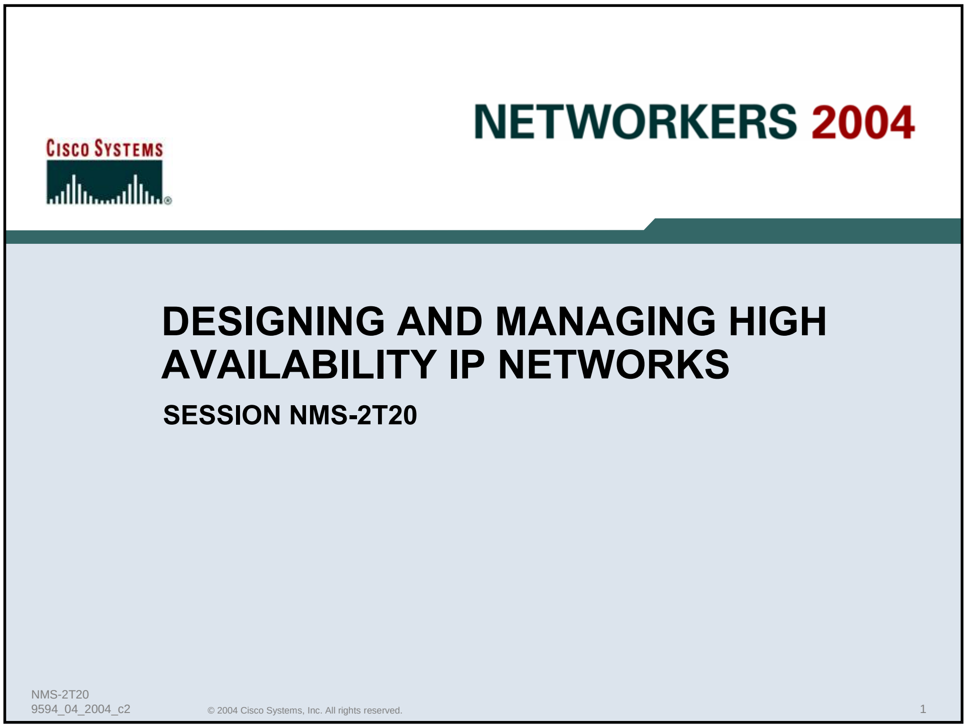
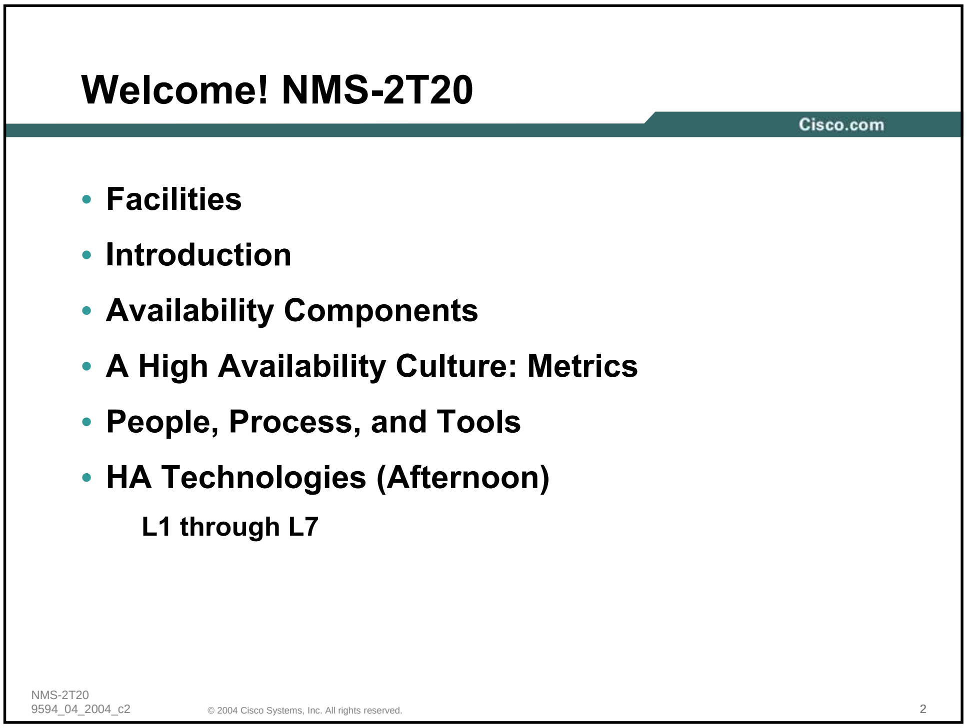


NETWORKERS 2004

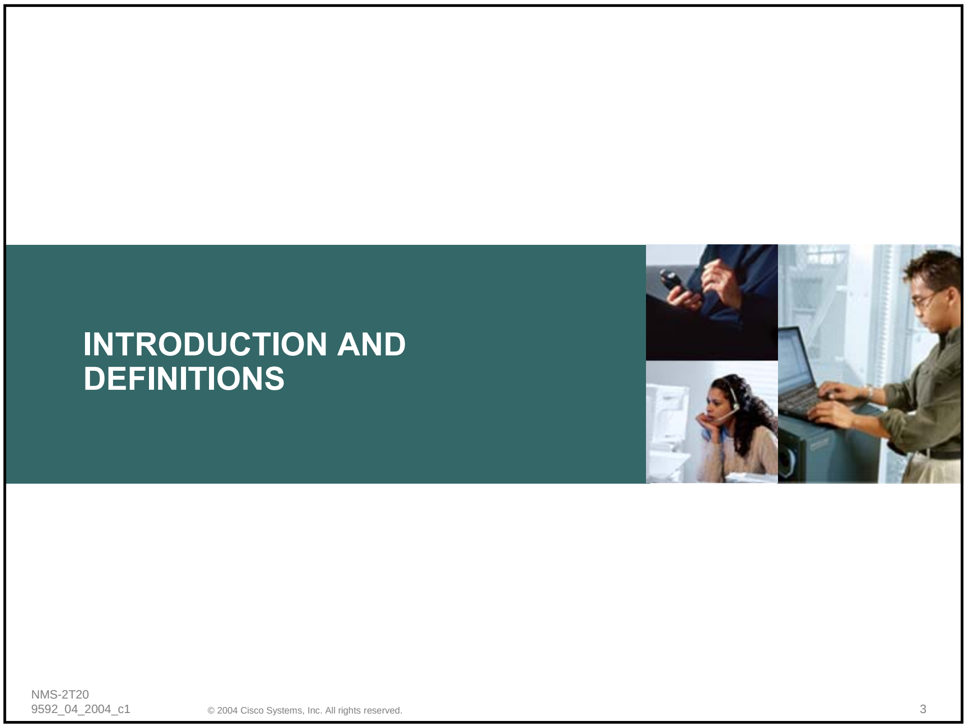
DESIGNING AND MANAGING HIGH AVAILABILITY IP NETWORKS

SESSION NMS-2T20

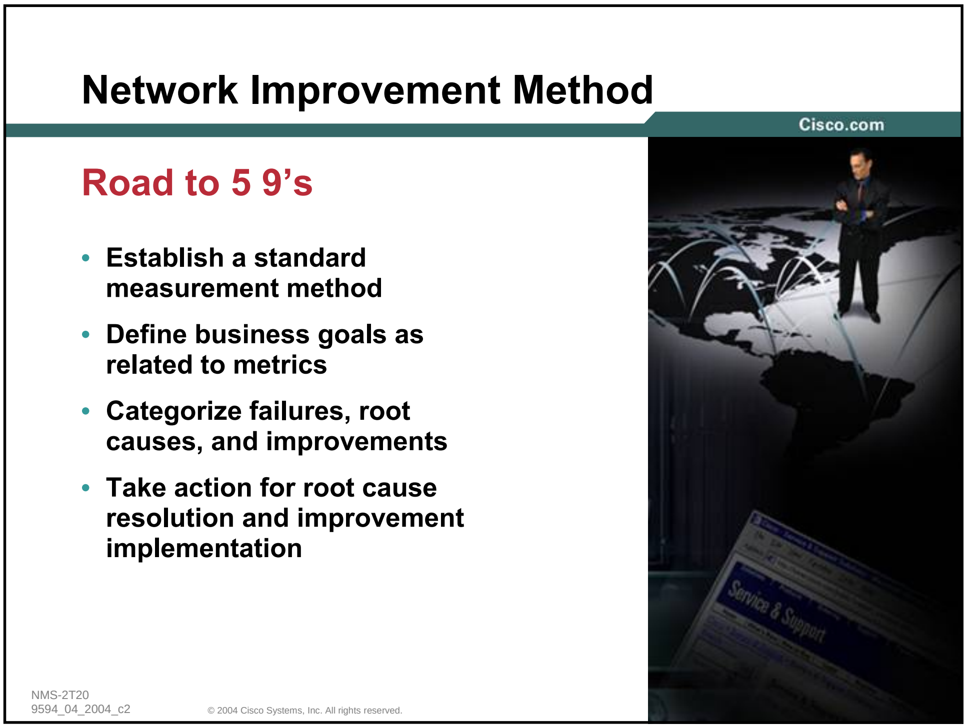


Welcome! NMS-2T20

- Facilities
- Introduction
- Availability Components
- A High Availability Culture: Metrics
- People, Process, and Tools
- HA Technologies (Afternoon)
    L1 through L7



INTRODUCTION AND DEFINITIONS

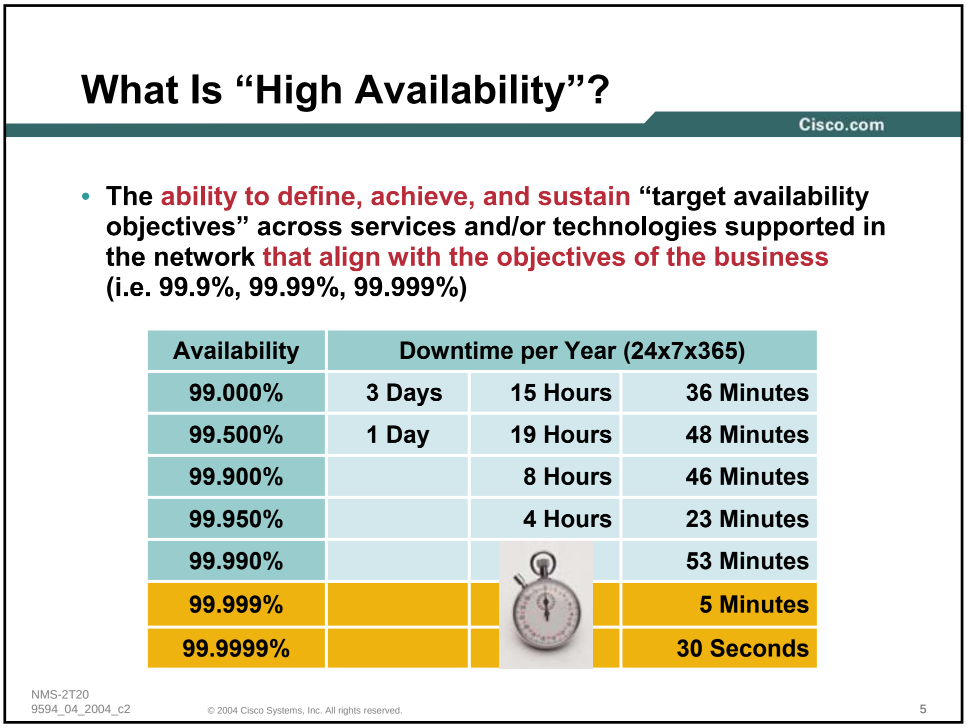


Network Improvement Method

Cisco.com

Road to 5 9’s

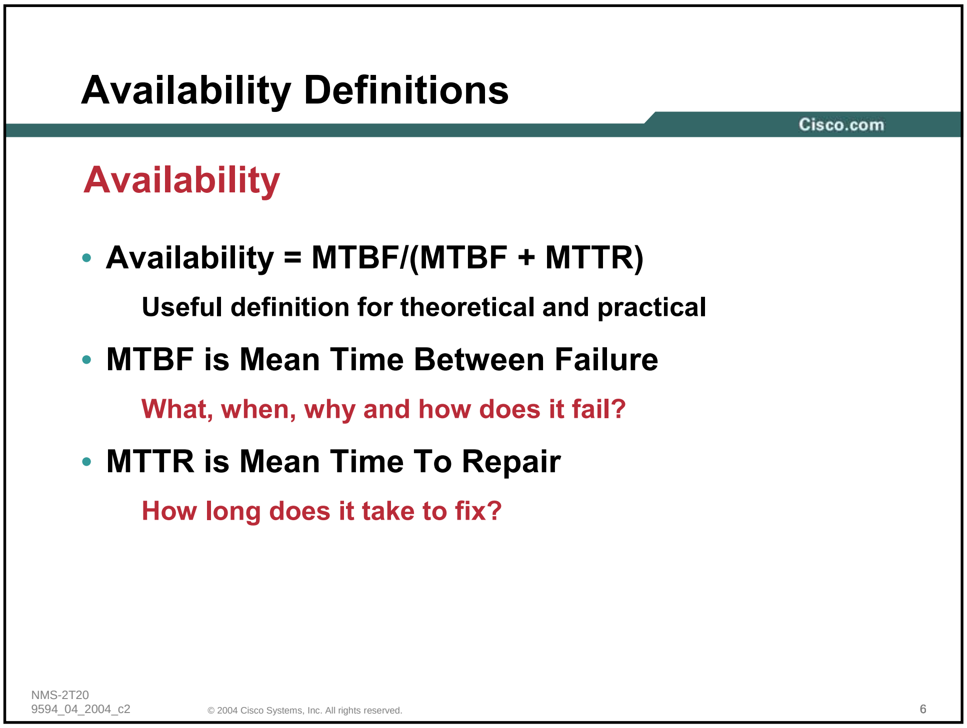
- Establish a standard measurement method
- Define business goals as related to metrics
- Categorize failures, root causes, and improvements
- Take action for root cause resolution and improvement implementation



What Is "High Availability"?

- The ability to define, achieve, and sustain "target availability objectives" across services and/or technologies supported in the network that align with the objectives of the business (i.e. 99.9%, 99.99%, 99.999%)

Availability	Downtime per Year (24x7x365)		
99.000%	3 Days	15 Hours	36 Minutes
99.500%	1 Day	19 Hours	48 Minutes
99.900%		8 Hours	46 Minutes
99.950%		4 Hours	23 Minutes
99.990%			53 Minutes
99.999%			5 Minutes
99.9999%			30 Seconds



Availability Definitions

Availability

- Availability = MTBF/(MTBF + MTTR)

  Useful definition for theoretical and practical

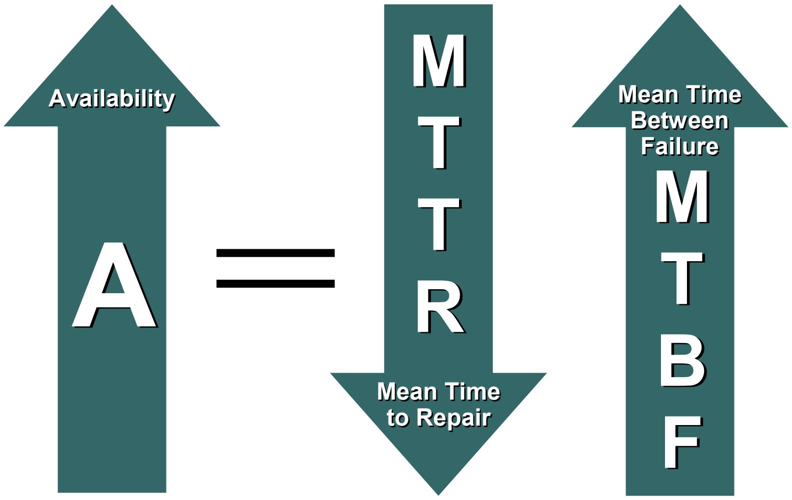
- MTBF is Mean Time Between Failure

  What, when, why and how does it fail?

- MTTR is Mean Time To Repair

  How long does it take to fix?

Increasing Availability



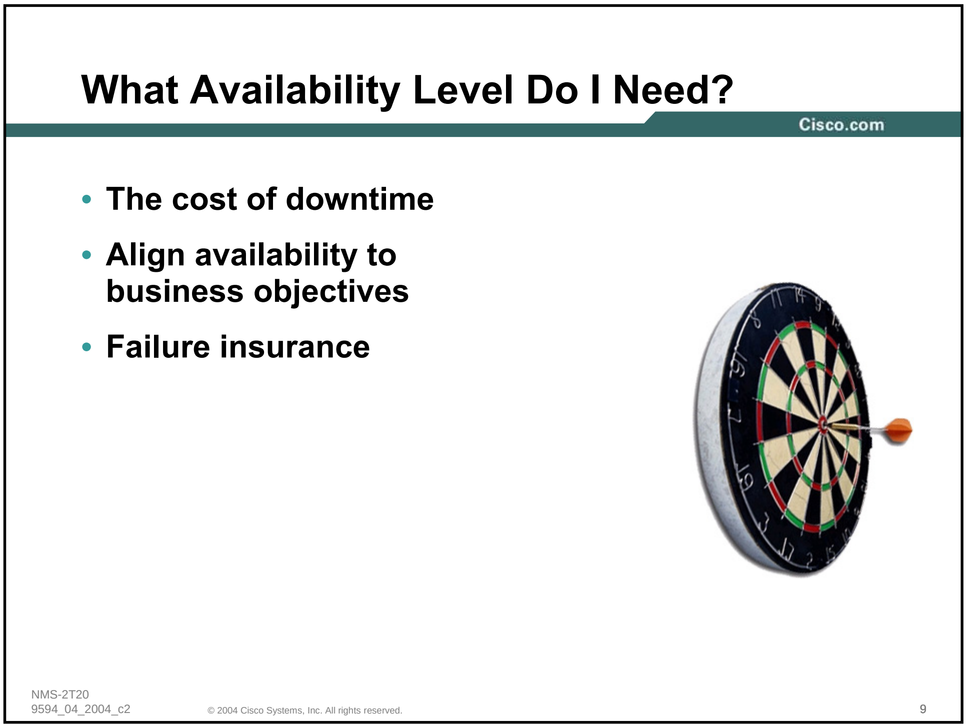
Why Improve Network Availability?

Recent Studies by Sage Research Determined That US-Based Service Providers Encountered:

- **Percent of downtime that is unscheduled: 44%**
- **18% of customers experience over 100 hours of unscheduled downtime or an availability of 98.5%**
- **Average cost of network downtime per year: $21.6 million or $2,169 per minute!**

Downtime: Costs Too Much!!!

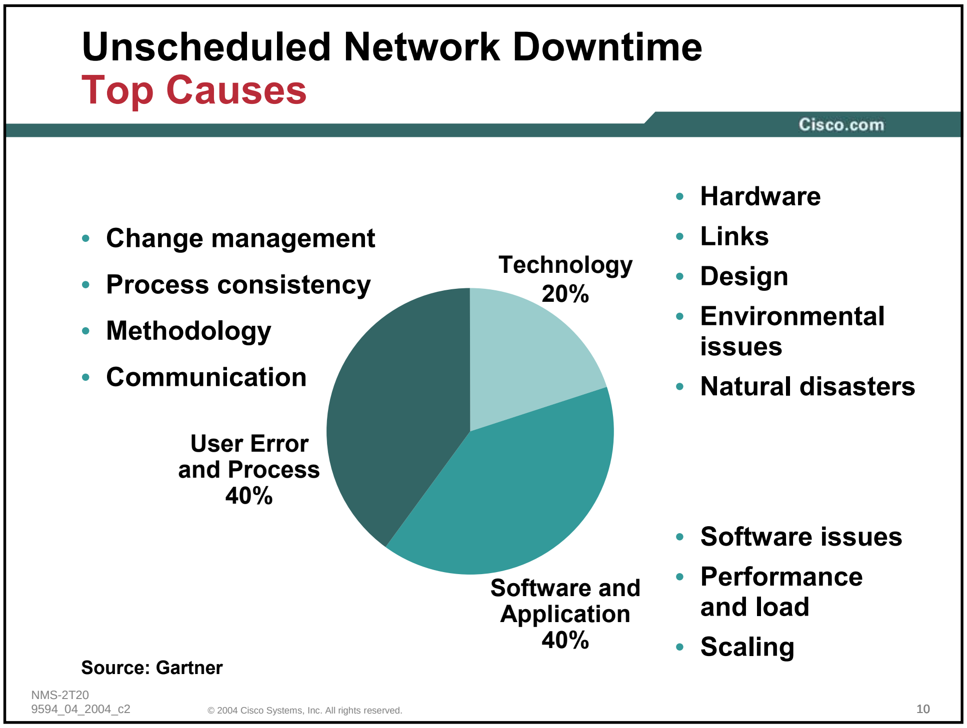
SOURCE: Sage Research, IP Service Provider Downtime Study: Analysis of Downtime Causes, Costs and Containment Strategies, August 17, 2001, Prepared for Cisco SPLOB



What Availability Level Do I Need?

Cisco.com

- The cost of downtime
- Align availability to business objectives
- Failure insurance



Unscheduled Network Downtime
Top Causes

Cisco.com

- Change management
- Process consistency
- Methodology
- Communication

User Error and Process 40%

Technology 20%

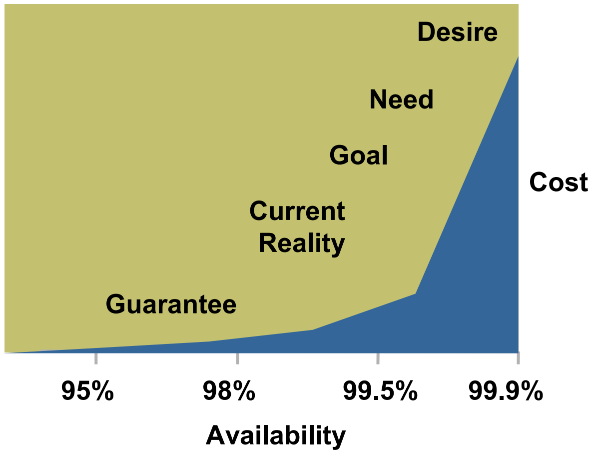
- Hardware
- Links
- Design
- Environmental issues
- Natural disasters

Software and Application 40%

- Software issues
- Performance and load
- Scaling

Source: Gartner

What Is the Reality?

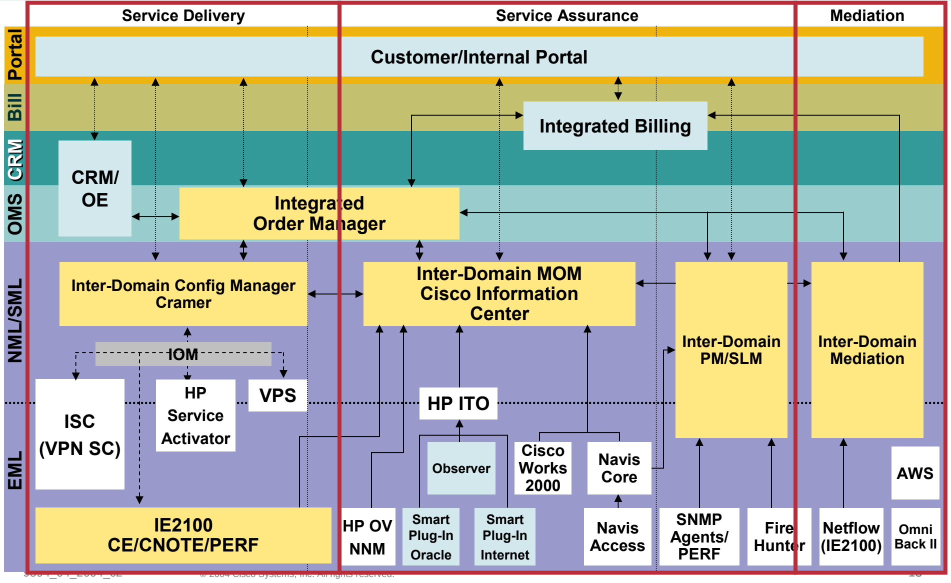


Source: Gartner, Copyright ®2001

WORKING IN A NETWORK MANAGEMENT FRAMEWORK

Accenture Best of Breed Architecture

Cisco.com



Service Delivery
Service Assurance
Mediation

Portal
Bill
CRM
OMS
NML/SML
EML

Customer/Internal Portal

Integrated Billing

CRM/ OE

Integrated Order Manager

Inter-Domain Config Manager Cramer

Inter-Domain MOM Cisco Information Center

Inter-Domain PM/SLM

Inter-Domain Mediation

IOM

ISC (VPN SC)

HP Service Activator

VPS

HP ITO

Observer

Cisco Works 2000

Navis Core

AWS

IE2100 CE/CNOTE/PERF

HP OV NNM

Smart Plug-In Oracle

Smart Plug-In Internet

Navis Access

SNMP Agents/ PERF

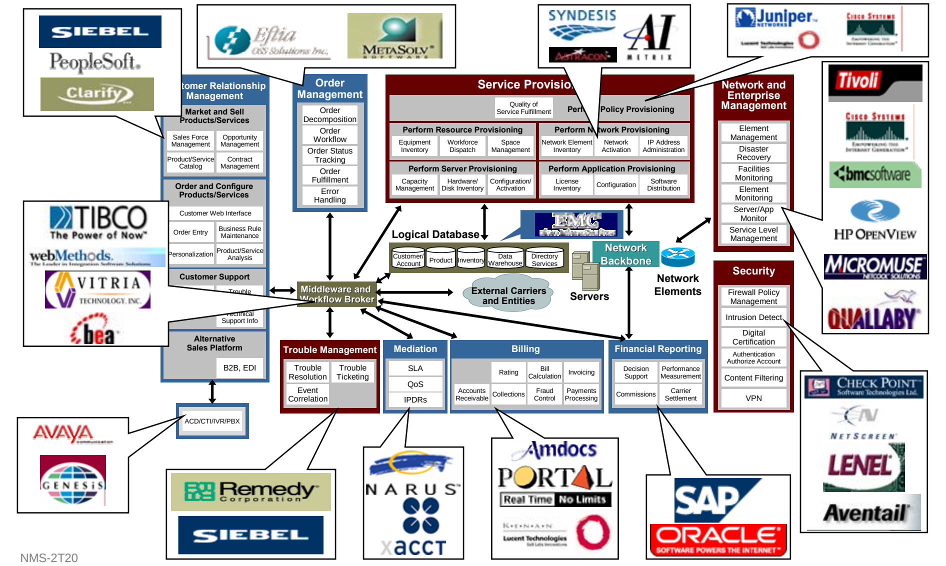
Fire Hunter

Netflow (IE2100)

Omni Back II

Deloitte Best of Breed

Cisco.com



Customer Relationship Management

Market and Sell Products/Services
Sales Force Management
Opportunity Management
Product/Service Catalog
Contract Management

Order and Configure Products/Services
Customer Web Interface
Order Entry
Business Rule Maintenance
Personalization
Product/Service Analysis

Customer Support
Trouble
Technical Support Info

Alternative Sales Platform
B2B, EDI

ACD/CTI/IVR/PBX

Order Management

Order Decomposition
Order Workflow
Order Status Tracking
Order Fulfillment
Error Handling

Service Provisioning

Quality of Service Fulfillment
Perform Policy Provisioning

Perform Resource Provisioning
Equipment Inventory
Workforce Dispatch
Space Management

Perform Network Provisioning
Network Element Inventory
Network Activation
IP Address Administration

Perform Server Provisioning
Capacity Management
Hardware/ Disk Inventory
Configuration/ Activation

Perform Application Provisioning
License Inventory
Configuration
Software Distribution

Network and Enterprise Management

Element Management
Disaster Recovery
Facilities Monitoring
Element Monitoring
Server/App Monitor
Service Level Management

Security

Firewall Policy Management
Intrusion Detect
Digital Certification
Authentication Authorize Account
Content Filtering
VPN

Logical Database
Customer/ Account
Product
Inventory
Data Warehouse
Directory Services

Middleware and Workflow Broker

External Carriers and Entities

Servers

Network Backbone

Network Elements

Trouble Management

Trouble Resolution
Trouble Ticketing
Event Correlation

Mediation

SLA
QoS
IPDRs

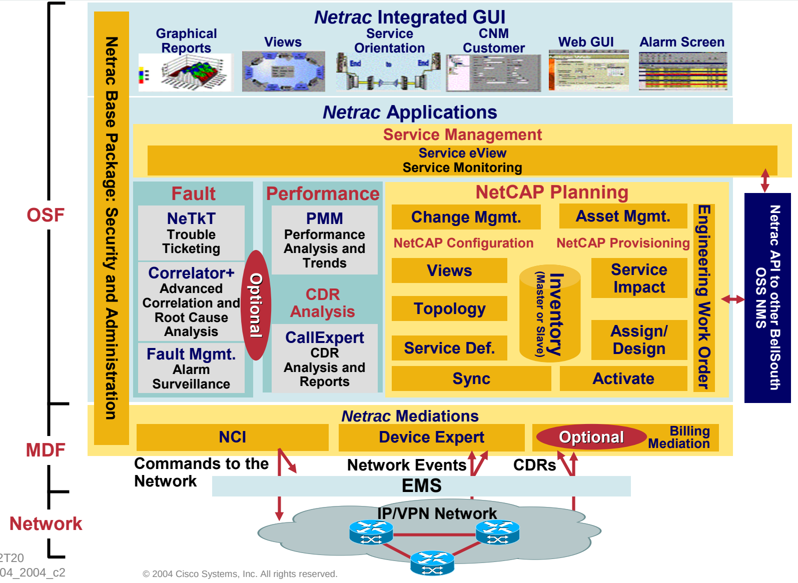
Billing

Rating
Bill Calculation
Invoicing
Accounts Receivable
Collections
Fraud Control
Payments Processing

Financial Reporting

Decision Support
Performance Measurement
Commissions
Carrier Settlement

TTI's Best of Class Architecture



OSF
MDF
Network

Netrac Base Package: Security and Administration

Netrac Integrated GUI
Graphical Reports
Views
Service Orientation
CNM Customer
Web GUI
Alarm Screen

Netrac Applications
Service Management
Service eView
Service Monitoring

Fault
NeTkT
Trouble Ticketing
Correlator+
Advanced Correlation and Root Cause Analysis
Fault Mgmt.
Alarm Surveillance

Optional

Performance
PMM
Performance Analysis and Trends
CDR Analysis
CallExpert
CDR Analysis and Reports

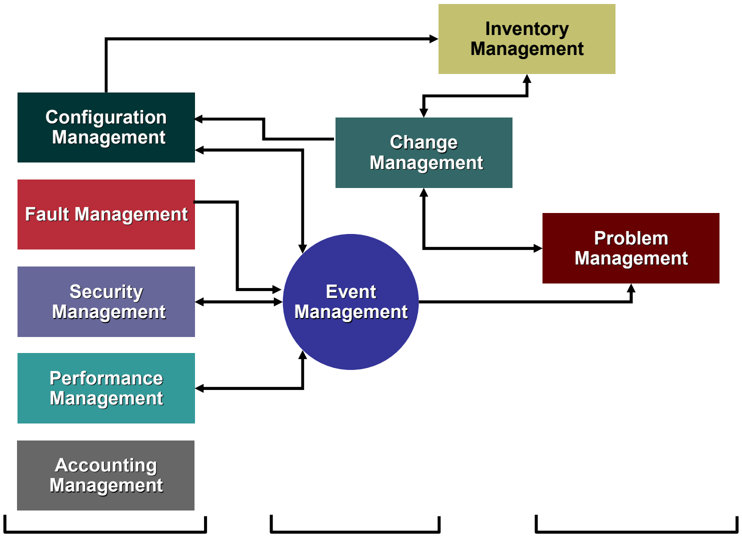
NetCAP Planning
Change Mgmt.
Asset Mgmt.
NetCAP Configuration
NetCAP Provisioning
Views
Topology
Service Def.
Sync
Inventory (Master or Slave)
Service Impact
Assign/ Design
Activate
Engineering Work Order

Netrac API to other BellSouth OSS NMS

Netrac Mediations
NCI
Device Expert
Optional
Billing Mediation

Commands to the Network
Network Events
CDRs
EMS
IP/VPN Network

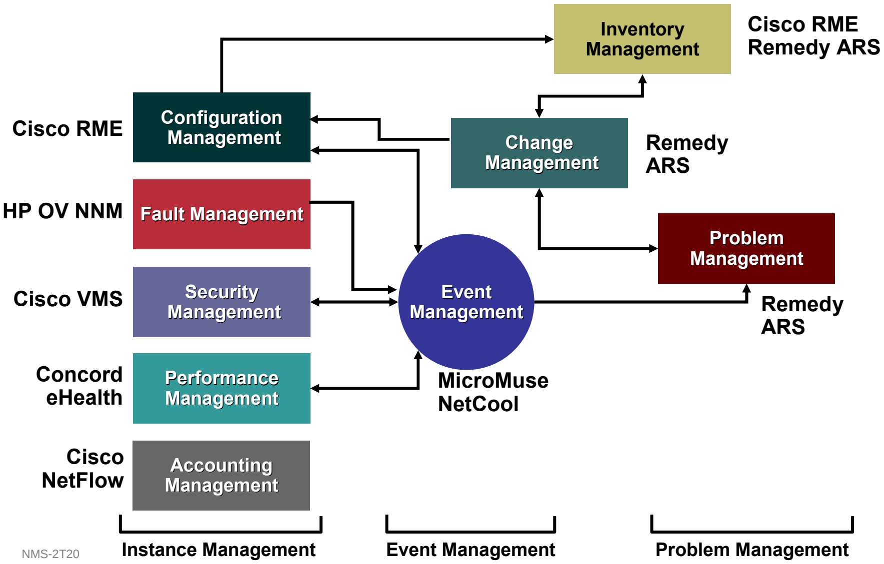
Simplified Network Management Framework



Inventory Management
Configuration Management
Change Management
Fault Management
Problem Management
Security Management
Event Management
Performance Management
Accounting Management

Instance Management
Event Management
Problem Management

Practical Application of Framework



Cisco RME
Configuration Management

HP OV NNM
Fault Management

Cisco VMS
Security Management

Concord eHealth
Performance Management

Cisco NetFlow
Accounting Management

Inventory Management
Cisco RME
Remedy ARS

Change Management
Remedy ARS

Event Management
MicroMuse NetCool

Problem Management
Remedy ARS

Instance Management

Event Management

Problem Management

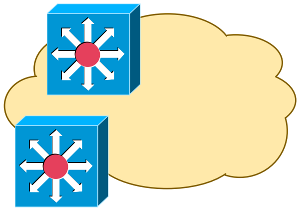
AVAILABILITY COMPONENTS

HARDWARE, SOFTWARE, POWER/ ENVIRONMNENT, LINK/CARRIER, CONFIGURATION/CHANGE, RESOURCE UTILIZATION, DESIGN

Hardware

Redundancy Options

Highly Available Networks Tend to Have Both

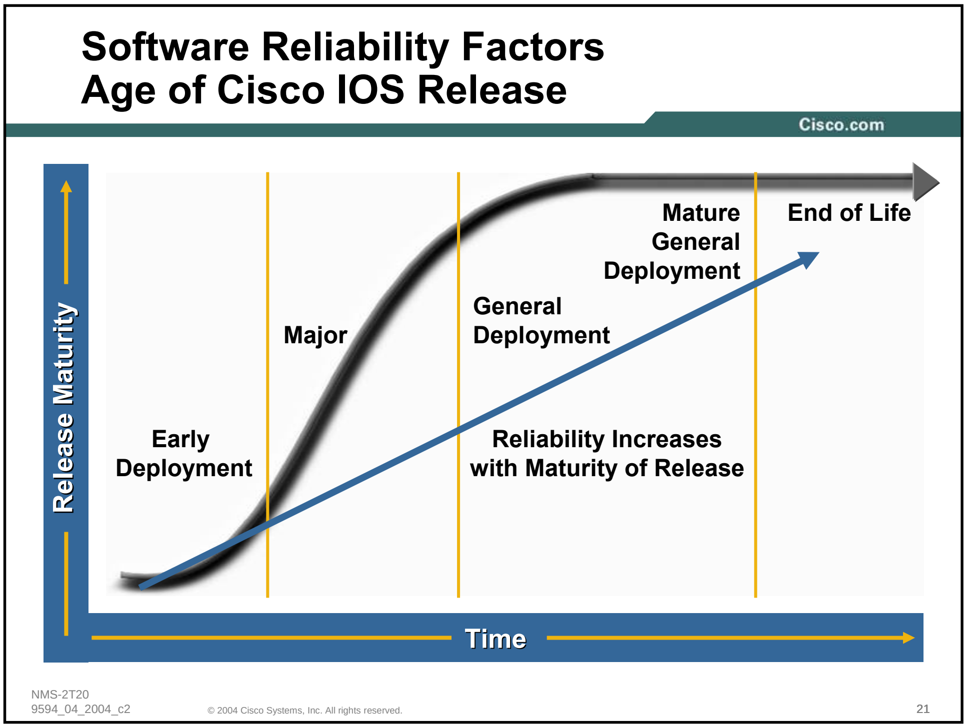


- − Failover redundant modules only
  - Operating system determines failover
- + Typically cost-effective
- + Often only option for edge devices (point to point)

- + All modules are redundant
  - Protocols determine failover
- − Increased cost and complexity
- + Load balancing

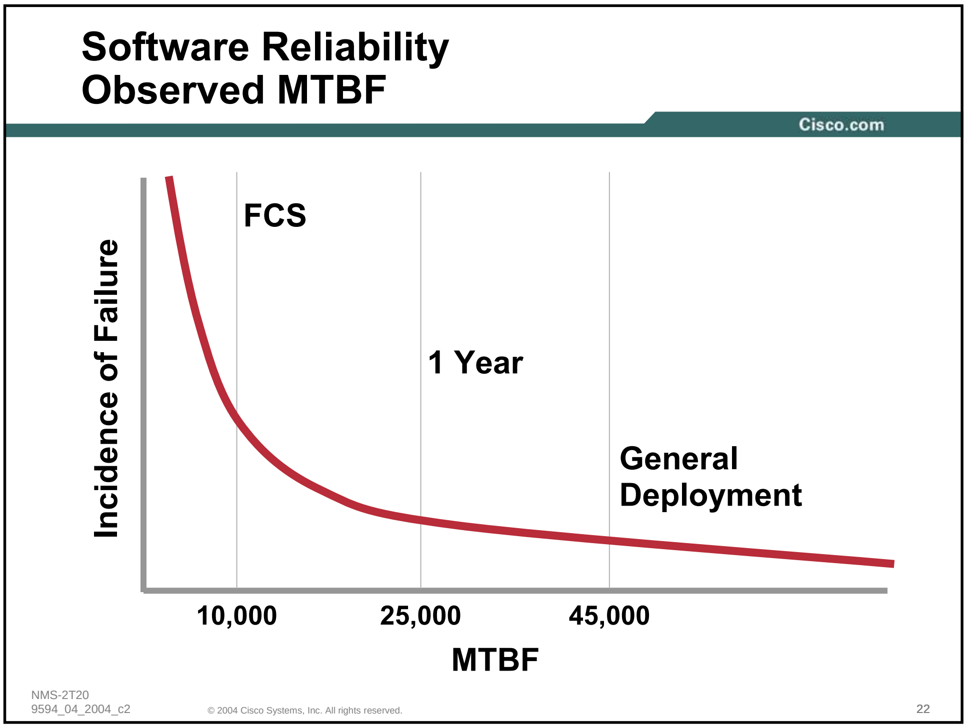
Improving Hardware Availability

- Load sharing redundancy
- Active/standby redundancy (processor, power, fans, line-cards)
- Active/standby fault detection
- Card MTBF (100,000 hrs)
- Separate control and forwarding plane
- Node rebuild time
- “Hitless” upgrades
- Robust hot swap (OIR)



Software Reliability Factors
Age of Cisco IOS Release

Cisco.com



Software Reliability
Observed MTBF

Cisco.com

Improving Software Availability

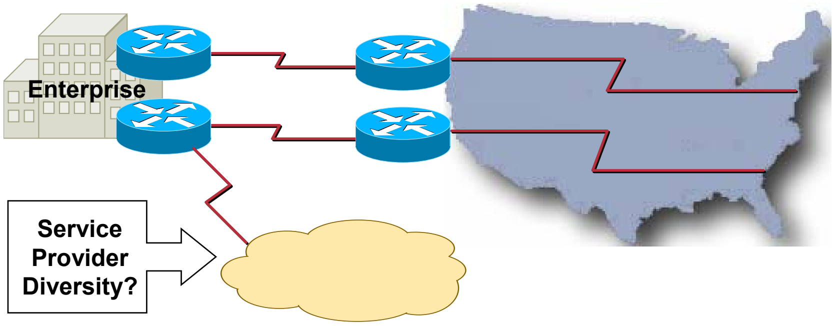
- Improved software quality goal (99.999%+)
- “Hitless” upgrade
- Process independence (restart and protected memory)
- Routing processor switchover
- NSF (non-stop forwarding)
- Line card switchover
- Faster reboot
- Uplink fast/backbone fast/HSRP
- Routing convergence enhancements

Circuit Diversity

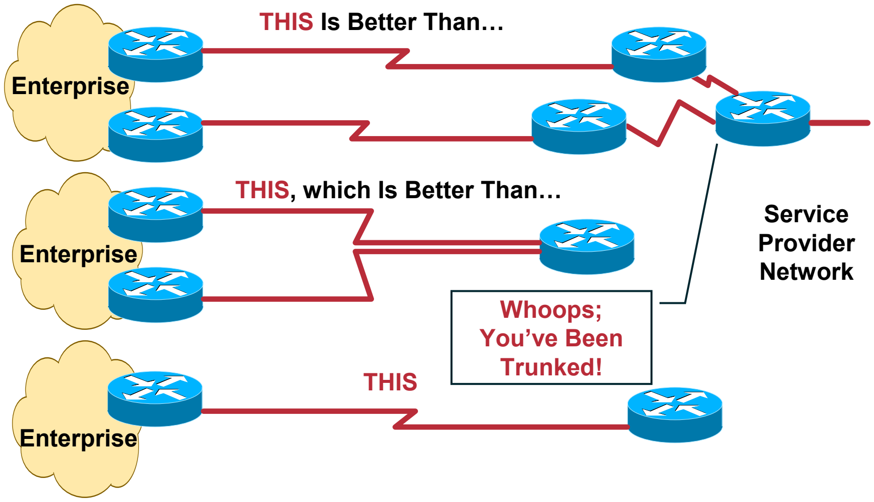
- Problem: if links follow a common path through service provider network, you are back to single-point-of-failure
- Solution: employ as much circuit diversity as possible

Links Terminate at Different Devices (Physical Diversity)

Links Use Different Paths in SP Network (Geographic Diversity)



Link/Circuit Diversity



THIS Is Better Than…

Enterprise

THIS, which Is Better Than…

Enterprise

Whoops;
You've Been
Trunked!

THIS

Enterprise

Service
Provider
Network

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

Cisco.com

Power Diversity

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

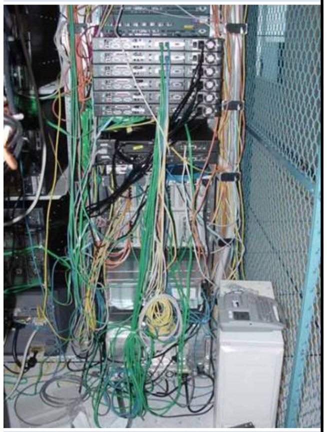
NMS-2T20
9594_04_2004_c2

Power/Environment

Cisco.com

Data Center Hardening

- Cable management
- Power: Diversity/UPS
- HVAC
- Hardware placement
- Physical security
- Labeling
- Environmental control systems



NMS-2T20
9594_04_2004_c2

Configuration/Change

- FCAPS processes (fault, configuration, accounting, performance, security)
- Emergency changes
- People, process, tools
- User error

Configuration/Change

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 performance management

Configuration/Change

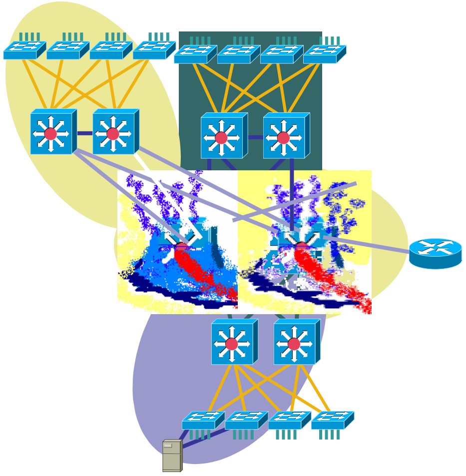
MTTR—Mean Time to Repair

- No identified tiered support mechanism with individuals who know and understand the network (lack of expertise)
- 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

Resource Utilization

What Happens when Networks Fail?

