>
<td>Follows network infrastructure Gathers metrics that can not be observed externally</td>
</tr>
<tr>
<td><strong>Disadvantages</strong></td>
<td>Performance monitoring has device-level performance implications</td>
</tr>
</tbody>
</table>

| **Definition** | Mechanisms for collection of network statistics are provided by a stand-alone device specifically designed to collect network performance statistics |
| **Advantages** | Validation of performance performed independent of the devices that transmit network traffic |
| **Disadvantages** | More hardware to administer Observed statistics limited to points of deployment |
### Scope of Measurement

#### Device or Link Oriented

- **Definition**
  Performance measurement based on analysis of specific device or device interface, and typically based on utilization rates.

- **Advantages**
  - Detailed application performance monitoring of critical network links.

- **Disadvantages**
  - When network-wide performance problems exist, how does one select which device or link to evaluate?

#### End-to-End

- **Definition**
  Performance measurement based on analysis of response time across two or more network devices, and typically based on latency.

- **Advantages**
  - Starting point performance troubleshooting.
  - Reflects end-user experience.

- **Disadvantages**
  - Prior knowledge of relevant end-to-end paths is needed.

### Perspective of Measurement

#### User

- **Definition**
  Measurement based on performance statistics measured at the end-user workstation.

- **Advantages**
  - Accurate measurement of end-user experience.

- **Disadvantages**
  - Scale and distribution issues.
  - Intrusive on the desktop.

#### Network

- **Definition**
  Measurement based on performance statistics measured in network devices.

- **Advantages**
  - Easy to deploy, and non-intrusive to the desktop.
  - Identifies network performance issue.

- **Disadvantages**
  - Imperfect understanding of end-user experience.
Service Level Management

Network Must Provide Each Application With Different Service Level Characteristics Simultaneously
Service Level Management Challenges

Traffic Management

Plus

End-to-End Abstraction

Service Management

• Measuring
  Current traffic and service metrics

• Defining
  Policies and services
  Demarcations
  Service elements

• Implementing
  Cross-Boundary
  Organization
  Technology

1. Gather Service And Traffic Metrics
2. Determine How to Shape SLAs, Business
3. Design and Alter to Suit
Measuring Current Metrics

- **Synthetic vs. Observed**
- **Collection Method**: Embedded Agents vs. External Probes
- **Scope of Measurement**: Device/Link vs. End-to-End/Path
- **Perspective of Measurement**: User vs. Network

Defining Policies and Services

- **Service Quality Level**
  - Latency
  - Errors
  - Jitter
  - Other
  - Throughput
  - Availability
  - (Mean) Time to Restore Service
  - (Mean) Time to Repair
  - (Mean) Provisioning Time

- **Service Intrinsic**
- **Operational**
Defining SLM Policies and Services

- Security
- Time
- Application/protocol
- People

Defining Demarcations

Other Domains
- Network Hardware
- Workstation Hardware
- Application Software
- Etc.
Defining Service Elements

- Network
- Path
- Link
- Firewall
- Application
- Server

Example: Service Elements in Content Delivery Networks

Content Delivery Services
- Web Hosting
- E-Commerce
- Streaming
- Applications

Content Delivery Networks
- Content Distribution and Management
- Content Routing
- Content Switching
- Content Edge Delivery

Intelligent Network Services

Highly Available, Scalable, Performance Network at Layer 2/3

Core Networking
Content Routing
Content Switching
Content Edge Delivery
Content-aware Services
Content Distribution and Management
Origin Web Servers
Origin Data Stores

Mobile
Fixed Wireless
Cable
DSL
Dedicated/ISDN/Dial
ATM/FR

NCM-208
2044_05_2001_c1
©2001, Cisco Systems, Inc. All rights reserved.
23

NCM-208
2044_05_2001_c1
©2001, Cisco Systems, Inc. All rights reserved.
24
Implementing SLM across Boundaries

