Improving Network Availability

Session NMS-1201
Welcome!—NMS-1201

- Facilities
- Availability Definitions
- Components of Availability
- Network Failures
- Improving Network Availability

Availability Definitions
Availability Definitions

**Availability:**

- The probability that an item (or network, etc.) is operational, and functional as needed, at any point in time
- Or, the expected or measured fraction of time the defined service, device or area is operational; annual uptime is the amount (in days, hrs., min., etc.) the item is operational in a year

Availability = \( \frac{MTBF}{MTBF + MTTR} \)

Useful definition for theoretical and practical

- **MTBF** is mean time between failure
  - What, When, Why and How does it fail?
- **MTTR** is mean time to repair
  - How long does it take to fix?
What Is High Availability?

<table>
<thead>
<tr>
<th>Availability</th>
<th>Downtime Per Year (24x7x365)</th>
</tr>
</thead>
<tbody>
<tr>
<td>99.000%</td>
<td>3 Days 15 Hours 36 Minutes</td>
</tr>
<tr>
<td>99.500%</td>
<td>1 Day 19 Hours 48 Minutes</td>
</tr>
<tr>
<td>99.900%</td>
<td>8 Hours 46 Minutes</td>
</tr>
<tr>
<td>99.950%</td>
<td>4 Hours 23 Minutes</td>
</tr>
<tr>
<td>99.990%</td>
<td>53 Minutes</td>
</tr>
<tr>
<td>99.999%</td>
<td>5 Minutes</td>
</tr>
<tr>
<td>99.9999%</td>
<td>30 Seconds</td>
</tr>
</tbody>
</table>

Components of Availability

Hardware, Software, Power/Environment, Link/Carrier, Configuration/change, Resource Utilization, Design
Hardware

Hardware Redundancy:

- Redundancy
  - Network vs. module
  - Load sharing
  - Active/standby
  - Chassis, card, port/trunk
  - End station NIC
- SPF (single point of failure)

Switchover Coverage:

- Switchover coverage
- Active and standby fault detection
- Integrity of detection circuits
- Switchover fallback
Hardware MTBF and Failure Propagation:

- Card MTBF (mean time between failure)
- Failure propagation (can failures propagate to other modules or cards?)

Recovery from Hardware Failures:

- Node rebuild time
- Standby processor update time
- Failure detection time
- Switchover time
- Card reset time
- Manual recovery
  - Fault diagnostics
  - Craft dispatch
  - Hardware repair or replacement time
Improving Hardware Availability

- Load sharing redundancy
- Active/standby redundancy (processor, power, line-cards)
- Active/standby fault detection
- Card MTBF
- Node rebuild time
- “Hitless” upgrades
- Hot swap

Software

**Failure Propagation**

- Failure Propagation
  - Control processing overload
  - Correlated software failures
  - Repetitive message streaming
Software

Software Rebuilds and Bugs

- Preventable rebuilds
  - Memory exhaustion
  - CPU Utilization
- Hitless vs. hard rebuilds
- Memory integrity
- Database corruption
- Design bugs

Improving Software Availability

- Improved software quality foal (99.999%+)
- “Hitless” upgrade
- Routing processor switchover
- NSF (non-stop forwarding)
- Line card switchover
- Faster reboot
- Uplink fast/backbone fast/HSRP
- Routing convergence enhancements
**Link/Carrier Connectivity**

- Campus LAN Core
- WAN Hub Building
- CSU/DSU
- SONET ADM
- BDF
- CSU/DSU
- Local Exchange
- Geophysical Diversity

- WAN Site
- Public Carrier
- Backup Public Carrier
- Long Distance Diversity

**Link/Circuit Diversity**

- Enterprise
- Enterprise
- Enterprise

- THIS Is Better than...
- THIS, which Is Better than...
- Service Provider Network
- Whoops. You've Been Trunked!
Power/Environment

- Power outages
  - UPS/generator power
  - UPS/generator switchover coverage
  - UPS/generator capacity
  - UPS generator management
- Power circuit capacity
- Air conditioning outages
- Temperature fluctuations
- Natural disaster
  - Earthquake
  - Flood
  - Hurricane
  - Disaster recovery plan

Power Environment

Power Diversity

- How redundant is the path the electricity travels?
- Separate:
  - Power supplies
  - Outlets
  - Circuits
  - Building entrances
  - Power grids
  - Generators
### Power/Environment

**Data Center Hardening**

- Cable Management
- Power–Diversity/UPS
- HVAC
- Hardware Placement
- Physical Security
- Labeling
- Environmental Control Systems

### Configuration/Change

- Change management processes
- Emergency changes
- Testing/validation/pilot (high-risk)
- What-if analysis
- Configuration management
  - Modularity
  - Hierarchy
  - Consistency
  - Software
**Configuration/Change**

**PDIO Model**

- The process to successfully deploy a new solution is based on the (PDIO) methodology.