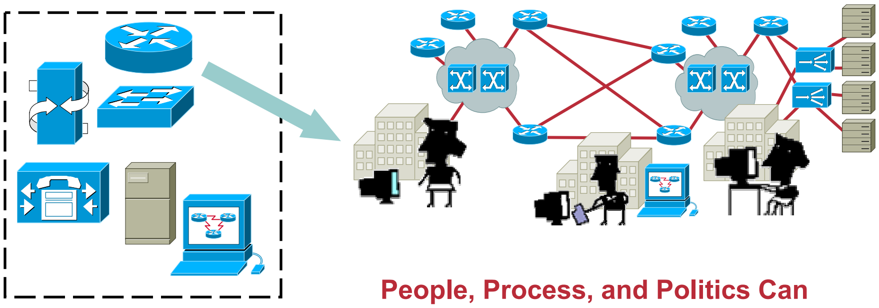
- Resource constraints
  - CPU/memory
  - Inability to process messages
  - Inability to process routing updates
  - Routing or bridging loops



Network Design

Cisco.com

Network Complexity



Technology Can Increase MTBF

People, Process, and Politics Can Increase Complexity

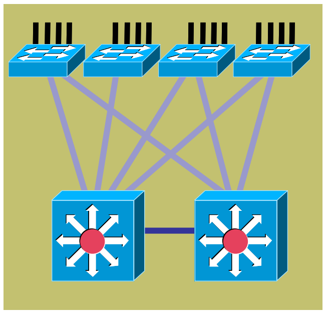
THIS DECREASES MTBF and Increases MTTR

Design

Cisco.com

Primary Design Considerations

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

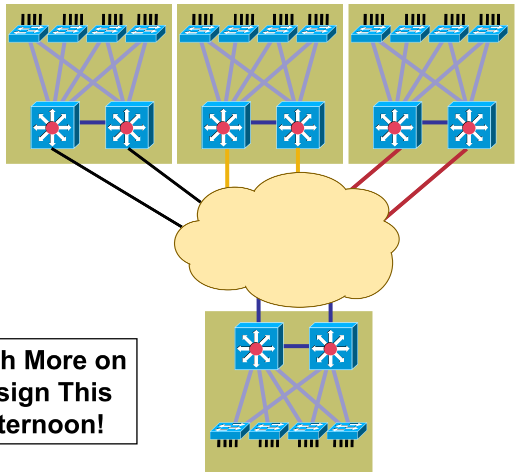


Design

Cisco.com

Technical Considerations

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



Much More on Design This Afternoon!

THE CULTURE OF AVAILABILITY

CALCULATING, MEASURING, AND IMPROVING AVAILABILITY

The Culture of Availability

- Identify gaps
- Root cause failure analysis
- Availability modeling
- Availability metrics
- Priority and ROI analysis
- 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?

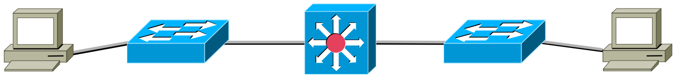
  People, process, tools, technology

Types of Reliability Models

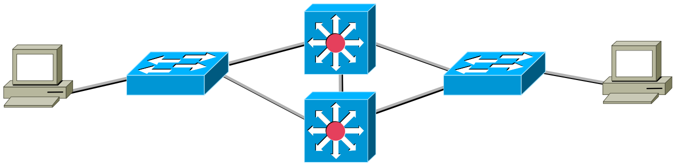
- Parts-count models
- Combinatorial model
  Reliability block diagrams, fault tree analysis
- Markov models
  Used in engineering to identify availability issues
- Petri Net models
- Monte Carlo simulation models

Examples of Hardware Reliability (Reliability Block Diagrams)

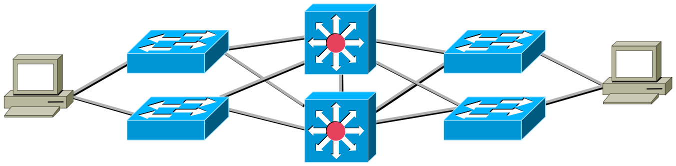
Hardware Reliability = 99.938% with 4 Hour MTTR (325 Minutes/Year)

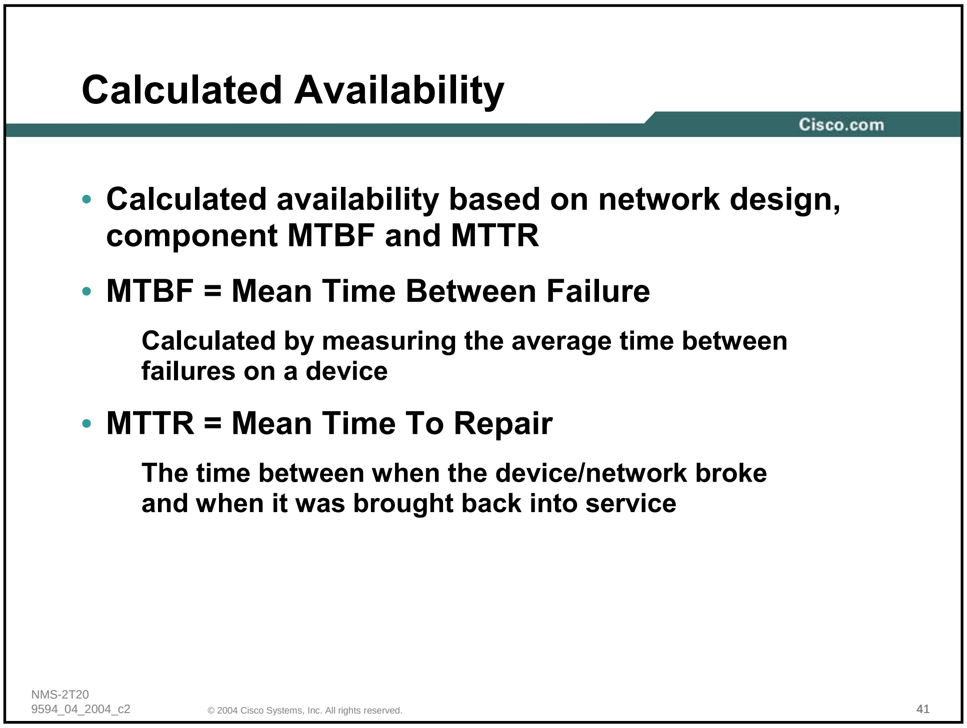


Hardware Reliability = 99.961% with 4 Hour MTTR (204 Minutes/Year)



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



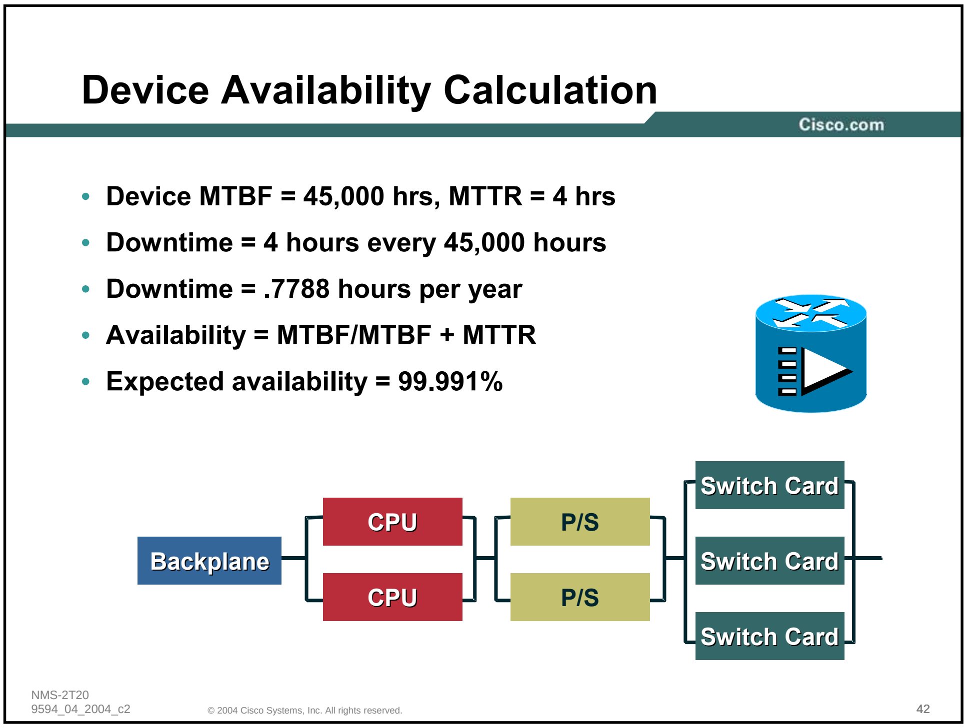


Calculated Availability

- Calculated availability based on network design, component MTBF and MTTR
- MTBF = Mean Time Between Failure

  Calculated by measuring the average time between failures on a device
- MTTR = Mean Time To Repair

  The time between when the device/network broke and when it was brought back into service

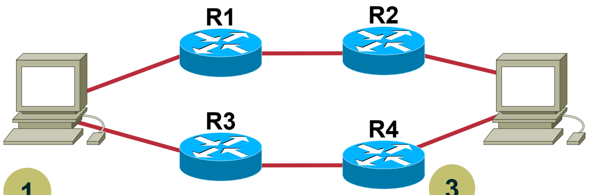


Device Availability Calculation

- Device MTBF = 45,000 hrs, MTTR = 4 hrs
- Downtime = 4 hours every 45,000 hours
- Downtime = .7788 hours per year
- Availability = MTBF/MTBF + MTTR
- Expected availability = 99.991%

Network Availability Calculation

Cisco.com



Router R1, R2, R3 and R4
MTBF = 16000 Hours
MTTR = 24 Hours

1

Router Availability R1, R2, R3 and R4
16000/(16000+24) = 0.9985
Can Include Hardware + Software Components

2

Availability of R1, R2 and R3, R4 in Series = (0.9985×0.9985) = 0.997006

3

Availability of R1, R2 in Parallel with R3, R4
= 1 - ((1-0.997)(1 - 0.997)) = 0.99999104

4

Network Availability = 99.999%
Only Base on Device Availability Values; Link Availability Not Included

---

Cisco Internal Tools: Calculated Availability

Cisco.com

Contact Your Sales Team for Quality Data

- **MTBF query tool**

  MTBF for components can be requested from Cisco

  User enters part number/product family and predicted MTBF is provided

  A system is a chassis populated with Field Replaceable Units (FRU) and software

- **NARC: Network Availability and Reliability Calculation**

  Excel spread sheet, calculates availability/downtime for a system/network given MTBF and MTTR

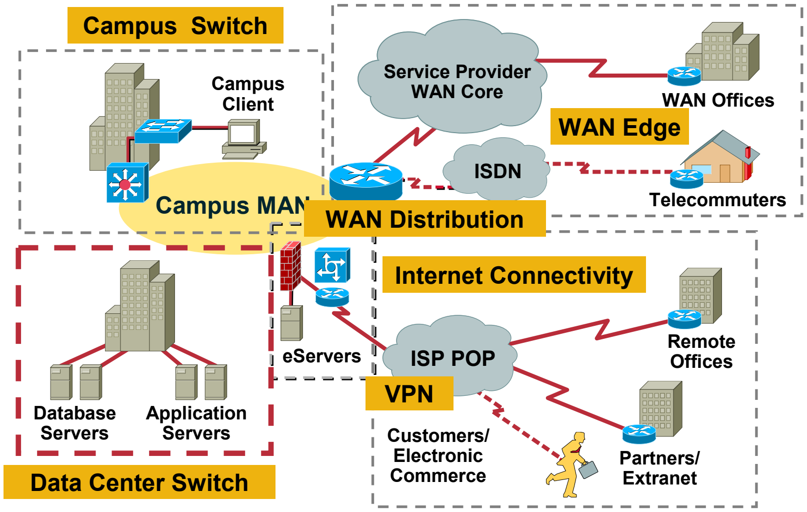
Calculated Availability Key Points

- Carried out at design time
- Availability can be increased by decreasing MTTR or increasing MTBF or both
- If service availability target is 99.999% calculated availability must be better than 99.999%

  Customer experience shows MTBF can be typically 2 x MTBF listed; this may not necessarily be a good thing
- Series components reduce availability, parallel (redundant) components increase availability
- Complex networks require modelling tools to calculate engineered availability
- Core networks are designed for high availability to a single point of failure; i.e., needs to be 99.999% available with any single network component (node/link) fails

---

Availability Metrics: Where? What?

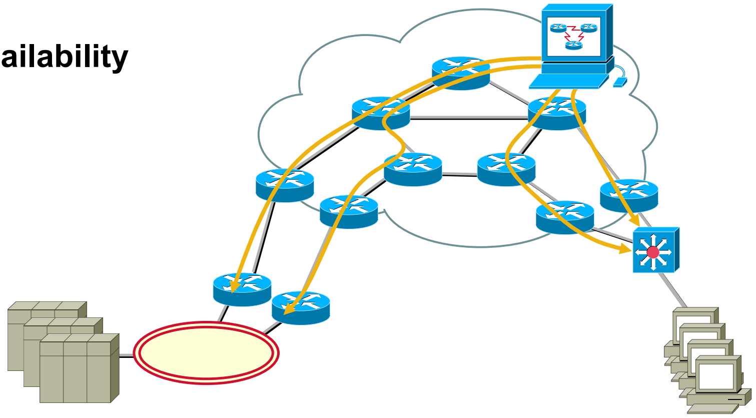


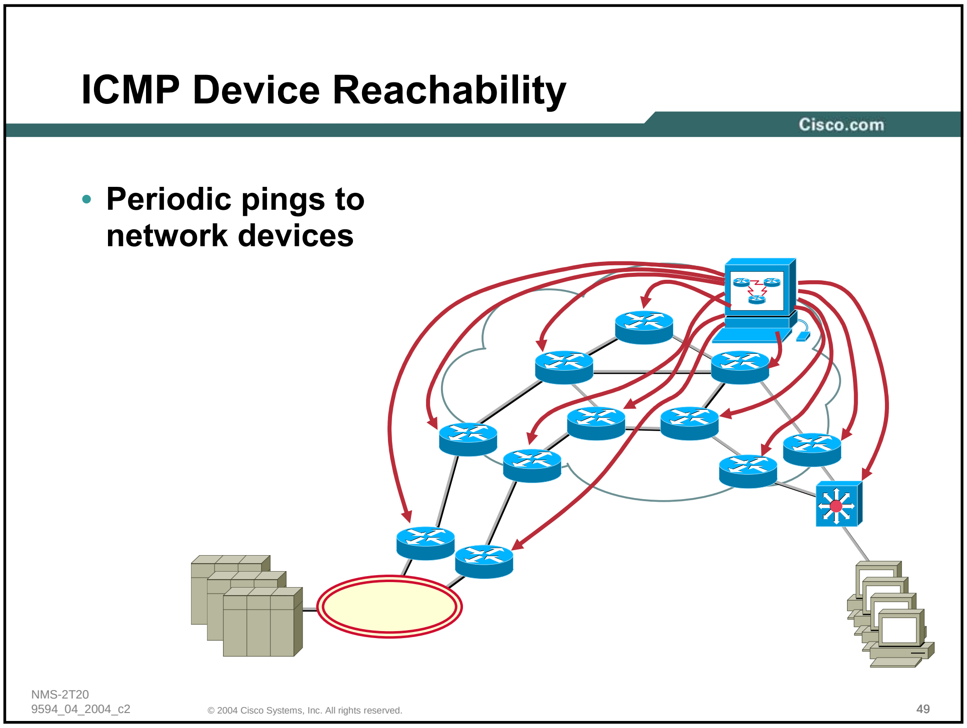
Availability Measurement Methodologies

- Ping (network availability, device availability)
- Service assurance agent
- Trouble ticket reporting
  - DPM: Defects Per Million
    - Defect may be one user/customer down for one minute or one hour
  - IUM: Impacted User Minutes
    - Number of users affected × outage in minutes
- RMON probe reporting
- Application request (SAP, SQL, etc.)

ICMP Reachability

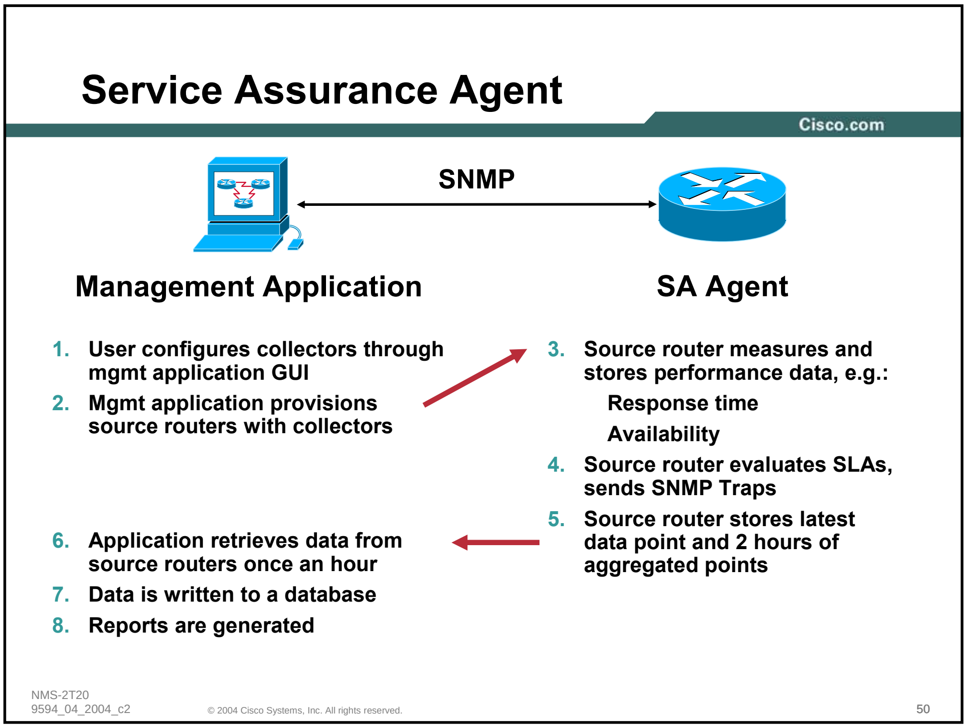
- Method definition
- How
- Unavailability





ICMP Device Reachability

- Periodic pings to network devices



Service Assurance Agent

SNMP

Management Application

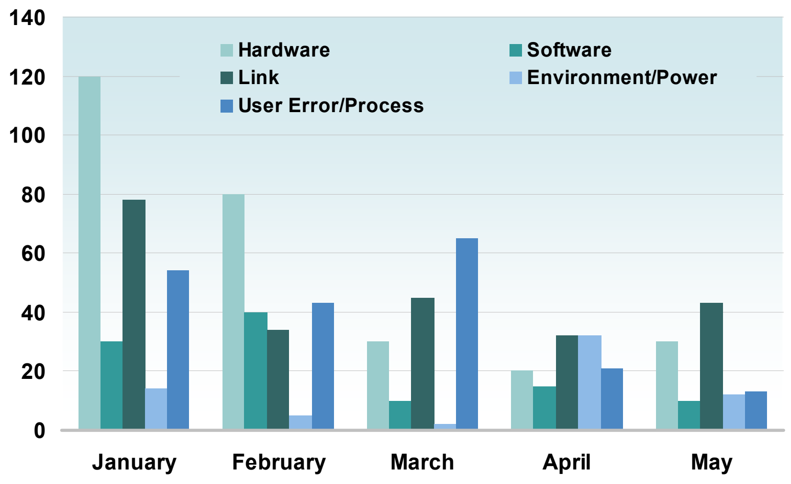
SA Agent

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
4. Source router evaluates SLAs, sends SNMP Traps
5. Source router stores latest data point and 2 hours of aggregated points
6. Application retrieves data from source routers once an hour
7. Data is written to a database
8. Reports are generated

Outage Logs

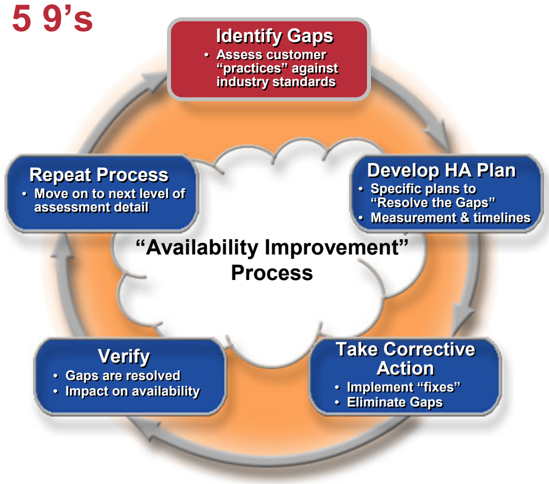
Date	Device	Problem	Cause	TTR	Cust Affected	DPM
3/13	Sf-rtr01	Bad RSP	Infant Mortality (Hardware)	271	250	145
3/17	DVR-rtr03	Connection Loss	Duplicate Subnet (User-Error)	342	100	57
3/17	NY-rtr17	Connection Loss	Software Bug (Software)	600	290	353
3/18	SEA-rtr02	Connection Loss	No UPS (Power)	60	37	21

Defects per Million



Continual Process Improvement

Road to 5 9's



Identify Gaps
- Assess customer "practices" against industry standards

Develop HA Plan
- Specific plans to "Resolve the Gaps"
- Measurement & timelines

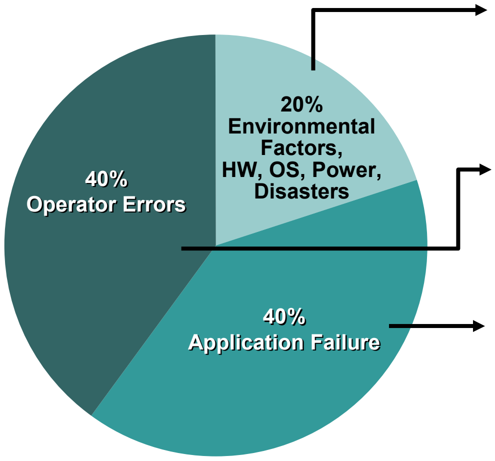
Take Corrective Action
- Implement "fixes"
- Eliminate Gaps

Verify
- Gaps are resolved
- Impact on availability

Repeat Process
- Move on to next level of assessment detail

"Availability Improvement" Process

Investing to Reduce Unplanned Downtime

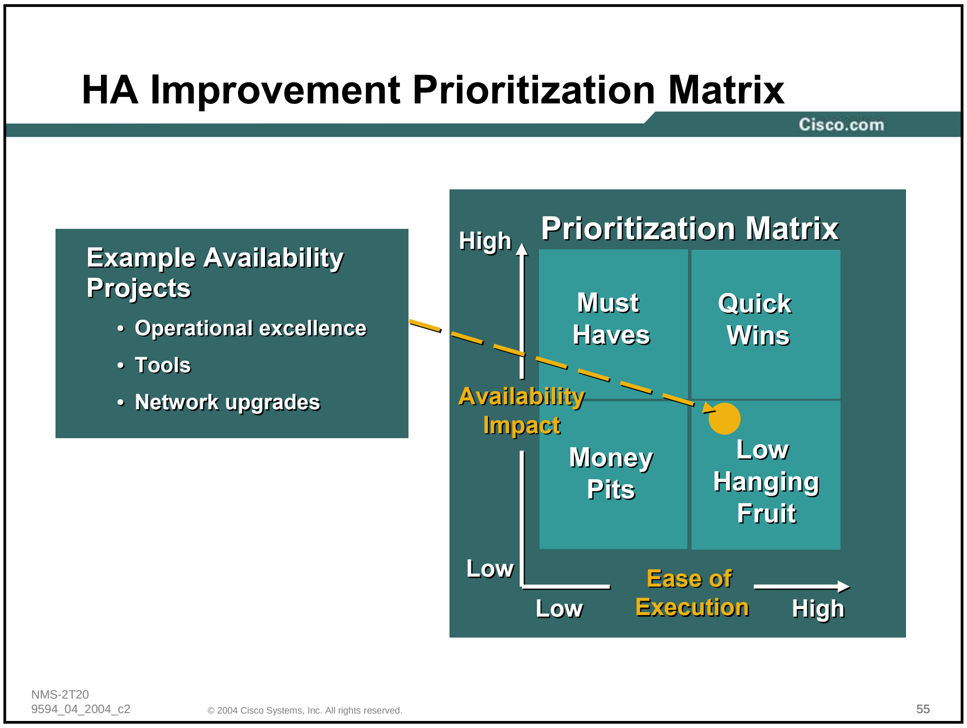


Investment Strategy
- ROI
- New technology
- Service contracts
- Availability monitoring

People and Process
- Hiring and training
- IT process maturity
- Automation
- Change and problem mgmt.

Application
- App. architecture/design
- Change management
- Problem management
- Configuration management
- Performance/capacity planning

Source: Gartner; Copyright ®2001



HA Improvement Prioritization Matrix

Cisco.com

Example Availability Projects

- Operational excellence
- Tools
- Network upgrades

Prioritization Matrix

High

Must Haves

Quick Wins

Availability Impact

Money Pits

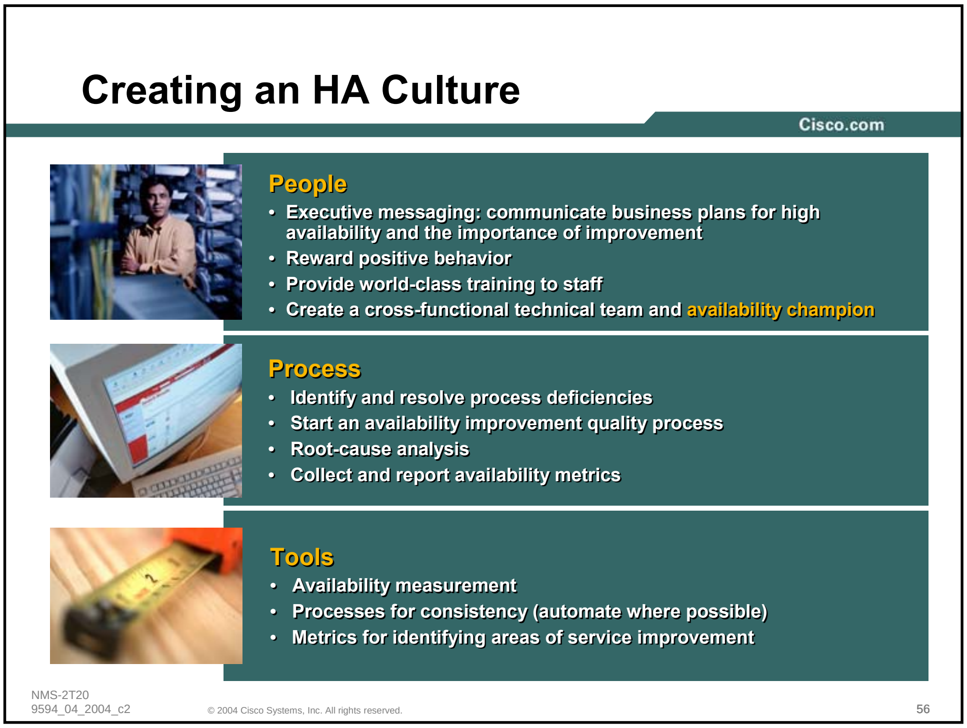
Low Hanging Fruit

Low

Low

Ease of Execution

High



Creating an HA Culture

Cisco.com

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

PEOPLE, PROCESS, AND TOOLS FOR HIGH AVAILABILITY

ADDRESSING 40% OF NETWORK OUTAGE TIME

Best-Practice Development

Cisco.com

Methodology:

- Cross-functional team with experience in network design, operations, and network management
- Experience and visibility with Cisco world class network environments
- Consulting experience in driving culture and technology changes

Design, Operations and NMS Experience

Identify Common Availability and Process Issues

Root Cause Analysis

Environment Comparisons

Best-Practice Definition

Best-Practice Development

Achieving High Availability; Best-Practices

Cisco.com

- Change Management
- New Solution Deployment
- Configuration Management
- Performance/Capacity Management
- Fault Management
- Problem Management
- Security Management
- Disaster Recovery

CHANGE MANAGEMENT

Change Management

- Change management refers to the consistent process of successfully managing change within an organization
- Process includes:
  - Change controller
  - Change documentation requirements
  - Risk level assignment
  - Validation and approval procedures
  - Change meetings
  - Emergency change procedures
  - Post mortem review and root-cause
  - Document change output requirements
  - Change management system and metrics

NEW SOLUTION DEPLOYMENT

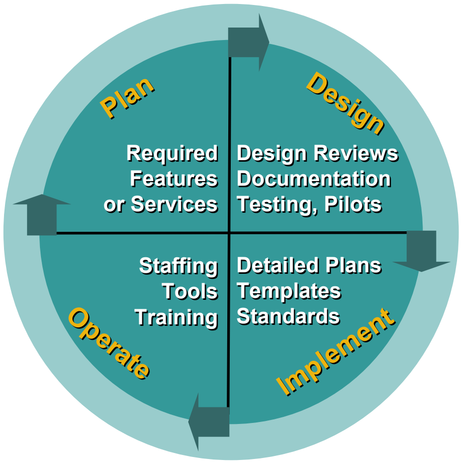
New Solution Deployment

- The biggest challenge is minimizing the impact on the existing networking environment
- Success requires structured processes that include resources from planning, design, network management, and implementation

---

New Solution Deployment

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



Plan

Required
Features
or Services

Design

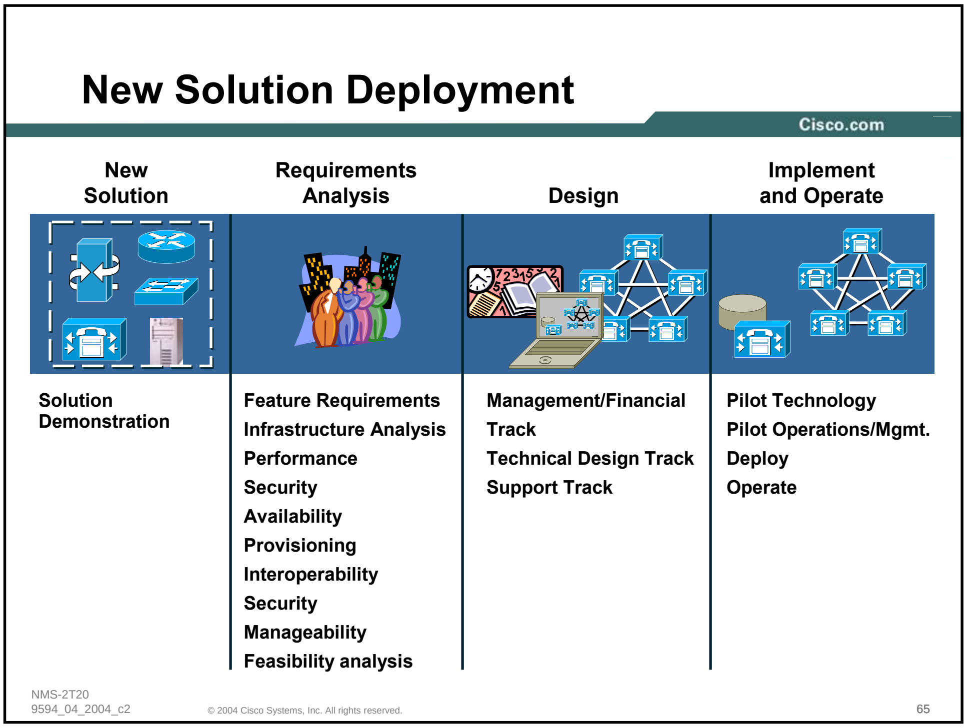
Design Reviews
Documentation
Testing, Pilots

Implement

Detailed Plans
Templates
Standards

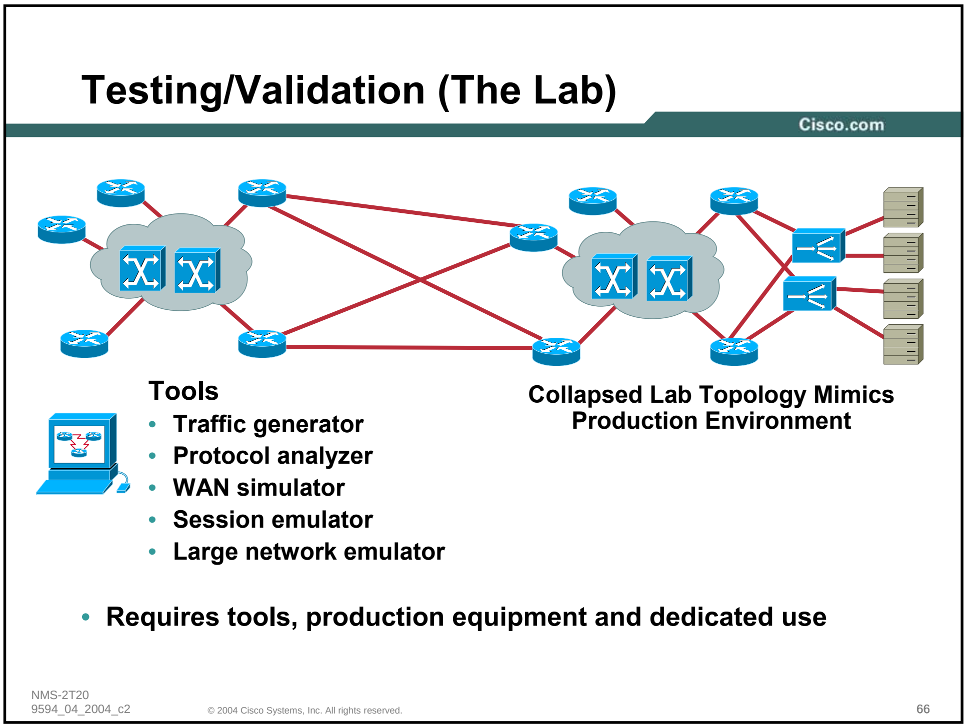
Operate

Staffing
Tools
Training



New Solution Deployment

New Solution	Requirements Analysis	Design	Implement and Operate
Solution Demonstration	Feature Requirements Infrastructure Analysis Performance Security Availability Provisioning Interoperability Security Manageability Feasibility analysis	Management/Financial Track Technical Design Track Support Track	Pilot Technology Pilot Operations/Mgmt. Deploy Operate



Testing/Validation (The Lab)

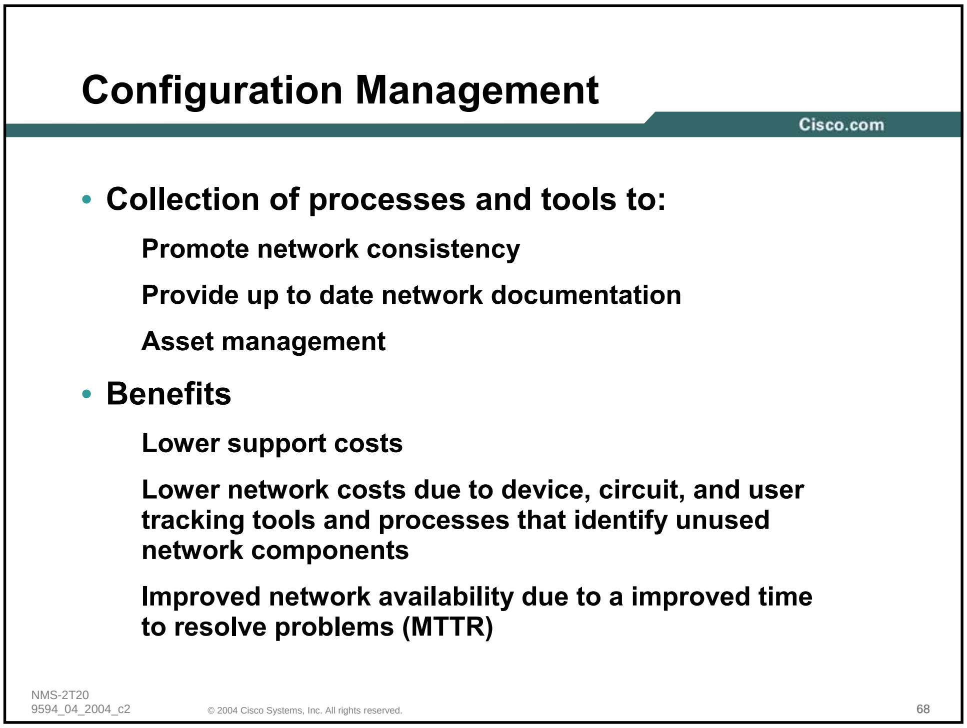
Tools

- Traffic generator
- Protocol analyzer
- WAN simulator
- Session emulator
- Large network emulator

Collapsed Lab Topology Mimics Production Environment

- Requires tools, production equipment and dedicated use

CONFIGURATION MANAGEMENT



Configuration Management

- Collection of processes and tools to:
    - Promote network consistency
    - Provide up to date network documentation
    - Asset management
- Benefits
    - Lower support costs
    - Lower network costs due to device, circuit, and user tracking tools and processes that identify unused network components
    - Improved network availability due to a improved time to resolve problems (MTTR)

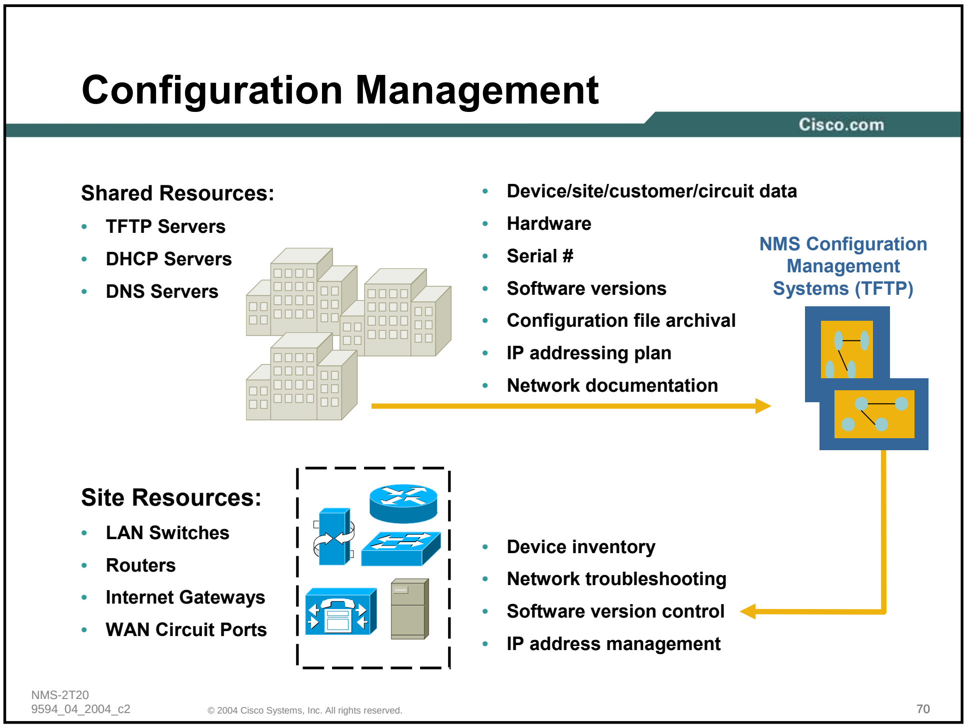
Create Standards

Cisco.com

- Configuration version control and management
- IP addressing standards and management
- Device naming conventions and DNS/DHCP assignments
- Standard configuration templates
- Configuration upgrade procedures
- Solution templates
- Network documentation (physical/logical)

Configuration Management

Cisco.com



Shared Resources:

- TFTP Servers
- DHCP Servers
- DNS Servers

- Device/site/customer/circuit data
- Hardware
- Serial #
- Software versions
- Configuration file archival
- IP addressing plan
- Network documentation

NMS Configuration Management Systems (TFTP)

Site Resources:

- LAN Switches
- Routers
- Internet Gateways
- WAN Circuit Ports

- Device inventory
- Network troubleshooting
- Software version control
- IP address management

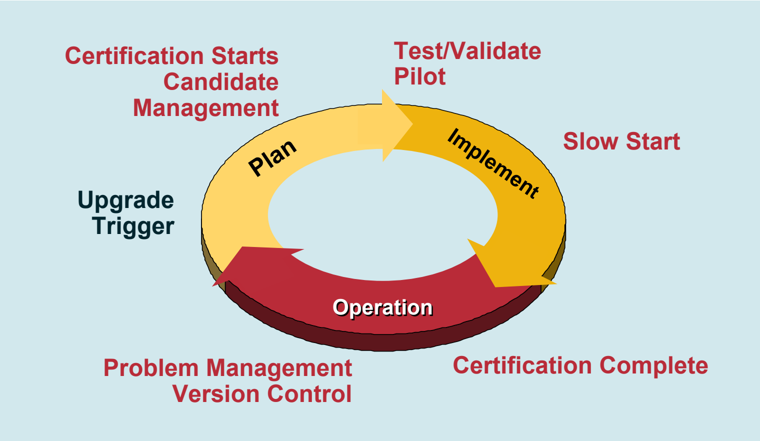
Configuration Management

- Versions of HW/SW
- Config files
- Config templates
- Backup configs
- IP address
- Feeds to change management

- Inventory
- Devices
- Vendors
- Support contacts
- Carrier
- Customer/device/link relationships

Software Lifecycle Management

Software Management



Certification Starts
Candidate
Management

Test/Validate
Pilot

Slow Start

Upgrade
Trigger

Problem Management
Version Control

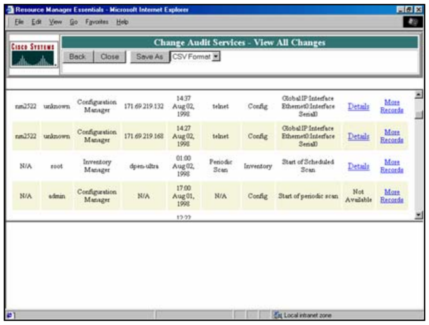
Certification Complete

Software Version Control

Cisco.com

The Process of Software Version Control Is Critical to Software Consistency and Overall Software Reliability!