- Enterprise
  - Measure from CPE
  - Measure network layer
  - Measure application response and availability
- Service provider
  - Measure edge-to-edge
- Both
  - Define common metrics
  - Define common tests
  - Define information interchange
# Tools and Technologies

## Measurement Technologies

<table>
<thead>
<tr>
<th><strong>NetFlow</strong></th>
<th><strong>ART MIB</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>MEASURES: Device interface traffic rate by s/d IP address, port number or AS</td>
<td>MEASURES: Response time of live application traffic to server device</td>
</tr>
<tr>
<td>Sampling: Observed</td>
<td>Sampling: Observed</td>
</tr>
<tr>
<td>Collection: Embedded</td>
<td>Collection: External Probe</td>
</tr>
<tr>
<td>Scope: Device/Link</td>
<td>Scope: End-to-End</td>
</tr>
<tr>
<td>Perspective: Network</td>
<td>Perspective: User/Network</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SA Agent</strong></th>
<th><strong>IPSec MIBs</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>MEASURES: Latency and Jitter between source router and specified target</td>
<td>MEASURE: Tunnel trends and failures, tunnel to policy mappings, IOS configurations</td>
</tr>
<tr>
<td>Sampling: Synthetic</td>
<td>Sampling: Observed</td>
</tr>
<tr>
<td>Collection: Embedded</td>
<td>Collection: Embedded</td>
</tr>
<tr>
<td>Scope: End-to-End</td>
<td>Scope: End-to-End</td>
</tr>
<tr>
<td>Perspective: User/Network</td>
<td>Perspective: User/Network</td>
</tr>
</tbody>
</table>
NetFlow Defined

- Flows are defined by 7 keys:
  - Source address
  - Destination address
  - Source port
  - Destination port
  - Layer 3 protocol
  - TOS byte (DSCP)
  - Input interface
- Flows are unidirectional
- Flows are enabled on a per input-interface basis
- Flows can be configured "on-demand" or continuous

Flow Data Exported to Management Application
NetFlow Data Record per Flow

RMON Accessible
- Packet count
- Byte count
- Source IP address
- Destination IP address
- Source prefix mask
- Destination prefix mask
- Source AS number
- Destination AS number
- Source TCP/UDP port
- Destination TCP/UDP port

Routing and Peering

Device Interface
- Input interface
- Output interface

Application

QoS
- Type of service
- TCP flags
- Protocol
- Source TCP/UDP port
- Destination TCP/UDP port

Non-RMON
- Number of flows
- Flow size distribution
- Source IP address
- Destination IP address
- Source prefix mask
- Destination prefix mask
- Source AS number
- Destination AS number

Time Stamp
- Start timestamp
- End timestamp
- Call duration
- Next hop address
- Lost datagrams

NetFlow Export

- Versions 1, 5, 8—Cisco IOS routers
- Version 7—Cat5000(NFFC), Cat6000(MSFC)
NetFlow v8 Aggregation

<table>
<thead>
<tr>
<th>Aggregation</th>
<th>Identifies</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASMatrix</td>
<td>Autonomous System-to-Autonomous</td>
</tr>
<tr>
<td></td>
<td>System Traffic Flow Data</td>
</tr>
<tr>
<td>DestinationPrefixMatrix</td>
<td>Destinations of Network Traffic</td>
</tr>
<tr>
<td>PrefixMatrix</td>
<td>Sources and Destinations of</td>
</tr>
<tr>
<td></td>
<td>Network Traffic</td>
</tr>
<tr>
<td>ProtocolPortMatrix</td>
<td>Network Usage by Traffic Type</td>
</tr>
<tr>
<td>SourcePrefixMatrix</td>
<td>Sources of Network Traffic</td>
</tr>
</tbody>
</table>