**Software Management**

- Certification Starts Candidate Management
- Test/Validate Pilot
- Slow Start
- Upgrade Trigger
- Plan
- Implement
- Operation
- Problem Management Version Control
- Certification Complete
Resource Utilization

- Control plane
  - CPU, memory, buffers
  - Congestive degradation
- Data plane
  - Packet loss/delay/jitter
  - QOS queue management
  - TCP synchronization
  - Packet size, transmission type UDP/TCP

Design

Primary Design Considerations

- Hierarchical
- Modular and consistent
- Scalable
- Manageable
- Reduced failure domain (Layer II/III)
- Interoperability
- Performance
- Availability
- Security
Design

Technical Considerations

• All routed links
• No spanning tree
• Intelligent broadcast and multicast control

Why Do Networks Fail?
Network Complexity

Technology Can Increase MTBF
Availability = MTBF/(MTBF + MTTR)

People, Process, and Politics Can Increase Complexity
THIS DECREASES MTBF

What Are the Time-Bombs?

• No technical ownership
• Large failure domains
• Layer (II/III) design
• Loose or non risk-aware change management
• High levels of network inconsistency
• Lack of network standards (SW, HW, Config)
• No capacity planning or perf management
What Happens when Networks Fail?

- Resource constraints
  - CPU/memory
  - Inability to process messages
  - Inability to process routing updates
  - Routing or bridging loops

Why Does It Take a Long Time to Fix?

- No identified tiered support mechanism with individuals who know and understand the network
- Poor documentation (topology and config)
- Large failure domain difficult to understand and determine root-cause
- Networks with control-plane resource issues require major topology, config and upgrade changes
Cause of Unscheduled Network Downtime

- Change
- Communication
- Process
- Design

Source: Gartner

Causes of Unscheduled Downtime

<table>
<thead>
<tr>
<th>Category</th>
<th>Percent of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Operations Failures</td>
<td>87%</td>
</tr>
<tr>
<td>Physical Link Failures</td>
<td>87%</td>
</tr>
<tr>
<td>Network Hardware Failures</td>
<td>79%</td>
</tr>
<tr>
<td>Network Software Failures</td>
<td>67%</td>
</tr>
<tr>
<td>Customer Premises Equipment Failures</td>
<td>67%</td>
</tr>
<tr>
<td>Physical Environment Failures</td>
<td>62%</td>
</tr>
<tr>
<td>Congestion/overload</td>
<td>44%</td>
</tr>
<tr>
<td>Unknown</td>
<td>37%</td>
</tr>
<tr>
<td>Acts of Nature</td>
<td>37%</td>
</tr>
<tr>
<td>Malicious Damage</td>
<td>25%</td>
</tr>
</tbody>
</table>

Source: Sage Research, IP Service Provider Downtime Study: Analysis of Downtime Causes, Costs and Containment Strategies, August 17, 2001, Prepared for Cisco SPLOB
### Duration of Downtime

- **100 or More Hours:**
  - Total Scheduled Downtime: 20%
  - Total Unscheduled Downtime: 18%
- **50 to 99 Hours:**
  - Total Scheduled Downtime: 13%
  - Total Unscheduled Downtime: 0%
- **10 to 49 Hours:**
  - Total Scheduled Downtime: 37%
  - Total Unscheduled Downtime: 43%
- **Less than 10 Hours:**
  - Total Scheduled Downtime: 30%
  - Total Unscheduled Downtime: 39%

18% report having had more than 100 hours of unscheduled downtime.

Source: Sage Research, IP Service Provider Downtime Study: Analysis of Downtime Causes, Costs and Containment Strategies, August 17, 2001, Prepared for Cisco SPLOB

### What Is the Reality?

- **95%**
- **98%**
- **99.5%**
- **99.9%**
- **Desire**
- **Need**
- **Goal**
- **Current Reality**
- **Guarantee**
- **Cost**

Source: Gartner
Improving Network Availability

- Identify gaps
- Root cause failure analysis
- Availability metrics
- Priority and ROI analysis
- Quality improvement
What Is Your Availability Level?

**Analyze the Gaps: Reactive ~ 99%**

- Few if any identified processes (except maybe to fix problems as reported by users)
- Significant number of SPFs
- Low tool utilization
- Low level of consistency (HW, SW, config, design)
- No quality improvement processes

**Analyze the Gaps: Proactive ~ 99.9%**

- Good change management processes including what-if analysis and change validation
- Low number of SPFs
- Fault and configuration management tools
- Improved consistency (HW, SW, config, design)
- Typically no quality improvement process
What Is Your Availability Level?