- Publish and communicate certified device software version standards for identified software tracks
- Quality gates during implementation process
- Scheduled periodic audits to ensure network is in sync with the certified standard
- Utilize tools to identify, track and sort software versions



nm2522	unknown	Configuration Manager	171.69.219.132	14:37 Aug 02, 1998	telnet	Config	Global:IP:Interface Ethernet0:Interface Serial0	Details	More Records
nm2522	unknown	Configuration Manager	171.69.219.168	14:27 Aug 02, 1998	telnet	Config	Global:IP:Interface Ethernet0:Interface Serial0	Details	More Records
N/A	root	Inventory Manager	dpen-ultra	01:00 Aug 02, 1998	Periodic Scan	Inventory	Start of Scheduled Scan	Details	More Records
N/A	admin	Configuration Manager	N/A	17:00 Aug 01, 1998	N/A	Config	Start of periodic scan	Not Available	More Records
				12:22					

Maintain Documentation

Cisco.com

- Current device, link, and end-user inventory
- Configuration version control system
- Software version control
- TACACS configuration log
- Network topology

Validate and Audit Standards

- Configuration integrity checks
- Device, protocol, and media audits
- Standards and documentation review

Configuration Consistency Simplifies a Network, Resulting in Fewer Problems and Faster Problem Resolution

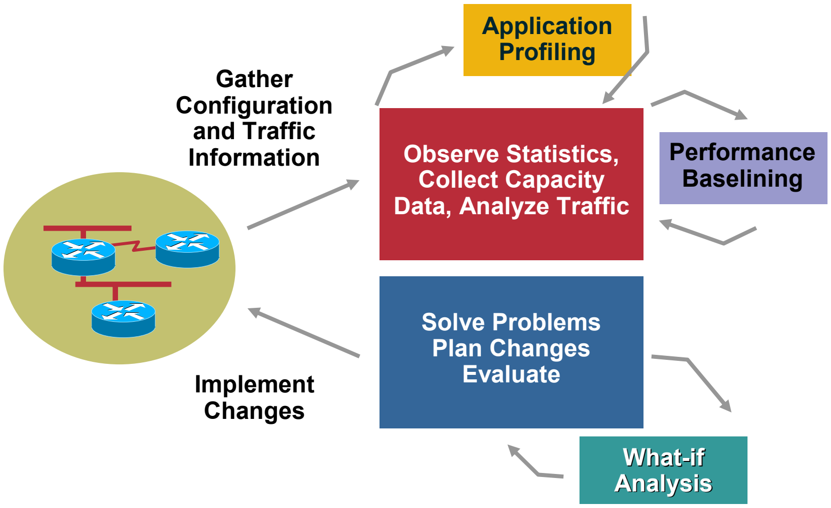
---

Tools for Configuration Management

- Often technology or product family-specific (Cisco Element Managers)
- CW2000
- Micromuse Netcool/Precision
- Visionael (change and configuration)
- Aperature (change and configuration)

PERFORMANCE MANAGEMENT

Capacity and Performance Management Process



Application Profiling

Gather Configuration and Traffic Information

Observe Statistics, Collect Capacity Data, Analyze Traffic

Performance Baselining

Solve Problems Plan Changes Evaluate

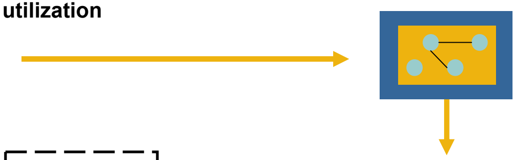
Implement Changes

What-if Analysis

Performance Management

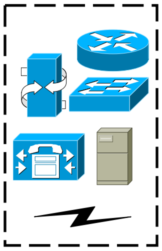
- SNMP polling, RMON
- Data includes utilization, CPU, memory, buffers, link utilization

- NMS performance
- Management systems
- Collection and archival



Site Resources

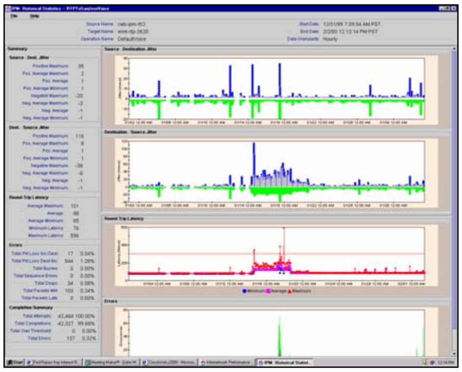
- LAN Switches
- Routers
- Switch Gateway Modules
- Gateways
- WAN and PSTN Circuit Ports



- Performance reports
- Exception reports
- Capacity planning

Baselining

- How does the network behave normally?
- CPU, memory, backplane, buffers, link utilization
- Collect data (show commands, performance data)
- Determine non-normal thresholds

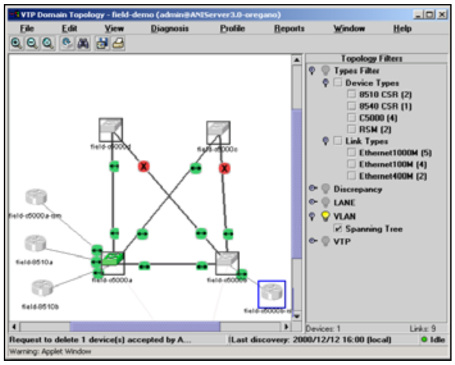


Develop a Capacity Planning Strategy, Including Common Techniques, Tools, MIB Variables, and Thresholds Used for Capacity Planning

Baselining and Exception Management

Cisco.com

- Alert mechanisms for performance exceptions
- Create trouble ticket to track proactive issues
- Investigate and make recommendations accordingly



Request to delete 1 device(s) accepted by A...

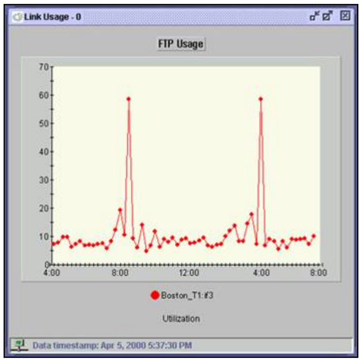
Last discovery: 2000/12/12 16:00 (local)

What-If Analysis

Cisco.com

What-If Analysis Centers around Network Change and How the Change Affects the Environment

- Identify higher risk changes
- Determine potential resource issues (CPU, memory, buffer, backplane, link util, device resources)
- Ask questions
- If possible, take it to the lab
- If possible, slow start implementation and measure key resource areas



Data timestamp: Apr 5, 2000 5:37:30 PM

Tools for Performance Management

- CW 2000 Service Assurance Agent
- NetScout nGenius
- Cisco NetFlow Collector/Analyzer
- SMARTS inCharge for performance
- Lucent VitalNet
- InfoVista
- Concorde Ehealth

FAULT MANAGEMENT

FAULT DETECTION AND REPORTING

Fault Management

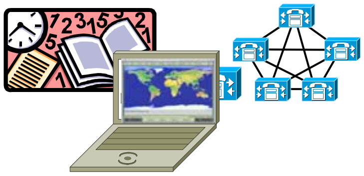
Cisco.com

- Fault management
  - Process of identifying faults through the use of network management toolsets
  - NMS architecture design and resiliency
  - Syslog collection, monitoring and Analysis
  - SNMP trap collection and notification
  - Exception reporting and analysis

Fault Management

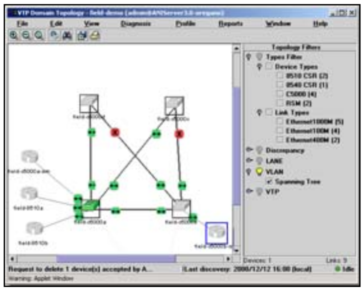
Cisco.com

- Detection, notification, of network failures
  - SNMP polling
  - SNMP traps
  - Syslog
- Proactive fault analysis
  - MIB variables
  - Threshold violations
  - Syslog
- Fault infrastructure
  - TFTP, NTP, time-stamps, out-of-band management and vendor access



Fault Management Architecture

- **NMS stations:**
  - Centralized vs. distributed architecture
  - Located close to the network core
  - Adequate bandwidth and separation from other services
  - Redundant hardware/network connectivity
- **NMS UPS (Uninterruptible Power Supply)**
  - All NMS systems should be protected against power failures



Request to delete 1 device(s) accepted by A...

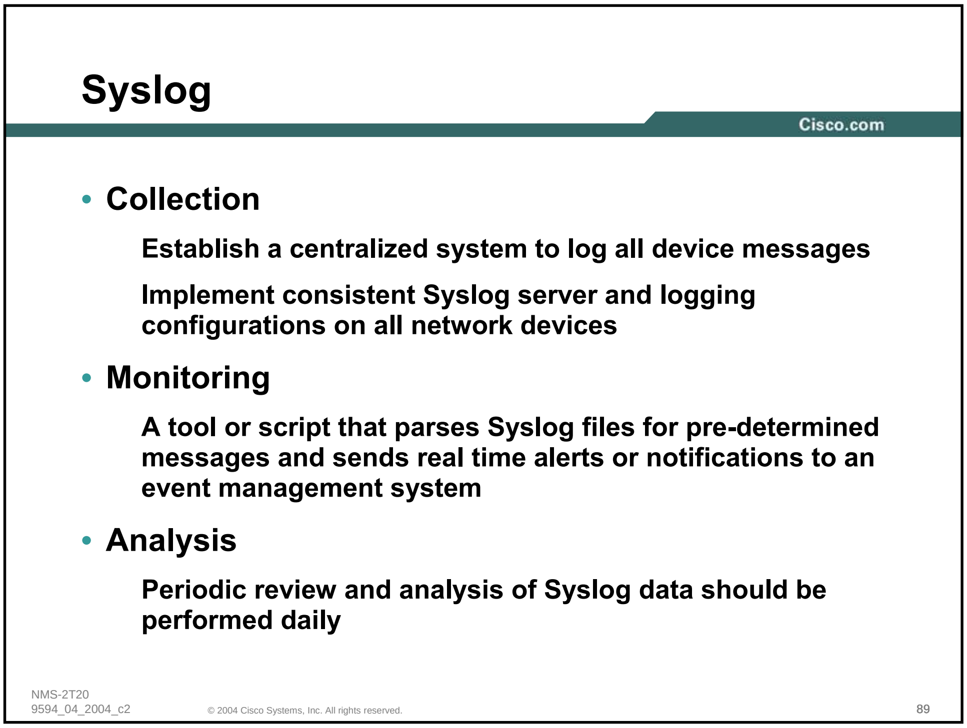
Last discovery: 2000/12/12 16:00 (local)

SNMP Trap Collection and Notification

The Collection and Notification of SNMP Traps Is Essential to Rapid Identification and Resolution

- **SNMP trap collection**
  - SNMP traps include generic traps and platform or technology specific traps
  - Traps must be properly and consistently configured on all network devices as well as the network management systems
- **SNMP trap notification**
  - NMS systems should notify and alert when a trap has been received

---



Syslog

Cisco.com

- Collection

  Establish a centralized system to log all device messages

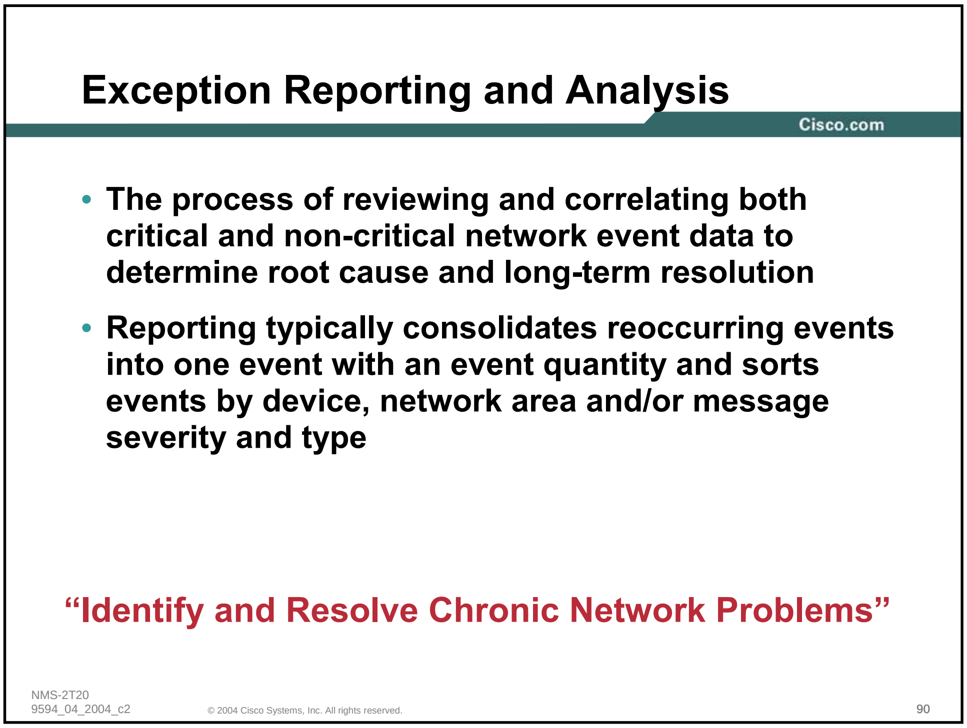
  Implement consistent Syslog server and logging configurations on all network devices

- Monitoring

  A tool or script that parses Syslog files for pre-determined messages and sends real time alerts or notifications to an event management system

- Analysis

  Periodic review and analysis of Syslog data should be performed daily



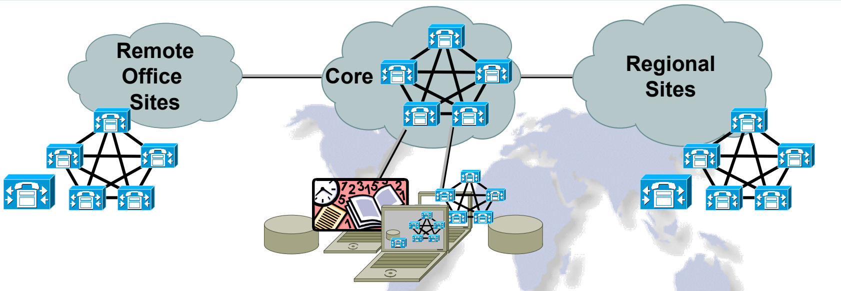
Exception Reporting and Analysis

Cisco.com

- The process of reviewing and correlating both critical and non-critical network event data to determine root cause and long-term resolution
- Reporting typically consolidates reoccurring events into one event with an event quantity and sorts events by device, network area and/or message severity and type

“Identify and Resolve Chronic Network Problems”

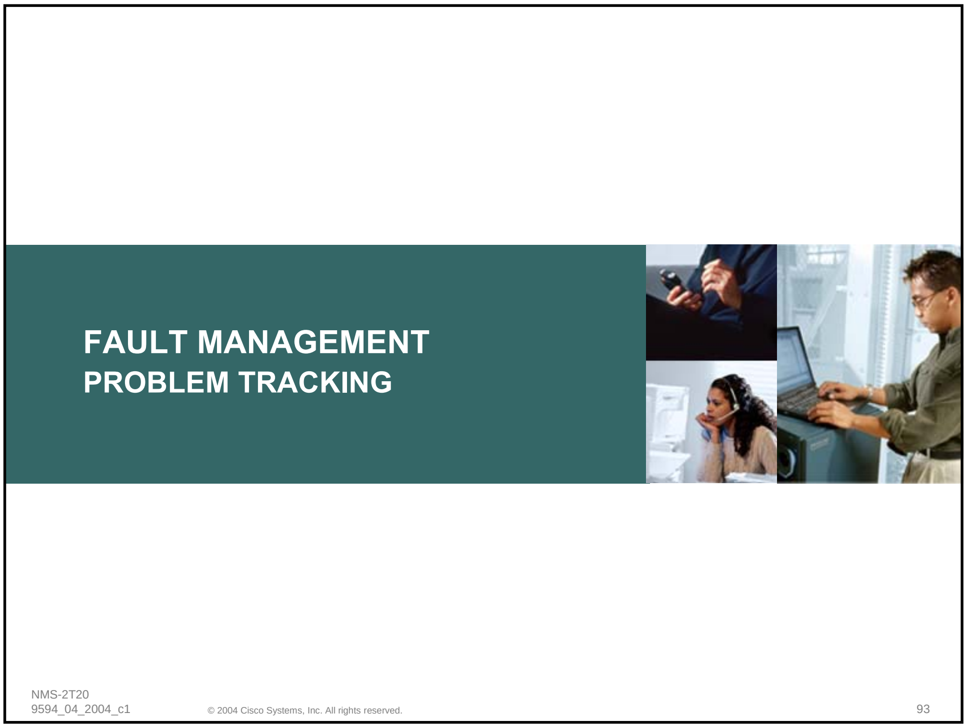
Fault Management



Data Collection	Monitoring	Alerting Notification	Reporting and Analysis
• SNMP traps • SNMP polling • Syslog • Performance • RMON	• Links errors • Devices memory CPU • Applications • Thresholds	• Visual (graphics) • Text • Page • Audible	• Report availability • SNMP exceptions • Syslog review • Fault metrics

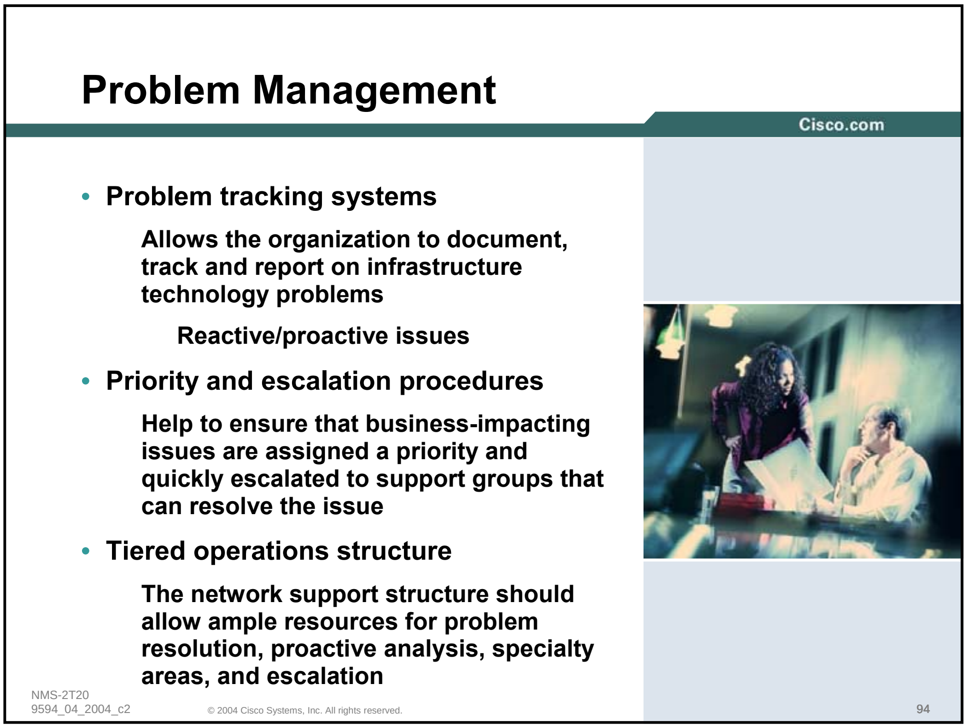
Fault Management Tools

- CiscoWorks Device Fault Manager
- HP OpenView Network Node Manager
- Aprisma Spectrum
- SMARTS InCharge for Fault
- IBM Tivoli
- MicroMuse NetCool



FAULT MANAGEMENT

PROBLEM TRACKING

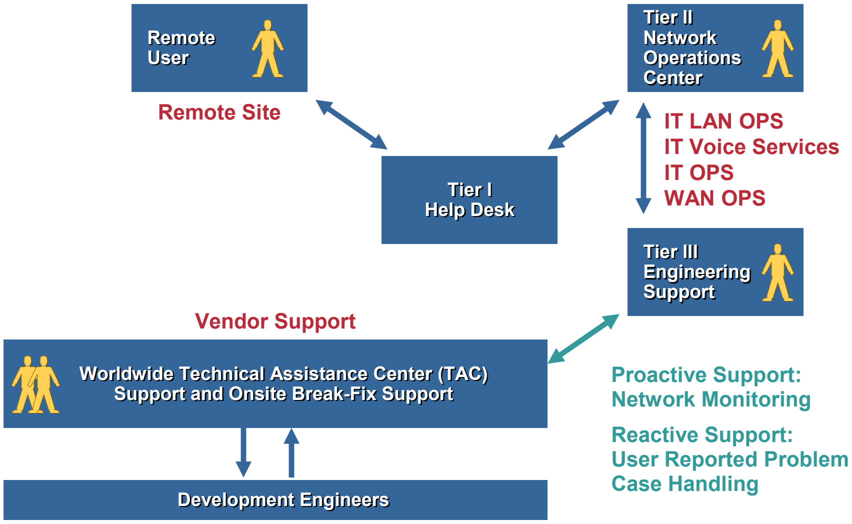


Problem Management

- **Problem tracking systems**
  - **Allows the organization to document, track and report on infrastructure technology problems**
    - **Reactive/proactive issues**
- **Priority and escalation procedures**
  - **Help to ensure that business-impacting issues are assigned a priority and quickly escalated to support groups that can resolve the issue**
- **Tiered operations structure**
  - **The network support structure should allow ample resources for problem resolution, proactive analysis, specialty areas, and escalation**

Problem Management
Trouble Flow

Cisco.com

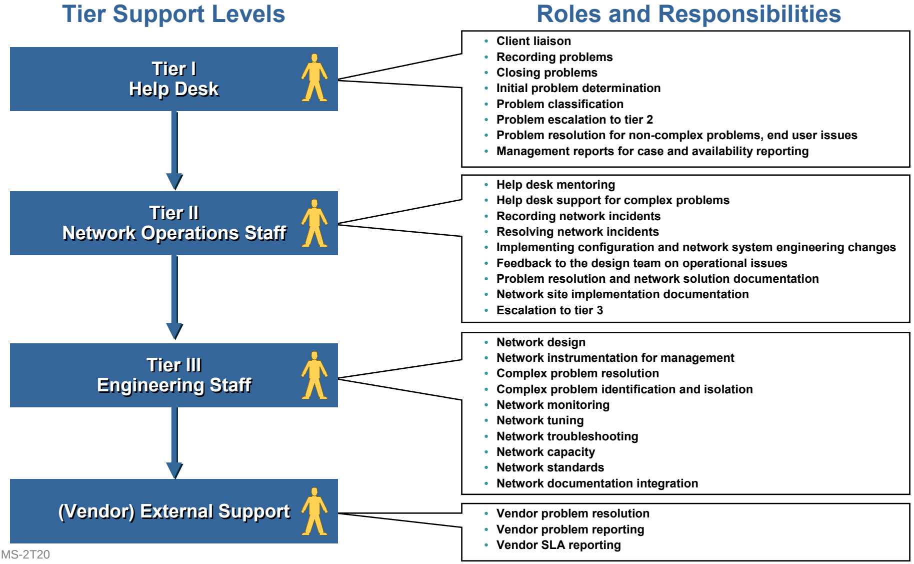


Proactive Support:
Network Monitoring

Reactive Support:
User Reported Problem
Case Handling

Problem Management
Tiered Operations Structure

Cisco.com



Tier I Help Desk
- Client liaison
- Recording problems
- Closing problems
- Initial problem determination
- Problem classification
- Problem escalation to tier 2
- Problem resolution for non-complex problems, end user issues
- Management reports for case and availability reporting

Tier II Network Operations Staff
- Help desk mentoring
- Help desk support for complex problems
- Recording network incidents
- Resolving network incidents
- Implementing configuration and network system engineering changes
- Feedback to the design team on operational issues
- Problem resolution and network solution documentation
- Network site implementation documentation
- Escalation to tier 3

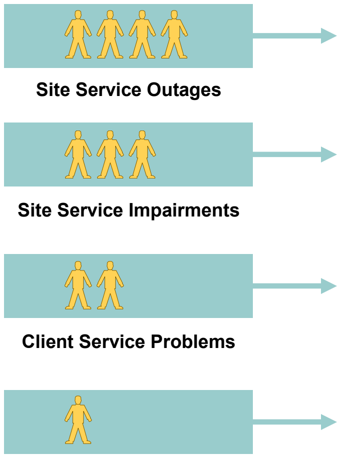
Tier III Engineering Staff
- Network design
- Network instrumentation for management
- Complex problem resolution
- Complex problem identification and isolation
- Network monitoring
- Network tuning
- Network troubleshooting
- Network capacity
- Network standards
- Network documentation integration

(Vendor) External Support
- Vendor problem resolution
- Vendor problem reporting
- Vendor SLA reporting

Problem Management
Problem Priority Definitions

Cisco.com

Problem Types



Site Service Outages

Site Service Impairments

Client Service Problems

Client Admin and Change Requests

Problem Priority Categories

Urgent: P1

- Severe business impact
- Loss of service or outage at a location

High: P2

- High business impact
- Degradation, possible workaround exists
- Service impairment

Medium: P3

- Minimal business impact
- Some specific network functionality is lost
- Loss of redundancy

Low: P4

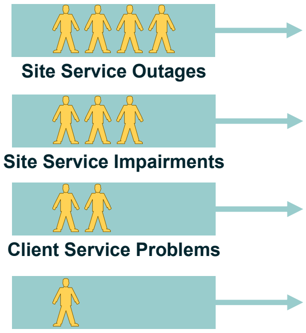
- No business impact
- A functional query

MTTR Objectives/SLAs

Cisco.com

Support Objectives

Problem Types



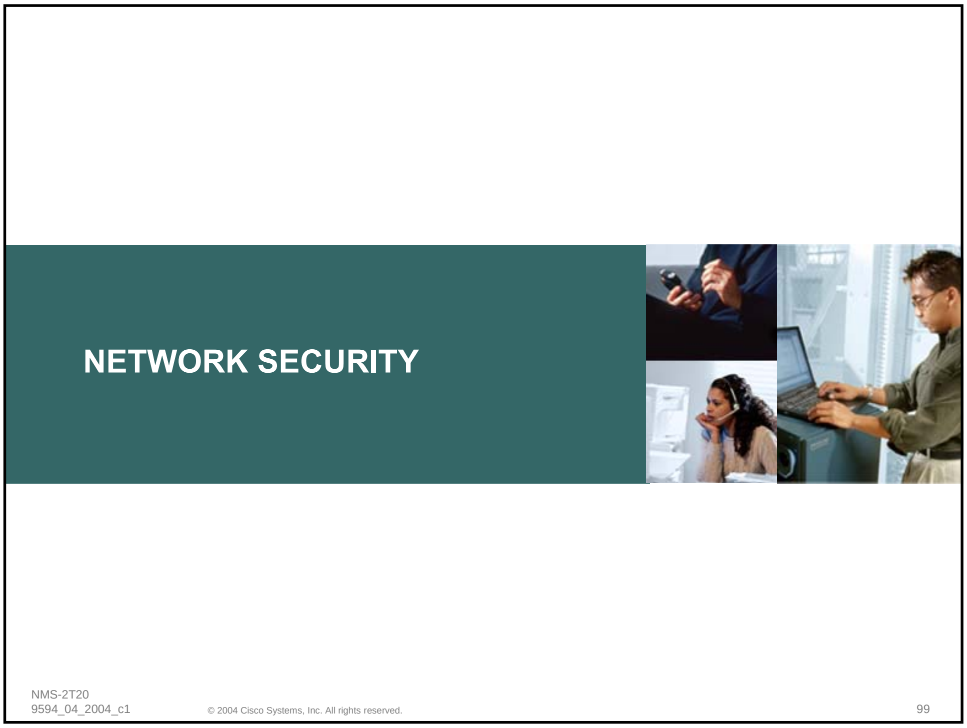
Site Service Outages

Site Service Impairments

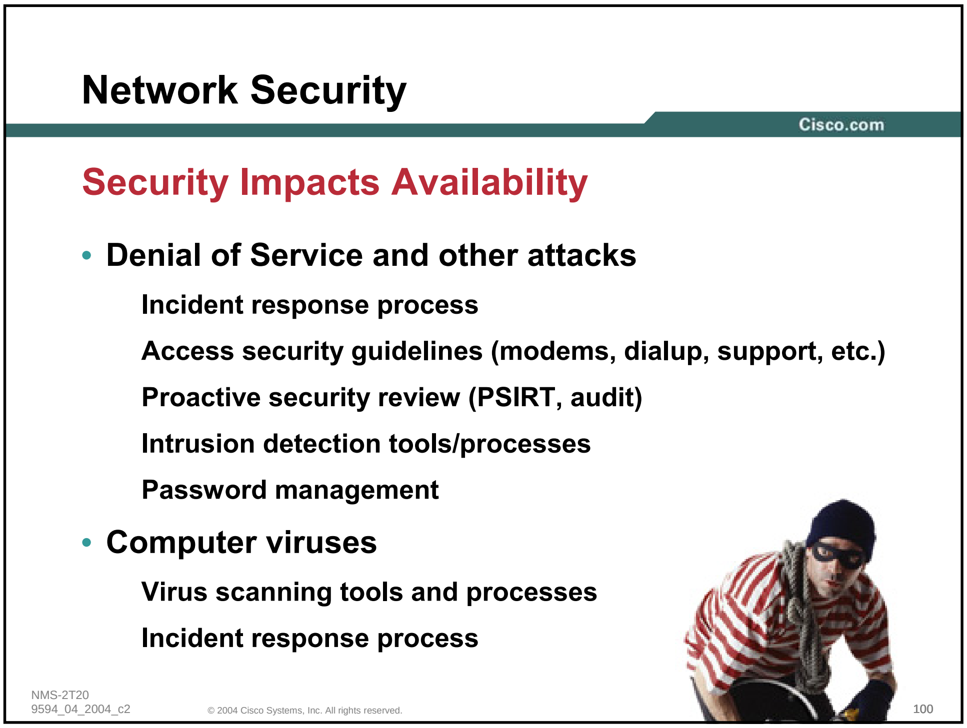
Client Service Problems

Client Admin and Change Requests

Problem Category Type	Response Time during Prime Time	Response Time During Off-Peak	Mean Time to Repair Objective
Urgent	15 Minutes	15 Minutes	2 Hours
High	1 Hour	2 Hours	4 Hours
Medium	1 Business Day	1 Business Day	2 Business Days
Low	1 Business Day	1 Business Day	5 Business Days



NETWORK SECURITY

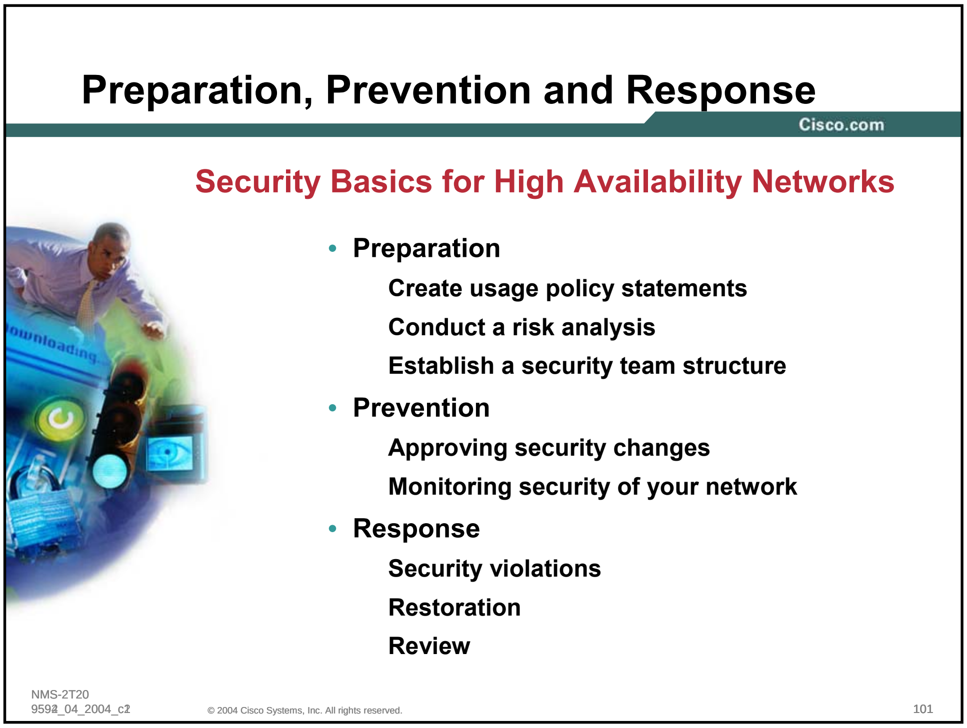


Network Security

Cisco.com

Security Impacts Availability

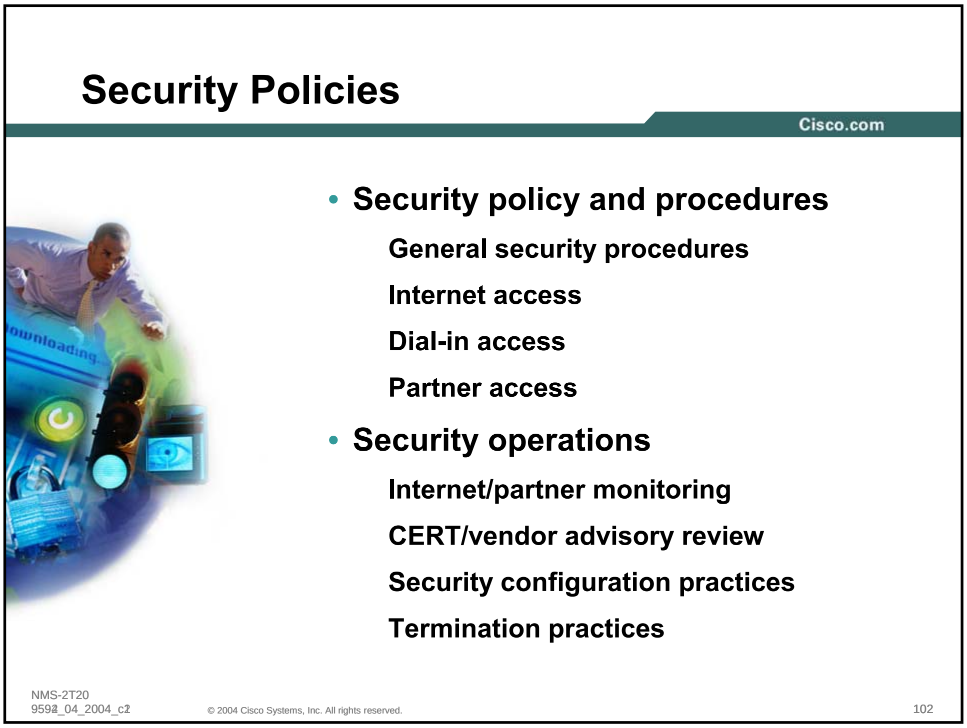
- Denial of Service and other attacks
  - Incident response process
  - Access security guidelines (modems, dialup, support, etc.)
  - Proactive security review (PSIRT, audit)
  - Intrusion detection tools/processes
  - Password management
- Computer viruses
  - Virus scanning tools and processes
  - Incident response process



Preparation, Prevention and Response

Security Basics for High Availability Networks

- Preparation
  - Create usage policy statements
  - Conduct a risk analysis
  - Establish a security team structure
- Prevention
  - Approving security changes
  - Monitoring security of your network
- Response
  - Security violations
  - Restoration
  - Review



Security Policies

- 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

Device Security

Cisco.com

- Device access control

  Secure access to devices via remote login, console access and SNMP

  - AAA (TACACS+, RADIUS)
  - SNMP access lists
  - SNMP views

- Passwords

  "Enable Secret"

  "Service password-encryption"

DISASTER RECOVERY

Disaster Recovery

- A disaster recovery plan covers
    - The hardware and software required to run critical business applications
    - The associated processes to transition smoothly in the event of a disaster
- Assess your mission-critical business processes and associated applications before creating the full disaster recovery plan
- Critical steps for best-practice disaster recovery:
    - Disaster recovery planning
    - Resiliency and backup services
    - Vendor support services

Disaster Recover Planning Process

- Establish a planning group
- Perform risk assessments and audits
- Establish priorities for your network and applications
- Develop resiliency design and recovery strategy
- Prepare up-to-date inventory and documentation of the plan
- Develop verification criteria and procedures
- Implementation

Resiliency and Backup Services

- Resiliency and backup services are a key part of disaster recovery
- Cisco defines network resiliency as the ability to recover from any network failure or issue whether it is related to a disaster, link, hardware, design, or network services
- A HA network design is often the foundation for disaster recovery and might handle some minor or local disasters
- Key tasks for resiliency planning and backup services include the following:
  - Assess the resiliency of your network, identify gaps and risks
  - Review your current backup services
  - Implement network resiliency and backup services

Vendor Support Services

- Having support services from your major vendors in place adds a strong value to disaster recovery planning
- For example, specific managed hot standby sites or on-site services with rapid response times can significantly ease disaster recovery
- Key questions regarding vendor support include:
  - Are support contracts in place?
  - Has the disaster recovery plan been reviewed by the vendors, and are the vendors included in the escalation processes?
  - Does the vendor have sufficient resources to support the disaster recovery?
- Most vendors have experience handling disaster situations and can offer additional support

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

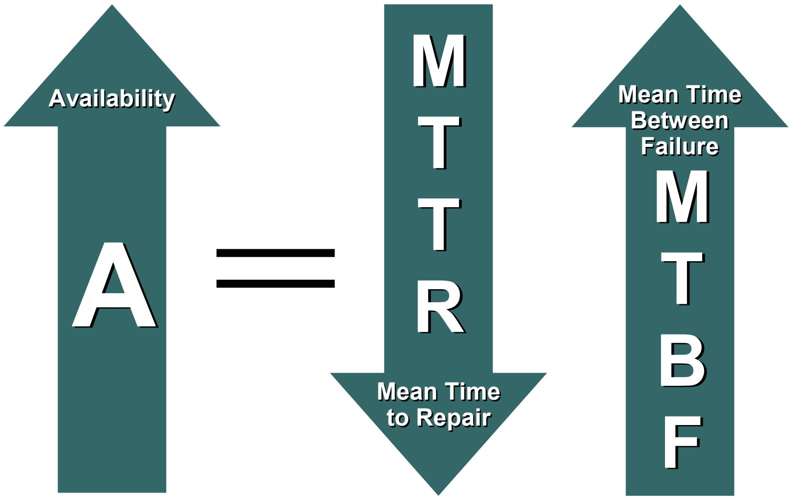
CISCO SYSTEMS

NETWORKERS 2004

DESIGNING AND MANAGING HIGH AVAILABILITY IP NETWORKS

LUNCH

Increasing Availability



Technology Perspective to Improve High Availability

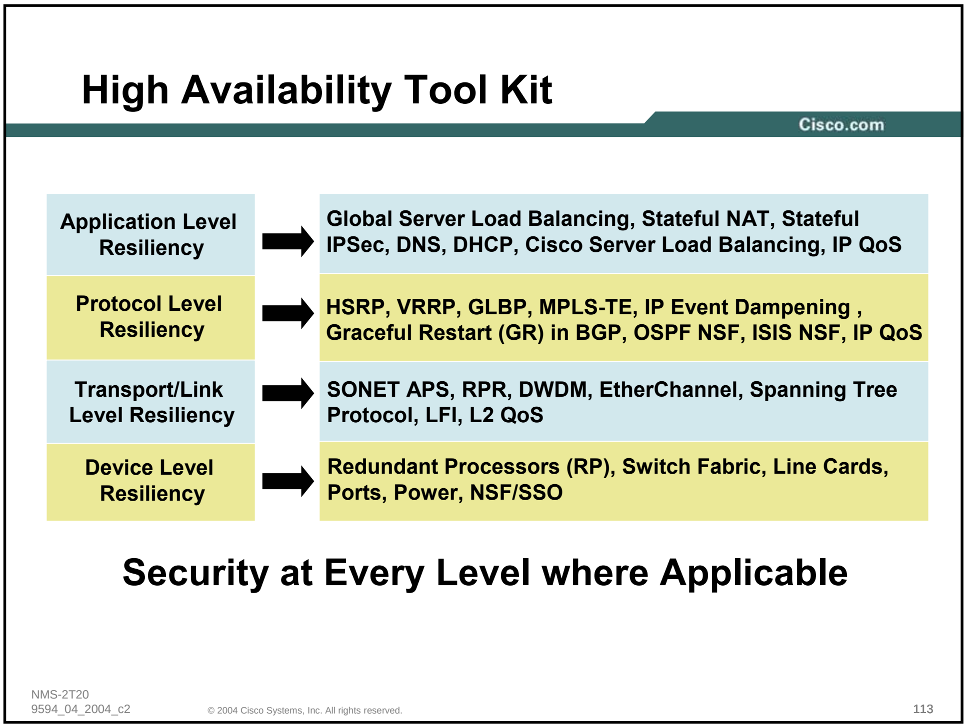
- Provide intelligent redundant elements

  Dual homing, multi-link options, box redundancy
- Leverage load balancing in redundant elements when possible

  MLPPP, EtherChannel®
- Detect failures faster

  Fine tuning failure detection intervals
- Recover from failures faster

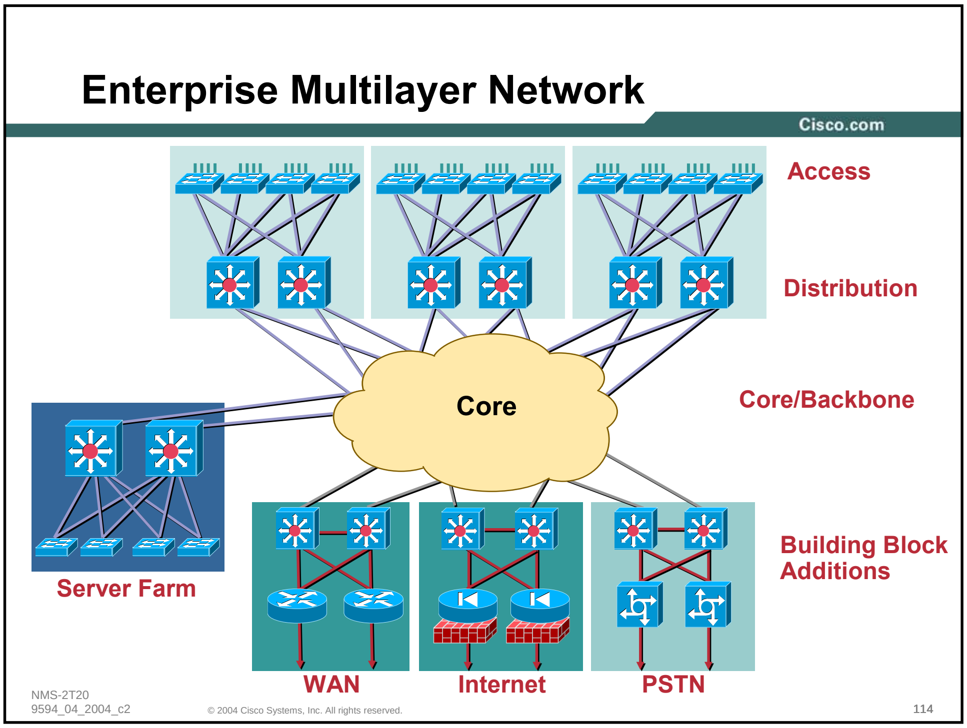
  Fine tune routing protocol convergence, L2 recovery mechanisms (APS)
- Security and Quality of Service



High Availability Tool Kit

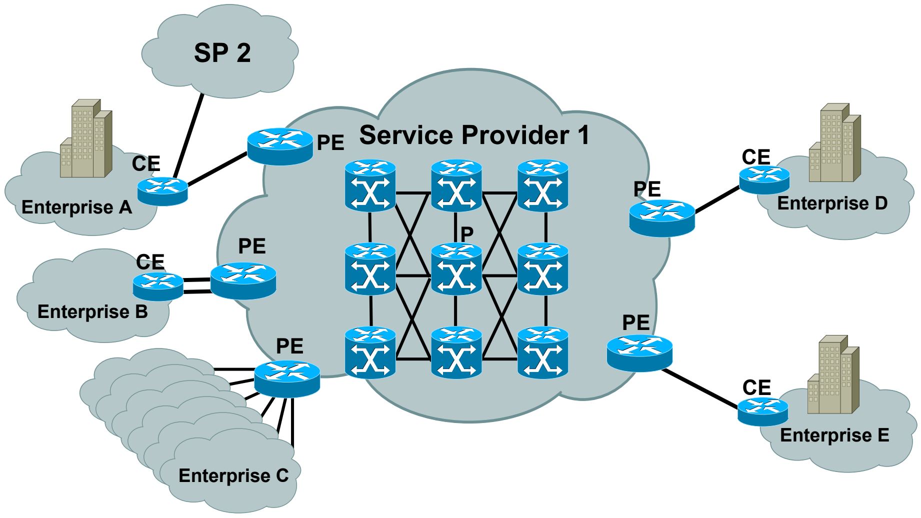
Application Level Resiliency	Global Server Load Balancing, Stateful NAT, Stateful IPSec, DNS, DHCP, Cisco Server Load Balancing, IP QoS
Protocol Level Resiliency	HSRP, VRRP, GLBP, MPLS-TE, IP Event Dampening , Graceful Restart (GR) in BGP, OSPF NSF, ISIS NSF, IP QoS
Transport/Link Level Resiliency	SONET APS, RPR, DWDM, EtherChannel, Spanning Tree Protocol, LFI, L2 QoS
Device Level Resiliency	Redundant Processors (RP), Switch Fabric, Line Cards, Ports, Power, NSF/SSO

Security at Every Level where Applicable



Enterprise Multilayer Network

Service Provider Network



Agenda

- High Availability in Layer 2 Networks
  - Access
  - Distribution
  - Core
- High Availability in Layer 3 Networks
  - Access
  - Distribution
  - Core
- High Availability Components Layer 4 and Above

