cisco

TOMORROW
starts here.

Cisco Connect

Data Center Disaster Recovery

Customer Case Study

Nadir Lakhani

Systems Engineer

Jim Robshaw

Director IS

House Keeping Notes

Thank you for attending Cisco Connect Toronto 2014, here are a few housekeeping notes to ensure we all enjoy the session today.

- Please ensure your cellphones are set on silent to ensure no one is disturbed during the session
- Please hold all questions until the end of these session to ensure all material is covered

Complete Your Paper Session Evaluation

Give us your feedback and you could win 1 of 2 fabulous prizes in a random draw.

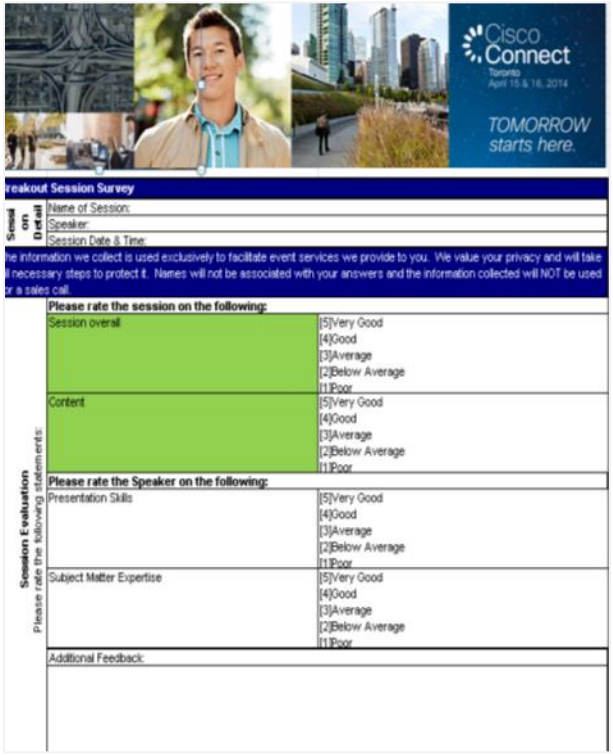
Complete and return your paper evaluation form to the Room Attendant at the end of the session.

Winners will be announced today at the end of the session. *You must be present to win!*

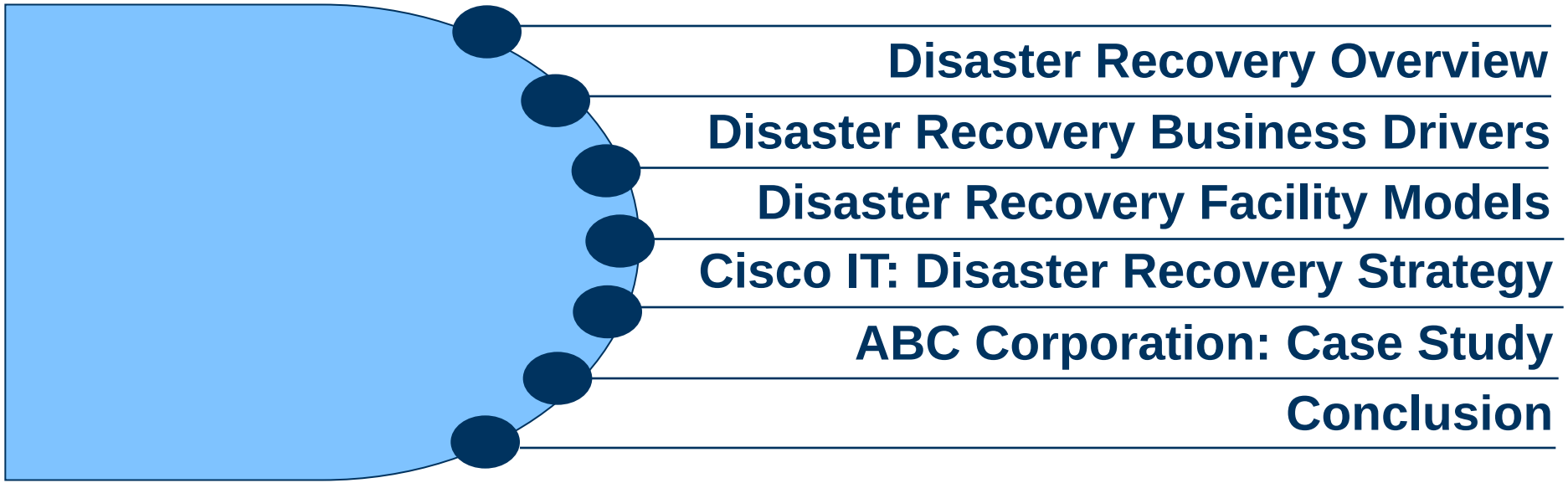
Please visit the Concierge desk to pick up your prize redemption slip.