**Analyze the Gaps: Predictive ~ 99.99+%**

- Consistent processes for fault, configuration, performance and security
- No SPFs except at edge of network
- Fault, configuration, performance and workflow process tools
- Excellent consistency (HW, SW, config, design)
- HA culture of quality improvement

Root Cause Failure Analysis

- Priority 1 and 2 business impacting
- Why did the failure occur?
  - HW, SW, link, power/env, change, design
- How could the failure have been prevented?
  - People, process, tools, technology
Availability Metrics—Where? What?

ICMP Reachability

- Method definition
- How
- Unavailability
ICMP Device Reachability

- Periodic pings to network devices

Service Assurance Agent

Management Application
1. User configures collectors through mgmt application GUI
2. Mgmt application provisions source routers with collectors
3. Source router measures and stores performance data, e.g.:
   - Response time
   - Availability
6. Application retrieves data from source routers once an hour
7. Data is written to a database
8. Reports are generated
4. Source router evaluates SLAs, sends SNMP traps
5. Source router stores latest data point and 2 hours of aggregated points

SNMP

SA Agent
### Outage Logs

<table>
<thead>
<tr>
<th>Date</th>
<th>Device</th>
<th>Problem</th>
<th>Cause</th>
<th>TTR</th>
<th>Cust Affected</th>
<th>DPM</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/13</td>
<td>Sf-rtr01</td>
<td>Bad RSP</td>
<td>Infant Mortality (Hardware)</td>
<td>271</td>
<td>250</td>
<td>145</td>
</tr>
<tr>
<td>3/17</td>
<td>DVR-rtr03</td>
<td>Connection Loss</td>
<td>Duplicate Subnet (User-Error)</td>
<td>342</td>
<td>100</td>
<td>57</td>
</tr>
<tr>
<td>3/17</td>
<td>NY-rtr17</td>
<td>Connection Loss</td>
<td>Software Bug (Software)</td>
<td>600</td>
<td>290</td>
<td>353</td>
</tr>
<tr>
<td>3/18</td>
<td>SEA-rtr02</td>
<td>Connection Loss</td>
<td>No UPS (Power)</td>
<td>60</td>
<td>37</td>
<td>21</td>
</tr>
</tbody>
</table>

### Defects per Million

- Hardware
- Software
- Link
- Environment/Power
- Other

- January: 120
- February: 100
- March: 80
- April: 60
- May: 40
Investing to Reduce Unplanned Downtime

- Investment strategy
  - ROI
  - New technology
  - Service contracts
  - Availability monitoring
- People and process
  - Hiring and training
  - IT process maturity
  - Automation
  - Change and problem mgt.
- Application
  - App. architecture/design
  - Change management
  - Problem management
  - Configuration management
  - Performance/capacity planning

Source: Gartner

Operator Errors 40%
Application Failure 40%
Environmental Factors, HW, OS, Power, Disasters 20%

Operator Errors 40%
Environmental Factors, HW, OS, Power, Disasters 20%
Application Failure 40%

Cisco Services

- FTS—Focused Technical Support
  Fix it faster!
- NOS—Network Optimization Services
  Make proactive improvements (design, software selection, optimization)
- NAIS—Network Availability Improvement Support
  Identify gaps with gap closure assistance

Source: Gartner
HA Improvement Prioritization Matrix

Example Availability Projects
- Operational Excellence
- Tools
- Network upgrades

Creating an HA Culture

People
- Executive messaging - communicate business plans for high availability and the importance of improvement
- Reward positive behavior
- Provide world class training to staff
- Create a cross-functional technical team and availability champion

Process
- Identify and resolve process deficiencies
- Start an availability improvement quality process
- Root-cause analysis
- Collect and report availability metrics

Tools
- Availability measurement
- Processes for consistency (automate where possible)
- Metrics for identifying areas of service improvement
Availability Quality Improvement Process

- Identify gaps
- Develop plan
  Projects
  Availability metrics
- Implement fixes
- Verify results
- Repeat process

Identify Gaps
- Assess customer practices against industry standards

Develop HA Plan
- Specific plans to "Bridge the Gaps"
- Measurement and timelines

Repeat Process
- Move on to next level of assessment detail

Verify
- Gaps are resolved
- Impact on availability

Take Corrective Action
- Implement "fixes"
- Eliminate Gaps

Recommended Reading

High Availability Network Fundamentals
ISBN: 1587130173

Enhanced IP Services for Cisco Networks
ISBN: 1578701066

Available on-site at the Cisco Company Store
Please Complete Your Evaluation Form

Session NMS-1201