LAYER 2 HIGH AVAILABILITY

High Availability Tool Kit

Application Level Resiliency	➡	**Global Server Load Balancing, Stateful NAT, Stateful IPSec, DNS, DHCP, Cisco Server Load Balancing, IP QoS**
Protocol Level Resiliency	➡	**HSRP, VRRP, GLBP, MPLS-TE, IP Event Dampening , Graceful Restart (GR) in BGP, OSPF NSF, ISIS NSF, IP QoS**
Transport/Link Level Resiliency	➡	**SONET APS, RPR, DWDM, EtherChannel, Spanning Tree Protocol, LFI, L2 QoS**
Device Level Resiliency	➡	**Redundant Processors (RP), Switch Fabric, Line Cards, Ports, Power, NSF/SSO**

Networking Transport Evolution Enterprise Scenario

- Traffic originating in Enterprise network are transported using
  - Ethernet/Fast Ethernet/Gigabit Ethernet for a majority of local area networks
  - ATM and Frame Relay for WAN connectivity
  - Metro Ethernet/Metro Optical
  - DPT/RPR, ATM over SONET, Packet over SONET, etc.
  - MPLS/IPSec

Networking Transport Evolution Service Provider Scenario

- Traffic originating on service provider network backbone include
  - Circuit-based like TDM voice and fax
  - Packet-based like IP
  - Cell-based like ATM or Frame Relay
- Majority of traffic is transported over SONET/SDH
- Explosive growth of data compared to voice: POS
- Scalable technologies like DPT/RPR use SONET/SDH framing and infrastructure: Metro and access networks
- DWDM provides scalable solutions to prevent fiber exhaustion: Metro and long haul networks

L1/L2 High Availability

- We will focus on the following L1/ L2 technologies from an HA perspective
    - Ethernet
    - RPR
    - SONET

Transport Technology Comparison

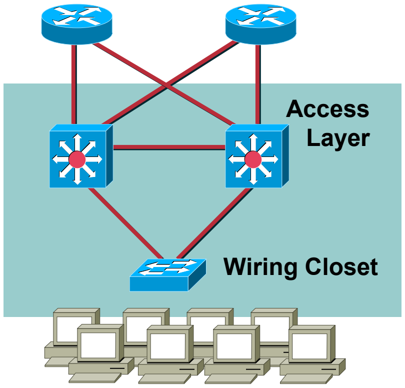
	GigE	SONET	DPT/RPR
Topology	Good for PtoP, Mesh	Ring	Ring
Recovery	Depends	< 50ms	< 50ms
Main Advantage	Simple, Low Cost	Ring-Based, Fast Fault Detection	Efficient, Simple, Ring-Based, Fast Fault Detection

LAYER 2 HIGH AVAILABILITY

ETHERNET

Access Layer Detail

- **Access switch availability directly effect end user experience**
- **Wiring closet up-links**
  - **Up-link fail-over redundancy**
  - **Fast convergence across multiple up-links**
- **Bandwidth scalability**
  - **All uplinks actively forwarding traffic**

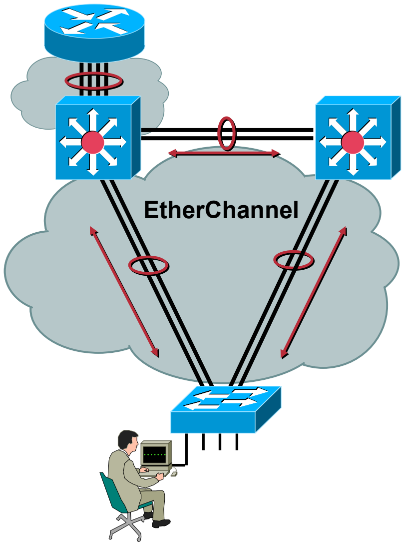


**Related Sessions: RST-2505 Campus Design Fundamentals
RST-2514 High Availability in Campus Networks**

EtherChannel Protocol

Cisco.com

- A logical aggregation of similar links (up to 8): 10/100/1000/10GE ports
- Operates between switches, routers, and certain vendors' NICs
- Channel always point-to-point
- Two flavors
  - Cisco's PAgP
  - IEEE 802.3ad
- Sub second recovery



Configuring EtherChannel

Cisco.com

On a Catalyst® 6000:

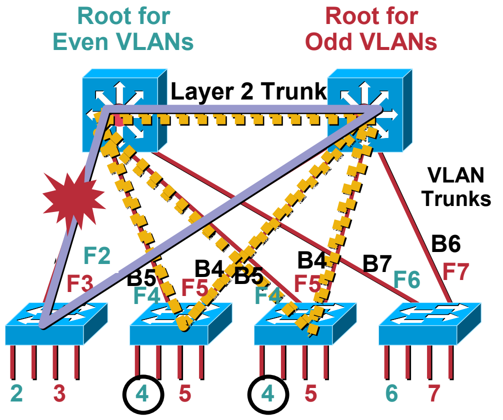
```
Console> (enable) set port channel 2/2-8 mode desirable
Ports 2/2-8 left admin_group 1.
Ports 2/2-8 joined admin_group 2.
Console> (enable)
```

On a Cisco 7500:

```
Router(config)# interface port-channel 1
Router(config)#  ip address 10.0.0.1 255.255.255.0
Router(config)#  ip route-cache distributed
Router(config)# interface fasteth 0/0
Router(config)#  no ip address
Router(config)#  channel-group 1
Router(config)# interface fasteth 0/1
Router(config)#  no ip address
Router(config)#  channel-group 1
FastEthernet 0/1 added as member-2 to fechannel1
```

Access Layer, Layer-2 Mode Load Sharing

- Dependent on spanning tree protocol
- Multiple VLANs
- Per-VLAN STP allows for load sharing
- STP permits forwarding around failures



F = Forward, B = Block

Spanning Tree Processing

Spanning Tree State Machine

Blocking Time to Detect that Root Bridge Not Available: 20 Secs

↓

Listening Discarding Frames while Calculating New Root: 15 Secs

↓

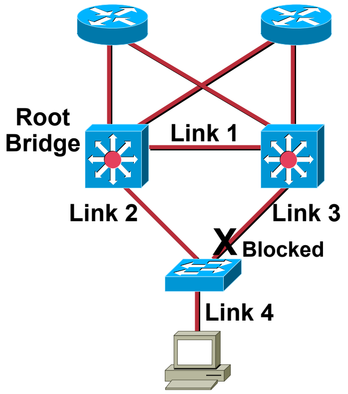
Learning Discarding Frames while Learning Addresses: 15 Secs

↓

Forwarding Finally Forwarding Frames; to Reach this State: 50 Secs

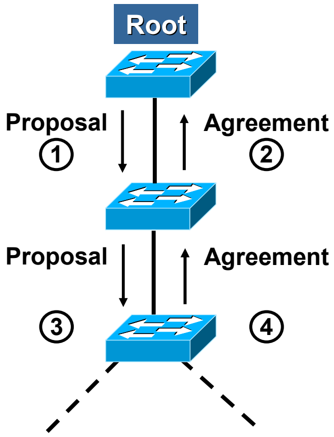
Spanning Tree Extensions

- Extensions decrease STP convergence time
- PortFast for access ports (Link4) bypasses listening-learning phases
- UplinkFast for direct root link failure (Link2): about 3 to 5 seconds convergence
- BackboneFast for indirect link failure (Link1): cuts convergence time by Max_Age seconds
- Standardized with IEEE 802.1w



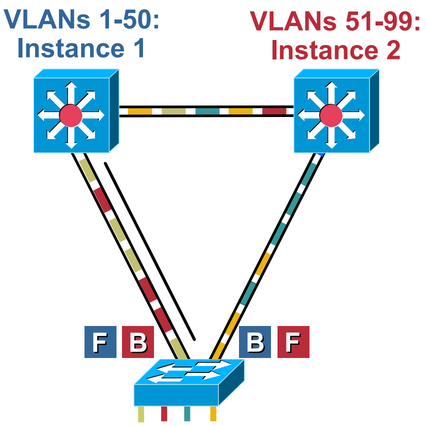
IEEE 802.1w: Rapid Spanning Tree

- Takes advantage of today's topologies (full-duplex point-to-point links)
- Remarkably similar to Uplinkfast/Backbonefast ☺
- No more network-wide timers when all switches run 802.1w
- Handshake mechanism between bridges
- Proposal-Agreement messaging ("I want to become designated: do you agree?")
- Can achieve 1+ second of convergence



IEEE 802.1s: Multiple Instance Spanning Tree

- IEEE802.1q only requires one Spanning Tree
- Scales Per-VLAN-Spanning-Tree (PVST)
- Two active topologies
- All VLANs mapped to one of two topologies
- Lower BPDU counts
- Simpler implementation
- Much less CPU utilization
- Very high scalability



LAYER 2 HIGH AVAILABILITY

RESILIENT PACKET RING (RPR)

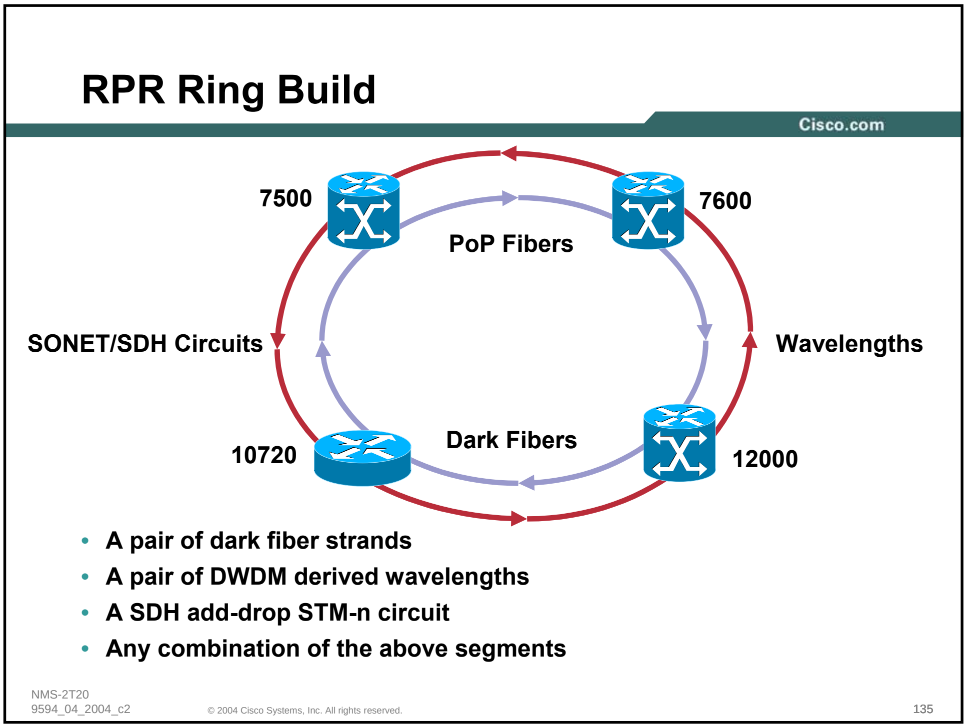
Resilient Packet Ring (RPR) Standard

- RPR is a layer 2 transport architecture
  - Based on dual counter-rotating ring architecture
  - Uses the best of Ethernet and SONET/SDH
  - Uses SRP-fairness algorithm
- Standards-based on IEEE 802.17 RPR Protocol Draft
- IEEE 802.17 is based on Cisco’s SRP (RFC 2892)
- Supported on high-end devices
- DPT/RPR name used interchangeably
- Cisco is committed to SRP and IEEE standards

Related Session: OPT 2043 802.17 and
Spatial Reuse Protocol (SRP) Protocols

Application Areas of RPR Networks

- PoP
  - Intra-PoP LANs, Inter-PoP MANs and WANs
  - 10–500+ meters over fiber
- Access Metro areas
  - Single and multi-provider customer access MANs
  - 25–100+ km over dark fibre
- Regional Metro area
  - 100–250+ km over dark fibre, DWDM
  - Metro Core, Campus LAN, Enterprise MANs and WANs
- Long Distance Core area
  - Long haul
  - 500–2500+ km over DWDM



RPR Ring Build

Cisco.com

7500

7600

PoP Fibers

SONET/SDH Circuits

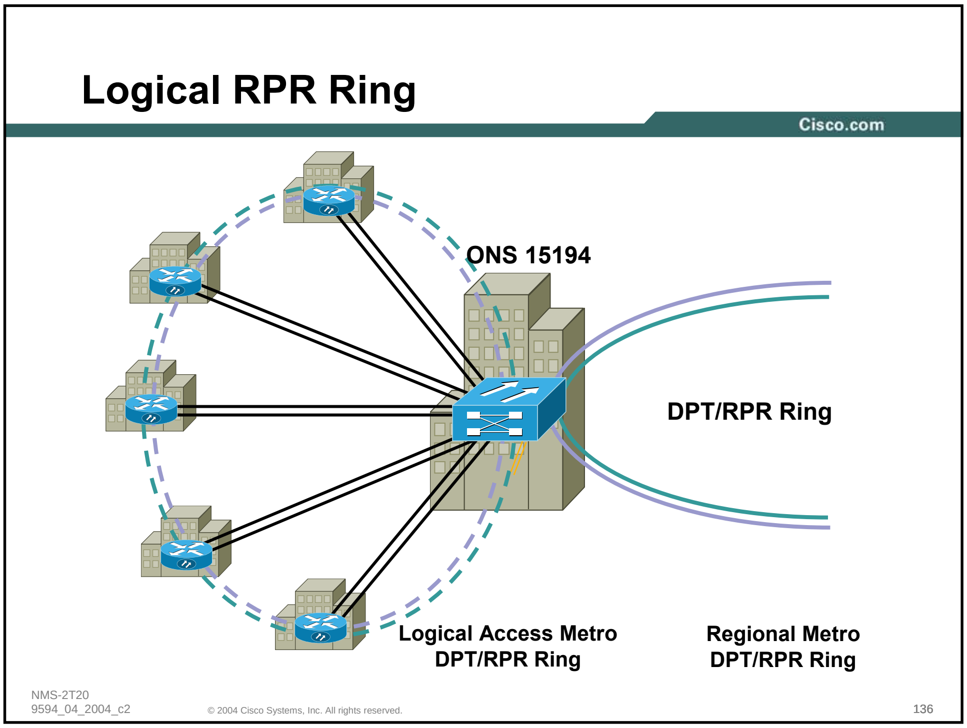
Wavelengths

10720

Dark Fibers

12000

- A pair of dark fiber strands
- A pair of DWDM derived wavelengths
- A SDH add-drop STM-n circuit
- Any combination of the above segments



Logical RPR Ring

Cisco.com

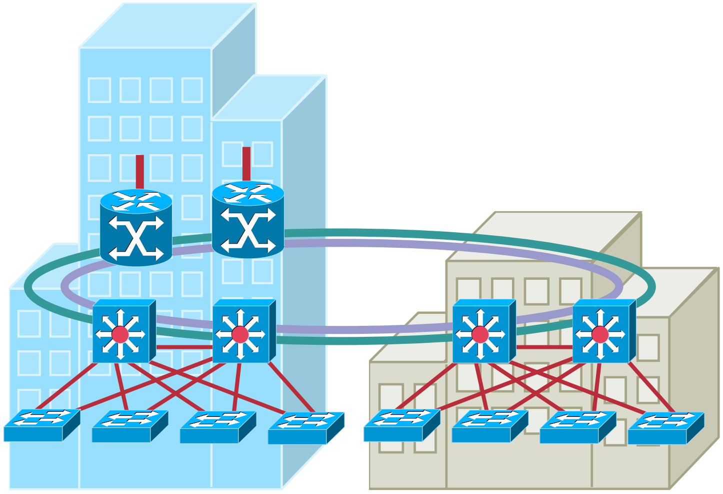
ONS 15194

DPT/RPR Ring

Logical Access Metro
DPT/RPR Ring

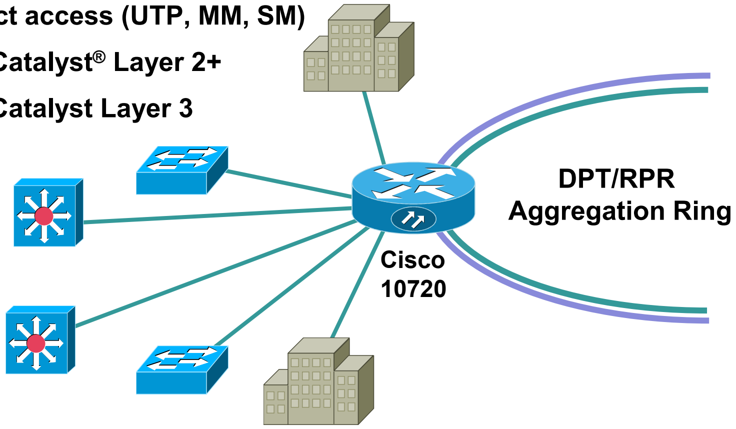
Regional Metro
DPT/RPR Ring

Campus/Metro Deployment



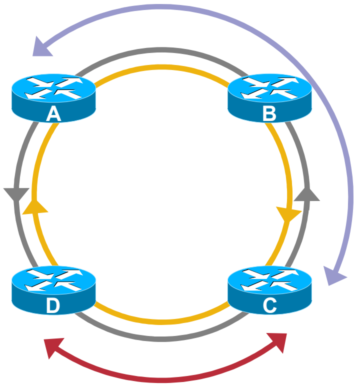
SP Edge Deployment

- 10/100/1000 Mbps access
- Direct access (UTP, MM, SM)
- Via Catalyst® Layer 2+
- Via Catalyst Layer 3



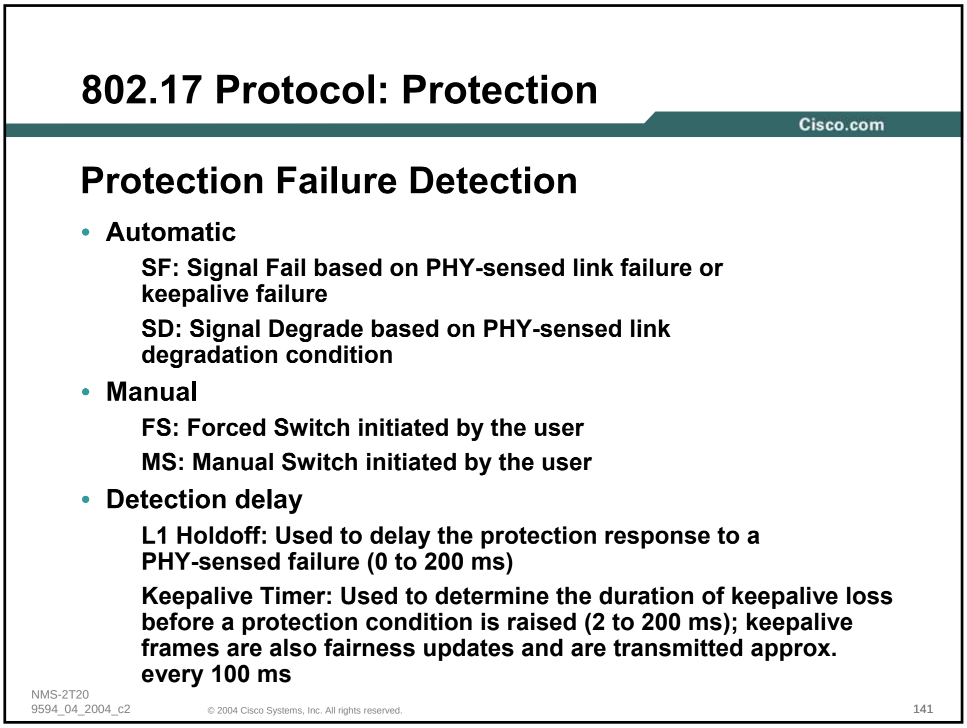
RPR Features: Spatial Reuse

- Spatial reuse: Increases overall ring aggregate bandwidth
  - Unicast packets are “destination” stripped
  - Multicast is source stripped
- Multiple nodes can transmit simultaneously
- Both rings used for carrying traffic: No reserved protection bandwidth



RPR Protection Switching: Intelligent Protection Switching (IPS)

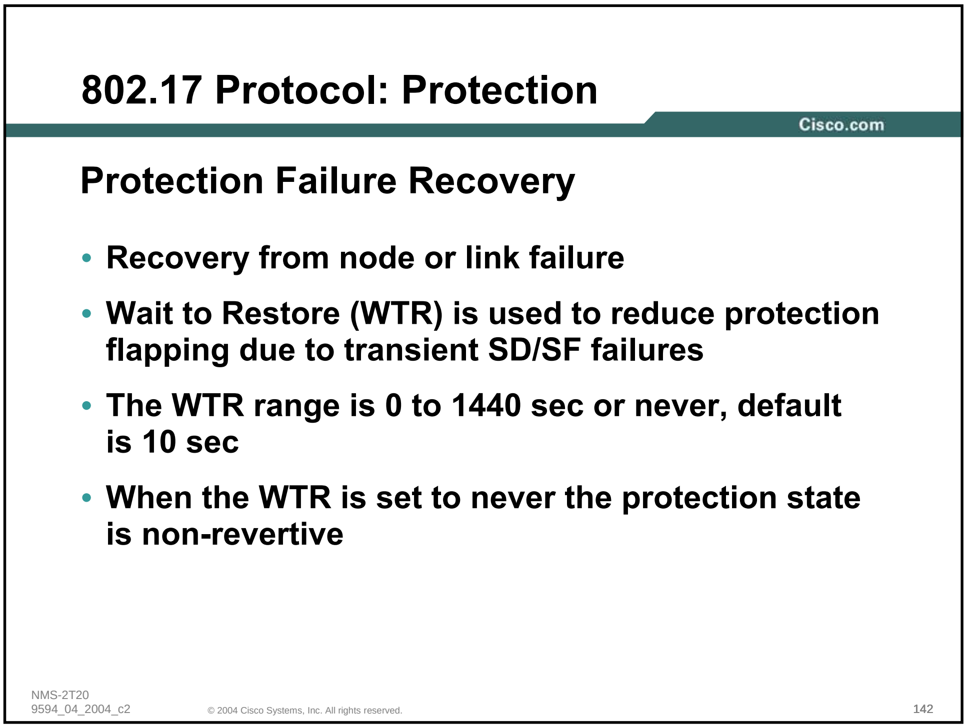
- Less than 50msec restoration if there is fiber/ node failure or signal degrade
- Two protection methods: Wrapping OR Steering around failure
- No reserved protection bandwidth unlike SONET APS
- Protection mechanism works with SONET/ SDH, Dark Fiber
- Does not depend on layer 3 routing protocol for convergence



802.17 Protocol: Protection

Protection Failure Detection

- Automatic
  - SF: Signal Fail based on PHY-sensed link failure or keepalive failure
  - SD: Signal Degrade based on PHY-sensed link degradation condition
- Manual
  - FS: Forced Switch initiated by the user
  - MS: Manual Switch initiated by the user
- Detection delay
  - L1 Holdoff: Used to delay the protection response to a PHY-sensed failure (0 to 200 ms)
  - Keepalive Timer: Used to determine the duration of keepalive loss before a protection condition is raised (2 to 200 ms); keepalive frames are also fairness updates and are transmitted approx. every 100 ms



802.17 Protocol: Protection

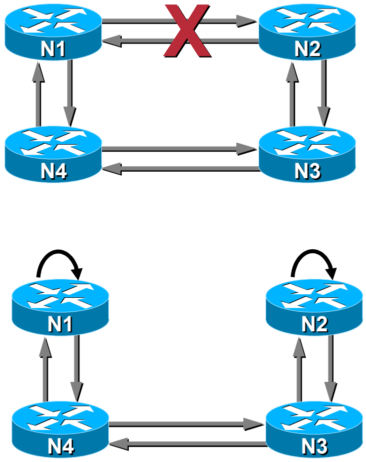
Protection Failure Recovery

- Recovery from node or link failure
- Wait to Restore (WTR) is used to reduce protection flapping due to transient SD/SF failures
- The WTR range is 0 to 1440 sec or never, default is 10 sec
- When the WTR is set to never the protection state is non-revertive

RPR Protection Switching: Protection Wrapping

- Neighbor nodes direct packets away from failure
- Requires only two nodes adjacent to the failure to take action
- Other nodes send traffic as normal

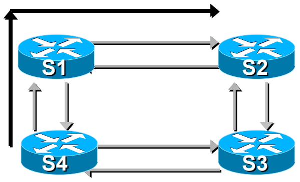
Fiber Cut/Signal Fail, etc.



802.17 Protocol: Protection

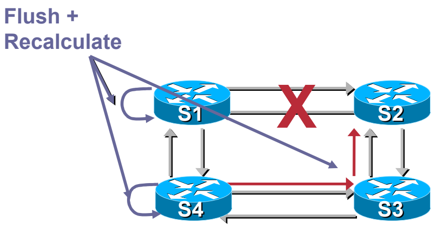
Protection Steering

- This protection mechanism requires all stations to exchange protection details, flush the existing queues (for strict traffic) and recalculate the new traffic path prior to completing the protection event



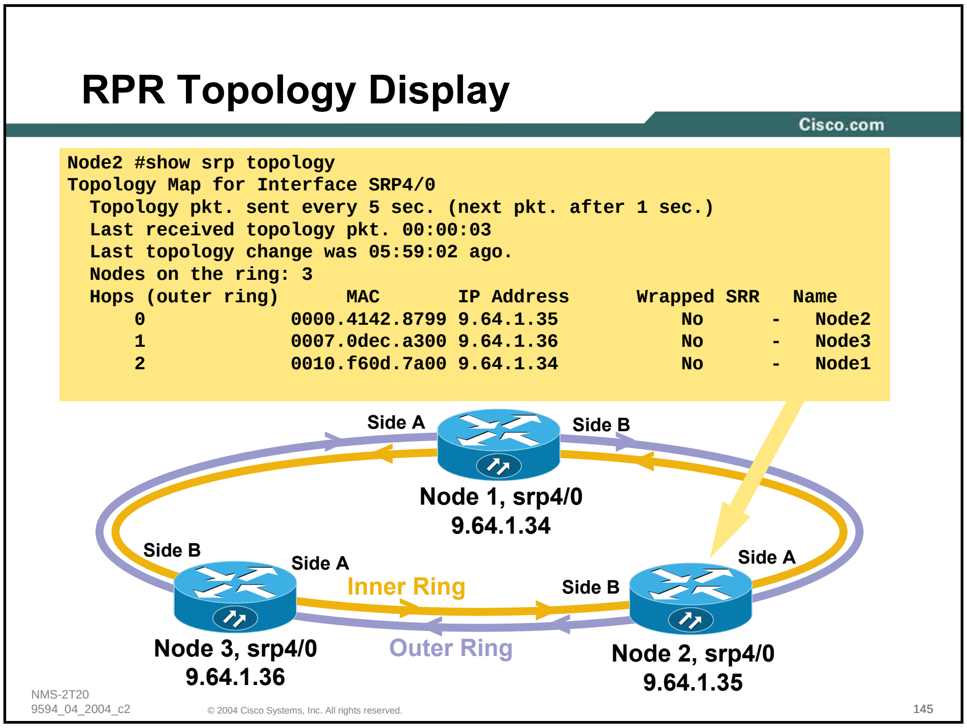
Normal Data Flow

S4–S1–S2 (Strip)



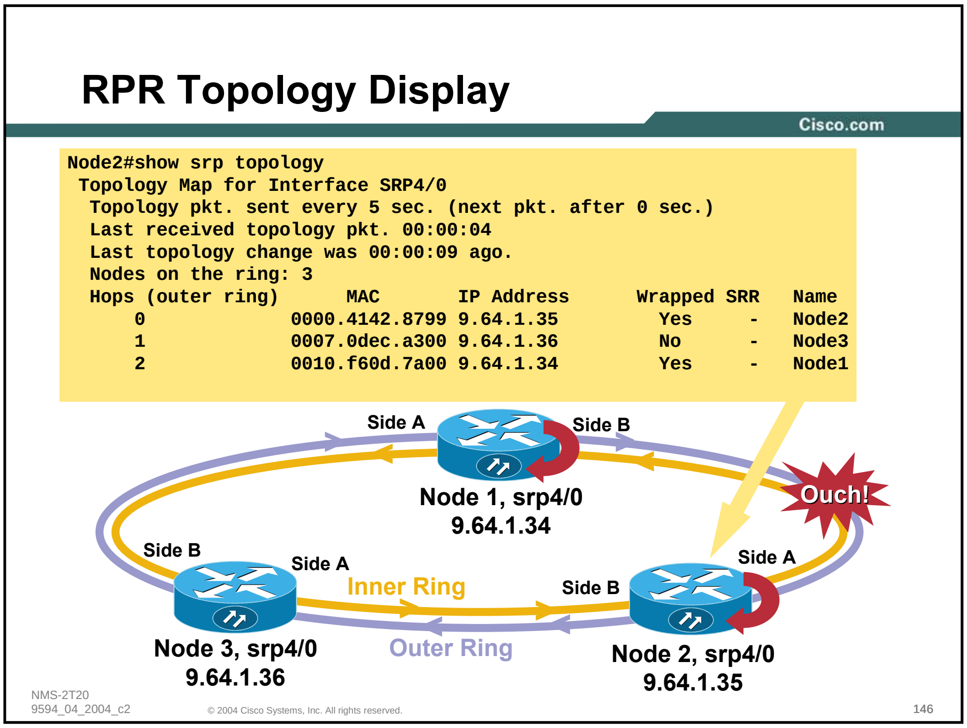
Steering Protection Data Flow

S4–3–S2 (Strip)



RPR Topology Display

```
Node2 #show srp topology
Topology Map for Interface SRP4/0
  Topology pkt. sent every 5 sec. (next pkt. after 1 sec.)
  Last received topology pkt. 00:00:03
  Last topology change was 05:59:02 ago.
  Nodes on the ring: 3
  Hops (outer ring)      MAC       IP Address      Wrapped SRR   Name
      0             0000.4142.8799 9.64.1.35          No      -   Node2
      1             0007.0dec.a300 9.64.1.36          No      -   Node3
      2             0010.f60d.7a00 9.64.1.34          No      -   Node1
```



RPR Topology Display

```
Node2#show srp topology
 Topology Map for Interface SRP4/0
  Topology pkt. sent every 5 sec. (next pkt. after 0 sec.)
  Last received topology pkt. 00:00:04
  Last topology change was 00:00:09 ago.
  Nodes on the ring: 3
  Hops (outer ring)      MAC       IP Address      Wrapped SRR   Name
      0             0000.4142.8799 9.64.1.35        Yes     -   Node2
      1             0007.0dec.a300 9.64.1.36        No      -   Node3
      2             0010.f60d.7a00 9.64.1.34        Yes     -   Node1
```

LAYER 2 HIGH AVAILABILITY

SONET/SDH

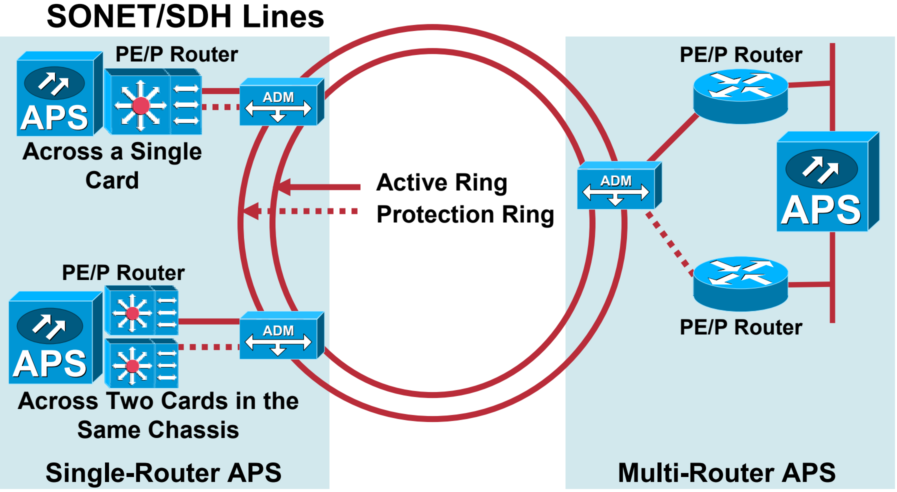
SONET/SDH

- Provides protection scheme for physical-layer restoration
- Restoration of failure within 50ms
- Physical state is communicated to L3
- Available on SONET/SDH line cards on routers
- K1/K2 link-layer control information of line overhead (LOH) frame
- Two types of APS
    - Single router APS
    - Multi-router APS

APS: Automatic Protection Switching

Cisco.com

Provides Automatic Failover Protection for SONET/SDH Lines



Single-Router APS

Cisco.com

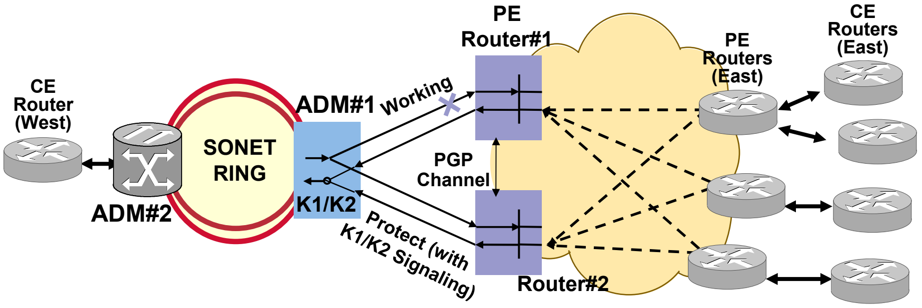
- Protects against fiber failures and linecard failures, but not whole router failures
- Switchovers are hidden from applications at upper levels
- On routers, it allows switchovers without causing a slow layer 3 reconvergence
- Conforms to Telcordia GR-253 for SONET and ITU G.841 for SDH
- The standards call for switchovers within 50msec after detecting the failure

Multi-Router APS

- The major benefit of multi-router APS is protection against fiber faults, linecard faults and even complete router failures
- Usually the working port is configured on one router and the protect port is configured on a different router
- Supported on Cisco high-end routing platforms
- Multi-Router APS is a hybrid which depends partially on APS switching and partially on layer 3 routing to direct the flow of packets
- The two routers communicate control information using protect group protocol

---

Anatomy of an MR-APS Switchover Due to LOS Detected by the Working Router



1. Initially packets are routed over the working lines which are active
2. PE Router#1 detects LOS on received Working line and starts to bring the interface down
3. Working router sends a PGP “State Change” message to the protect router
4. Protect router signals Switch-to-protect request to ADM using K1/K2 bytes
5. ADM selects the protect line and sends K1/K2 response back to protect router
6. Router selects protect line and sends PGP “Working Disable” message to working router
7. Working router deselects the working line
8. After the routers reconverge, packets get routed over the newly active protect lines

Protect Group Protocol

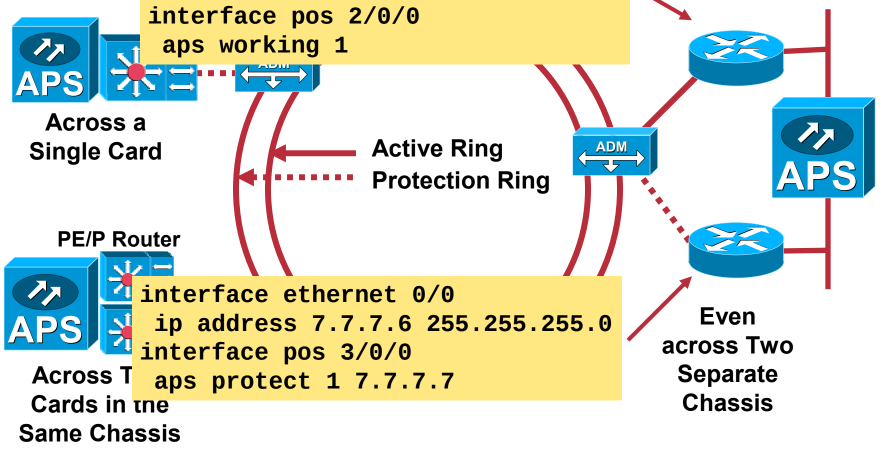
- Protect Group Protocol: Proprietary protocol sent as UDP packets (Port 172) between routers with MR-APS
- Messages are retransmitted if no reply or Ack
- PGP Hellos are sent at regular intervals
- Authenticated by a configurable authentication string sent with messages
- Supports protocol versioning
- Switching may occur due to

  LC/router crash, signal degradation, LOS (SF), manual switch

---

APS: Automatic Protection Switching

Provid n for
SONE



```
interface ethernet 0/0
 ip address 7.7.7.7 255.255.255.0
interface pos 2/0/0
 aps working 1
```

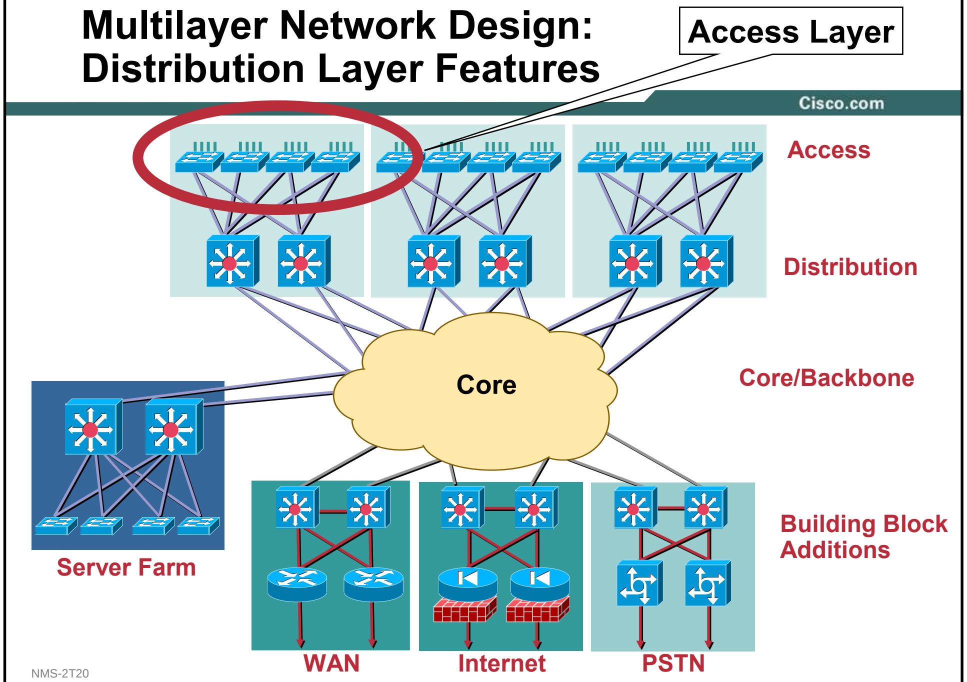
```
interface ethernet 0/0
 ip address 7.7.7.6 255.255.255.0
interface pos 3/0/0
 aps protect 1 7.7.7.7
```

LAYER 3 HIGH AVAILABILITY: ACCESS

High Availability Tool Kit

Application Level Resiliency	Global Server Load Balancing, Stateful NAT, Stateful IPSec, DNS, DHCP, Cisco Server Load Balancing, IP QoS
Protocol Level Resiliency	HSRP, VRRP, GLBP, MPLS-TE, IP Event Dampening , Graceful Restart (GR) in BGP, OSPF NSF, ISIS NSF, IP QoS
Transport/Link Level Resiliency	SONET APS, RPR, DWDM, EtherChannel, Spanning Tree Protocol, LFI, L2 QoS
Device Level Resiliency	Redundant Processors (RP), Switch Fabric, Line Cards, Ports, Power, NSF/SSO

Multilayer Network Design: Distribution Layer Features



Access Layer

Access

Distribution

Core/Backbone

Core

Server Farm

Building Block Additions

WAN

Internet

PSTN

First Hop Redundancy Protocols

- **Hot Standby Router Protocol (HSRP)**
  - Cisco informational RFC 2281 (March 1998)
- **Virtual Router Redundancy Protocol (VRRP)**
  - IETF Standard RFC 2338 (April 1998)
- **Gateway Load Balancing Protocol (GLBP)**
  - Cisco designed, load sharing, patent pending

HSRP

Cisco.com

- A group of routers function as one virtual router by sharing ONE virtual IP address and ONE virtual MAC address
- One (Active) router performs packet forwarding for local hosts
- The rest of the routers provide "hot standby" in case the active router fails
- Standby routers stay idle as far as packet forwarding from the client side is concerned

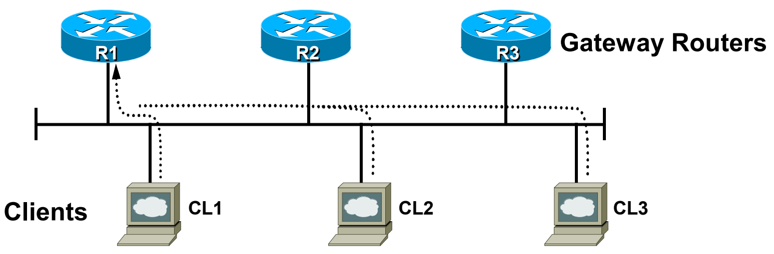
---

First Hop Redundancy with HSRP

Cisco.com

R1: Active, Forwarding Traffic; R2, R3: Hot Standby, Idle

	HSRP ACTIVE	HSRP STANDBY	HSRP LISTEN
IP:	10.0.0.254	10.0.0.253	10.0.0.252
MAC:	0000.0c12.3456	0000.0C78.9abc	0000.0cde.f123
vIP:	10.0.0.10		
vMAC:	0000.0c07ac00		



IP:	10.0.0.1	IP:	10.0.0.2	IP:	10.0.0.3
MAC:	aaaa.aaaa.aa01	MAC:	aaaa.aaaa.aa02	MAC:	aaaa.aaaa.aa03
GW:	10.0.0.10	GW:	10.0.0.10	GW:	10.0.0.10
ARP:	0000.0c07.ac00	ARP:	0000.0c07.ac00	ARP:	0000.0c07.ac00

VRRP

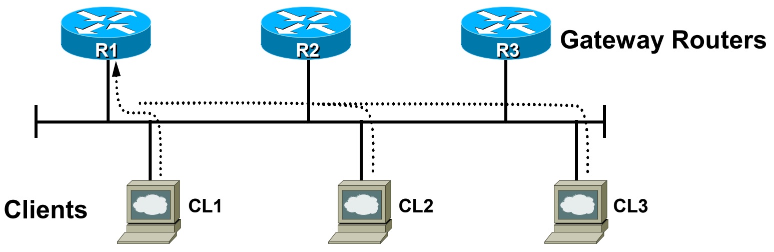
- Very similar to HSRP
- A group of routers function as one virtual router by sharing ONE virtual IP address and ONE virtual MAC address
- One (master) router performs packet forwarding for local hosts
- The rest of the routers act as “back up” in case the master router fails
- Backup routers stay idle as far as packet forwarding from the client side is concerned

---

First Hop Redundancy with VRRP

R1: Master, Forwarding Traffic; R2, R3: Backup

VRRP ACTIVE	VRRP BACKUP	VRRP BACKUP
IP: 10.0.0.254	IP: 10.0.0.253	IP: 10.0.0.252
MAC: 0000.0c12.3456	MAC: 0000.0C78.9abc	MAC: 0000.0cde.f123
vIP: 10.0.0.10	vIP:	vIP:
vMAC: 0000.5e00.0100	vMAC:	vMAC:

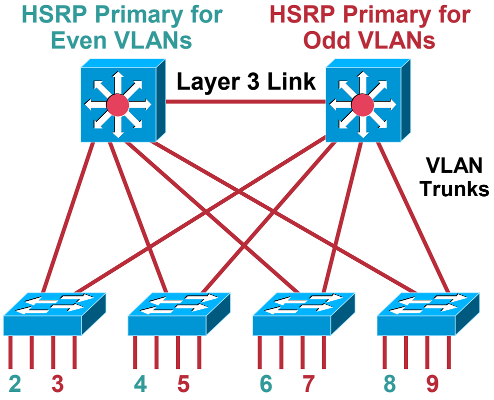


IP: 10.0.0.1	IP: 10.0.0.2	IP: 10.0.0.3
MAC: aaaa.aaaa.aa01	MAC: aaaa.aaaa.aa02	MAC: aaaa.aaaa.aa03
GW: 10.0.0.10	GW: 10.0.0.10	GW: 10.0.0.10
ARP: 0000.5e00.0100	ARP: 0000.5e00.0100	ARP: 0000.5e00.0100

Access Layer: Layer 3 Mode Load Sharing

Cisco.com

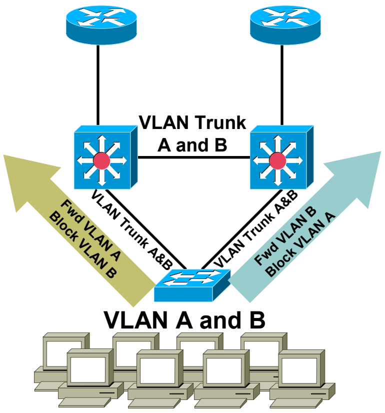
- **NOT dependent on Spanning Tree Protocol**
- **May use multiple VLANs for load sharing with Multi-group HSRP**
- **No need for Layer 2 trunk between switches**
- **Layer 3 link instead if summarizing routes**



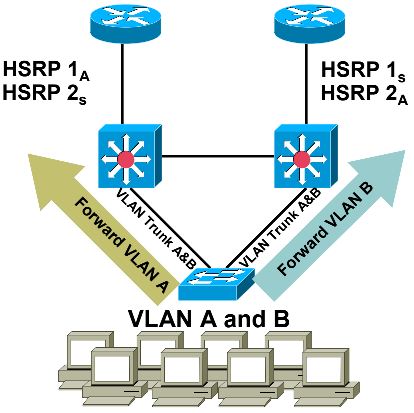
Multi-VLAN Load Balancing Methods

Cisco.com

Layer 2 Mode Load Balancing



Layer 3 Mode Load Balancing



LAYER 3 HA: ACCESS

GATEWAY LOAD BALANCING PROTOCOL

GLBP Problem Statement

- **Allow dynamic selection of multiple available gateways to destination within a subnet**
- **Provide automatic detection and re-routing to any gateway in the event of a failure**

Fully Utilize Resources (Available Bandwidth)
without Administrative Burden

GLBP Entities (Definitions)

Cisco.com

- GLBP Group

  A GLBP group consists of one or more GLBP gateways configured with the same GLBP group number

- GLBP Gateway

  A gateway or router running the Gateway Load Balancing Protocol; it may participate in one or more GLBP groups

- Virtual IP Address (vIP)

  An IPv4 address or IPv6 prefix; this is the IP address used as the hosts' default gateway

- Virtual MAC Address

  A MAC address that a host may receive when it issues an address resolution request for the virtual IP address; there MAY be multiple virtual MAC address for each GLBP group

GLBP Entities (Definitions) (Cont.)

