Introduction to High Availability Networking

Session 2609
Agenda

- Introduction
- Hardware
- Software
- Link/Carrier
- Power/Environment
- Network Design
- User Error/Process
- Modeling Availability
- Measuring Availability

Introduction
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>

Major Risk Q&A (How Many of You…)

- Congestive degradation
- Capacity (peaks unanticipated)
- Solutions validation
- Software quality
- Inadvertent configuration change
- Major fiber cut or carrier failure
- Power
- Attack
- Critical services failure (e.g., DNS/DHCP)
- Protocol implementations/misbehavior
- Hardware fault
Cause of Network Outages

- Change management
- Process consistency

- User Error Process 40%
- Technology 20%
- Software Application 40%

- Hardware
- Links
- Environmental issues
- Natural disasters

- Software issues
- Performance and load
- Scaling

Source: Gartner Group

The Cost of Downtime

- Lost productivity
  Employee’s salary weighting factor
- Lost revenue
- Lost customer goodwill
- Support costs
What Availability Level Do I Need?

- The cost of downtime
- Business driven availability-based ROI analysis
- Failure insurance

Availability Definitions

- Availability = \( \frac{MTBF}{MTBF + MTTR} \)
- \( = 1 - \frac{\text{Total connection outage time}}{\text{total in service connection time}} \)
- \( = 1 - \left[ \sum (\text{No. connections affected in outage } i \times \text{duration of outage } i) \right] \div (\text{No. connections in service } \times \text{operating time}) \)
- Unavailability = \( 1 - \text{availability} \)
Defects Per Million

- Started with mass produced items like toasters
- For PVCs,
  \[ \text{DPM} = \frac{\text{#conns} \times \text{outage minutes}}{\text{#conns} \times \text{total minutes}} \]
- For SVCs or phone calls,
  \[ \text{DPM} = \frac{\text{#existing calls lost} + \text{#new calls blocked}}{\text{total calls attempted}} \]
- For connectionless traffic (application dependent),
  \[ \text{DPM} = \frac{\text{#end users} \times \text{outage minutes}}{\text{#end users} \times \text{total minutes}} \]

What Does it Take to Achieve?

- Hardware resiliency
- Software reliability/features
- Link/carrier resiliency
- Environment/power
- Network design
- User-error/process
Hardware Resiliency and Reliability

Hardware Availability Elements

Factors Affecting Hardware Availability

- Redundancy
  - Load sharing
  - Active/standby
  - Chassis, card, port/trunk
  - End station NIC
- Switchover coverage
  - Active and standby fault detection
  - Integrity of detection circuits
  - Switchover fallback
- Single point of failure
- Card MTBF
- Failure propagation
- Standby failure

Recovery Time

- Node rebuild time
- Standby processor update time
- Failure detection time
- Switchover time
- Card reset time
- Manual Recovery
  - Fault Diagnostics and isolation time
  - Craft Dispatch
  - Hardware repair or replacement time

Network Service

- Hardware upgrades
- Redundancy exercising
- Card servicing
Types of Redundancy

Module Redundancy Versus Chassis Redundancy

- Failover redundant modules only
- Failover time may be significant
- Failover coverage (active/standby)
- In-service upgrades possible
- Significant MTBF improvement
- Failover time by protocols
- No active/standby issues
- Upgrades cause convergence

Types of Redundancy

Parallel—Series Redundancy

\[
\text{Availability} = (1 - (1-A_{\text{orange}})^2) \times (1 - (1-A_{\text{yellow}})^2) \times (1 - (1-A_{\text{brown}})^3)
\]
**Types of Redundancy**

- **Module Redundancy**
  - Fits parallel series model with N:M redundancy
  - Does not include active standby switchover coverage
  - Does not include switchover time

\[ A_{\text{Backplane}} \times (1 - (1-A_{\text{CPU}})^2) \times (1 - (1-A_{\text{Power}})^2) \times (1 - (1-A_{\text{Switch}})^3) \]