Use NetFlow FlowCollector Version 3.0 to obtain v8 Records

NetFlow Aggregation Config Example

Router(config)#ip flow-aggregation cache as
Router(config-flow-cache)#cache entries 2046
Router(config-flow-cache)#cache timeout inactive 200
Router(config-flow-cache)#cache timeout active 45
Router(config-flow-cache)#export destination 10.42.42.1 9992
Router(config-flow-cache)#enabled
NetFlow in SLM

NetFlow/Flow Collectors/Management Application/End-User Information

NetFlow Activation and Data Collection Strategy

• Meter at edge, NOT on “hot” core routers
• Accounting applications—originating/terminating flow information
• Monitoring applications—more data intensive end-to-end view
• Key aggregation routers = less duplication in flow collection
Measurement Technologies

SA Agent

Service Assurance Agent

- Synthetic traffic for various protocols
- Supports IP precedence for QoS
- Measures latency, jitter and availability
- Deterministic testing methodology
Service Assurance Agent Operation Types

Note: IP Precedence Can Be Combined With Other Operation Types to Simulate QoS Traffic Marking

SA Agent in SLM

- Demarcation
- Deterministic
- Repeatable
Example: Creating an echo probe (TOS bits enabled, life is 200 seconds)

```
(config)#rtr 1
(config-rtr)#type jitter dest-ipaddr 10.0.0.1 dest-port 14384 source-ipaddr 10.0.0.2 source-port 14383 num-packets 47 interval 10
(config-rtr)#rtr schedule 1 life 10000000 start-time now
```

On CCO


MIB Names

CISCO-RTTMON-MIB-120_5_T.my
CISCO-RTTMON-MIB.my

Accessing SAA Data: CLI

```
(config-rtr)

---

  * Show rtr
    Configuration
    Operation
    Distribution-stats
    History
    ...  
```
Accessing SAA Data: Applications

- Cisco
  - CiscoWorks2000
  - SMS
  - IPM
  - VPN Solution Center
- Other
  - MRTG
  - Concord
  - InfoVista

Measurement Technologies

ART MIB
ART MIB Implementation Example

- Dedicated RMON probes for critical links and high-speed backbones
- ART monitoring option installed on key probes
- Application monitoring tools for measuring application performance and response time

ART MIB Functionality

- TCP protocols only (1.0)
- Based upon well-known destination port
- Default protocols:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Default MIB Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOL</td>
<td>NNTP</td>
</tr>
<tr>
<td>COMPUSRV</td>
<td>NOTESTCP</td>
</tr>
<tr>
<td>DLSW_RD</td>
<td>ORACLESQL</td>
</tr>
<tr>
<td>DLSW_WR</td>
<td>REALAUD</td>
</tr>
<tr>
<td>DNS_TCP</td>
<td>SMTP</td>
</tr>
<tr>
<td>DOOM</td>
<td>SNA_TCP</td>
</tr>
<tr>
<td>FTP-CTRL</td>
<td>SOCKET</td>
</tr>
<tr>
<td>FTP-DATA</td>
<td>SOLNET_N</td>
</tr>
<tr>
<td>HTTP</td>
<td>SUNRPC_T</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TELNET</td>
</tr>
<tr>
<td>NB_DGM_T</td>
<td>XWINDOW</td>
</tr>
<tr>
<td>NB_NS_T</td>
<td></td>
</tr>
<tr>
<td>NB_SSN_T</td>
<td></td>
</tr>
<tr>
<td>N2V3_TC</td>
<td></td>
</tr>
</tbody>
</table>

Application Level Response Time

- Client Latency
- Server Latency

Network Flight Time

Identify Application

Example: FTP

Packet-Level Measurement
ART MIB Example of Reporting

- Web accessible
  For monitoring application and web flows from anywhere, anytime
- URL visibility
  For control of your site
- Proactive management
  Alarm on responsiveness of the site or your mission critical applications
- Seamless real-time and historical
  Current statistics with look back capability

Measurement Technologies

IPSec MIBs
**IPSec VPN Types**

- **Site-to-site connection**
  - Long session lifetimes
  - Simplest form: Leased line replacement