Cisco.com

- Active Virtual Gateway (AVG)

  One Virtual Gateway in a GLBP group is elected Active Virtual Gateway (AVG), and is responsible for operation of the protocol, i.e. allocating MAC addresses

- Active Virtual Forwarder (AVF)

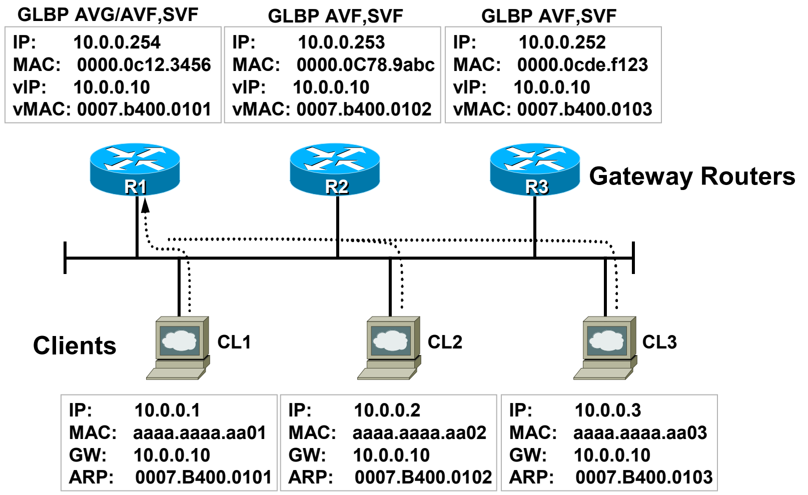
  One Virtual Forwarder in a GLBP group elected the Active Virtual Forwarder (AVF), and is responsible for forwarding packets sent to a particular virtual MAC address; there may be multiple Active Virtual Forwarders in a GLBP group

- Secondary Virtual Forwarder (SVF)

  A Virtual Forwarder that has learned the virtual MAC address from a Hello message

First Hop Redundancy with GLBP

R1: AVG; R1, R2, R3 All Forward Traffic



GLBP AVG/AVF,SVF
IP: 10.0.0.254
MAC: 0000.0c12.3456
vIP: 10.0.0.10
vMAC: 0007.b400.0101

GLBP AVF,SVF
IP: 10.0.0.253
MAC: 0000.0C78.9abc
vIP: 10.0.0.10
vMAC: 0007.b400.0102

GLBP AVF,SVF
IP: 10.0.0.252
MAC: 0000.0cde.f123
vIP: 10.0.0.10
vMAC: 0007.b400.0103

IP: 10.0.0.1
MAC: aaaa.aaaa.aa01
GW: 10.0.0.10
ARP: 0007.B400.0101

IP: 10.0.0.2
MAC: aaaa.aaaa.aa02
GW: 10.0.0.10
ARP: 0007.B400.0102

IP: 10.0.0.3
MAC: aaaa.aaaa.aa03
GW: 10.0.0.10
ARP: 0007.B400.0103

GLBP

- GLBP routers function as one virtual router sharing one virtual IP address but using multiple virtual MAC addresses to forward traffic

  GLBP uses multicast to communicate between GLBP members with following detail: 224.0.0.102, UDP port 3222

  Virtual MAC addresses will be of the form: 0007.b4yy.yyyy

    where yy.yyyy equals the lower 24 bits;

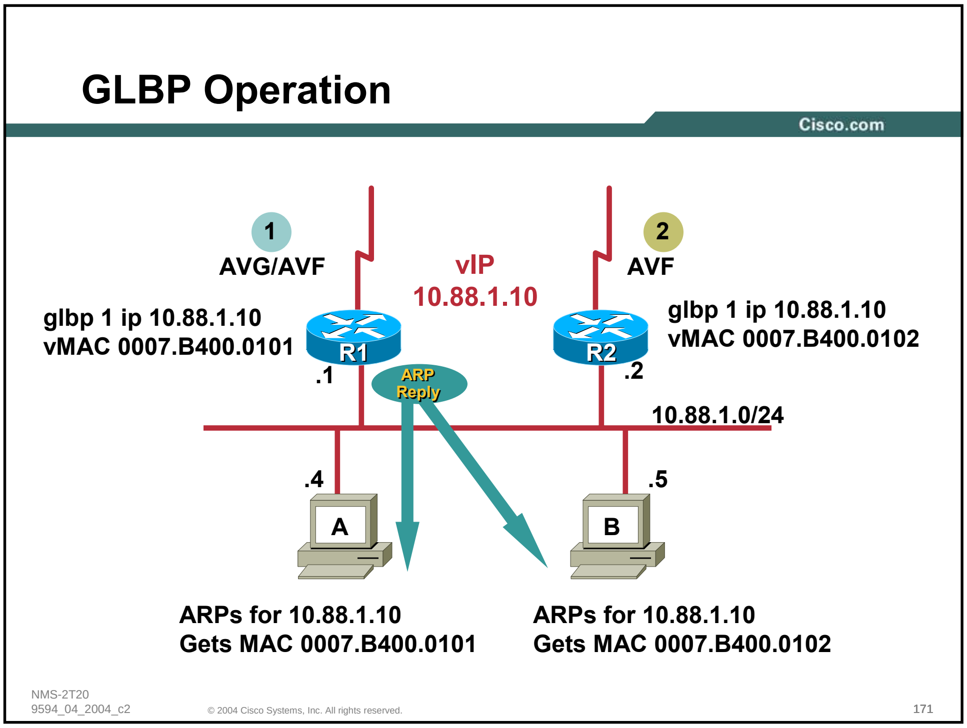
    these bits consist of 6 zero bits,

    10 bits that correspond to the GLBP group number,

    and 8 bits that correspond to the virtual forwarder number

    0007.b400.0102 : last 24 bits = 0000 0000 0000 0001 0000 0010 = GLBP group 1, forwarder 2

- Allows traffic from a single common subnet to go through multiple redundant gateways using a single virtual IP address



GLBP Operation

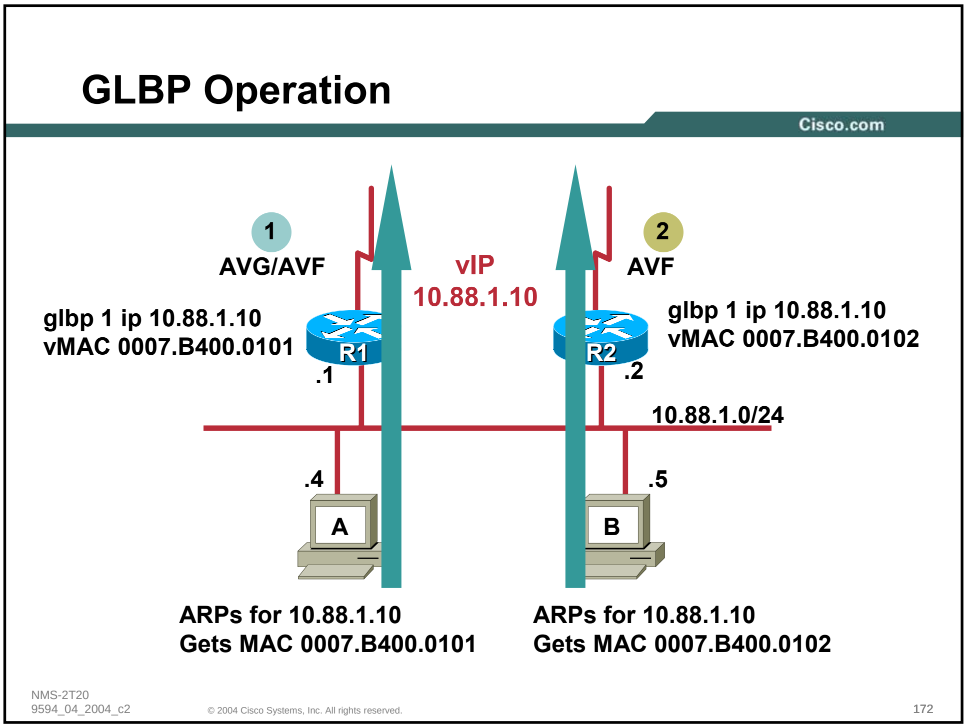
Cisco.com

glbp 1 ip 10.88.1.10
vMAC 0007.B400.0101

glbp 1 ip 10.88.1.10
vMAC 0007.B400.0102

ARPs for 10.88.1.10
Gets MAC 0007.B400.0101

ARPs for 10.88.1.10
Gets MAC 0007.B400.0102



GLBP Operation

Cisco.com

glbp 1 ip 10.88.1.10
vMAC 0007.B400.0101

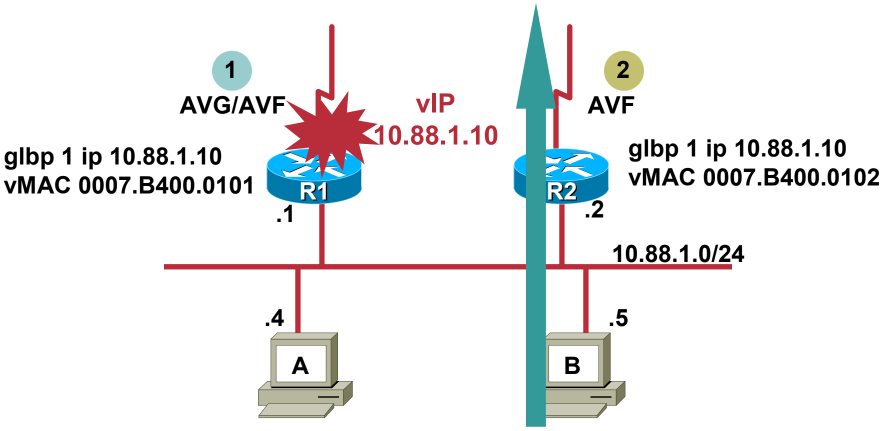
glbp 1 ip 10.88.1.10
vMAC 0007.B400.0102

ARPs for 10.88.1.10
Gets MAC 0007.B400.0101

ARPs for 10.88.1.10
Gets MAC 0007.B400.0102

GLBP Operation

Cisco.com

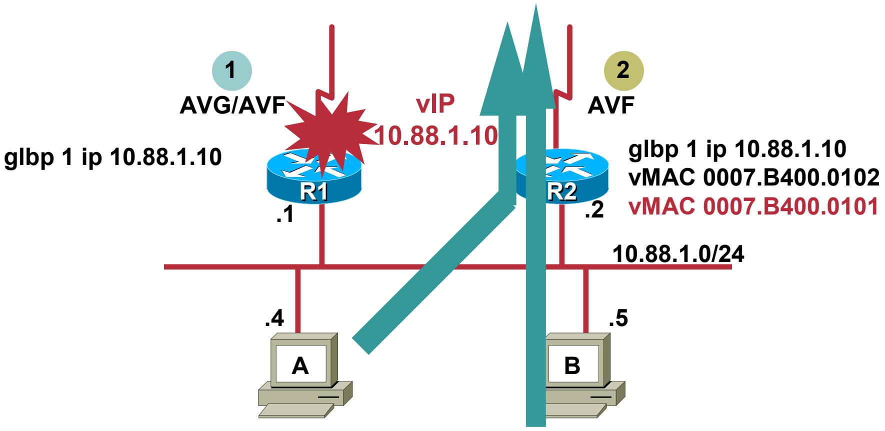


ARPs for 10.88.1.10
Gets MAC 0007.B400.0101

ARPs for 10.88.1.10
Gets MAC 0007.B400.0102

GLBP Operation

Cisco.com

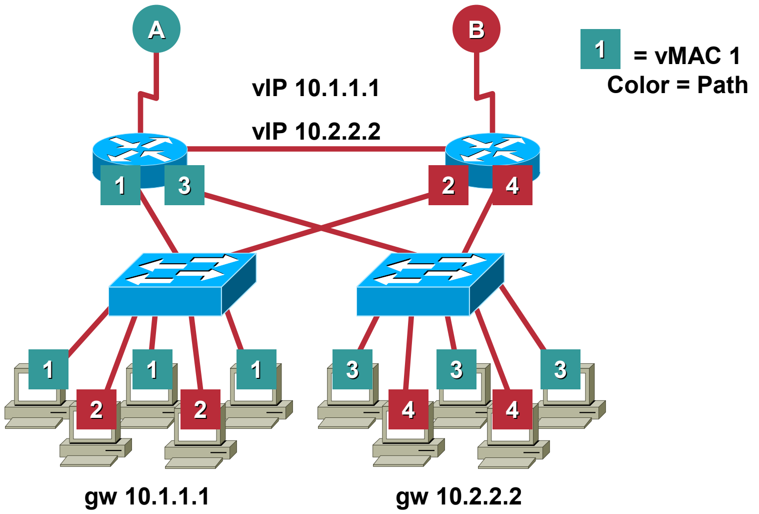


ARPs for 10.88.1.10
Gets MAC 0007.B400.0101

ARPs for 10.88.1.10
Gets MAC 0007.B400.0102

GLBP Operation

Cisco.com



GLBP Configuration Example

Cisco.com

```
!
interface FastEthernet2/0
 ip address 10.88.49.1 255.255.255.0
 duplex full
 glbp 1 ip 10.88.49.10
 glbp 1 priority 105
 glbp 1 authentication text magicword
 glbp 1 weighting 100 lower 95
 glbp 1 weighting track 10 decrement 10
```

GLBP Configuration Rules

Cisco.com

- Load balancing operates on a per-host basis
  - All outbound traffic for a given host will use the same gateway
- Maximum of 4 MAC addresses per GLBP Group
- Load balancing algorithm, 3 types:
  - Round-robin
    - Each virtual forwarder MAC takes turns
  - Weighted
    - Directed load determined by advertised weighting factor
  - Host-dependent
    - Ensures that each host is always given the same vMAC
- Default algorithm is round-robin

GLBP Implementation Issues

Cisco.com

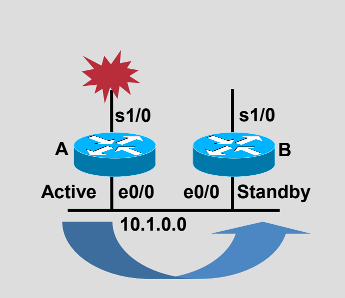
- Four entries per GLBP group will be used in the MAC address filter of Ethernet interfaces configured with GLBP groups
  - This may limit the number of groups configurable on an interface that supports only a hardware MAC address filter
- Security includes MD5 authentication
- Only use GLBP for layer 2 switched environments
  - So duplicate IP addresses will not be noticed
- Be careful with other IP services
  - NAT, IPSec, Mobile IP, HA

LAYER 3 HA: ACCESS

ENHANCED OBJECT TRACKING

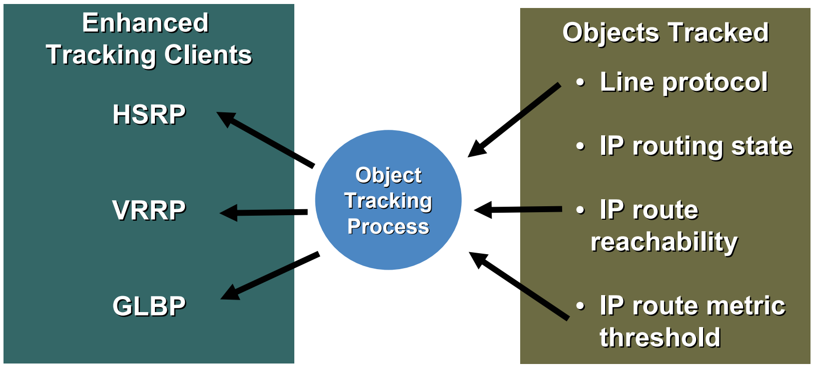
Enhanced Object Tracking

- HSRP allowed tracking of interface line protocol state
  - If the link failed, the HSRP Priority was reduced
  - Another HSRP router with a higher priority could then takeover



Enhanced Object Tracking

Cisco.com



Enhanced Tracking Clients

- HSRP
- VRRP
- GLBP

Object Tracking Process

Objects Tracked

- Line protocol
- IP routing state
- IP route reachability
- IP route metric threshold

- Enhanced Object Tracking is a stand-alone process that tracks objects
- HSRP, GLBP and VRRP act as clients seeking services of Enhanced Object Tracking

---

Benefits of Enhanced Object Tracking

Cisco.com

- More options to ensure high availability
- Can help verify end-to-end path good
- Provides scalable solution
- Support for GLBP, HSRP, and VRRP

What Can I Track?

- **Interface “line-protocol” state**

  Tracking process tracks the line-protocol state of the interface

- **Interface “routing” state**

  A tracked IP routing object is up when IP routing is enabled, the interface line-protocol is up and IP routing active on the interface

- **State of an IP route (reachability)**

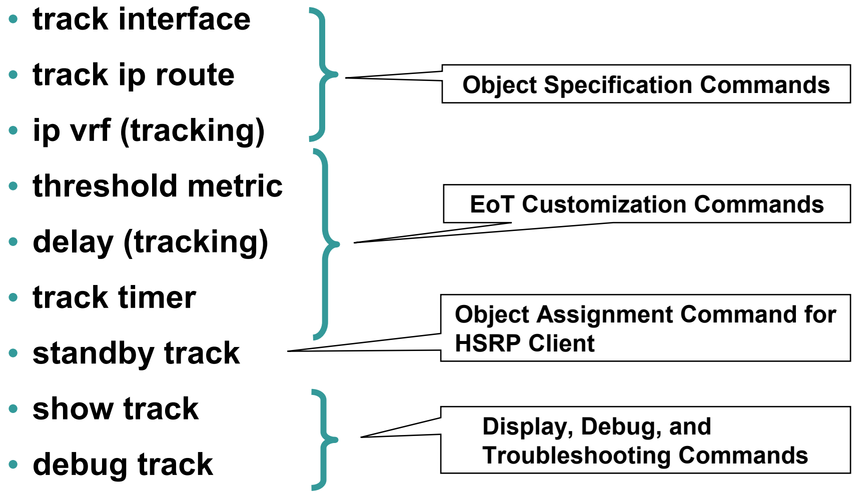
  A tracked IP route object is considered up and reachable when a routing table entry exists for the route and the route is reachable

- **IP route metric threshold**

  Tracks the scaled metric value of an IP route to determine if it is above or below a threshold

---

New CLI Commands and Options



- track interface
- track ip route
- ip vrf (tracking)
- threshold metric
- delay (tracking)
- track timer
- standby track
- show track
- debug track

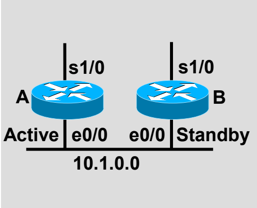
Enhanced Tracking Example
Line Protocol Tracking

```
track object-number interface type number
 {line-protocol | ip-routing}
 [up delay seconds][down delay seconds]
```

```
track 30 interface Serial3/0 line-protocol up delay 30
!
interface FastEthernet1/0
ip address 10.44.1.1 255.255.255.0
duplex full
glbp 1 ip 10.44.1.10
glbp 1 weighting 100 lower 95
glbp 1 weighting track 30
```

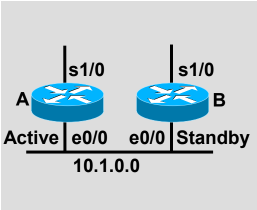
Enhanced Tracking Example
Interface IP Routing Tracking

```
Router A Configuration
track 100 interface serial1/0 ip routing
interface Ethernet0/0
  ip address 10.1.0.21 255.255.0.0
  standby 1 ip 10.1.0.1
  standby 1 priority 105
  standby 1 track 100 decrement 10
```



- Interface IP routing will go down if:
  - IP routing is disabled globally
  - Interface IP address is unknown (or IP is disabled or failed to negotiate)
  - Interface line-protocol is down
- Useful for interfaces where IP address is negotiated
  - For example, on a serial interface that uses PPP then the line-protocol could be up (LCP negotiated successfully), but IP could be down (IPCP negotiation failed)

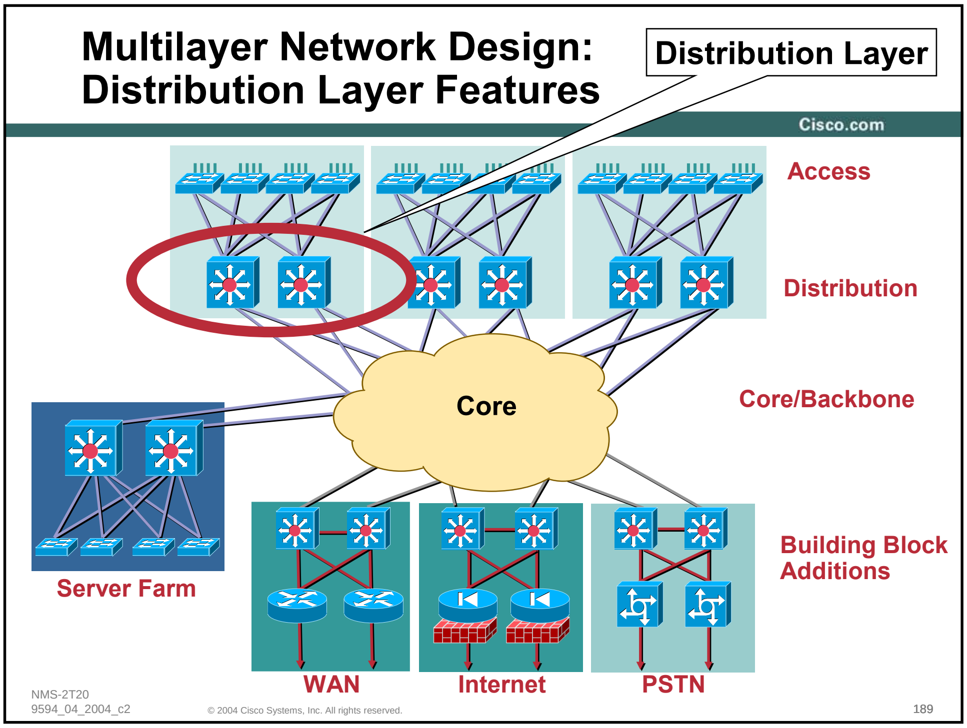
Enhanced Tracking Example
IP Route Reachability Tracking



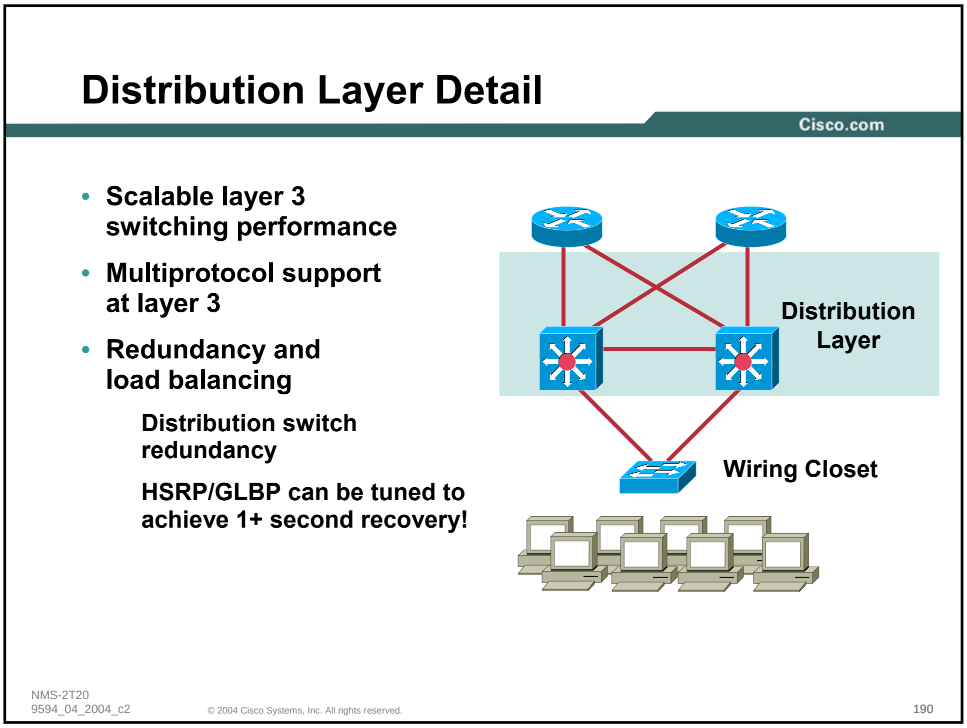
Router A Configuration:

```
track 100 interface serial1/0 ip routing
!
track 101 ip route 10.22.0.0/16 reachability
!
interface Ethernet0/0
  ip address 10.1.0.21 255.255.0.0
  standby 1 ip 10.1.0.1
  standby 1 priority 105
  standby 1 track 100 decrement 10
  standby 1 track 101 decrement 10
```

LAYER 3 HA:
DISTRIBUTION AND CORE

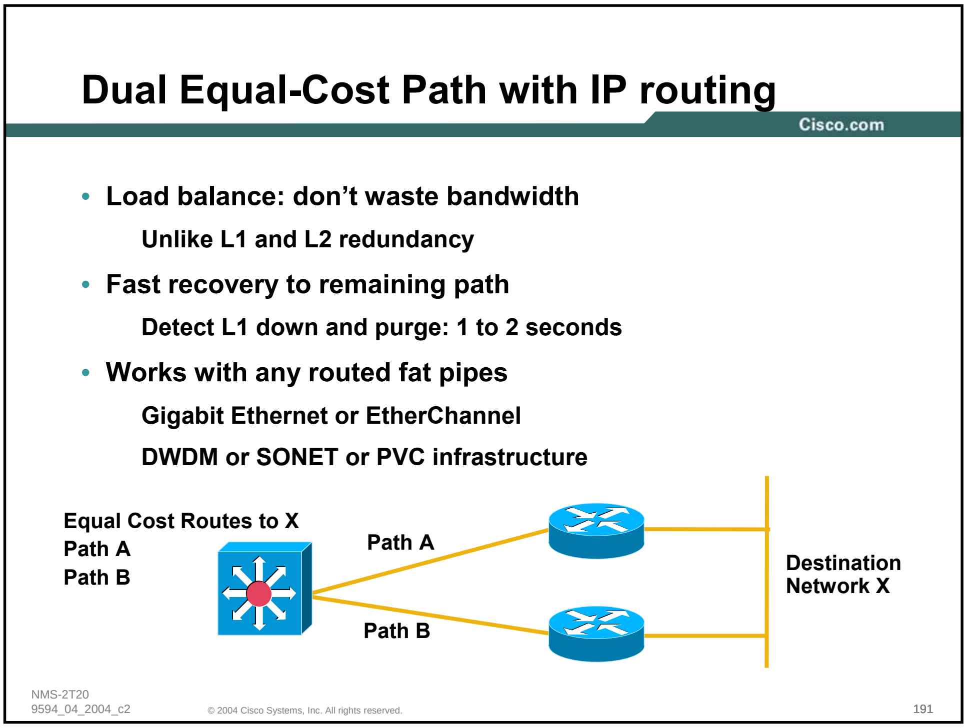


Multilayer Network Design: Distribution Layer Features



Distribution Layer Detail

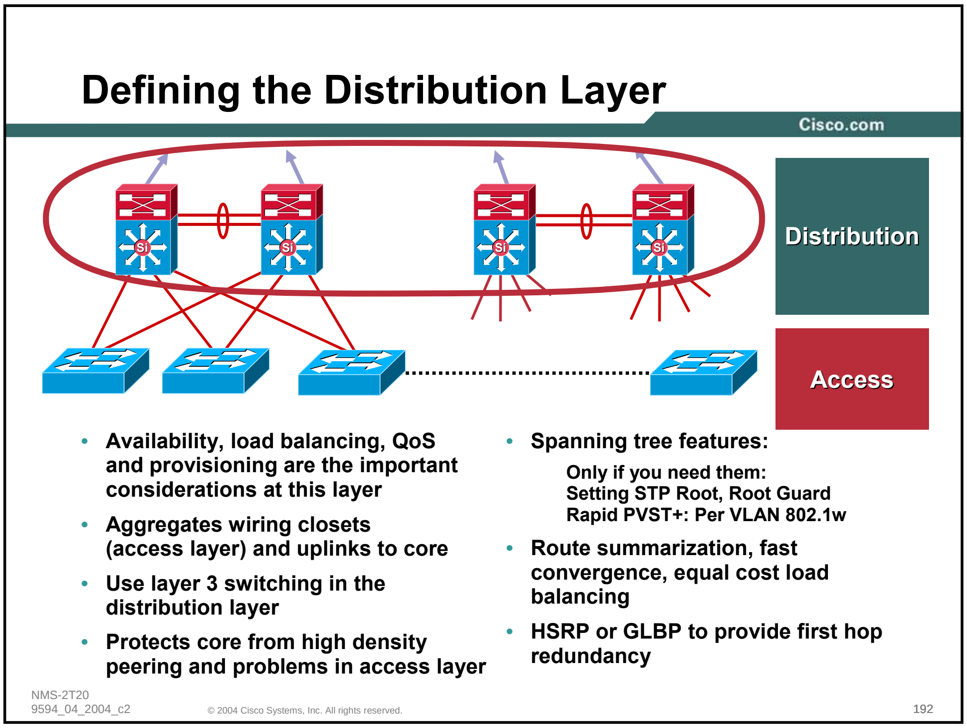
- Scalable layer 3 switching performance
- Multiprotocol support at layer 3
- Redundancy and load balancing
    - Distribution switch redundancy
    - HSRP/GLBP can be tuned to achieve 1+ second recovery!



Dual Equal-Cost Path with IP routing

Cisco.com

- Load balance: don’t waste bandwidth
  - Unlike L1 and L2 redundancy
- Fast recovery to remaining path
  - Detect L1 down and purge: 1 to 2 seconds
- Works with any routed fat pipes
  - Gigabit Ethernet or EtherChannel
  - DWDM or SONET or PVC infrastructure



Defining the Distribution Layer

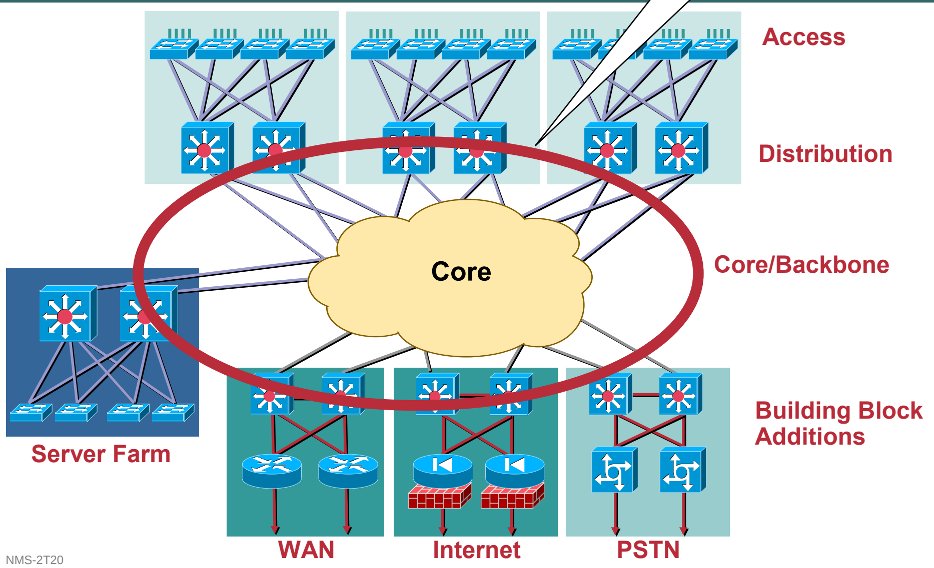
Cisco.com

- Availability, load balancing, QoS and provisioning are the important considerations at this layer
- Aggregates wiring closets (access layer) and uplinks to core
- Use layer 3 switching in the distribution layer
- Protects core from high density peering and problems in access layer
- Spanning tree features:
  - Only if you need them:
    Setting STP Root, Root Guard
    Rapid PVST+: Per VLAN 802.1w
- Route summarization, fast convergence, equal cost load balancing
- HSRP or GLBP to provide first hop redundancy

Multilayer Network Design: Core Layer Features

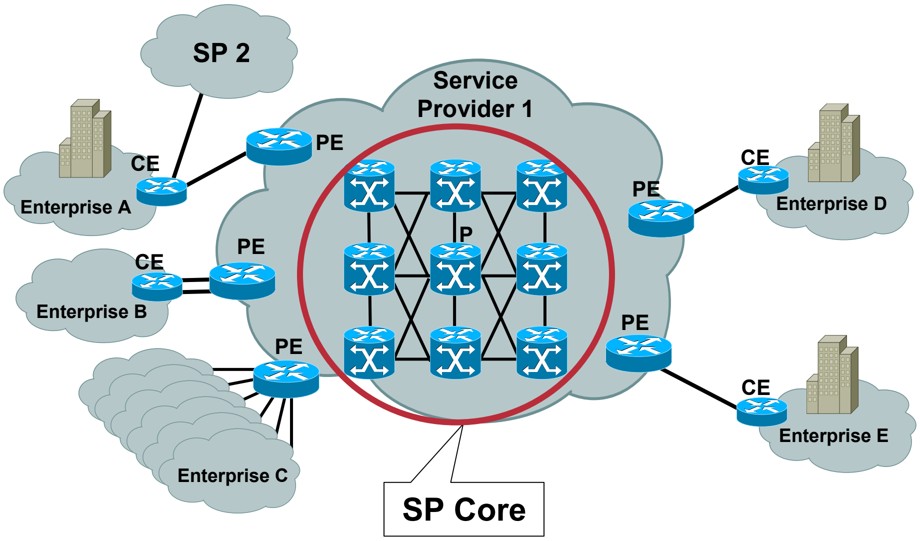
Core Layer

Cisco.com



Service Provider Network

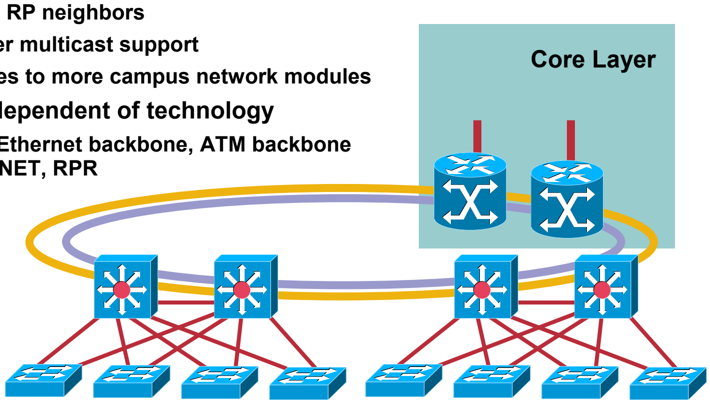
Cisco.com



SP Core

Core Layer Detail

- Redundant, fast-converging core
- Choice to be made for Layer 2 or Layer 3:
  - Layer 3 favored:
    - Less RP neighbors
    - Better multicast support
    - Scales to more campus network modules
- Design independent of technology
  - Gigabit Ethernet backbone, ATM backbone (L2), SONET, RPR



Improving Convergence Time

- Failure Detection Tuning
- IP Event Dampening
- BGP Multi-path
- MPLS Fast Re-Route (FRR)

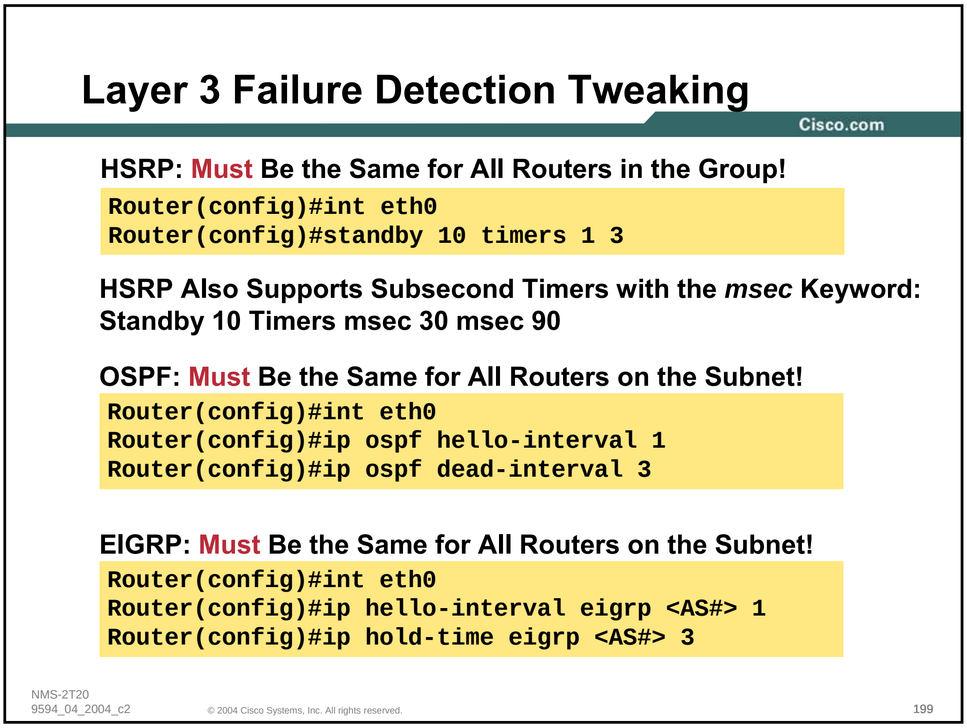
LAYER 3 HA: DISTRIBUTION AND CORE

FAILURE DETECTION AND FAILURE RECOVERY TUNING

Failure Detection Tuning

Cisco.com

- Cisco IOS® exposes some timers which can be tuned to speed failure detection/convergence
- Tweaking will not help a network that already has significant problems
- Only tweak if:
  - You have a stable, predictable network
  - You have a lab which can provide an accurate simulation
  - You have a backout plan



Layer 3 Failure Detection Tweaking

HSRP: Must Be the Same for All Routers in the Group!

```
Router(config)#int eth0
Router(config)#standby 10 timers 1 3
```

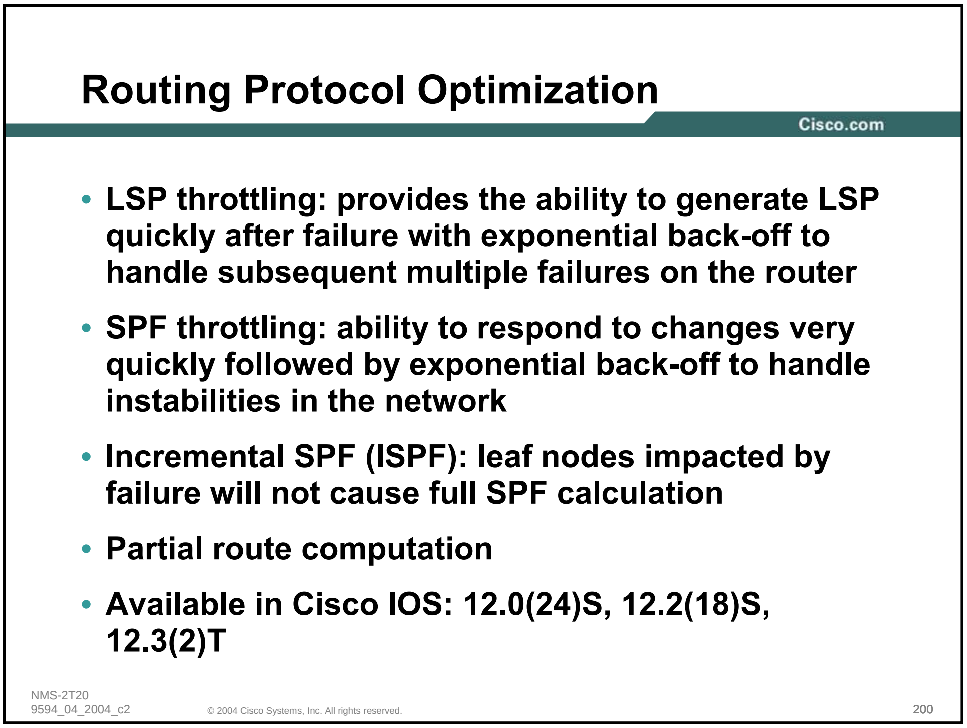
HSRP Also Supports Subsecond Timers with the *msec* Keyword: Standby 10 Timers msec 30 msec 90

OSPF: Must Be the Same for All Routers on the Subnet!

```
Router(config)#int eth0
Router(config)#ip ospf hello-interval 1
Router(config)#ip ospf dead-interval 3
```

EIGRP: Must Be the Same for All Routers on the Subnet!

```
Router(config)#int eth0
Router(config)#ip hello-interval eigrp <AS#> 1
Router(config)#ip hold-time eigrp <AS#> 3
```



Routing Protocol Optimization

- LSP throttling: provides the ability to generate LSP quickly after failure with exponential back-off to handle subsequent multiple failures on the router
- SPF throttling: ability to respond to changes very quickly followed by exponential back-off to handle instabilities in the network
- Incremental SPF (ISPF): leaf nodes impacted by failure will not cause full SPF calculation
- Partial route computation
- Available in Cisco IOS: 12.0(24)S, 12.2(18)S, 12.3(2)T

Events Triggered by Link Failure

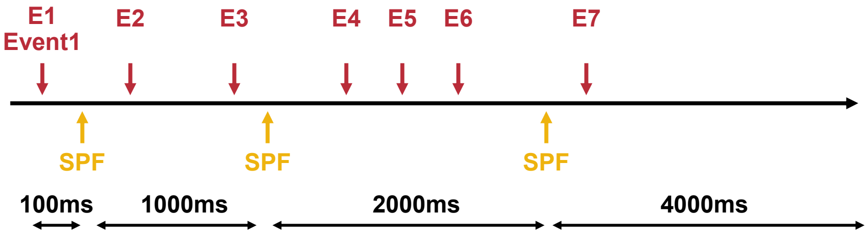
- Link fails
  - Traffic is interrupted
- Local node
  - LSP (LSA) generated by router local to failure (Time T1)
  - SPF computation at local node and re-convergence (Time T2)
- Remote node
  - Remote nodes receive LSP (LSA)
  - Remote nodes re-compute SPF and re-converge (Time T3)
- Traffic flow resumes
- Can we reduce MTTR by tuning T1, T2 and T3?