**Types of Redundancy**

- **Series—parallel redundancy**

\[ \text{Availability} = 1 - [(1-A_{\text{Orange}}) \times (1-A_{\text{Yellow}})]^2 \]
Hardware Availability Features

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

Sensitivity Analysis of BCC Hardware Availability

![Graph showing connection downtime in minutes per year for different MTBF, recovery time, and coverage values.]
Hardware Failure Recovery Model

“Two Biggest Issues Are a Lack of Background Diagnostics Running on Standby Cards and a Lack of Fault Insertion Testing (H/W and S/W) During Validation Testing”

Customer Comment

MTBF of Cards Should Be >100K Hours

Yes; P=0.9999 (Desired)

Switch to Standby?

Yes; P=0.9999 (Desired)

Standby OK?

Yes; P=0.9999 (Desired)

Signal CPE (A-Bit, OAM)

Rapid Recovery

BPX-AXIS Availability Improvement by Release

Connection Downtime (Minutes Per Year)

Release 8.4

Release 9.1

Release 9.2

BCC MTBF 25K to 50K hr. Rebuild Prevention

Cross-Point Detection Concentris Circles Hitless Rebuild SONET APS

BCC H/W

Software Aborts

BPX Trunk Side

BPX Port Side

AXIS Core Group

AXIS Service Module
Core/Backbone

Catalyst L3 Switch = Router

Catalyst L2 Switch

Server Farm

Dual-Homed Server—Primary NIC Recovery (Time 1–2 Seconds)

Redundant Server NIC

Checklist/Caveats/Notes

- Used INTEL “Adaptive Fault Tolerant” Drivers and NICs
- NIC Has a Single IP/MAC Address (Active on One NIC at a Time)
- Turning on “Portfast” Feature on Server Ports Doesn’t Really Help in this Case, Since Backup Link, Keeps Link-Up Continuously
- NIC Uses L2 Broadcast for Keep-Alives
- When Faulty Link Repaired, Does not Fail Back to Avoid Flapping

Hardware Resiliency and Reliability Conclusions

- Understand your MTBFs
- Know reliability of key paths
- Understand key availability factors and recovery times
- Build MTTR processes that fit business requirements
### Software Availability Elements

<table>
<thead>
<tr>
<th>Factors Affecting Software Availability</th>
<th>Recovery Time</th>
<th>Network Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Failure Propagation</td>
<td>• Automatic Recovery</td>
<td>• Software upgrades</td>
</tr>
<tr>
<td>Control processing</td>
<td>Node rebuild time</td>
<td></td>
</tr>
<tr>
<td>overload</td>
<td>Standby processor update time</td>
<td></td>
</tr>
<tr>
<td>Correlated software failures</td>
<td>Software resync time</td>
<td></td>
</tr>
<tr>
<td>Repetitive message streaming</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Preventable rebuilds</td>
<td>• Manual Recovery</td>
<td></td>
</tr>
<tr>
<td>Memory exhaustion</td>
<td>Fault Diagnostics and isolation time</td>
<td></td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>Craft dispatch</td>
<td></td>
</tr>
<tr>
<td>• Hitless vs. hard rebuilds</td>
<td>Software patch or workaround time</td>
<td></td>
</tr>
<tr>
<td>• Memory integrity</td>
<td>Service affecting event duration</td>
<td></td>
</tr>
<tr>
<td>• Database corruption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Design bugs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Software Availability
Feature and Goals

- “Hitless” upgrade
- Routing processor switchover
- NSF (non-stop forwarding)
- Line card switchover
- Faster reboot
- Uplink fast/backbone fast/HSRP
- Sonet APS
- Routing convergence enhancements

Software Reliability
Measurement Program

- Engineering initiative to release 99.999% available software
- Measured on IOS in Cisco internal network with 2000 routers
- Uses sysuptime and syslog failure reports
- Fits log normal distribution
- Data shows age improves software reliability
- Cisco looking for customer partners to increase data sources
Current Observations