- **Remote access**
  - Relatively short-lived sessions
  - User authentication needed
  - Remote address not known in advance

**IPSec Terminology**

- Flows
- Tunnels
- IKE/ISAKMP
- SAs
- Peers
- End points
Flow vs. SAs

- IKE tunnel = 1 ISAKMP SA
- IPSec tunnel = non-ISAKMP SA bundle
- CLI reports on SAs
- Flow MIB reports on tunnels

IPSec End Points/IKE Peers

- “End points” of the IPSec tunnel are Bob and Alice
- B and C are IKE peers
IPSec MIBs

- IPSec flow monitor MIB
- IPSec tunnel-to-policy MIB (IOS)
- IPSec configuration MIB (IOS)
- Cisco 3000 Concentrators
  - Active tunnel MIBs
  - Active sessions MIBs

IPSec Flow Monitor MIB

- Monitor IKE tunnels
- Monitor IPSec tunnels
- Tunnel structure and end points
- Trending and failures
- Notifications
- SNMPv1 and v2C
Flow Monitor MIB: Phase 1 Group

- IKE global statistics
  Metrics pertaining to activity of IKE tunnels system-wide
- IKE tunnel table
  Record of all active IKE tunnels
- IKE peer table
  Record of all IKE peers of the device

Use Cases: Phase 1 Group

- Monitors device-wide IKE statistics
- Identifies active IKE tunnels
- Lists the IKE tunnels to a specified peer
- Lists the IPSec tunnels to a specified peer
Flow Monitor MIB: Phase 2 Group

- IPSec global statistics
- IPSec tunnel table
- End point table
- SA table

Use Cases: Phase 2 Group

- Monitors device-wide IPSec (data) tunnel statistics
- Identifies active IPSec tunnels
- Lists
  - IPSec tunnels of an IKE tunnel
  - End points/protocols using an IPSec tunnel
  - Structure (SAs) of an IPSec tunnel
Flow Monitor MIB: Failure Group

- IKE/IPsecTunnel setup failures
  - Invalid/unacceptable proposal, authorization failure, etc.
- IKE/IPsecTunnel operational failures
  - Operator deletion, protocol failure, etc.

Phase 1 Failures

- Setup failures
  - Authentication failure
  - “Proposal failure”
  - PKI failure (certificate/CRL unavailable)
  - Encryption failure
  - System capacity failure
- Tunnel failures
  - Tunnel deleted (by CLI or notification)
  - Connection to peer lost
  - System capacity failure
  - Unknown SA (“No SA”)
  - Encryption/hash failure
IPSec MIBs: Application

Management Aspects

- Policy definition/deployment
- Monitor VPN throughput/performance
- Monitor historical trends
- Monitor failures
- Troubleshooting

Monitoring: What Can Go Wrong

- Setup failures
- Crypto hardware failure
- Protocol failure
- Security breaches
- Monitor failures

IPSec MIB Reporting Example

- Real-time status, fault, and performance
- Configuration inconsistencies
- IPSec, PPTP and L2TP
- Site-to-site, remote access
- IPSec, L2TP, PPTP
- VPN C3000, IPSec MIB (IOS)
Case Studies

Case Study 1: IPSec VPN

- Environment
  Site-to-site VPN links HQ to remote branches across Internet/SP network

- Goal
  To monitor VPN service delivery to ensure consistent availability
What to Monitor

- Router resources
  - CPU
  - Memory
  - Active tunnels/sessions
- Throughput
- Failures
  - Key management
  - Data management

What Happened Here?
Explanation   IKE maintains state for a communication in the form of security associations; no security association exists for this packet and it is not an initial offer from the peer to establish one; this situation could denote a denial of service attack

Recommended Action   Contact the remote peer’s administrator

---

Explanation   A received IPSEC packet specifies an SPI that does not exist in the security association database (SADB); this may be a temporary condition resulting from slight differences in the aging of SAs between the IPSEC peers, or because the local SAs have been cleared; it may also be caused by bogus packets being sent by the IPSEC peer; some might consider this a hostile event