Backoff Timer Algorithm

spf-interval <Max> [<Init> <Inc>]

- **Maximum interval**: Maximum amount of time the router will wait between consecutives executions
- **Initial delay**: Time the router will wait before starting execution
- **Incremental interval**: Time the router will wait between consecutive execution; this timer is variable and will increase until it reaches maximum-interval

spf-interval 10 100 1000



E1
Event1
E2
E3
E4
E5
E6
E7

SPF
SPF
SPF

100ms
1000ms
2000ms
4000ms

>>> then 8000ms

>>> then maxed at 10sec

>>> 20s without Trigger is required
before resetting the SPF timer to 100ms

Default Values

- **Maximum-interval:**

  SPF: 10 seconds

  PRC: 5 seconds

  LSP-Generation:
  5 seconds

- **Initial-wait:**

  SPF: 5.5 seconds

  PRC: 2 seconds

  LSP-Generation:
  50 milliseconds

- **Incremental-interval:**

  SPF: 5.5 seconds

  PRC: 5 seconds

  LSP-Generation:
  5 seconds

```
router isis
  spf-interval 1 1 50

  prc-interval 1 1 50
```

Timers for Fast Convergence

Cisco.com

- The timers are designed to optimize the propagation of the information to other nodes
  - Init-Wait = 1ms, 49ms faster than default
  - Exp-Inc = 50ms

```
router isis
  lsp-gen-interval 5 1 50
```

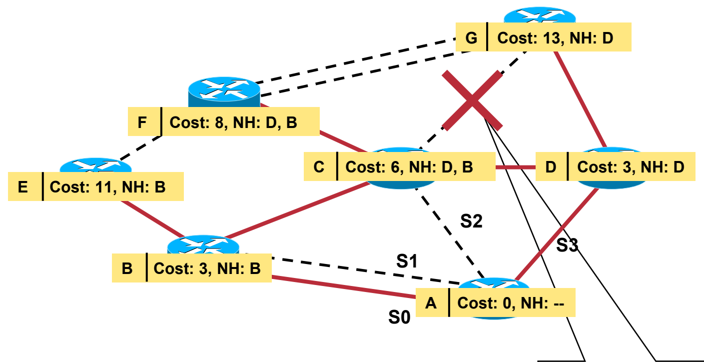
Incremental-SPF

Cisco.com

- When the topology has changed, instead of building the whole SPT from scratch just fix the part of the SPT that is affected
- Only the leaves of the nodes re-analyzed during that process are updated in the RIB

Incremental-SPF

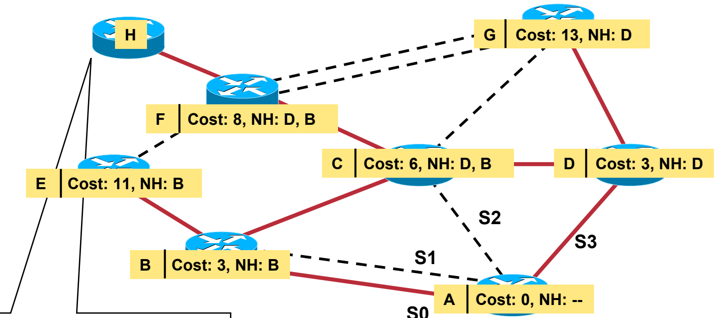
Cisco.com



C-G Link Is Down;
C-G Link Was Not Used in
SPT Anyway, Therefore,
There Is No Need to Run SPF

Incremental-SPF

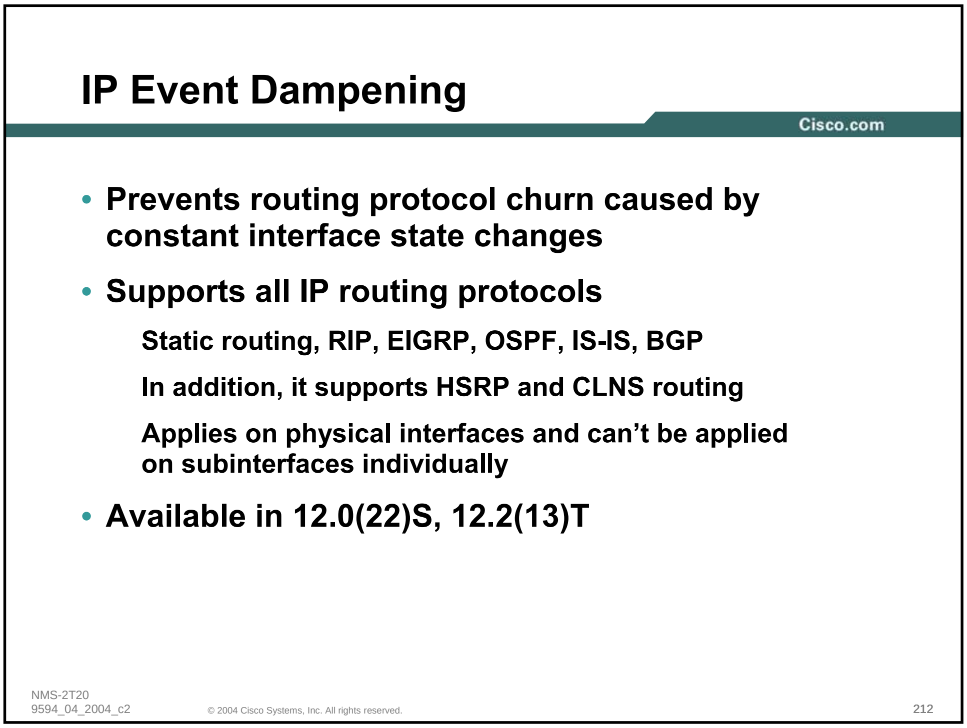
Cisco.com



F Reports a New Neighbor;
the SPT Need Only to Be
Extended behind F; There
Is No Need for Router a to
Recompute the Whole SPT
Router a Will Compute SPF
from Node F

LAYER 3 HA: DISTRIBUTION AND CORE

IP EVENT DAMPENING



IP Event Dampening

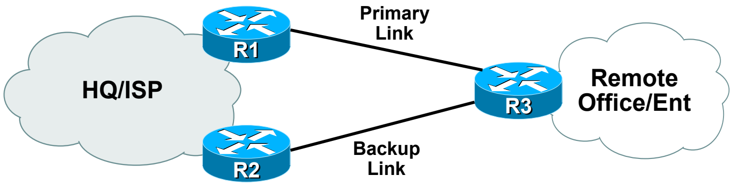
- Prevents routing protocol churn caused by constant interface state changes
- Supports all IP routing protocols
  - Static routing, RIP, EIGRP, OSPF, IS-IS, BGP
  - In addition, it supports HSRP and CLNS routing
  - Applies on physical interfaces and can’t be applied on subinterfaces individually
- Available in 12.0(22)S, 12.2(13)T

IP Event Dampening: Concept

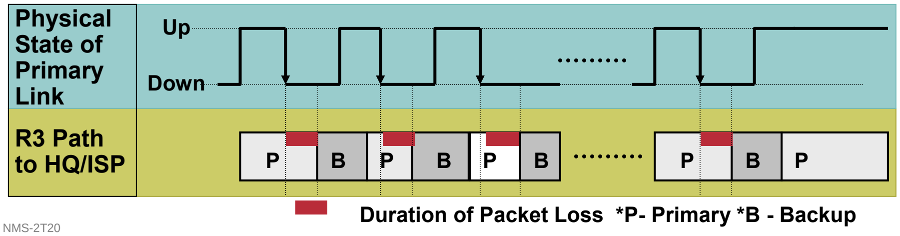
- Takes the concept of BGP route-flap dampening and applies it at the interface level, so all IP routing protocols can benefit
- Tracks interface flapping, applying a “penalty” to a flapping interface
- Puts the interface in “down” state from routing protocol perspective if the penalty is over a threshold tolerance
- Uses exponential decay algorithm to decrease the penalty over time and brings the interface back to “up” state

---

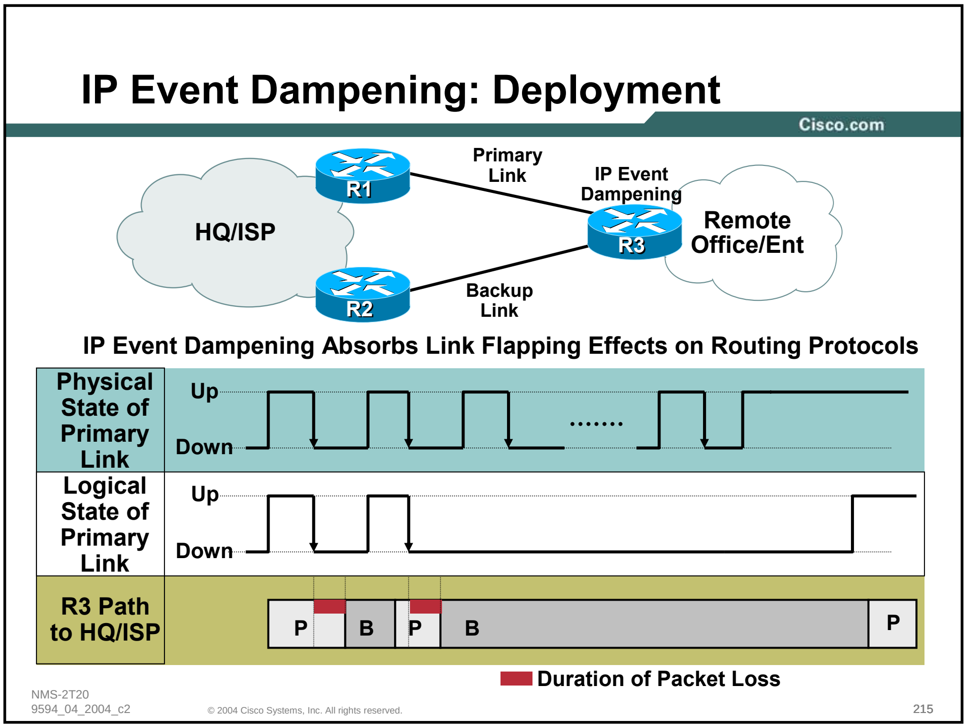
IP Event Dampening—Deployment



Link Flapping Causes Routing Reconvergence and Packet Loss



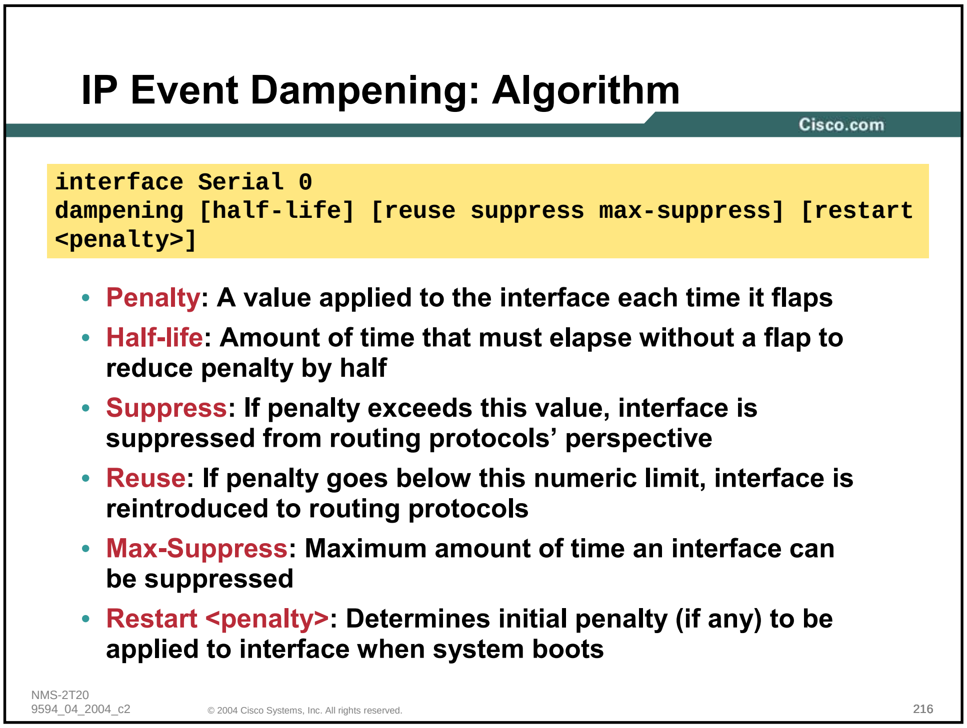
🟥 Duration of Packet Loss *P- Primary *B - Backup



IP Event Dampening: Deployment

IP Event Dampening Absorbs Link Flapping Effects on Routing Protocols

🟥 Duration of Packet Loss

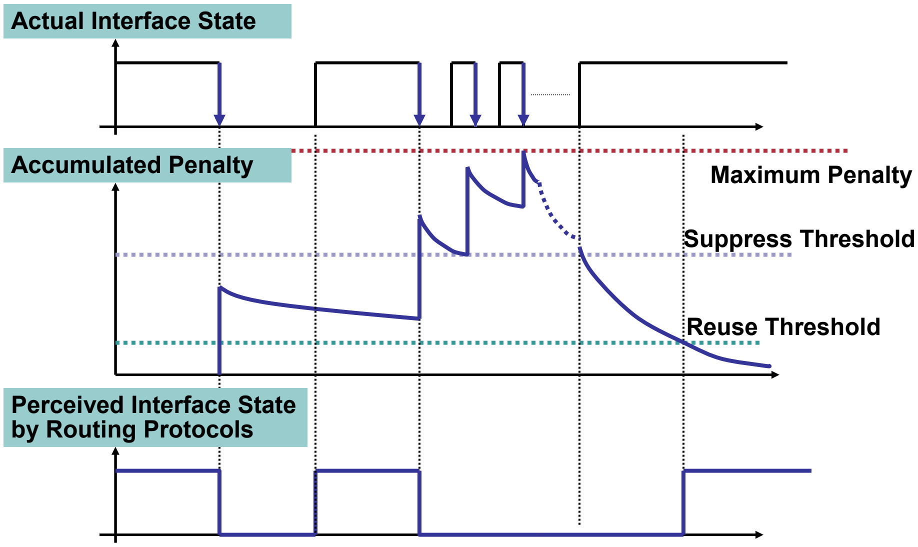


IP Event Dampening: Algorithm

```
interface Serial 0
dampening [half-life] [reuse suppress max-suppress] [restart
<penalty>]
```

- **Penalty**: A value applied to the interface each time it flaps
- **Half-life**: Amount of time that must elapse without a flap to reduce penalty by half
- **Suppress**: If penalty exceeds this value, interface is suppressed from routing protocols’ perspective
- **Reuse**: If penalty goes below this numeric limit, interface is reintroduced to routing protocols
- **Max-Suppress**: Maximum amount of time an interface can be suppressed
- **Restart <penalty>**: Determines initial penalty (if any) to be applied to interface when system boots

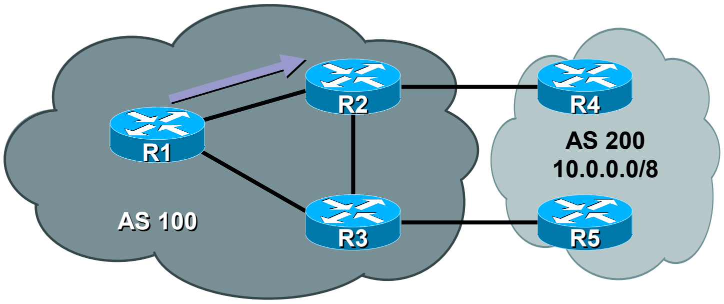
IP Event Dampening: Algorithm Illustration



LAYER 3 HA: DISTRIBUTION AND CORE

BGP MULTI-PATH

iBGP Multi-path:
BGP Behavior before iBGP Multi-path



- R1 has two paths for 10.0.0.0/8
- Both paths have identical < weight, AS-PATH, origin, localpref, MED >; ONLY next HOPS are different
- R1 selects one path as best and send all traffic for 10.0.0.0/8 towards one of the exit points
- BGP installs only the best path unlike other routing protocols!!

BGP Multi-path Review

- Allows a router to install multi-path in the RIB
- Traffic will be sent to destinations on multiple paths for load balancing and efficient link utilization
- Conditions for iBGP multipath selection

  All attributes (weight, local preference, AS-path entire attribute not just length), origin, MED, and IGP distance are same

  The next-hops of the paths are different

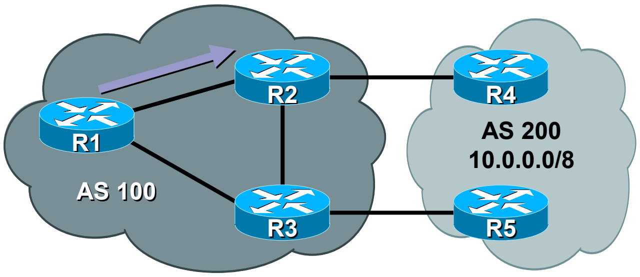
iBGP Multi-path

- Flag multiple iBGP paths as ‘multi-path’
  - Each path must have a unique NEXT_HOP
- Number of multi-paths can be controlled
  - `maximum-paths ibgp <1-6>`
- The best path as determined by the decision algorithm will be advertised to our peers
- Each BGP next-hop is resolved and mapped to available IGP paths
- Support iBGP multi-path 12.0(16.6)ST, 12.2(14)S

---

iBGP Multi-path

- R1 has two paths for 10.0.0.0/8
- Both paths are flagged as “multipath”



```
R1#sh ip bgp 10.0.0.0
  200
   20.20.20.3 from 20.20.20.3 (3.3.3.3)
   Origin IGP, metric 0, localpref 100, valid, internal, multipath
  200
   20.20.20.2 from 20.20.20.2 (2.2.2.2)
   Origin IGP, metric 0, localpref 100, valid, internal, multipath, best
```

iBGP Multi-path

```
R1#sh ip route 10.0.0.0
Routing entry for 10.0.0.0/8
  * 20.20.20.3, from 20.20.20.3, 00:00:09 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    20.20.20.2, from 20.20.20.2, 00:00:09 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1

R1#show ip cef 10.0.0.0
10.0.0.0/8, version 237, per-destination sharing
0 packets, 0 bytes
  via 20.20.20.3, 0 dependencies, recursive
    traffic share 1
    next hop 20.20.20.3, FastEthernet0/0 via 20.20.20.3/32
    valid adjacency
  via 20.20.20.2, 0 dependencies, recursive
    traffic share 1
    next hop 20.20.20.2, FastEthernet0/0 via 20.20.20.2/32
    valid adjacency
```

- These two paths are installed in the RIB/FIB
- Traffic is load-balanced across the two paths/exit points

eiBGP Multi-path for MPLS VPN Networks

- Enables PE routers to send traffic to the destination via multiple paths for load balancing

  via iBGP peer [or]

  via eBGP peer
- Applicable for MPLS VPN environment ONLY
- Improves load balancing traffic in MPLS VPN network
- Useful on PE routers that import eBGP and iBGP paths from multi-homed and stub networks
- Supported in 12.0(24)S image

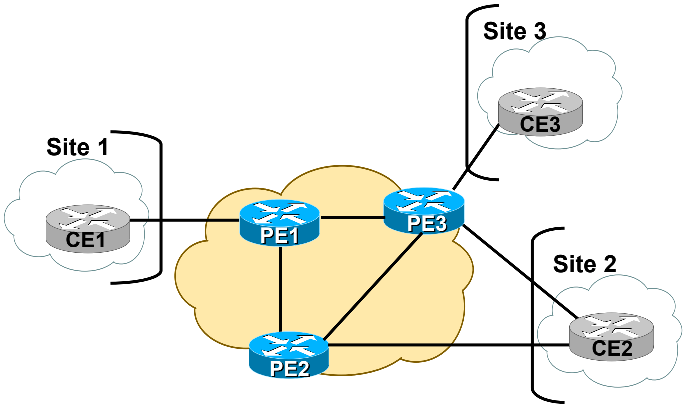
eiBGP Multi-path: Packet Flow Rules

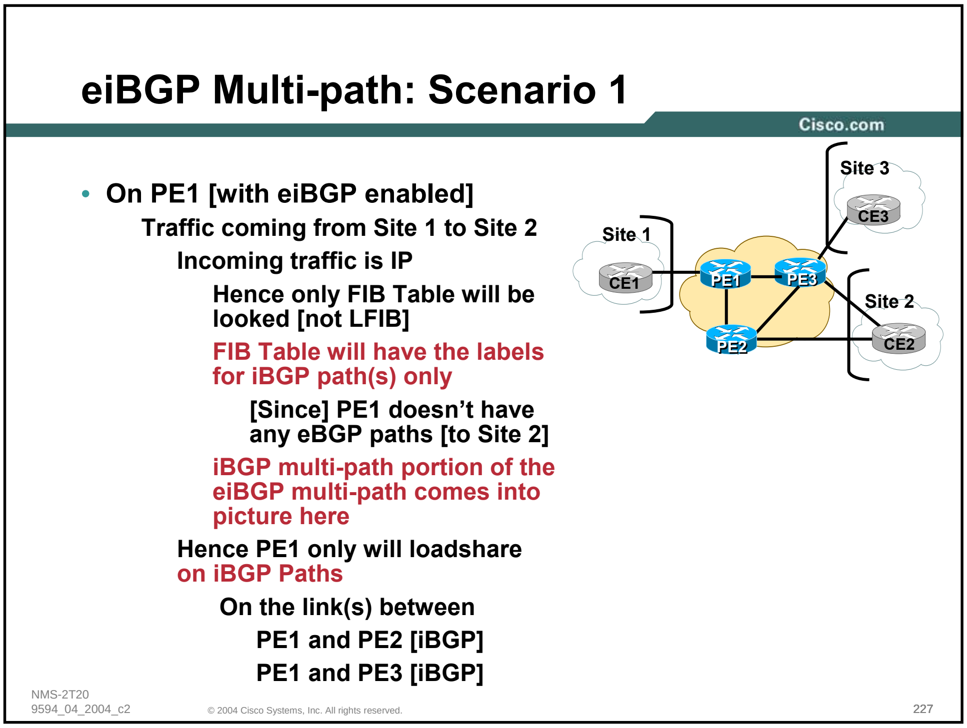
Cisco.com

- **Labeled traffic: forwarding information on eBGP paths used**
- **IP traffic: forwarding information on eBGP and iBGP paths used**

eiBGP Multipath: Deployment Scenario

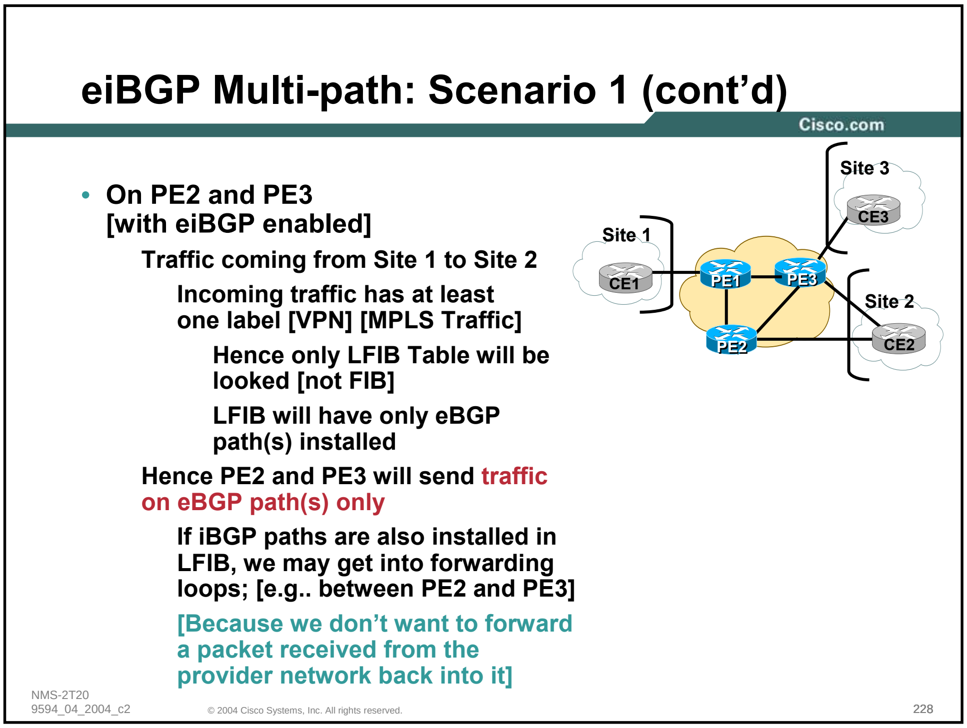
Cisco.com





eiBGP Multi-path: Scenario 1

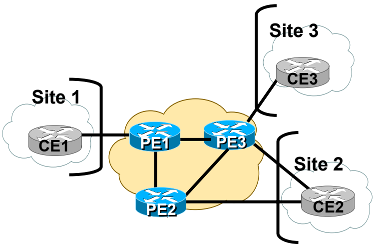
- On PE1 [with eiBGP enabled]
  - Traffic coming from Site 1 to Site 2
    - Incoming traffic is IP
      - Hence only FIB Table will be looked [not LFIB]
      - FIB Table will have the labels for iBGP path(s) only
        - [Since] PE1 doesn't have any eBGP paths [to Site 2]
      - iBGP multi-path portion of the eiBGP multi-path comes into picture here
    - Hence PE1 only will loadshare on iBGP Paths
      - On the link(s) between
        - PE1 and PE2 [iBGP]
        - PE1 and PE3 [iBGP]



eiBGP Multi-path: Scenario 1 (cont'd)

- On PE2 and PE3 [with eiBGP enabled]
  - Traffic coming from Site 1 to Site 2
    - Incoming traffic has at least one label [VPN] [MPLS Traffic]
      - Hence only LFIB Table will be looked [not FIB]
      - LFIB will have only eBGP path(s) installed
  - Hence PE2 and PE3 will send traffic on eBGP path(s) only
    - If iBGP paths are also installed in LFIB, we may get into forwarding loops; [e.g.. between PE2 and PE3]
    - [Because we don't want to forward a packet received from the provider network back into it]

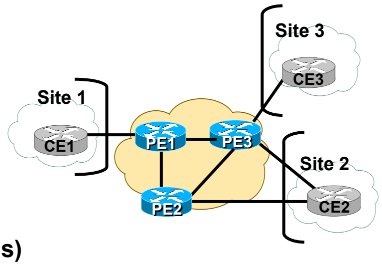
eiBGP Multi-path: Scenario 2



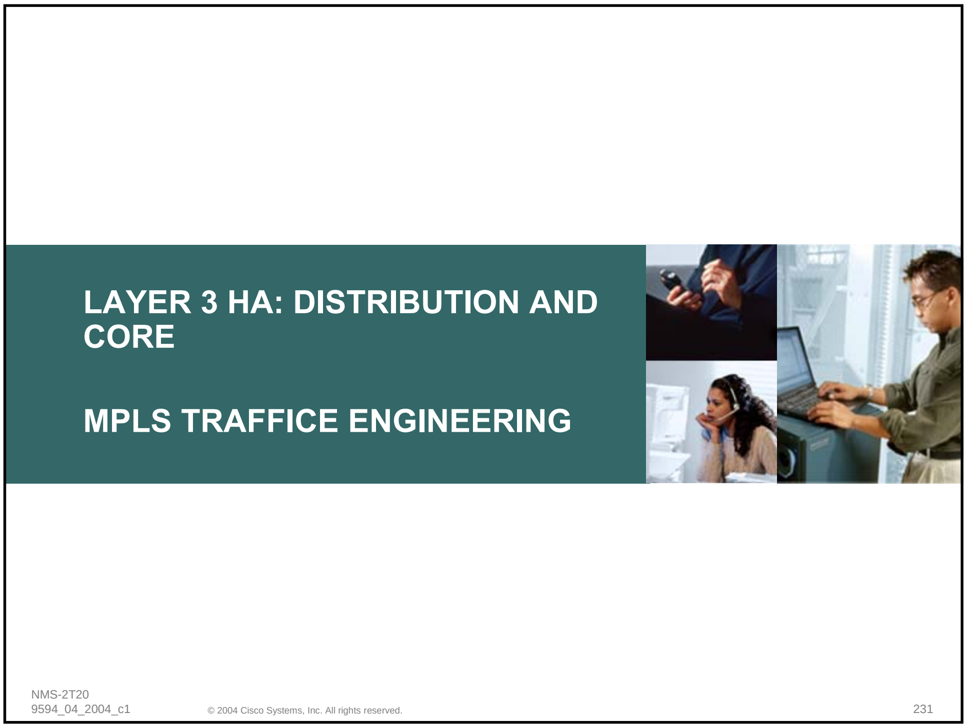
- On PE3 [with eiBGP enabled]
  - Traffic coming from Site 3 to Site 2
    - Incoming traffic is IP
      - Hence only FIB Table will be looked [not LFIB]
      - FIB Table will have the label for iBGP path(s) and IP Forwarding Information for eBGP path(s)
        - [Layer 2 Header, Output Interface]
    - Hence PE3 will send traffic on both eBGP and iBGP path(s)
      - On the link between
        - PE3 and PE2 [iBGP]
        - PE3 and CE2 [eBGP]

---

eiBGP Multi-path: Scenario 2

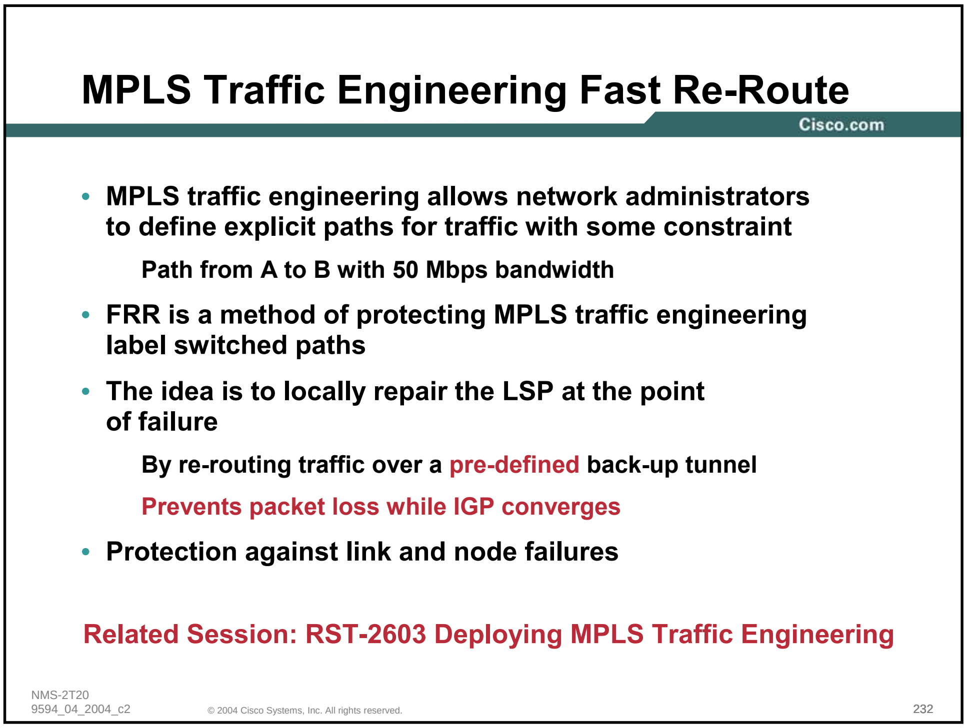


- On PE2 [with eiBGP enabled]
  - Traffic coming from Site 3 to Site 2
    - Incoming traffic has at least one label [VPN] [MPLS Traffic]
      - Hence only LFIB Table will be looked [not FIB]
      - LFIB will have only eBGP path(s) installed
    - Hence PE2 will send traffic on eBGP Path(s) only
      - If iBGP paths are also installed in LFIB, we may get into routing loops [e.g., between PE2 and PE3]
      - [Because we don't want to forward a packet received from the Provider Network back into it]



LAYER 3 HA: DISTRIBUTION AND CORE

MPLS TRAFFICE ENGINEERING

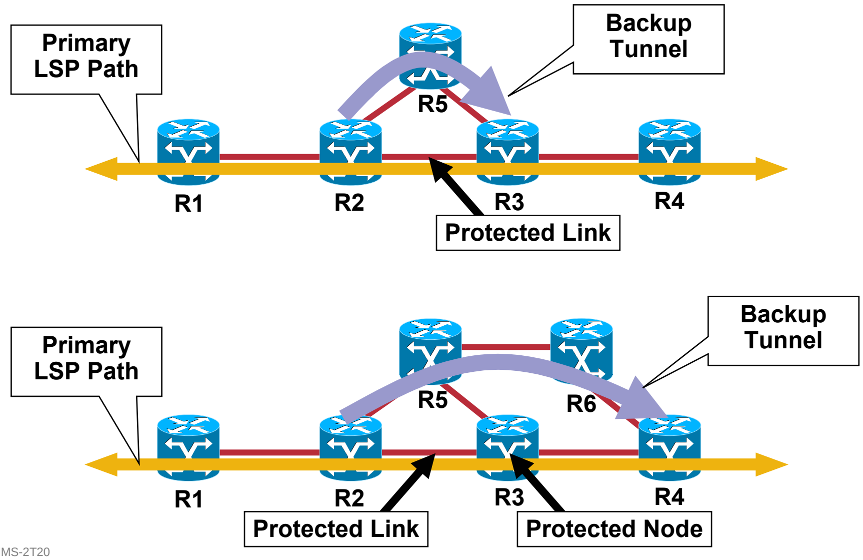


MPLS Traffic Engineering Fast Re-Route

- MPLS traffic engineering allows network administrators to define explicit paths for traffic with some constraint
    - Path from A to B with 50 Mbps bandwidth
- FRR is a method of protecting MPLS traffic engineering label switched paths
- The idea is to locally repair the LSP at the point of failure
    - By re-routing traffic over a pre-defined back-up tunnel
    - Prevents packet loss while IGP converges
- Protection against link and node failures

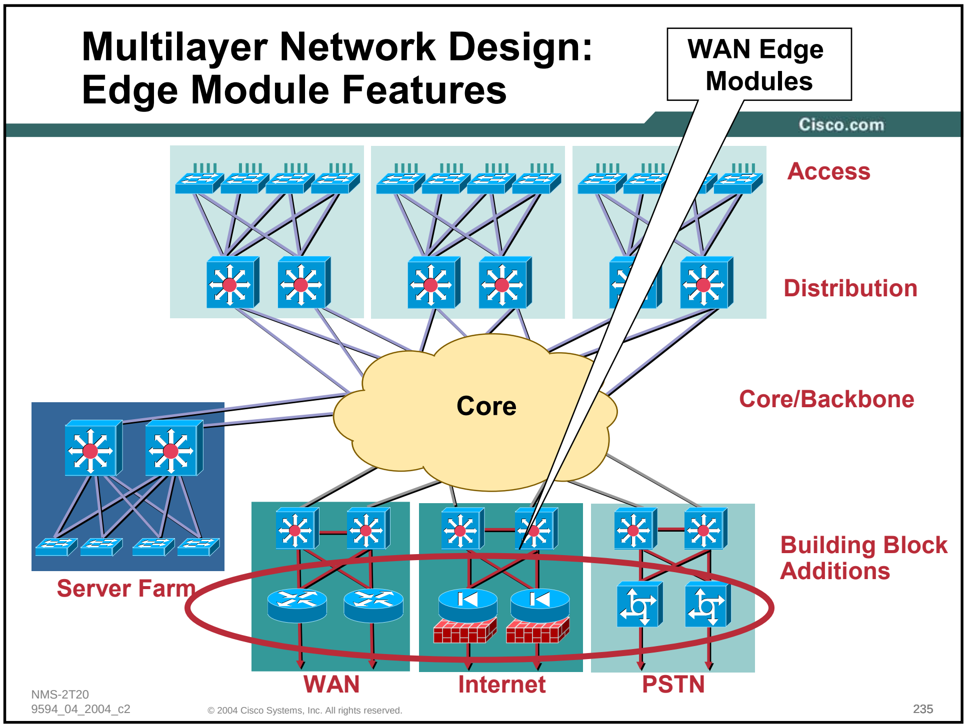
Related Session: RST-2603 Deploying MPLS Traffic Engineering

Link vs. Node Protection

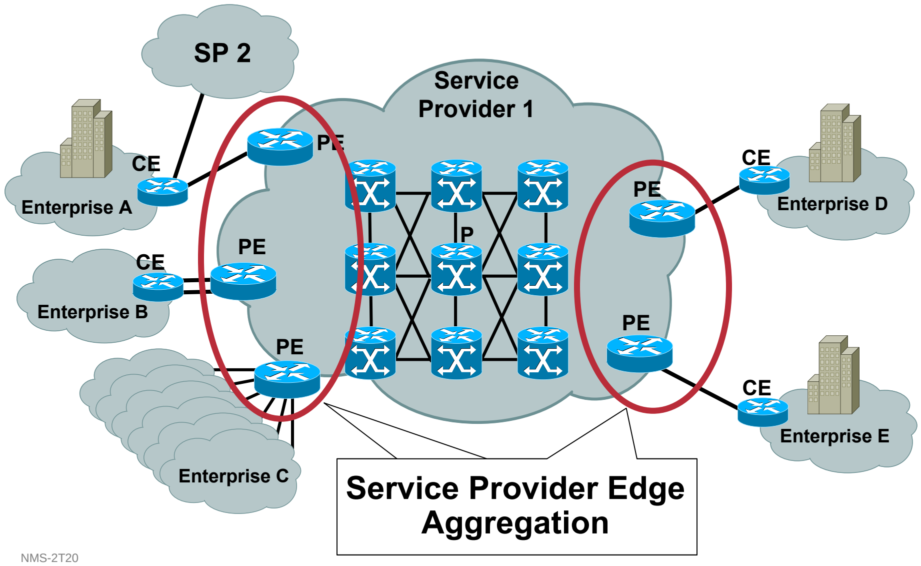


LAYER 3 HIGH AVAILABILITY: NETWORK EDGE

Multilayer Network Design: Edge Module Features



Service Provider Network

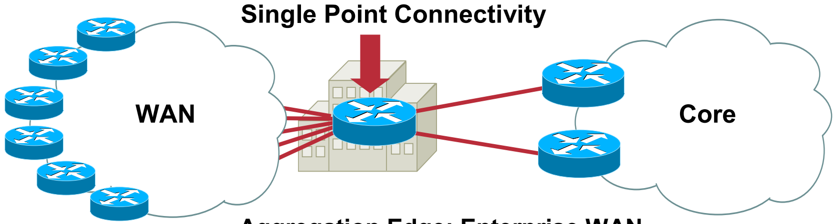


High Availability Tool Kit

Application Level Resiliency ➡	**Global Server Load Balancing, Stateful NAT, Stateful IPSec, DNS, DHCP, Cisco Server Load Balancing, IP QoS**
Protocol Level Resiliency ➡	**HSRP, VRRP, GLBP, MPLS-TE, IP Event Dampening , Graceful Restart (GR) in BGP, OSPF NSF, ISIS NSF, IP QoS**
Transport/Link Level Resiliency ➡	**SONET APS, RPR, DWDM, Ether Channel, Spanning Tree Protocol, LFI, L2 QoS**
Device Level Resiliency ➡	**Redundant Processors (RP), Switch Fabric, Line Cards, Ports, Power, NSF/SSO**

Aggregation Edge Is Vulnerable

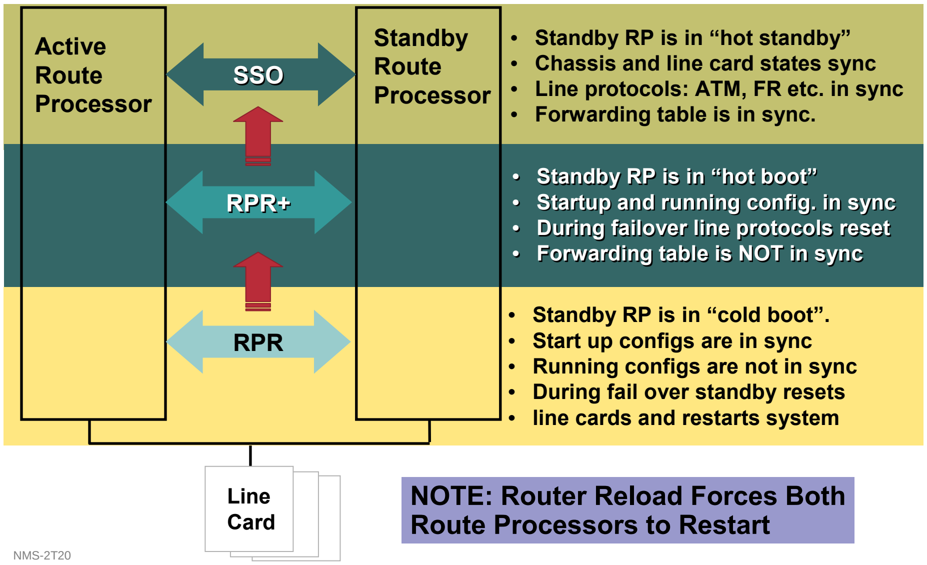
Single Point Connectivity



Aggregation Edge: Enterprise WAN Edge or SP Aggregation Router

- Single point of failure for 100's to 1000's of circuit terminations
- Redundant components used: fans, power, fabric, route processors

Route Processor Redundancy



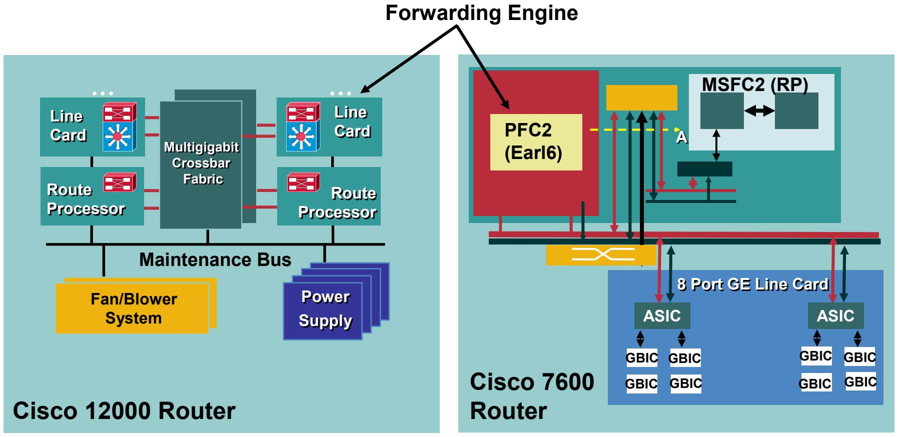
- Standby RP is in “hot standby”
- Chassis and line card states sync
- Line protocols: ATM, FR etc. in sync
- Forwarding table is in sync.