<table>
<thead>
<tr>
<th>Release</th>
<th>Failures</th>
<th>Exposure (Years)</th>
<th>MTBF (Years)</th>
<th>Availability Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>192</td>
<td>123.19</td>
<td>16.352</td>
<td>99.9999%</td>
</tr>
<tr>
<td>11.2</td>
<td>117</td>
<td>361.66</td>
<td>10.364</td>
<td>99.9999%</td>
</tr>
<tr>
<td>11.3</td>
<td>243</td>
<td>171.116</td>
<td>8.836</td>
<td>99.9999%</td>
</tr>
<tr>
<td>12.0</td>
<td>370</td>
<td>234.509</td>
<td>2.059</td>
<td>99.9994%</td>
</tr>
<tr>
<td>12.1 M+</td>
<td>161</td>
<td>48.32</td>
<td>1.204</td>
<td>99.9991%</td>
</tr>
</tbody>
</table>

Cisco IOS Reliability Growth

MTBF (Years)

- 95% Upper
- Expected
- 95% Lower
Cisco IOS Reliability Conclusions

- Data fits log normal distribution model
- Software methodology measured meets 99.999% goal
- Software reliability increases with age
- Current model may only fit internal IT feature set; (other feature sets planned)
- Customers still need feature validation, what-if analysis/testing and software version control for HA

Link/Carrier Availability
Link/Carrier Availability Elements

Factors Affecting Link/Carrier Availability
- All availability issues required in carrier network management including hardware, software, link, network design, power/environment, user-error/process
- Geophysical diversity
- Link redundancy
- Carrier redundancy
- Local loop redundancy
- Single point of failure
- Cable management
- Wiring infrastructure
- Carrier management

Recovery Time
- Automatic Recovery
  - Fault detection time (software)
  - Routing, spanning tree or PVC convergence time
  - SONET protect
- Manual Recovery
  - Manual backup
  - Fault detection time
  - NOC or network management
  - Repair time
  - Craft dispatch
  - Service affecting event duration

Network Service
- Hardware/software upgrades
- Cable infrastructure migration
- Cable/link testing

Link/Carrier Connectivity

Campus LAN Core
BDF
SONET ADM
CO

WAN Hub Building

Public Carrier
Backup Public Carrier
Long Distance Diversity

Also Fiber Repeaters, DACS, Long Distance Carrier Equipment
Carrier Management

- Understand carrier network
- Model and understand carrier availability
- Understand diversity
- Monitor carrier availability
  
  Enhanced services
  
  Utilize carrier SLAs
- Notification and escalation procedures

Cable Management

- Color coding
- Device card/chassis access
- Cable labels
- Path diversity
- Documentation
Link/Carrier Availability Conclusions

- Model carrier availability
- ROI analysis on redundant services
  Insurance factor for large outages
- Usefulness of carrier SLAs
- Review carrier notification/escalation procedures to reduce repair times
- Cable management to facilitate problem isolation and equipment swap

Power/Environment Availability
# Power/Environment Availability Elements

## Factors Affecting Power/Environment Availability

<table>
<thead>
<tr>
<th>Availability Elements</th>
<th>Recovery Time</th>
<th>Network Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power outages</td>
<td>• Automatic recovery</td>
<td>• Power upgrades</td>
</tr>
<tr>
<td>UPS/generator power</td>
<td>• Problem detection time</td>
<td>• Power service</td>
</tr>
<tr>
<td>UPS/generator</td>
<td>• Manual recovery</td>
<td></td>
</tr>
<tr>
<td>switchover coverage</td>
<td>• Disaster recovery plan</td>
<td></td>
</tr>
<tr>
<td>UPS/generator capacity</td>
<td>• Craft dispatch</td>
<td></td>
</tr>
<tr>
<td>UPS generator</td>
<td>• Problem identification time</td>
<td></td>
</tr>
<tr>
<td>management</td>
<td>• Problem repair time</td>
<td></td>
</tr>
<tr>
<td>Power circuit capacity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Air conditioning outages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temperature fluctuations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Natural disaster</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Earthquake</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flood</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hurricane</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster recovery plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Availability Affects of UPS and Generator