plantronics

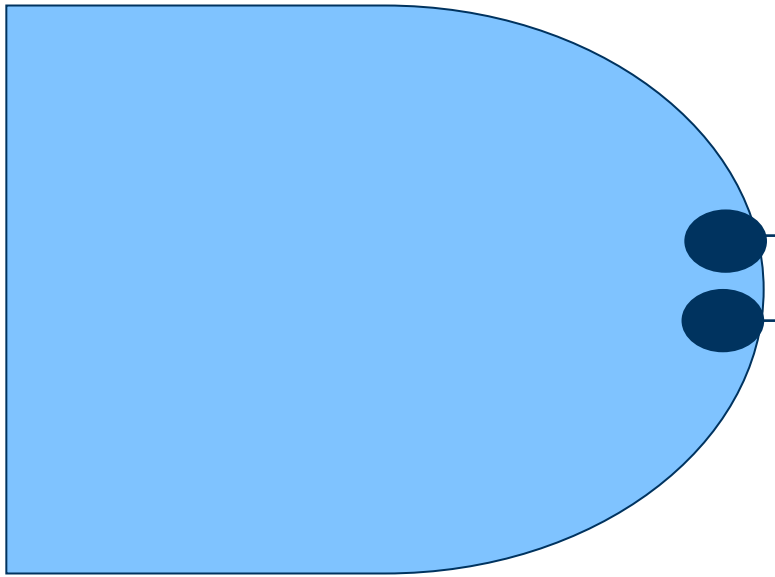
Visit them at BOOTH# 407



AGENDA



AGENDA



Disaster Recovery Overview

What is Disaster Recovery ?

Disaster Recovery (DR) is the process, policies and procedures that are related to preparing for recovery of technology infrastructure which are vital to an organization’s business continuation after a natural or human-induced disaster.

Disaster Recovery focuses on the IT or Technology Systems that support business functions, and involves planning for keeping all aspects of a business functions in the midst of disruptive events.

Disaster Recovery vs. High Availability

Disaster Recovery

- Addresses service continuity, so that in case of disaster, service is maintained through a standby geographically isolated site.
- Two independent environments, typically in separate and distinct facilities, each contain their own data (in the file system and database) and executable.
- Data and configuration information are replicated between the production and standby sites.

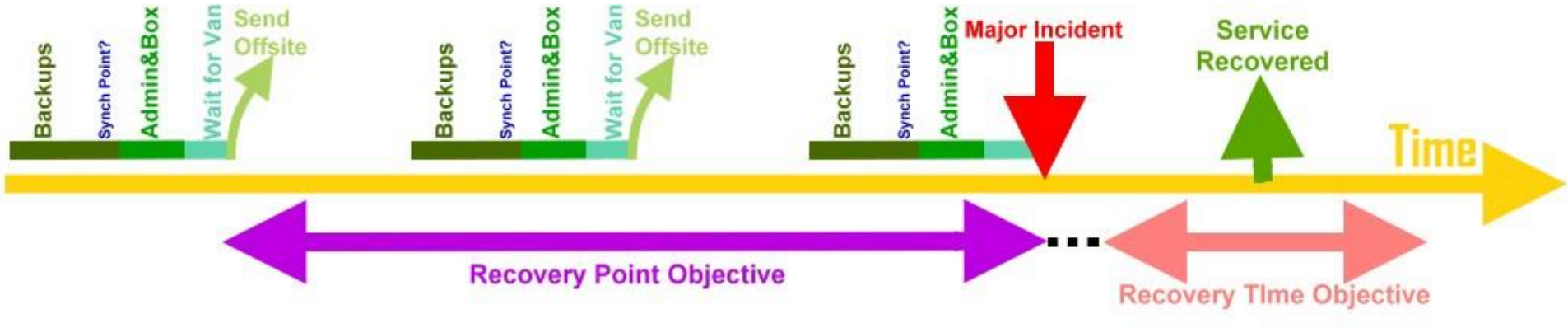
High Availability

- Addresses service availability, providing redundancy so that if one infrastructure component (network, servers, processes) becomes unavailable, overall service remains available locally within the site.
- A single system contains its own data (in the file system and database) and executable.
- Data replication is unnecessary (although data should be backed up).

Why Disaster Recovery ?

- The primary objective of a disaster recovery is to minimize downtime and data loss in the event of the failure of an active site.

- Minimizing downtime and data loss is measured in terms of two concepts: the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO).

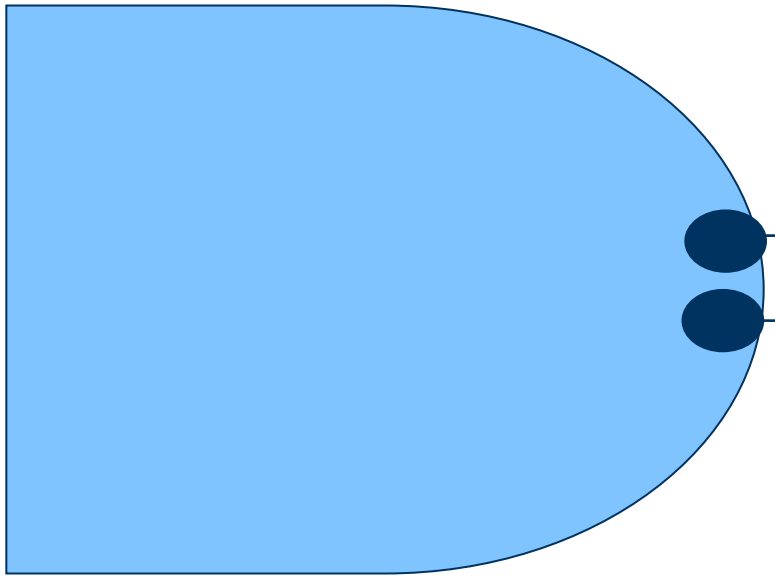


Recovery Time Objective / Recovery Point Objective

- Recovery time objective (RTO) is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels.