- Standby RP is in “hot boot”
- Startup and running config. in sync
- During failover line protocols reset
- Forwarding table is NOT in sync

- Standby RP is in “cold boot”.
- Start up configs are in sync
- Running configs are not in sync
- During fail over standby resets
- line cards and restarts system

NOTE: Router Reload Forces Both Route Processors to Restart

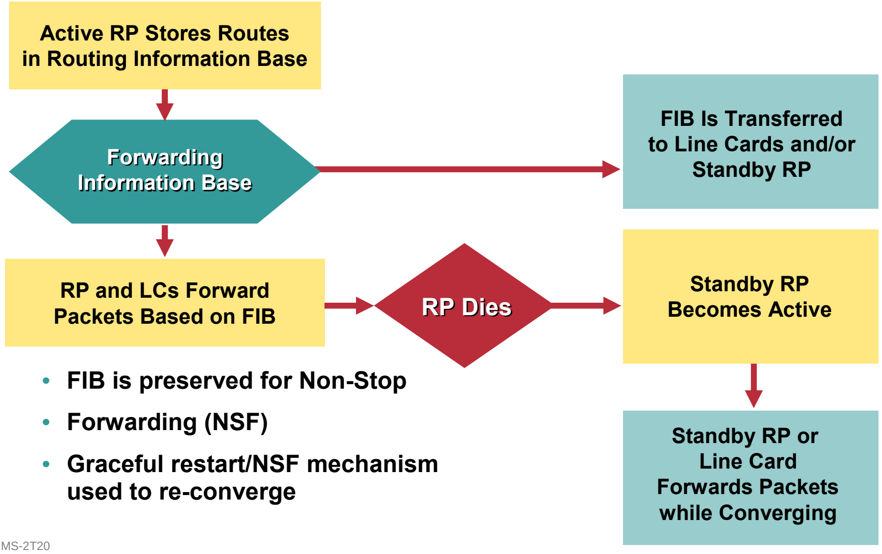
Router Internals Overview…



More Details: RST 2311 Packet Forwarding Operation on Mid to High-End Routers and Switches

RST 2312 Control Plane Operation on Mid to High-End Routers and Switches

Non-Stop Forwarding



Active RP Stores Routes in Routing Information Base

Forwarding Information Base

FIB Is Transferred to Line Cards and/or Standby RP

RP and LCs Forward Packets Based on FIB

RP Dies

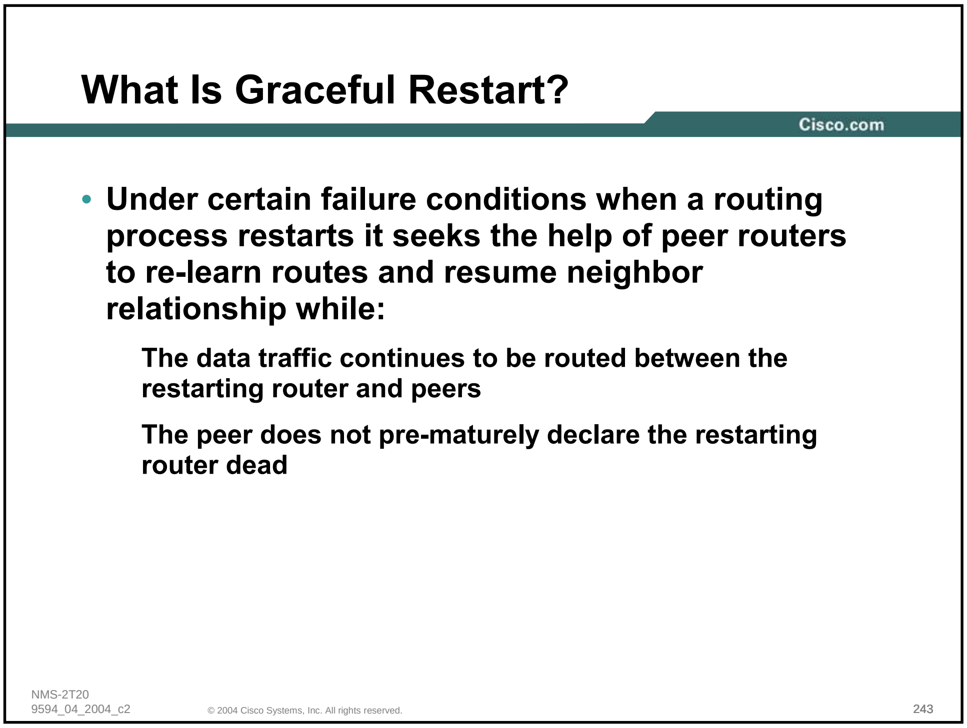
Standby RP Becomes Active

Standby RP or Line Card Forwards Packets while Converging

- FIB is preserved for Non-Stop
- Forwarding (NSF)
- Graceful restart/NSF mechanism used to re-converge

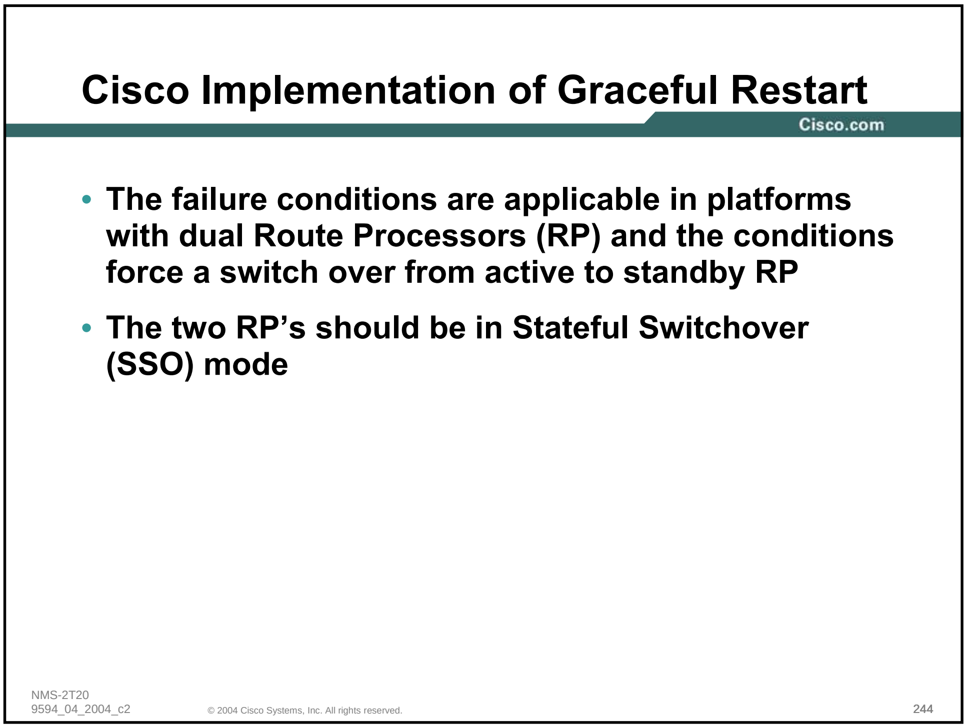
How Does the Redundant RP Handle Routing Protocols?

- Using the Graceful restart (or NSF) mechanisms



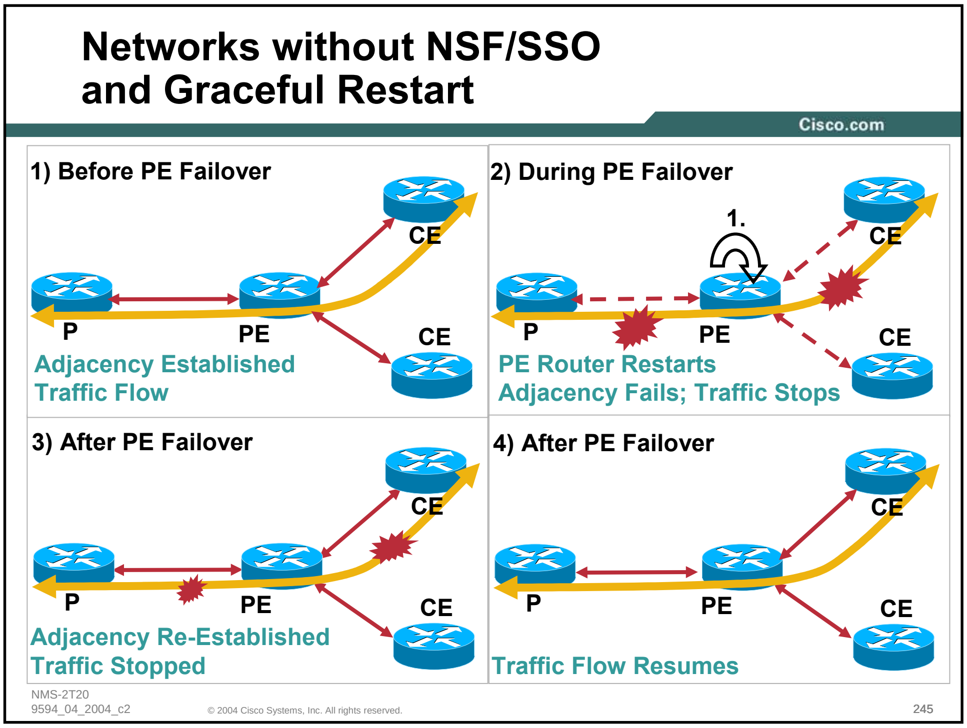
What Is Graceful Restart?

- Under certain failure conditions when a routing process restarts it seeks the help of peer routers to re-learn routes and resume neighbor relationship while:
  - The data traffic continues to be routed between the restarting router and peers
  - The peer does not pre-maturely declare the restarting router dead



Cisco Implementation of Graceful Restart

- The failure conditions are applicable in platforms with dual Route Processors (RP) and the conditions force a switch over from active to standby RP
- The two RP's should be in Stateful Switchover (SSO) mode



Networks without NSF/SSO and Graceful Restart

Cisco.com

1) Before PE Failover

Adjacency Established
Traffic Flow

2) During PE Failover

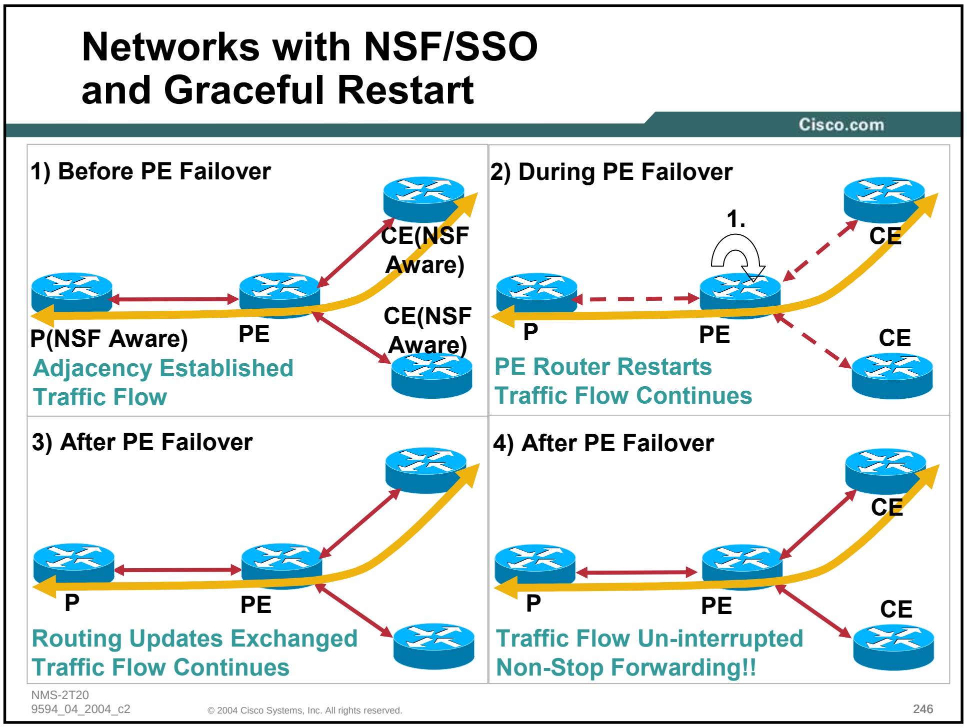
PE Router Restarts
Adjacency Fails; Traffic Stops

3) After PE Failover

Adjacency Re-Established
Traffic Stopped

4) After PE Failover

Traffic Flow Resumes



Networks with NSF/SSO and Graceful Restart

Cisco.com

1) Before PE Failover

Adjacency Established
Traffic Flow

2) During PE Failover

PE Router Restarts
Traffic Flow Continues

3) After PE Failover

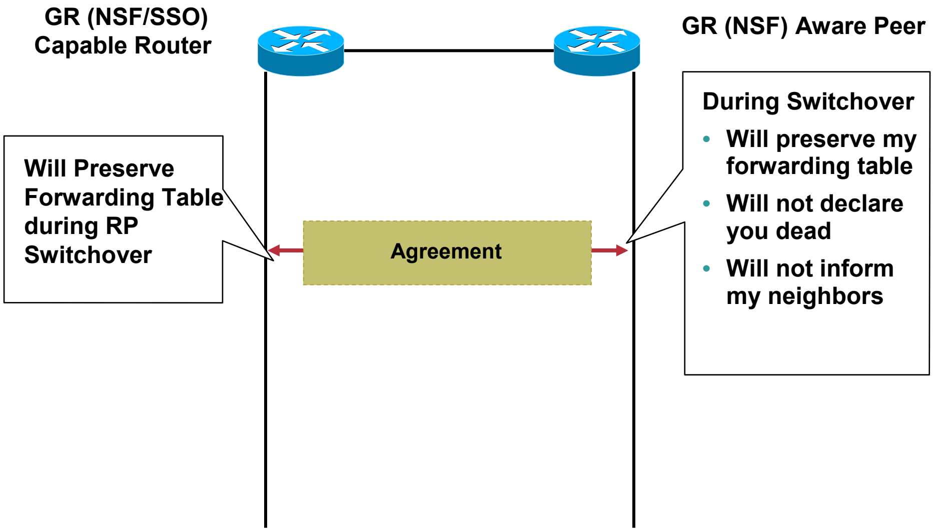
Routing Updates Exchanged
Traffic Flow Continues

4) After PE Failover

Traffic Flow Un-interrupted
Non-Stop Forwarding!!

Relationship Building Exercise: 1

Cisco.com



GR (NSF/SSO) Capable Router

GR (NSF) Aware Peer

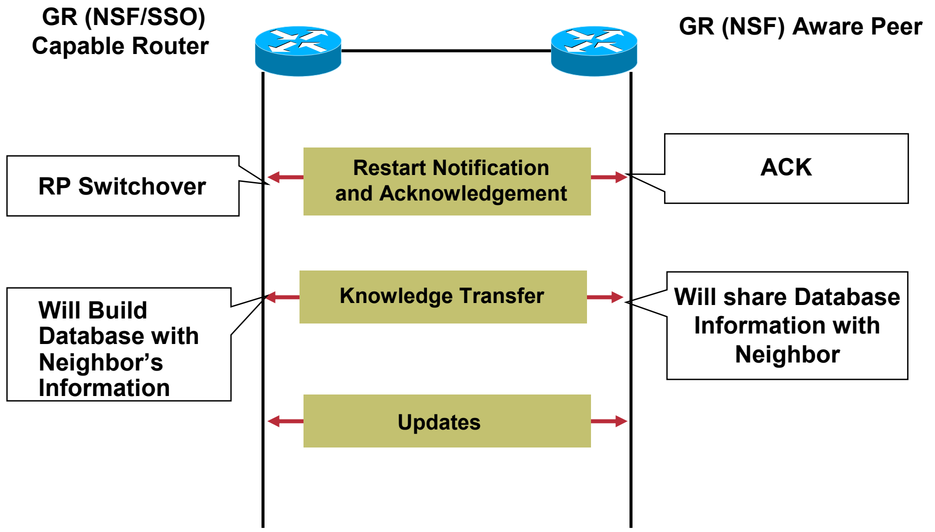
Will Preserve Forwarding Table during RP Switchover

Agreement

During Switchover
- **Will preserve my forwarding table**
- **Will not declare you dead**
- **Will not inform my neighbors**

Relationship Building Exercise: 2

Cisco.com



GR (NSF/SSO) Capable Router

GR (NSF) Aware Peer

RP Switchover

Restart Notification and Acknowledgement

ACK

Will Build Database with Neighbor's Information

Knowledge Transfer

Will share Database Information with Neighbor

Updates

NSF/SSO Terminology

Cisco.com

- **NSF capable router (restarting router)**

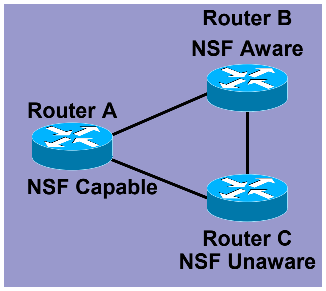
  A router that preserves it's forwarding table and rebuilds it's routing topology after an RP switch over; currently a dual RP router

  ex: Cisco 7500, 10000, 12000, 7304
- **NSF aware router (peer)**

  A router that assists an NSF capable during restart and can preserve routes reachable via the restarting router

  ex: Cisco 7200, 3600, 2600, 1700
- **NSF unaware router**

  A router that is not capable of assisting an NSF Capable router during an RP switchover
- **NSF capable router is NSF aware too!!!!**



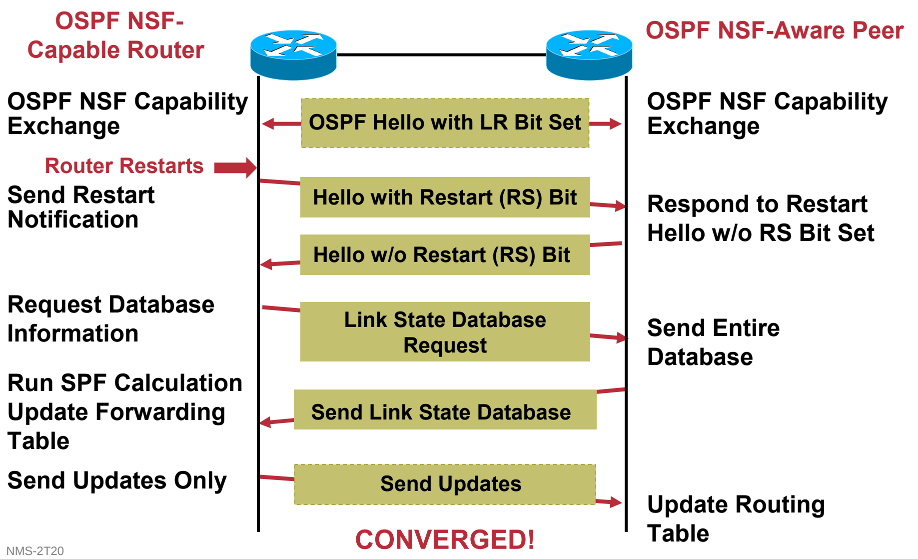
LAYER 3 HA: NETWORK EDGE

GRACEFUL RESTART
IN ROUTING PROTOCOLS

OSPF NSF

- Competing drafts proposed in IETF
- Cisco calls it’s implementation OSPF NSF, others call their implementation OSPF hitless restart
- Cisco implementation is Cisco IOS:12.0(22)S, 12.2T, 12.2S (release and device dependent)

OSPF NSF Operation Summary



OSPF NSF-Capable Router

OSPF NSF-Aware Peer

OSPF NSF Capability Exchange — OSPF Hello with LR Bit Set — OSPF NSF Capability Exchange

Router Restarts

Send Restart Notification — Hello with Restart (RS) Bit — Respond to Restart Hello w/o RS Bit Set

Hello w/o Restart (RS) Bit

Request Database Information — Link State Database Request — Send Entire Database

Send Link State Database

Run SPF Calculation Update Forwarding Table

Send Updates Only — Send Updates — Update Routing Table

CONVERGED!

Relevant Show Commands

Cisco.com

Active RP: show ip ospf

esr2#show ip ospf

```
 Routing Process "ospf 1" with ID 2.2.2.1 and Domain ID
0.0.0.1
 Supports only single TOS(TOS0) routes
 <snip>
 Number of areas in this router is 1. 1 normal 0 stub 0
nssa
 External flood list length 0
 Nonstop Forwarding enabled, last NSF restart 00:02:51 ago
(took 37 secs)
    Area BACKBONE(0)
        Number of interfaces in this area is 1 (0 loopback)
```

Relevant Show Commands (Cont.)

Cisco.com

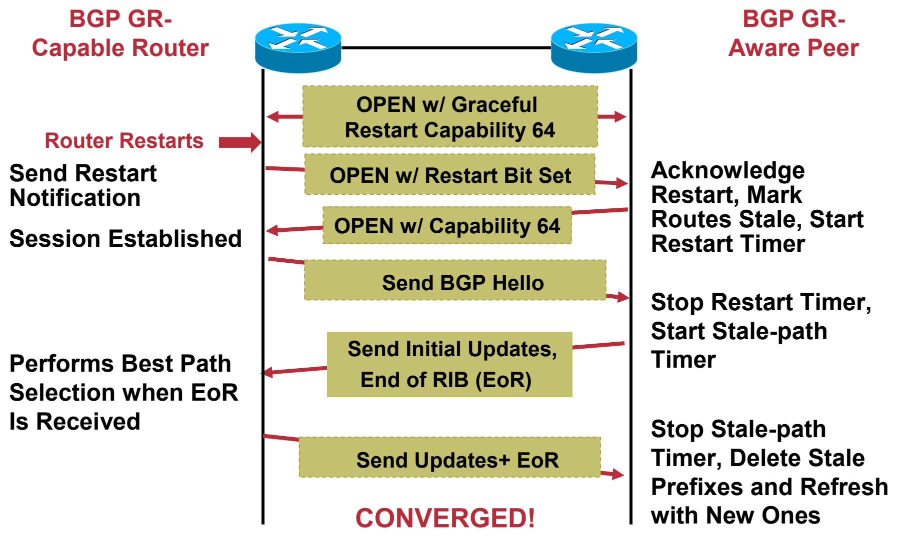
Active RP: show ip ospf neighbor detail

```
esr2#show ip ospf neighbor det
 Neighbor 3.3.3.1, interface address 192.10.0.3
    In the area 0 via interface GigabitEthernet1/0/0
    Neighbor priority is 1, State is FULL, 7 state
changes
    DR is 192.10.0.3 BDR is 192.10.0.2
    Options is 0x52
    LLS Options is 0x1 (LR), last OOB-Resync 00:03:08
ago
    Dead timer due in 00:00:37
    Neighbor is up for 00:03:32
```

BGP Graceful Restart

- IETF draft:draft-ietf-idr-restart-06.txt
- Provides a graceful recovery mechanism for a restarting BGP process
- Cisco implementation is Cisco IOS:12.0(22)S, 12.2T, 12.2S (release and device dependent)
- Requires a graceful restart aware neighbor

Graceful Restart BGP Operation Summary



BGP GR-Capable Router

BGP GR-Aware Peer

OPEN w/ Graceful Restart Capability 64

Router Restarts

Send Restart Notification

OPEN w/ Restart Bit Set

Acknowledge Restart, Mark Routes Stale, Start Restart Timer

Session Established

OPEN w/ Capability 64

Send BGP Hello

Stop Restart Timer, Start Stale-path Timer

Performs Best Path Selection when EoR Is Received

Send Initial Updates, End of RIB (EoR)

Send Updates+ EoR

Stop Stale-path Timer, Delete Stale Prefixes and Refresh with New Ones

CONVERGED!

BGP Graceful Restart Timers

- Restart timers are used by peers to set the amount of time it waits for a restarting router to establish a BGP session after it has indicated a restart
- Stalepath timers are used by peers to set the amount of time it waits to receive an End of RIB marker (end of RIB indicates the neighbor has converged) from the restarting router

---

BGP Graceful Restart Timers

- Important to keep restart timer below hold time
- Default values

  BGP hold time 180 seconds (3 x 60 sec keepalive)

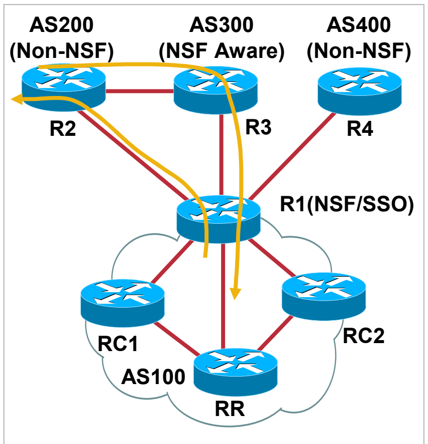
  Restart timer default 120 seconds

  Stale path timer default 180 seconds

- Restart timer is advertised to the peer
- Stale path timer is used internally by the router

BGP GR: Deployment Consideration: 1

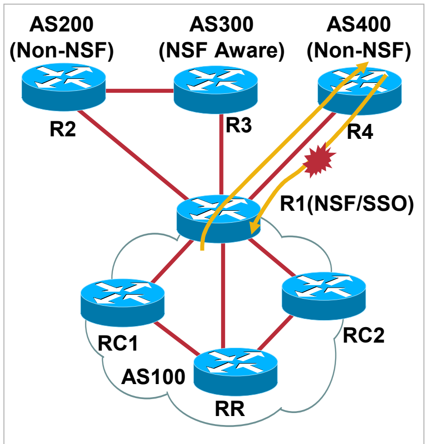
- Consider routes between R1 and R2 when R1 undergoes graceful restart
  - R1 preserves all routes to AS200 and continues forwarding traffic
  - R2 reaches AS100 via AS300
  - All traffic from R2 to R1 goes via R3
  - All traffic from R1 to R2 goes directly; this can lead to temporary asymmetric routing
  - No packet loss will be experienced from R1 to R2
  - Some packet loss from R2 to R1 during the re-convergence



ALL Routers Are NSF Aware Unless Indicated

BGP GR: Deployment Consideration: 2

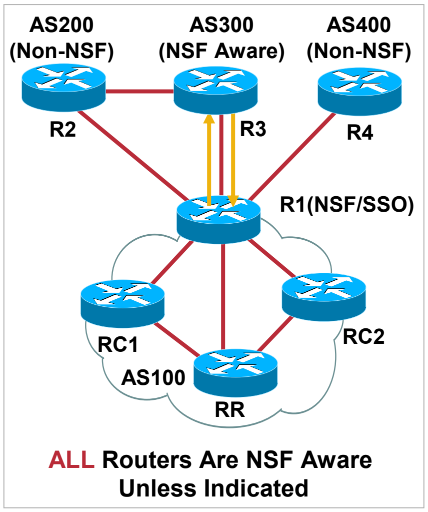
- Consider routes between R1 and R4 when R1 undergoes graceful restart
  - R1 preserves all routes to AS400 and continues forwarding traffic
  - R4 removes all routes to A
  - R1 continues to forward traffic to R4
  - R4 does not forward traffic to R1 till R1 re-converges



ALL Routers Are NSF Aware Unless Indicated

BGP GR: Deployment Consideration: 3

- Consider routes between R1 and R3 when R1 undergoes graceful restart
  - R1 preserves all routes to AS300 and continues forwarding traffic
  - R3 preserves all routes to AS100 and continues forwarding traffic



ALL Routers Are NSF Aware Unless Indicated

BGP Graceful Restart Commands

```
R18C12KRP(config)#router bgp 100
R18C12KRP(config-router)# bgp graceful-restart
R18C12KRP(config-router)# bgp graceful-restart restart-time 120
R18C12KRP(config-router)# bgp graceful-restart stalepath-time
   360
```

BGP Graceful Restart Commands

```
R18C12KRP#sh ip bgp nei
BGP neighbor is 10.10.104.1,  remote AS 100, internal link
BGP version 4, remote router ID 10.10.104.1
BGP state = Established, up for 00:00:10
Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
Route refresh: advertised and received(new)
Address family IPv4 Unicast: advertised and received
Graceful Restart Capabilty: advertised and received
Remote Restart timer is 140 seconds
Address families preserved by peer:
IPv4 Unicast
```

Indicates Neighbor Is NSF Aware

Show Command on Peer Router

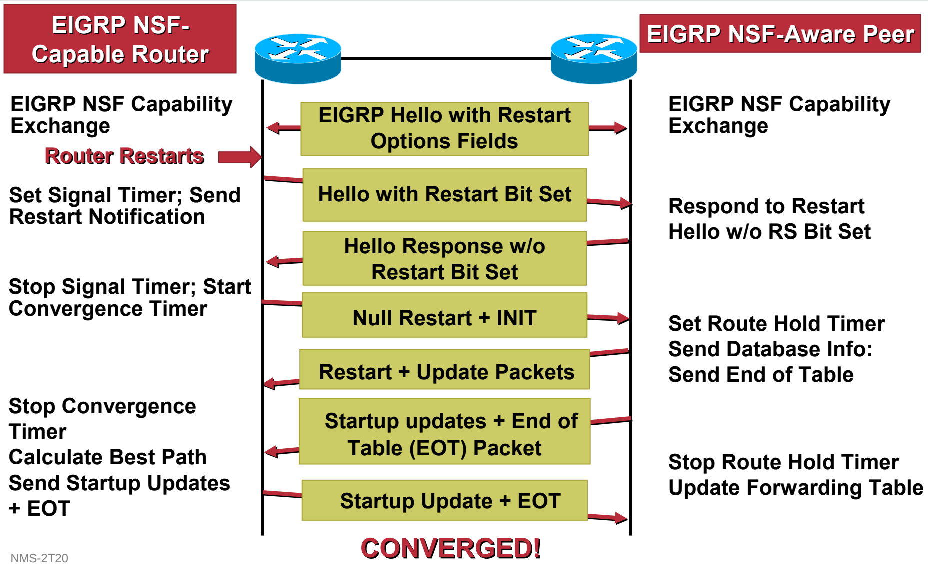
On Peer of Restarting Router

```
ip9-75b# show ip bgp
BGP table version is 209, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i – internal
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network            Next Hop      Metric    LocPrf    Weight   Path
*>  11.0.0.0          0.0.0.0          0       32768         i
*> S 170.10.10.0/24   180.10.10.3      0           0       200   101e
*> S 180.10.10.0/24   180.10.10.3      0           0       200   101e
*> S 190.10.10.0/24   180.10.10.3      5           0       200   101e
```

Marked Stale

EIGRP NSF Operation Summary

Cisco.com



EIGRP NSF-Capable Router

EIGRP NSF-Aware Peer

EIGRP NSF Capability Exchange

EIGRP Hello with Restart Options Fields

EIGRP NSF Capability Exchange

Router Restarts

Set Signal Timer; Send Restart Notification

Hello with Restart Bit Set

Respond to Restart Hello w/o RS Bit Set

Hello Response w/o Restart Bit Set

Stop Signal Timer; Start Convergence Timer

Null Restart + INIT

Set Route Hold Timer
Send Database Info:
Send End of Table

Restart + Update Packets

Startup updates + End of Table (EOT) Packet

Stop Convergence Timer
Calculate Best Path
Send Startup Updates + EOT

Startup Update + EOT

Stop Route Hold Timer
Update Forwarding Table

CONVERGED!

EIGRP NSF Timers

Cisco.com

- On restart router

  Signal timer: Used to send Hello with Restart bit set; when this timer expires Hellos' are sent without Restart bit set

  Convergence timer: Used to set the amount of time the restarting router waits to receive EOT marker from peers

- On the peer

  Route hold timer: Used by peer to indicate the amount of time the peer waits to receive routing updates and EOT marker from restarting router

EIGRP NSF: Configuration Commands

Cisco.com

- On restarting router

```
router eigrp 100
    nsf
    timers nsf signal
    timers nsf converge
```

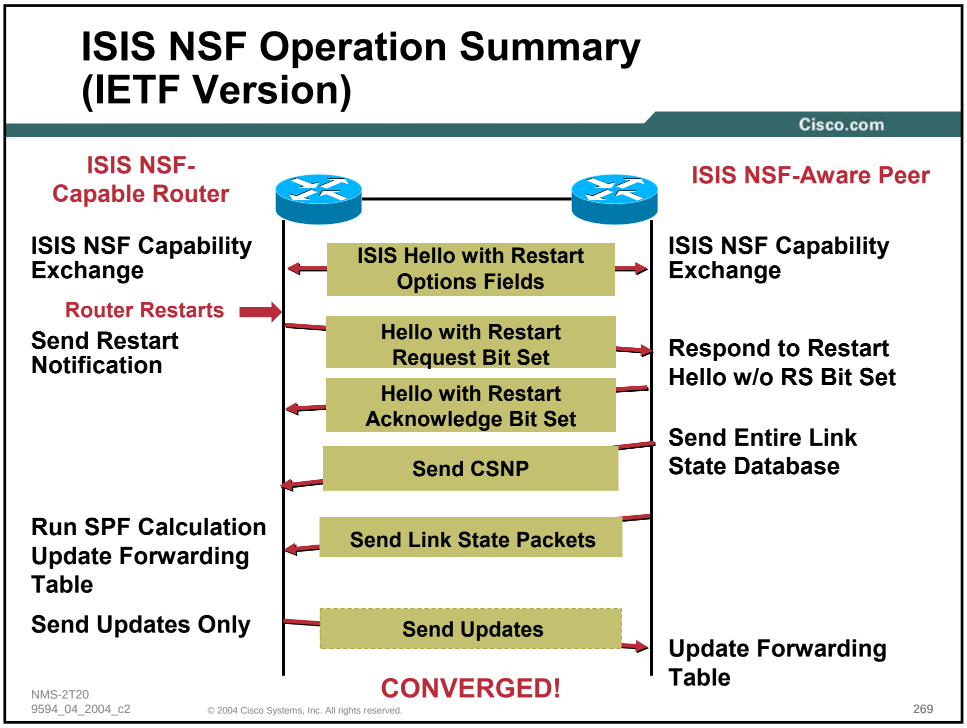
- On peer

```
router eigrp 100
    nsf
    timers nsf route-hold
```

ISIS NSF

Cisco.com

- Cisco's ISIS NSF implementation comes in two flavors
  - IETF version: draft-ietf-isis-restart-0X
  - Cisco version
- The difference between them
  - IETF version depends on neighbors to rebuild the routing table
  - Cisco version does not depend on neighbors to rebuild routing table; peer can be non-NSF aware



ISIS NSF Operation Summary (IETF Version)

Cisco.com

ISIS NSF-Capable Router

ISIS NSF-Aware Peer

ISIS NSF Capability Exchange

ISIS Hello with Restart Options Fields

ISIS NSF Capability Exchange

Router Restarts

Send Restart Notification

Hello with Restart Request Bit Set

Respond to Restart Hello w/o RS Bit Set

Hello with Restart Acknowledge Bit Set

Send Entire Link State Database

Send CSNP

Run SPF Calculation Update Forwarding Table

Send Link State Packets

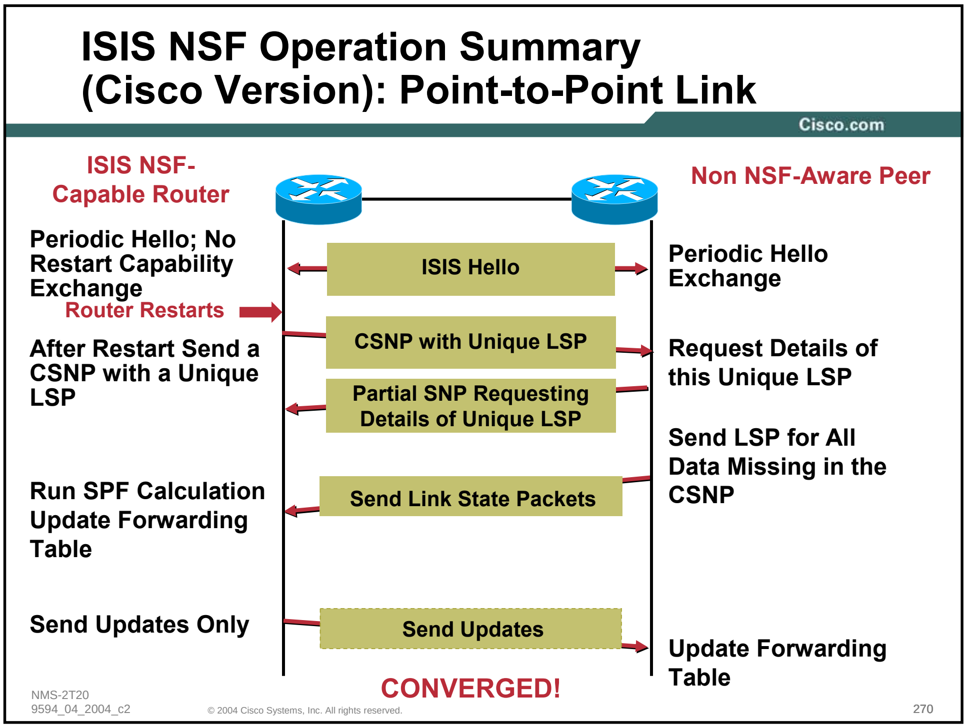
Send Updates Only

Send Updates

Update Forwarding Table

CONVERGED!

NMS-2T20
9594_04_2004_c2



ISIS NSF Operation Summary (Cisco Version): Point-to-Point Link

Cisco.com

ISIS NSF-Capable Router

Non NSF-Aware Peer

Periodic Hello; No Restart Capability Exchange

ISIS Hello

Periodic Hello Exchange

Router Restarts

After Restart Send a CSNP with a Unique LSP

CSNP with Unique LSP

Request Details of this Unique LSP

Partial SNP Requesting Details of Unique LSP

Send LSP for All Data Missing in the CSNP

Run SPF Calculation Update Forwarding Table

Send Link State Packets

Send Updates Only

Send Updates

Update Forwarding Table

CONVERGED!

NMS-2T20
9594_04_2004_c2

ISIS NSF: Configuration Command

IETF Draft-Based

```
router(config)# router isis
router(config-router)# nsf [cisco/ietf]
```

Cisco Internal
Implementation

Show and Debug Commands: IETF Version

show clns neighbor detail

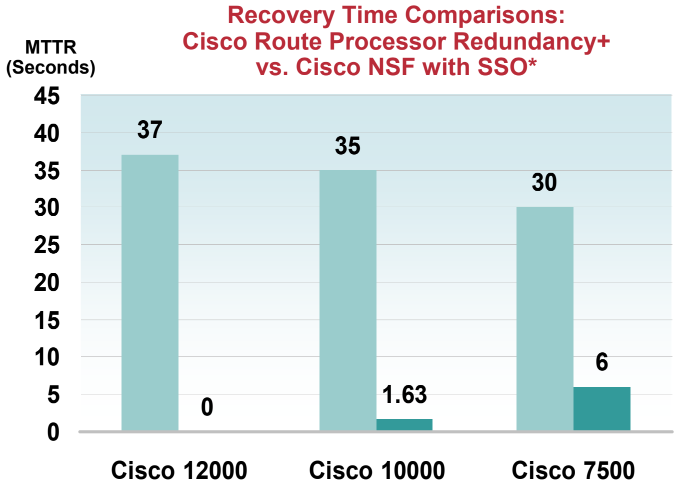
```
Router#show clns nei detail
System Id Interface SNPA State Holdtime Type Protocol
esr2 PO1/0/0 *HDLC* Up 24 L2 IS-IS
Area Address(es): 49.0002
IP Address(es): 180.10.10.1*
Uptime: 00:02:27
NSF capable
```

Show and Debug Commands: IETF Version

show isis nsf

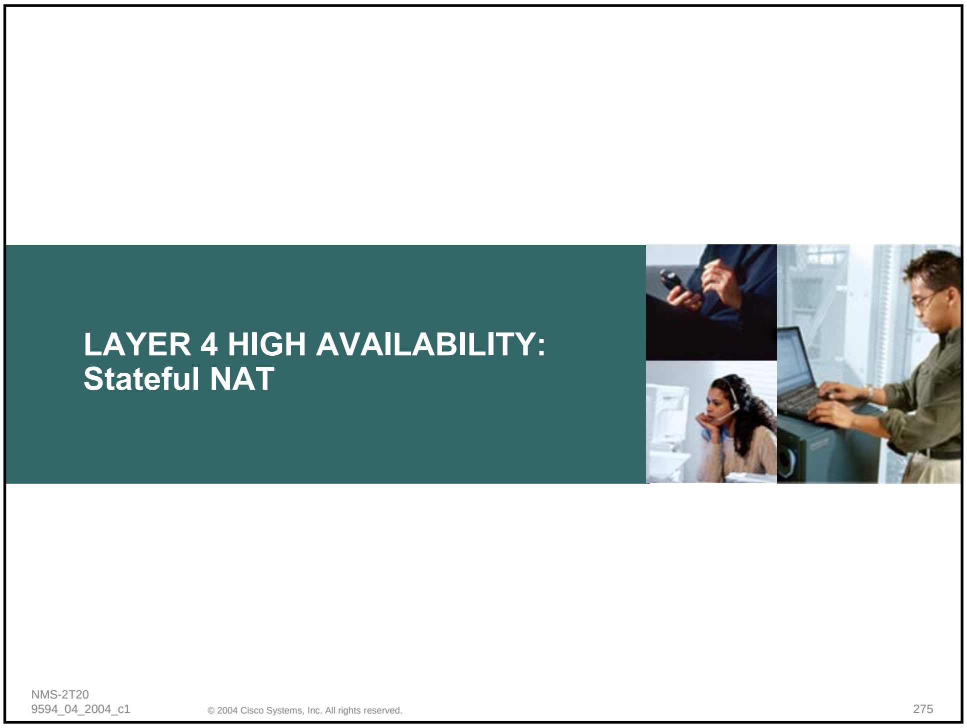
```
Router#show isis nsf
NSF is ENABLED, mode 'ietf'
NSF pdb state:
NSF L1 active interfaces: 0
NSF L1 active LSPs: 0
8.2.2.1.1.1.1 NSF interfaces awaiting L1 CSNP: 0
Awaiting L1 LSPs:
NSF L2 active interfaces: 0
NSF L2 active LSPs: 0
NSF interfaces awaiting L2 CSNP: 0
Awaiting L2 LSPs:
```

Effect of NSF/SSO on MTTR



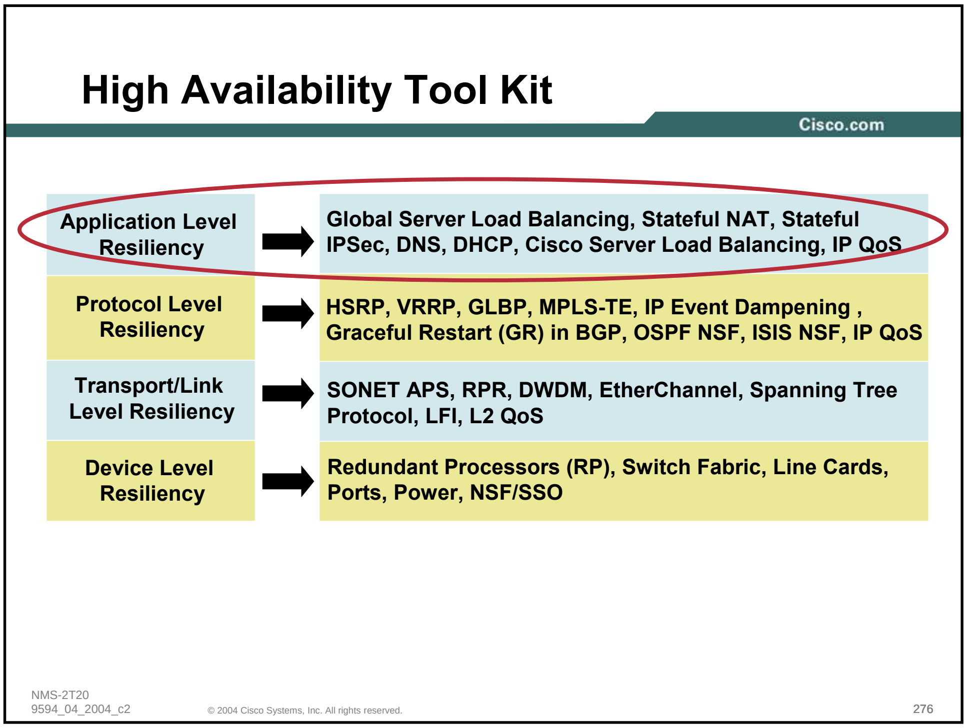
Recovery Time Comparisons:
Cisco Route Processor Redundancy+
vs. Cisco NSF with SSO*

*Source: Miercom Copyright ®2002



LAYER 4 HIGH AVAILABILITY: Stateful NAT

NMS-2T20
9594_04_2004_c1



High Availability Tool Kit

Cisco.com

Application Level Resiliency	➡	Global Server Load Balancing, Stateful NAT, Stateful IPSec, DNS, DHCP, Cisco Server Load Balancing, IP QoS
Protocol Level Resiliency	➡	HSRP, VRRP, GLBP, MPLS-TE, IP Event Dampening , Graceful Restart (GR) in BGP, OSPF NSF, ISIS NSF, IP QoS
Transport/Link Level Resiliency	➡	SONET APS, RPR, DWDM, EtherChannel, Spanning Tree Protocol, LFI, L2 QoS
Device Level Resiliency	➡	Redundant Processors (RP), Switch Fabric, Line Cards, Ports, Power, NSF/SSO