<table>
<thead>
<tr>
<th>Event Outages</th>
<th>Raw AC</th>
<th>5 Min UPS</th>
<th>1 Hour UPS</th>
<th>UPS w/Generator</th>
<th>Power Array w/Generator</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 Events</td>
<td>1 Event</td>
<td>.15 Events</td>
<td>.01 Events</td>
<td>.001 Events</td>
<td></td>
</tr>
<tr>
<td>Annual Downtime</td>
<td>189 minutes</td>
<td>109 minutes</td>
<td>10 minutes</td>
<td>1 minute</td>
<td>.1 minute</td>
</tr>
<tr>
<td>Availability</td>
<td>99.96%</td>
<td>99.979%</td>
<td>99.998%</td>
<td>99.9998%</td>
<td>99.999999%</td>
</tr>
</tbody>
</table>

- Data assumes staffed 1 hour response for UPS
- Additional downtime for remote UPS service

Source: American Power Conversion, Tech Note #26
Affect of Temperature on Failure Rate

- Failure rate increases by factor of 1.7 to 2.2 for every 10o C
- Normal equipment operating temp up to 40o C, (104o F) in standard temperature controlled environment

Power/Environment Practices for High Availability

- Power/environment facilities planning and management
- Power circuit to device mapping and management
- Remote power management
  www.servertech.com
- Power facilities auditing/consulting
  www.apcc.com
- Disaster recovery plan (facilities access)
## Network Design

### Availability Elements

**Factors Affecting Network Design Availability**
- HA solutions
- Modularity
- Hierarchy
- Network complexity
- Network manageability
- Failure domain size
- Control plane resources
- Design testing/validation
- Network scalability

**Recovery Time**
- Automatic recovery
  - Failover
  - Convergence time
- Manual recovery
  - Network complexity
  - Multiple vendors and finger pointing
  - Craft dispatch
  - Problem identification time
  - Problem repair time
  - Out-of-band management
  - Network documentation

**Network Service**
- Network upgrades
Modularity and Hierarchy

Access Switches

Blocked for Even

Layer 2

Blocked for Odd

Distribution Switches

Root Odd VLAN

+ Layer 3

Root Odd VLAN

+ Layer 3

Backbone Switches

Layer 2 Convergence Failure Domain

• 1–4 s

Layer 3 Convergence Failure Domain

• Depend on the Protocol
  • OSPF 1–15 s
  • EIGRP 1–15 s

Complexity and Manageability

• Defined modules
• Repeated templates
• Standard configuration
• Standard hardware
• Standard software
Control Plane Resources

- CPU
- Memory
- Buffers
- Backplane utilization
- Bus utilization
- Messaging/query storms

Testing and Validation Components

Traffic Generator
- Pagent Router
- Network Under Test

Large Network Emulation
- 1000s or Routes/100s of Routers
- Network Under Test

Session Emulator
- Network Under Test

Traffic Analysis
- Traffic Analysis
- Traffic Analysis
Network Design Practices for High Availability

- Reduce complexity, increase modularity and consistency
- Consider solution manageability
- Minimize failure domain size (follow best-practice design guidelines)
- Consider control plane resource requirements and the affect of busy CPU/memory

Network Design Practices for High Availability

- Test/validate designs
- Consider problem repair times in design
  - Out-of-band management
  - Network documentation
- Model availability for design
Human Error and Process

Process Goals

- Consistent speedy repair times
  - Configuration management
  - Fault management
  - Performance management

- Quality improvement
  - Availability metrics
  - Fault management metrics
  - Root-cause analysis
  - Performance indicators
Process Goals

- Problem avoidance
  - Network design and resiliency
  - Security
  - Proactive fault management
  - Capacity and performance management
- Successful network evolution
  - Change planning management
  - Testing and validation

Network Life-Cycle Management
New Solution Deployment

- Design review with vendor
- Test plan (to reflect your app/network scenarios)
- Lab validation
- Solution pilot
- Solution templates
- Staffing
- Training
- Operational support handoff