Recommended Action   If the local SAs have been cleared, the peer may not know this; in this case, if a new connection is established from the local router, the two peers may reestablish successfully; if the problem occurs for more than a brief period, either attempt to establish a new connection or contact the peer’s administrator
Check Syslog

Quick Mode failure

Explanation  Negotiation with the remote peer failed

Recommended Action  If this situation persists contact the remote peer

Main Node failure

Explanation  Negotiation with the remote peer failed

Recommended Action  If this situation persists contact the remote peer

Audit Config Changes
What to Monitor

• Examples
  Default settings too long?
  IKE exchange/SA mismatches
  Natural goal is to minimize pain

Where to Monitor?

• Head end
  Can get most of needed data
  Consolidated info source

• Remote end
  Bring up tunnel just to manage
  Polling bandwidth?
  SA’s out of synch?
Service Monitoring Applications

- **CSPM**
  - Policy auditing and monitoring
  - Near-real time event data

- **CWVMS**
  - System, throughput, failures and events
  - Threshold violations
  - Real-time graph of key VPN parameters
  - Tunnel drill-downs

Case Study 2: VoIP

- **Environment**
  - Government agency with distributed offices using VoIP to reduce telephony charges
  - Wants ability to objectively monitor and report on voice quality in network
  - Voice QoS affected by Network QoS: when former detected, need to examine latter
VoIP Potential Problems

- Typical QoS problems
  - Packet Loss
  - Excessive Delay
  - Excessive Jitter
- Core problems do not always show evidence on edges
- Need means to inject at edges, track ingress to egress

Service Assurance Agent Jitter Probes

- Parameters
  - Source/destination devices
  - Source/destination ports
  - Sampling interval
  - Packets per sample
  - Payload size
  - Interpacket delay
  - Type of Service

```
Router acting as RTR probe

SAA Monitoring app
```

```bash
RTR 1
  type jitter dest-ipaddr 5.0.0.1 dest-port 99
  rtr schedule 1 life 10000000 start-time now
  rtr server 5.0.0.1
```

```bash
(config)#rtr responder
```
SAA Deployment—Coverage

- Core routers
- Distribution routers
- Access routers

SAA Deployment—CPU Impact

- Core routers
- Distribution routers
- Access routers

CPU Impact

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU

L  H
CPU
**Deployment—Probes and Responders**

![Diagram of network deployment with RTR Responder and Access routers acting as RTR probes]

**QoS Considerations**

- Probe traffic must have same QoS as real voice traffic
- LLQ or RTP Priority configurations on the router may need to be adjusted so that traffic from the RTR probes is subject to strict priority queuing

**Example:**

```plaintext
class-map VoiceRTP
    match access-group name IP-RTP
policy-map 192Kbps_site
    class VoiceTRP
    priority 110

ip access-list extended IP-RTP
    deny ip any any fragments
    permit udp <from> <mask> range 16384 32768 <to> <mask> range 16384 32768
    precedence critical
    permit udp any any eq 20000 precedence critical
    permit udp any any eq 20000 precedence critical
```
Tracking Results

- Define SLAs paralleling service guarantees
- View trends, threshold status
- APIs to access data for individual uses

What’s Acceptable?

- Delay, Jitter: It Depends!
  - Obtain workable delay and jitter figures
  - Compare similar sites in the same network
    - Baseline baseline baseline!
- Errors are a different story
  - In principle any non-zero error percentage is a red flag
  - RTR packets are given the same QoS treatment as voice packets
  - No level of congestion should cause packet loss or excessive delay
CLOSING SLIDES

Other Presentations of Interest

- NCM-101—Introduction to Network Management
- NCM-207—Understanding Fault Management
- NCM-301—Network Troubleshooting Tools and Techniques
Understanding Service Level and Traffic Management

Session NCM-208

Please Complete Your Evaluation Form

Session NCM-208