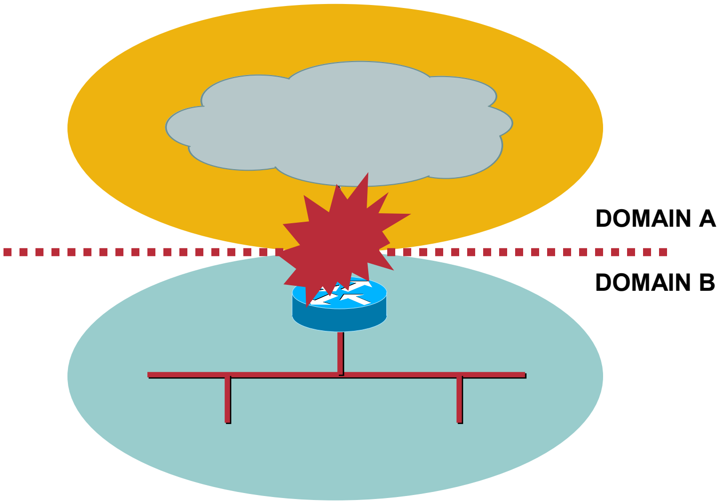
NMS-2T20
9594_04_2004_c2

Network Address Translation (NAT)

- Originally defined in RFC 1631
- NAT has been a factor in:
    - Reducing address depletion
    - Allowing interconnection of private networks using addresses as defined in RFC 1918
    - Hiding networks from outside the administrative domain
- Typically at domain edges
    - To connect B2B
    - To connect to Internet
    - For VPN connections
    - Between “test” and “production” networks
- These domain interconnect points become critical points of failure

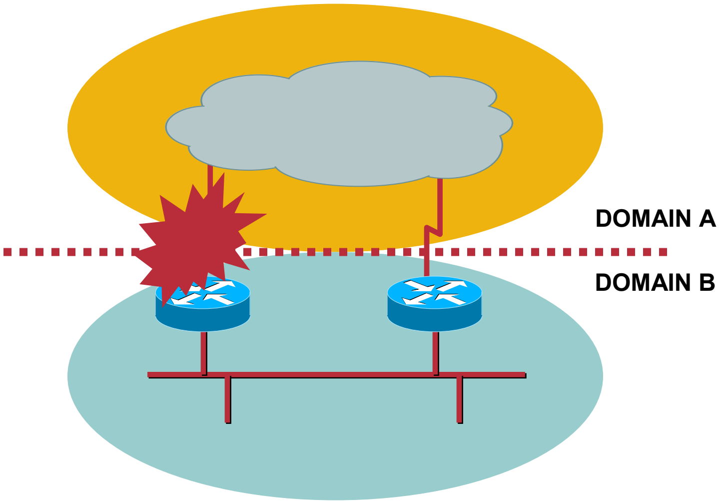
More about NAT: 2102 Deploying and Troubleshooting NAT

Critical Points of Failure



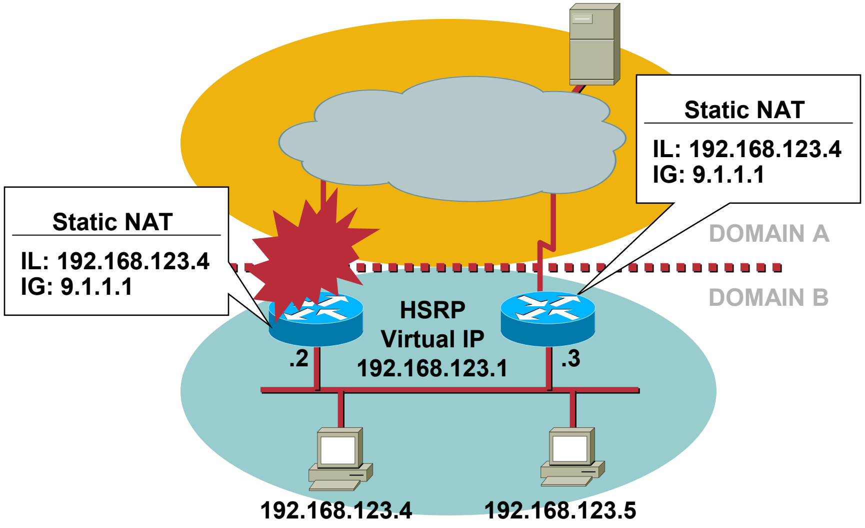
Critical Points of Failure

Cisco.com



NAT Redundancy with HSRP

Cisco.com

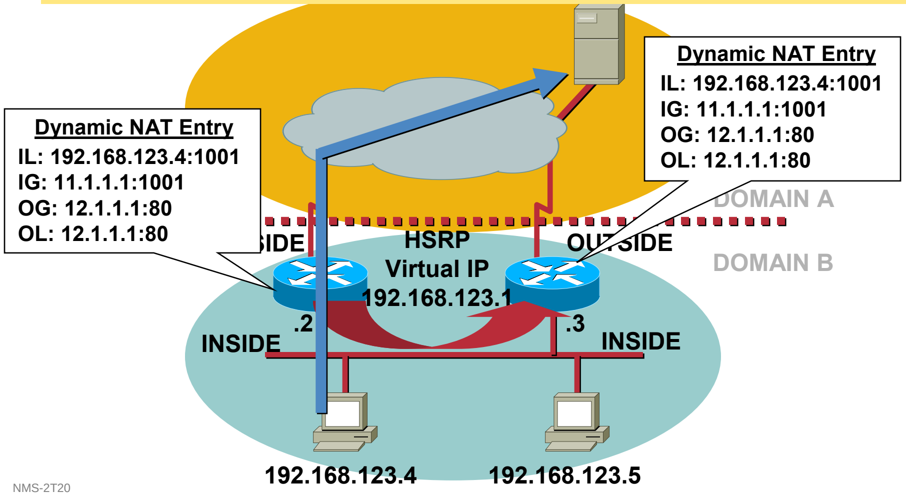


Stateful NAT Adds Redundancy for Dynamic NAT Entries

- Supports dynamic pools and port address translation (PAT/NAPT)
- Entries created on primary NAT router are distributed to backup NAT router
- Messages exchanged between SNAT peers over TCP
- SNAT router that created the entries is responsible for timing the entries
- Result is session resiliency in the event of critical failure when using NAT

Stateful NAT

```
ip nat pool SNATPOOL1 11.1.1.1 11.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1 mapping-id 10 overload
```

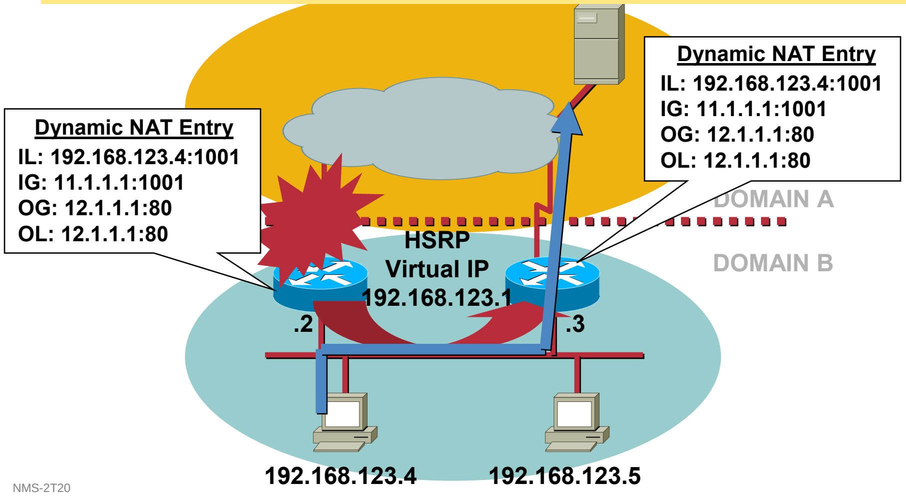


Dynamic NAT Entry
IL: 192.168.123.4:1001
IG: 11.1.1.1:1001
OG: 12.1.1.1:80
OL: 12.1.1.1:80

Dynamic NAT Entry
IL: 192.168.123.4:1001
IG: 11.1.1.1:1001
OG: 12.1.1.1:80
OL: 12.1.1.1:80

Stateful NAT

```
ip nat pool SNATPOOL1 11.1.1.1 11.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1 mapping-id 10 overload
```

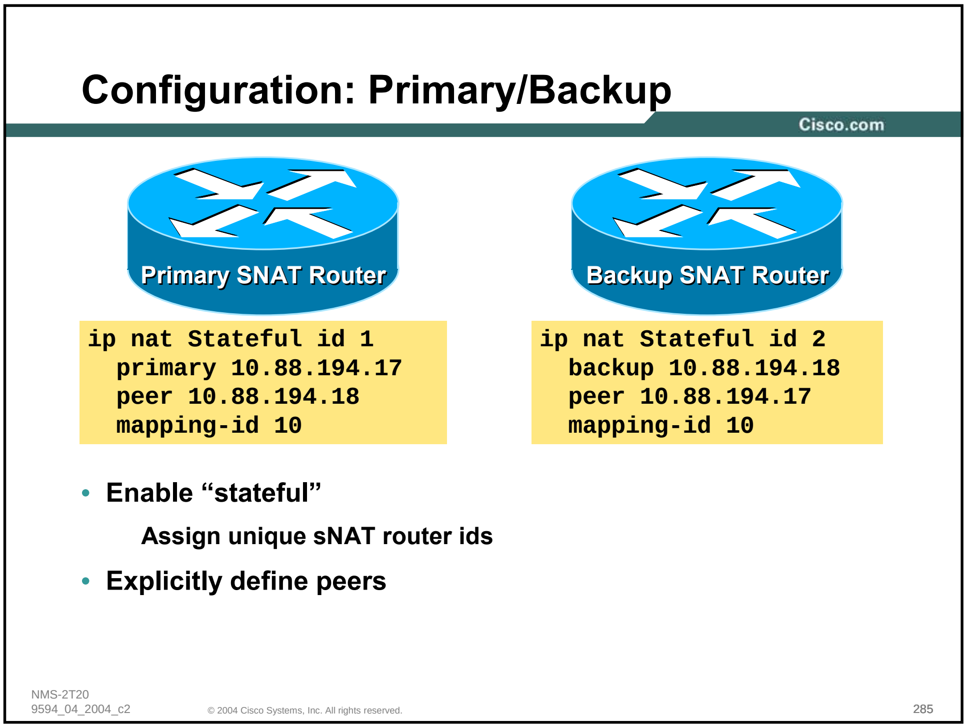


Dynamic NAT Entry
IL: 192.168.123.4:1001
IG: 11.1.1.1:1001
OG: 12.1.1.1:80
OL: 12.1.1.1:80

Dynamic NAT Entry
IL: 192.168.123.4:1001
IG: 11.1.1.1:1001
OG: 12.1.1.1:80
OL: 12.1.1.1:80

Phased Implementation

- Stateful NAT is being delivered with Cisco IOS in phases
- Phase I:
  - Provides support for protocols that do not imbed IP address and port information within the payload of the IP packet
    - Includes HTTP, ICMP, PING, rcp, rlogin, rsh, TCP, Telnet
  - Requires symmetric routing of return traffic
  - Supports only "inside" NAT pools
- Phase II:
  - The following protocols and applications are targeted for support in Phase II:
    - FTP, H225, H245, PPTP/GRE, NetMeeting Directory (ILS), RAS, SIP (both TCP and UDP based), Skinny, TFTP
  - Asymmetric routing support
  - Support for outside NAT pools, using the configuration command `ip nat outside source pool`
  - Dynamic entries, which are extended out of static definitions
  - Support for `ip nat inside destination`



Configuration: Primary/Backup

Cisco.com

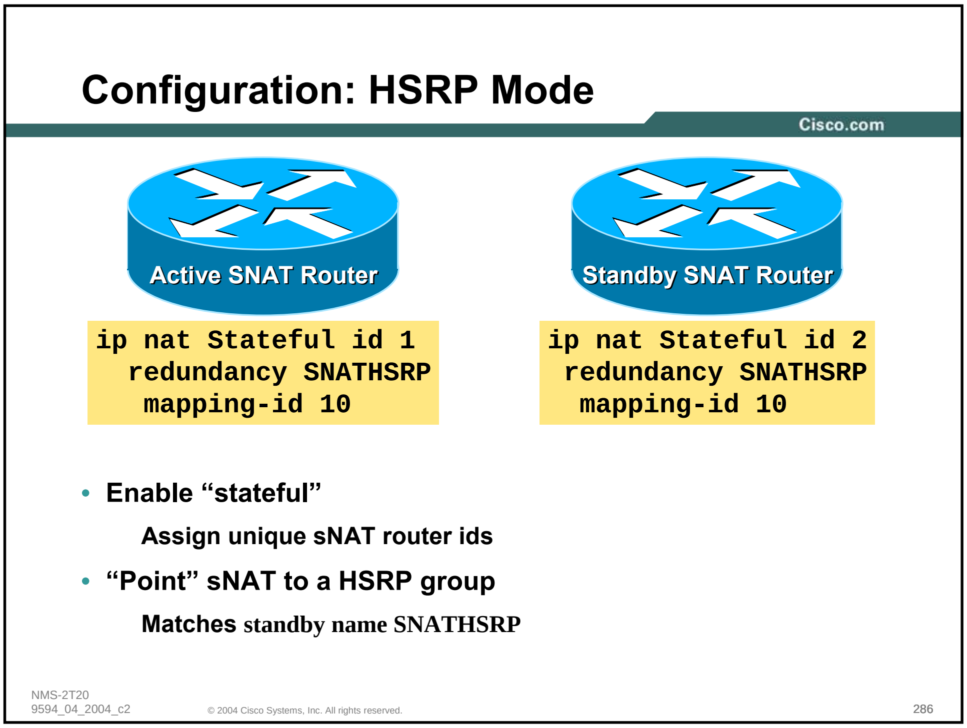
Primary SNAT Router

```
ip nat Stateful id 1
  primary 10.88.194.17
  peer 10.88.194.18
  mapping-id 10
```

Backup SNAT Router

```
ip nat Stateful id 2
  backup 10.88.194.18
  peer 10.88.194.17
  mapping-id 10
```

- Enable “stateful”
  - Assign unique sNAT router ids
- Explicitly define peers



Configuration: HSRP Mode

Cisco.com

Active SNAT Router

```
ip nat Stateful id 1
  redundancy SNATHSRP
   mapping-id 10
```

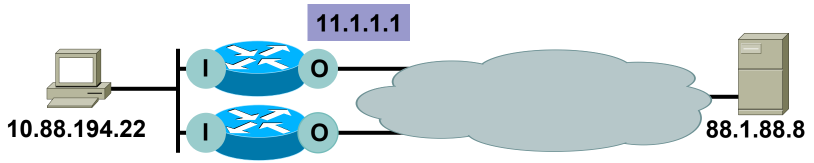
Standby SNAT Router

```
ip nat Stateful id 2
  redundancy SNATHSRP
   mapping-id 10
```

- Enable “stateful”
  - Assign unique sNAT router ids
- “Point” sNAT to a HSRP group
  - Matches standby name SNATHSRP

Configuration (Cont.)

```
ip nat pool SNATPOOL1 11.1.1.1 11.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1
  mapping-id 10 overload
!
ip route 11.1.1.0 255.255.255.0 Null0 250
!
access-list 101 permit ip 10.88.194.16 0.0.0.15 11.0.0.0
  0.255.255.255
access-list 101 permit ip 10.88.194.16 0.0.0.15 88.1.88.0
  0.0.0.255
!
route-map rm-101 permit 10
 match ip address 101
!
```



Mapping-ID?

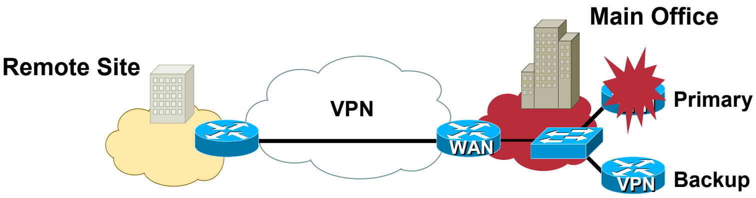
```
ip nat inside source route-map rm-101 pool SNATPOOL1
  mapping-id 10 overload
```

- Used to specify whether or not the local SNAT router will distribute a particular set of locally created entries to a peer SNAT router
- Each dynamically created entry inherits a mapping-id number
  - Comes from the mapping defined on the NAT rule
  - At the point of creation
- Mapping list
  - Specifies which of the entries will be forwarded to peers
  - Provides a way to specify that entries from particular NAT rules should be forwarded

```
ip nat Stateful id 1
     redundancy SNATHSRP
         mapping-id 10
         mapping-id 11
```

LAYER 4 HIGH AVAILABILITY: Stateful IPSec

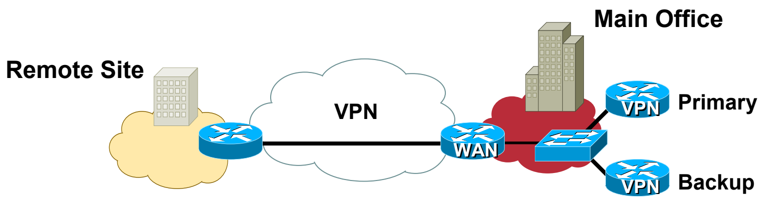
IPSec Connection Failures



- IPSec connection flows need to be maintained through the correct router in the case of multiple head-end devices
- HSRP is used for failover, but can an HSRP vIP be used as the VPN tunnel endpoint?

More IPSec VPN Session
SEC- 2011 Deploying Site to Site IPsec VPN

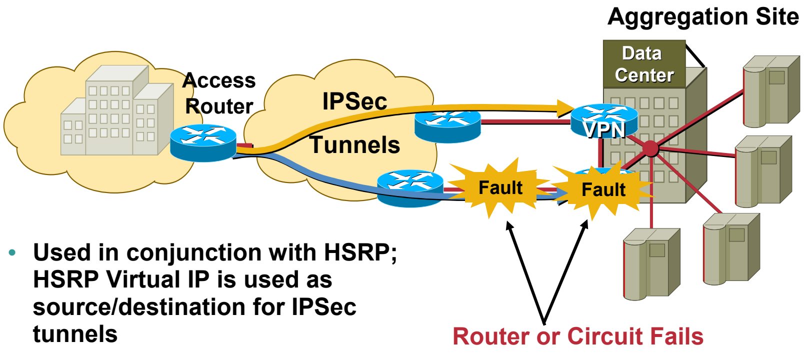
IPSec Stateful Failover



Features

- Ensures transport network is always available: business resiliency
- Delivers sub-second central site failover
- Scalable to 1000s of remote peers
- Transparent to remote sites

Stateful IPSec Tunneling



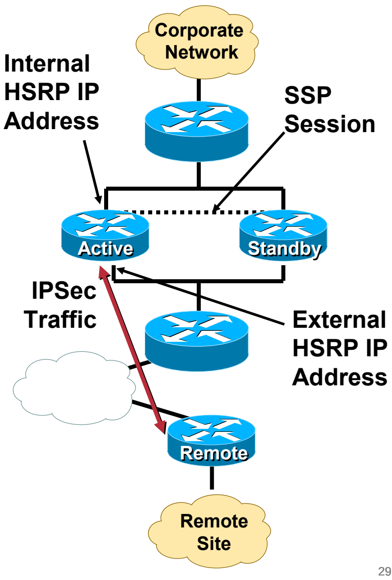
- Used in conjunction with HSRP; HSRP Virtual IP is used as source/destination for IPSec tunnels
- State Synchronization Protocol (SSP) is used to transfer state
- TCP connection formed from Active to each Standby router

Router or Circuit Fails

Stateful IPSec Maintains Connectivity to Users and Applications

Stateful Failover

- One HSRP IP address for inside interfaces
- One HSRP IP address for outside interfaces
- Active IKE and IPSec SAs mirrored on standby via SSP
- When active fails, standby takes over IPSec traffic without remote's knowledge



Stateful IPSec SSP Implementation

- Messages include ADD, DELETE, UPDATE, BULK-SYNC and Sync-check
- What is exchanged?
  - Sequence number counters and window states
  - IKE session keys
  - Security association attributes, such as cipher, authentication and compression algorithms
  - Standby Integrity (Sync check)
- Recommended to secure SSP sessions with IPSec

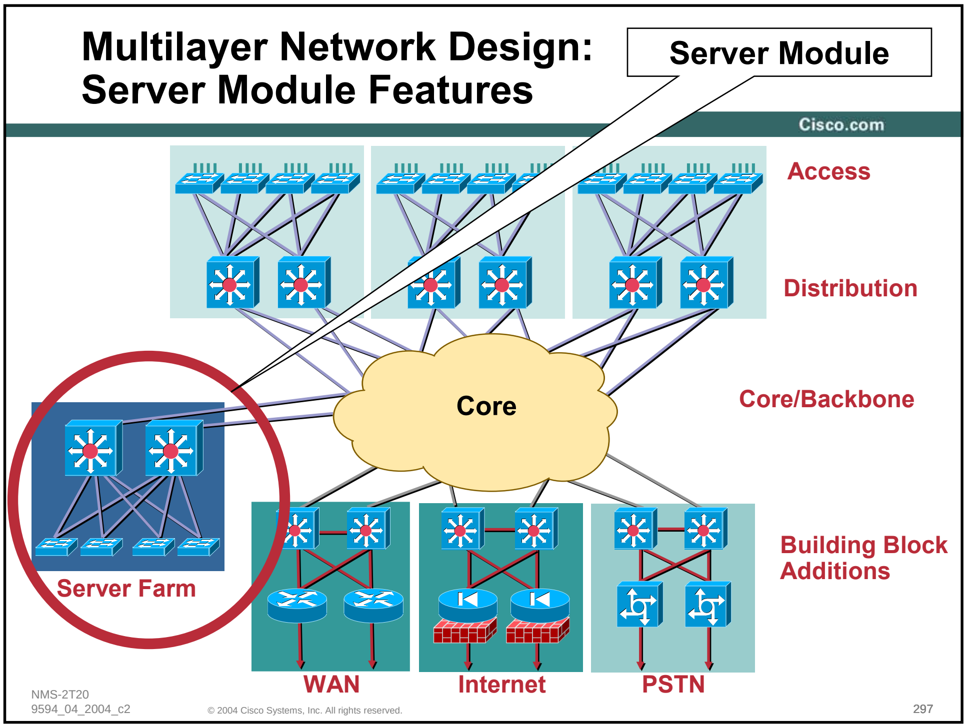
Stateful IPSec Configuration

```
ssp group 101
    local  10.1.1.1
    remote 10.1.1.2
    redundancy IPSEC-HA
!
crypto isakmp ssp 101
!
Interface Ethernet0/1
 ip address 10.1.1.1
 standby 1 ip 10.1.1.254
 standby 1 priority 150
 standby 1 preempt
 standby name IPSEC-HA
```

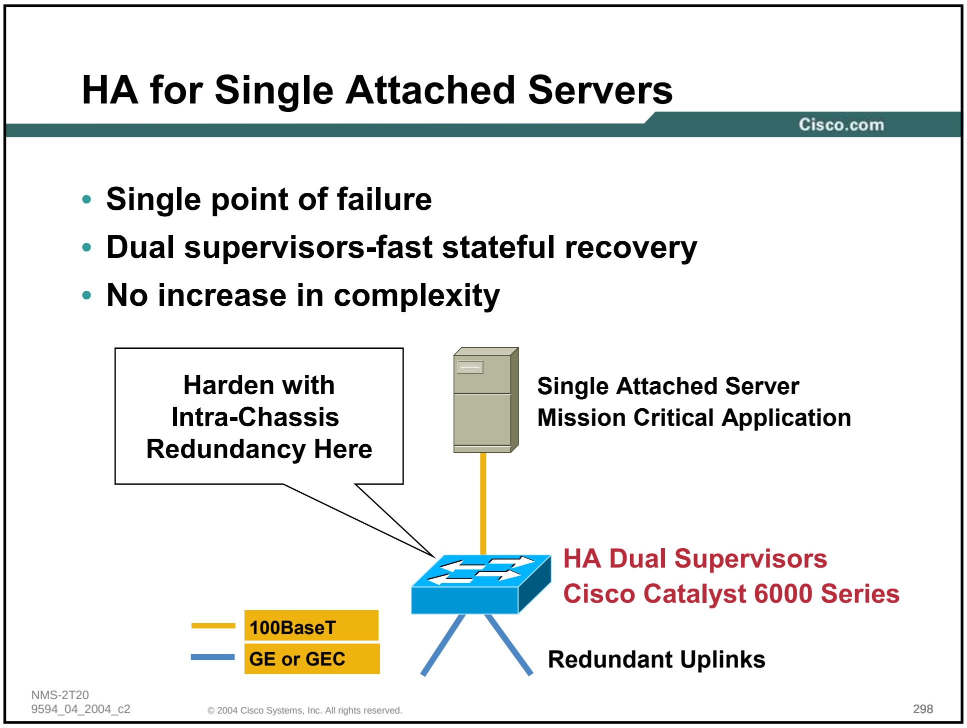
Ssp group-id Is Bound to Crypto isakmp

Standby Name Is Bound to ssp group

HIGH AVAILABILITY FOR SERVICES



Multilayer Network Design: Server Module Features

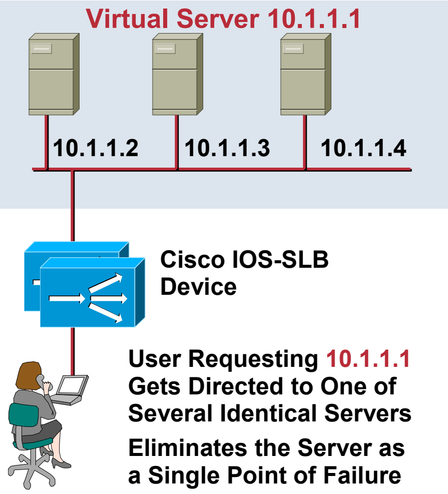


HA for Single Attached Servers

- Single point of failure
- Dual supervisors-fast stateful recovery
- No increase in complexity

Redundant Servers with Server Load Balancing

Cisco.com



User Requesting 10.1.1.1 Gets Directed to One of Several Identical Servers

Eliminates the Server as a Single Point of Failure

```
ip slb serverfarm WEB-FARM
 real 10.1.1.2
 inservice
 real 10.1.1.3
 inservice
 real 10.1.1.4
 Inservice
!
ip slb vserver WEBSVR
virtual 10.1.1.1
serverfarm WEB-FARM
inservice
```

Cisco IOS Server Load Balancing Image for the Cisco Catalyst 6000 or the Cisco 7200 or Content Switching Module (CSM)

Data Center Disaster Recovery

Cisco.com

- This is a topic unto itself
- Nevertheless, very important
- Let's consider one aspect where the network can help ensure continuous access to applications at multiple data centers

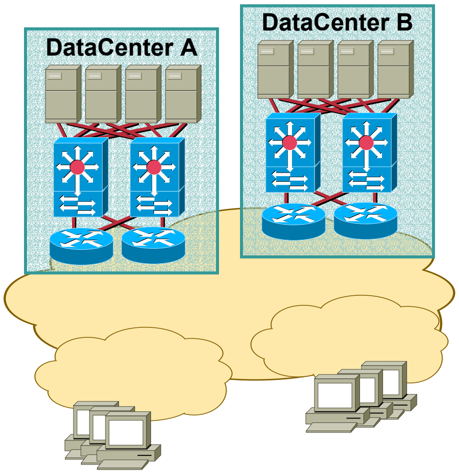
High Availability and Performance for Web-Based Business Applications

Problem:

- Want to intelligently and efficiently load balance client requests across multiple data centers
- Backup one data center to the other

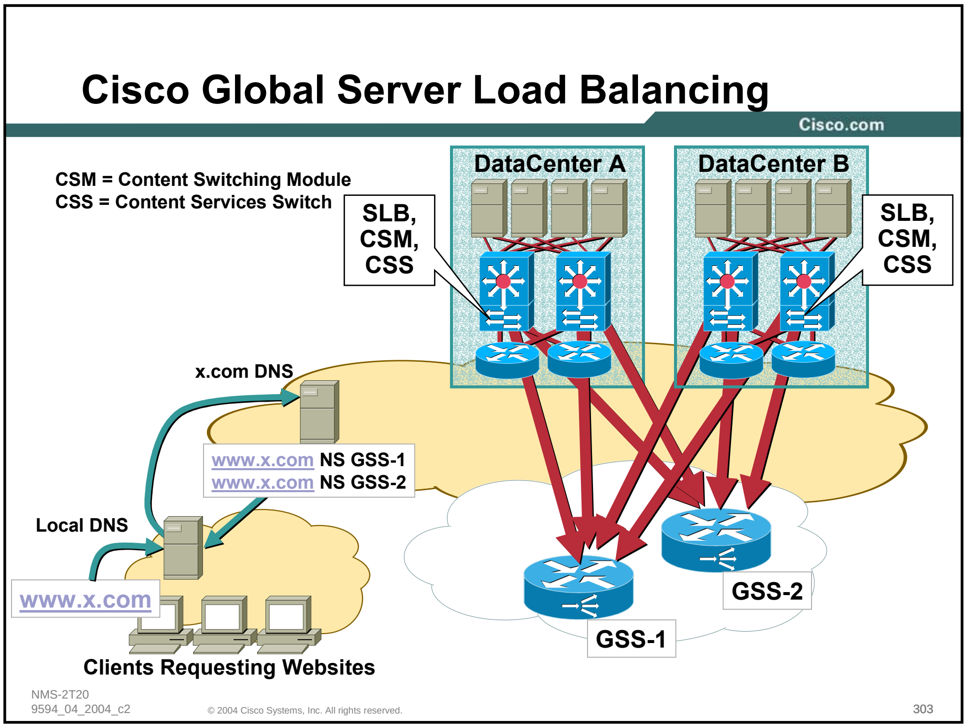
Solution:

- Use Cisco Global Site Selector (GSS) to add intelligent load balancing at the DNS resolution point in the Internet



Cisco Global Site Selector (GSS)

- GSS becomes authoritative name server for selected applications (ie, sub-domains)
  - Works with existing DNS infrastructure to connect client to SLB supporting the requested website
  - Monitors load and availability of SLB's to select the best SLB (site) to support the request
- Benefit:
  - Better control over request resolution process
  - High availability for disaster recovery and GSLB applications
  - Policy-determined, load-balanced resource utilization across sites
  - Improved performance and fast recovery yield positive user experience



Cisco Global Server Load Balancing

Cisco.com

CSM = Content Switching Module
CSS = Content Services Switch

DataCenter A

DataCenter B

SLB,
CSM,
CSS

SLB,
CSM,
CSS

x.com DNS

www.x.com NS GSS-1
www.x.com NS GSS-2

Local DNS

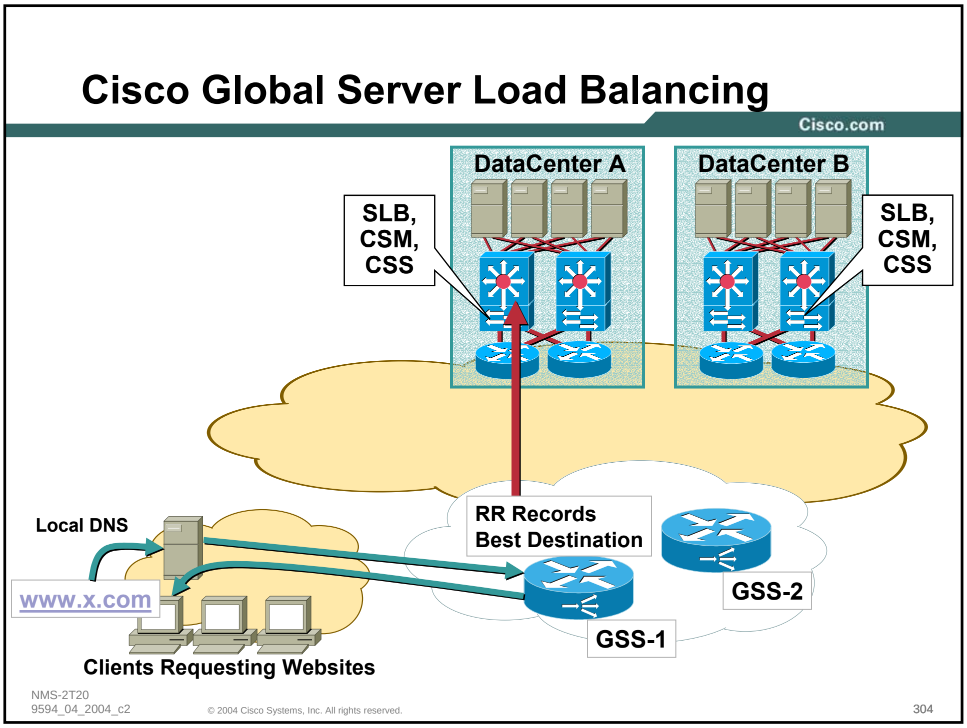
www.x.com

GSS-1

GSS-2

Clients Requesting Websites

NMS-2T20
9594_04_2004_c2



Cisco Global Server Load Balancing

Cisco.com

DataCenter A

DataCenter B

SLB,
CSM,
CSS

SLB,
CSM,
CSS

RR Records
Best Destination

Local DNS

www.x.com

GSS-1

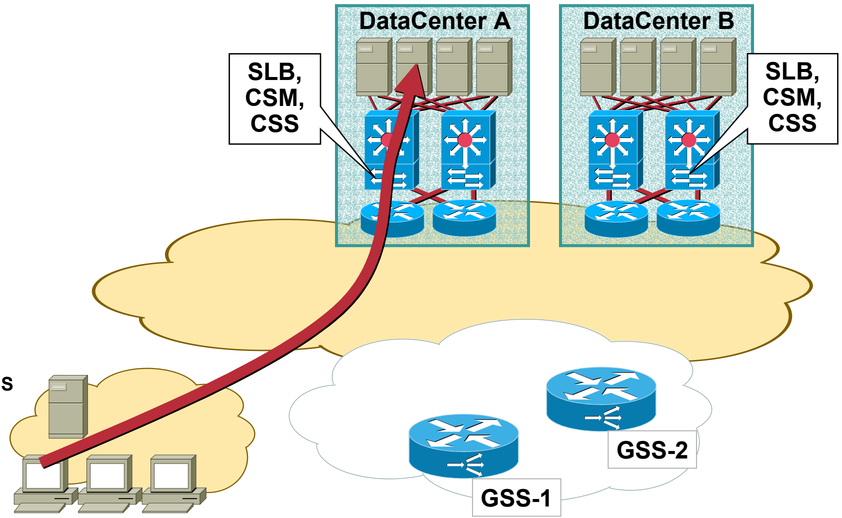
GSS-2

Clients Requesting Websites

NMS-2T20
9594_04_2004_c2

Cisco Global Server Load Balancing

Cisco.com



DataCenter A

DataCenter B

SLB,
CSM,
CSS

SLB,
CSM,
CSS

Local DNS

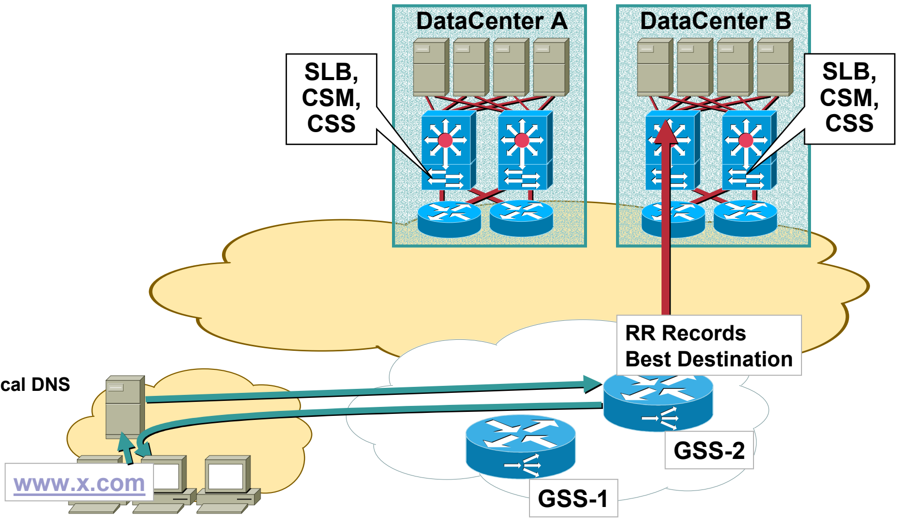
GSS-2

GSS-1

Clients Requesting Websites

Cisco Global Server Load Balancing

Cisco.com



DataCenter A

DataCenter B

SLB,
CSM,
CSS

SLB,
CSM,
CSS

RR Records
Best Destination

Local DNS

GSS-2

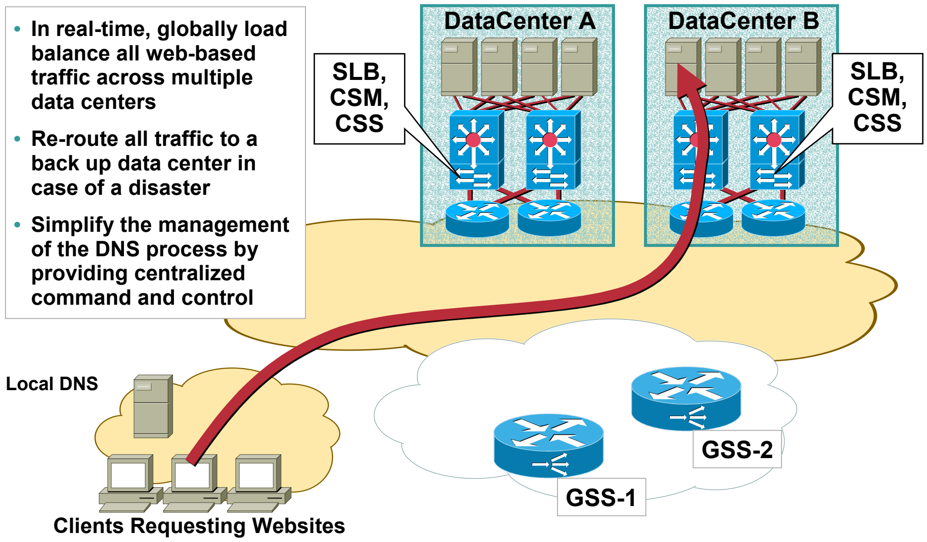
GSS-1

www.x.com

Clients Requesting Websites

Cisco Global Server Load Balancing

- In real-time, globally load balance all web-based traffic across multiple data centers
- Re-route all traffic to a back up data center in case of a disaster
- Simplify the management of the DNS process by providing centralized command and control



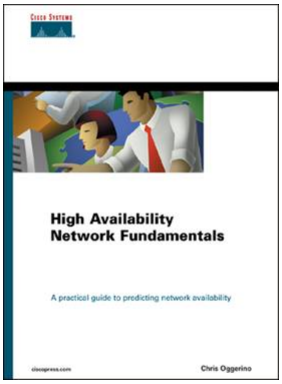
In Summary…

- For HA networking focus on network management, HA technologies and design optimization (we have covered two; break out sessions cover design optimization is detail)
- Understand and choose appropriate redundancy protocols available for each network layer
- Outfit critical edge systems with redundant intra-chassis components
    - Processor, power, fans, line cards, switch matrix
- Incorporate load sharing when possible
- Measure and evaluate improvements
- Keep user perspective

Recommended Reading

High Availability Network Fundamentals
ISBN: 1587130173

Data Center Fundamentals
ISBN: 1587050234
Available in Sept 2003



Available Onsite at the Cisco Company Store

Reference Materials

- High Availability in Routing
  http://www.cisco.com/en/US/partner/about/ac123/ac147/current_issue/high_availability_routing.html
- Disaster Recovery Best Practices
  http://www.cisco.com/en/US/partner/tech/tk869/tk769/technologies_white_paper09186a008014f92e.shtml
- Measuring High Availability in Cisco LAN network
  http://www.cisco.com/application/pdf/en/us/guest/tech/tk769/c1550/cdccont_0900aecd800b29ac.pdf
- Network Management Best Practices
  http://www.cisco.com/application/pdf/en/us/guest/tech/tk769/c1550/cdccont_0900aecd800b29ac.pdf
- Baseline Processes Best Practices
  http://www.cisco.com/en/US/partner/tech/tk869/tk769/technologies_white_paper09186a008014fb3b.shtml
- Measuring Delay, Jitter and Packet Loss
  http://www.cisco.com/en/US/partner/tech/tk869/tk769/technologies_white_paper09186a00801b1a1e.shtml

Associated Sessions

- NMS-2102: Deploying and Trouble-shooting NAT
- NMS-2201: Network Availability Measurement
- NMS-2306: Disaster Recovery and Geographic Load Balancing
- OPT- 2043: 802.17 and Spatial Reuse Protocol (SRP) Protocols
- RST-2311: Packet forwarding and Operation of Mid to High-End Routers and Switches
- RST-2312: Control Plane Operation of Mid to High-End Routers and Switches
- RST-2505: Campus Design Fundamentals
- RST-2514: High Availability in Campus Network Deployments
- RST-2603: Deploying MPLS Traffic Engineering
- RST- 4312: High Availability in Routing
- SEC- 2011: Deploying Site-to-Site IPSec VPNs

Appendix A: Acronyms 1

- AVG: Active Virtual Gateway (in GLBP)
- AVF: Active Virtual Forwarder (in GLBP)
- ADM: Add/ Drop Multiplexer
- APS: Automatic Protection Switching
- ATM: Asynchronous Transfer Mode
- CSM: Content Switching Module
- CSS: Content Services Switch
- DPT: Dynamic Packet Transport
- DWDM: Dense Wave Division Multiplexing
- FIB: Forwarding Information Base (Forwarding Table)
- FRR: Fast Re-Route
- GE: Gigabit Ethernet
- GLBP: Gateway Load Balancing Protocol
- GR: Graceful Restart
- GSS: Global Site Selector
- HA: High Availability
- HDLC: High Level Data Link Control
- HSRP: Hot Standby Routing Protocol
- IKE: Internet Key Exchange
- LC: Line Card
- LSP: Link State Path
- MAC: Media Access Control
- MARP: Multi-Access Reachability Protocol
- MIB: Management Information Base
- MLPPP: Multi-Link PPP
- MPLS: Multi-Protocol Label Switching
- MTBF: Mean Time Between Failure

Appendix A: Acronyms 2

- MTTR: Mean Time to Repair
- NAT: Network Address Translation
- NIC: Network Interface Card
- NSF: Non Stop Forwarding
- PAT: Port Address Translation
- PAgP: Port Aggregation Protocol
- PPP: Point to Point Protocol
- PVF: Primary Virtual Forwarder (in GLBP)
- RIB: Routing Information Base (Routing Table)
- RFC: Request For Comments
- RPR: Resilient Packet Ring (L1/L2 Resiliency Technology)
- RPR, RPR+: Cisco’s Route Processor Redundancy (Device Resiliency)
- RP: Route Processor
- RRI: Reverse Route Injection
- RU: Rack Unit
- SLB: Server Load Balancing
- sNAT: Stateful Network Address Translation
- SNMP: Simple Network Management Protocol
- SPF: Single Point of Failure: Shortest Path First (in routing protocols)
- SSO: Stateful Switch Over
- SSP: State Synchronization Protocol
- SVF: Secondary Virtual Forwarder (in GLBP)
- TCP: Transmission Control Protocol
- UDLD: Unidirectional Link Detection Protocol

Appendix A: Acronyms 3

- VF: Virtual Forwarder (in GLBP)
- vIP: Virtual IP Address
- VPN: Virtual Private Network
- VRRP: Virtual Router Redundancy Protocol

Q & A

Complete Your Online Session Evaluation!

Cisco.com

WHAT: Complete an online session evaluation and your name will be entered into a daily drawing

WHY: Win fabulous prizes! Give us your feedback!

WHERE: Go to the Internet stations located throughout the Convention Center

HOW: Winners will be posted on the onsite Networkers Website; four winners per day

CISCO SYSTEMS