Configuration Management—1

- Maintaining configuration consistency
- Inventory management
- IP address management
- Software version control
- Password management
- Wiring and naming conventions
- Documentation
Configuration Management—2

- Change Management
  - Change management procedures
  - Risk analysis
  - Testing/validation for high risk change
  - Backout plan
  - Network management and documentation update
  - Change management metrics

Performance and Capacity Management

- Performance and capacity management
- What-if analysis (network and application)
- Base-lining
- QoS management
- Periodic review plan and upgrade criteria
- Exception management
Fault Management

- Fault management
  - 24 x 7 detection, notification, escalation, resolution for link/hardware/network failures
  - Proactive fault analysis plan (MIB variables, threshold violations, syslog events, review plan)
  - Infrastructure (TFTP, syslog, NTP, time-stamps, out-of-band management, vendor access)
  - Help desk systems (metrics, accountability)

Security Management

- Security policy and procedures
- General security procedures
- Internet access
- Dial-in access
- Partner access
- Security operations
- Internet/partner monitoring
- CERT/vendor advisory review
- Security configuration practices
- Termination practices
Availability Modeling and Analysis

Why Model or Measure Network Availability?

- Service level management
- Service level agreements
- Availability-based ROI analysis
- Availability quality improvement process
Types of Reliability Models

- Parts-count models
- Combinatorial model
  Reliability block diagrams, fault tree analysis
- Markov models
  Used in engineering to identify availability issues
- Petri Net models
- Monte Carlo simulation models

MTBF and Availability (Reliability Block Diagram)

- Device MTBF = 45,000 hours
- Expected MTTR = 4 hours
- Downtime = 4 hours ever 45,000 hours
- Downtime = 0.7788 hours per year
- Availability = MTBF/MTBF + MTTR
- Expected availability = 99.991%
Examples of Hardware Reliability (Reliability Block Diagrams)

Hardware Reliability = 99.938% with 4 Hour MTTR (325 Minutes/Year)

Hardware Reliability = 99.961% with 4 Hour MTTR (204 Minutes/Year)

Hardware Reliability = 99.9999% with 4 Hour MTTR (30 Seconds/Year)

Series Availability Model with Multiple Availability Factors

<table>
<thead>
<tr>
<th>Availability Group</th>
<th>Hardware</th>
<th>Software</th>
<th>Power</th>
<th>Link Carrier</th>
<th>Network Design</th>
<th>User Error Process</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campus LAN</td>
<td>99.99%</td>
<td>99.999%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>99.99%</td>
<td>99.98%</td>
</tr>
<tr>
<td>Domestic WAN</td>
<td>99.95%</td>
<td>99.9995%</td>
<td>99.96%</td>
<td>99.95%</td>
<td>100%</td>
<td>99.99%</td>
<td>99.85%</td>
</tr>
<tr>
<td>Extranet</td>
<td>99.95%</td>
<td>99.999%</td>
<td>99.998%</td>
<td>99.95%</td>
<td>100%</td>
<td>99.99%</td>
<td>99.88%</td>
</tr>
</tbody>
</table>

Total Availability Calculated as Series (Product of All Categories)
Evaluating Software Reliability

- 99.999% to 99.9999% for established and GD releases
- 99.99% and above with established best-practices (per control, testing, pilots)
- Stay tuned for more data

Evaluating Power/Environment Reliability

- Use industry benchmark data available
- Evaluate power installation and management
- Reduce hardware MTBF for large temperature fluctuations
Evaluating Link/Carrier Reliability

- Use benchmark or measured data if possible
- Most WAN carrier and ISPs currently ~ 99.95% including local loop
- Don’t rely on SLAs for availability
- Evaluate internal cable management

Evaluating Network Design Reliability

- Evaluate current implementation
- Use benchmark or measured data if available
- Evaluate software switchover time based on estimated device/link failure (protocols)
Evaluating User-Error/Process Reliability

- Consider change success rate/metrics
- Consider MTTR for faults
- Understand process deficiencies for proactive management
- Understand expertise and training requirements
- Utilize existing benchmark or metrics if possible

Measuring Availability
Availability Results

- **DPM—Defects Per Million**
  Defect may be 1 user/customer down for one minute or one hour

- **IUM—Impacted User Minutes**
  Number of users affected × outage in minutes

- **Availability percentage**
  Percentage of availability based on measurement

Availability Measurement Methodologies

- **Ping** (network availability, device availability)
- **Trouble ticket reporting** (IUM, DPM)
- **RMON probe reporting**
- **RTR/SAA**
- **Application request**
Network Device Availability

- Periodic pings to network devices

Network Edge Availability

- Period ping to network leaf nodes
# 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

![Graph showing defects per million over months]

- **Red**: Hardware
- **Orange**: Software
- **Blue**: Link
- **Green**: Environment/Power
- **Purple**: User Error/Process

- January: 120
- February: 80
- March: 60
- April: 40
- May: 20
Case Study

HA Case Study—HA Profile
Initial Estimated Availability
Goal 99.999%

<table>
<thead>
<tr>
<th>Availability Group</th>
<th>Hardware</th>
<th>Software</th>
<th>Power</th>
<th>Link Carrier</th>
<th>Network Design</th>
<th>User Error Process</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campus LAN</td>
<td>99.99%</td>
<td>99.99%</td>
<td>100%</td>
<td>100%</td>
<td>99%?</td>
<td>99%?</td>
<td>97.99%</td>
</tr>
<tr>
<td>Frame Relay WAN</td>
<td>99.95%</td>
<td>99.995%</td>
<td>99.96%</td>
<td>99.95%</td>
<td>100%</td>
<td>99%?</td>
<td>98.86%</td>
</tr>
<tr>
<td>Internet</td>
<td>99.95%</td>
<td>99.995%</td>
<td>100%</td>
<td>99.99%</td>
<td>100%</td>
<td>99%?</td>
<td>98.93%</td>
</tr>
<tr>
<td>Data Center</td>
<td>99.99%</td>
<td>99.99%</td>
<td>100%</td>
<td>100%</td>
<td>99%?</td>
<td>99%?</td>
<td>97.99%</td>
</tr>
</tbody>
</table>

Network Design Root Cause

- EIGRP scalability (SIA count > 500/day)
- FDDI (time to resolve problems)
- Low modularity/hierarchy (lack of solution templates)
Network Design Changes

- BGP core
  - Reduced EIGRP failure domain
  - Increased scalability
- FDDI to FE migration
  - Fewer large outages
  - MTTR from 24 hours to 2 hours

User Error/Process Root Cause

- Emergency changes
- No test/validation
- Architecture/design solution template
- No software/hardware/config standards
User/Error Process Changes

- Change planning
  Testing/validation for high risk change
- Create architecture templates
  IOS, hardware, design, config standards
- Troubleshooting procedures
  Emergency change procedures

Measured Availability Improvement

<table>
<thead>
<tr>
<th>Availability Group</th>
<th>Hardware</th>
<th>Software</th>
<th>Power</th>
<th>Link Carrier</th>
<th>Network Design</th>
<th>User Error Process</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campus LAN</td>
<td>99.99%</td>
<td>99.99%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>99.95%</td>
<td>99.93%</td>
</tr>
<tr>
<td>Frame Relay WAN</td>
<td>99.95%</td>
<td>99.995%</td>
<td>99.96%</td>
<td>99.95%</td>
<td>100%</td>
<td>99.95%</td>
<td>99.8%</td>
</tr>
<tr>
<td>Internet</td>
<td>99.95%</td>
<td>99.995%</td>
<td>100%</td>
<td>99.99%</td>
<td>100%</td>
<td>99.95%</td>
<td>99.88%</td>
</tr>
<tr>
<td>Data Center</td>
<td>99.99%</td>
<td>99.99%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>99.95%</td>
<td>99.93%</td>
</tr>
</tbody>
</table>
Introduction to High Availability Networking

Session 2609

Please Complete Your Evaluation Form

Session 2609
Empowering the Internet Generation®