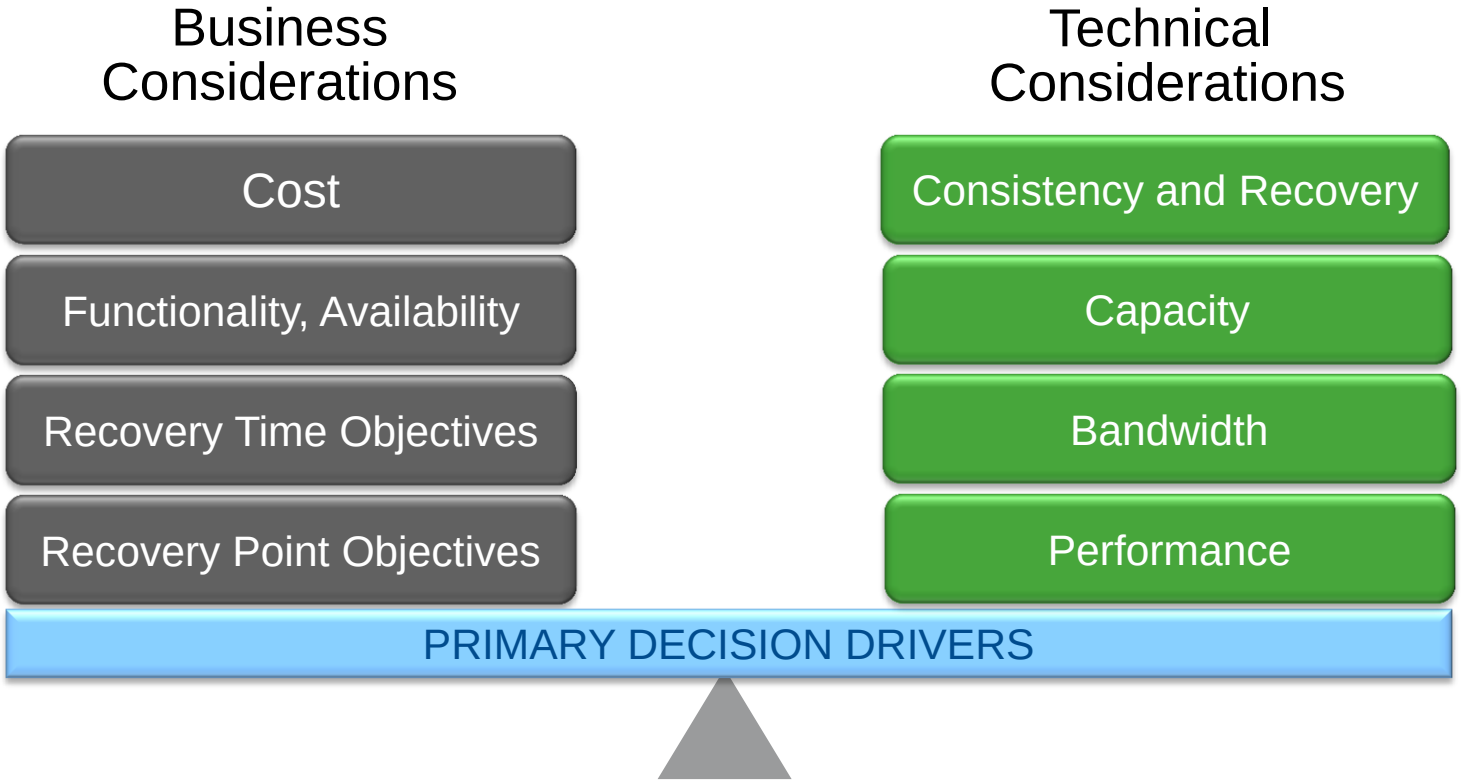
- A recovery point objective (RPO) is the maximum acceptable amount of data loss during the outage time. It is the delta of the data in storage & backup required to synchronize normal operation of systems.

AGENDA



Disaster Recovery Business Drivers

Disaster Recovery Decision Drivers



Disaster Recovery Importance for Main Stream Verticals

Business Type

- Large Enterprises
- Corporation
- SMB

Verticals

- Healthcare
- Utilities
- K-12
- Financials
- Airline
- Retails
- Manufacturing

Business Revenue Sensitivity

- Financials/Banking
- Retails
- Manufacturing

Disaster Recovery Importance for Main Stream Verticals

Business Type

- Large Enterprises
- Corporation
- SMB

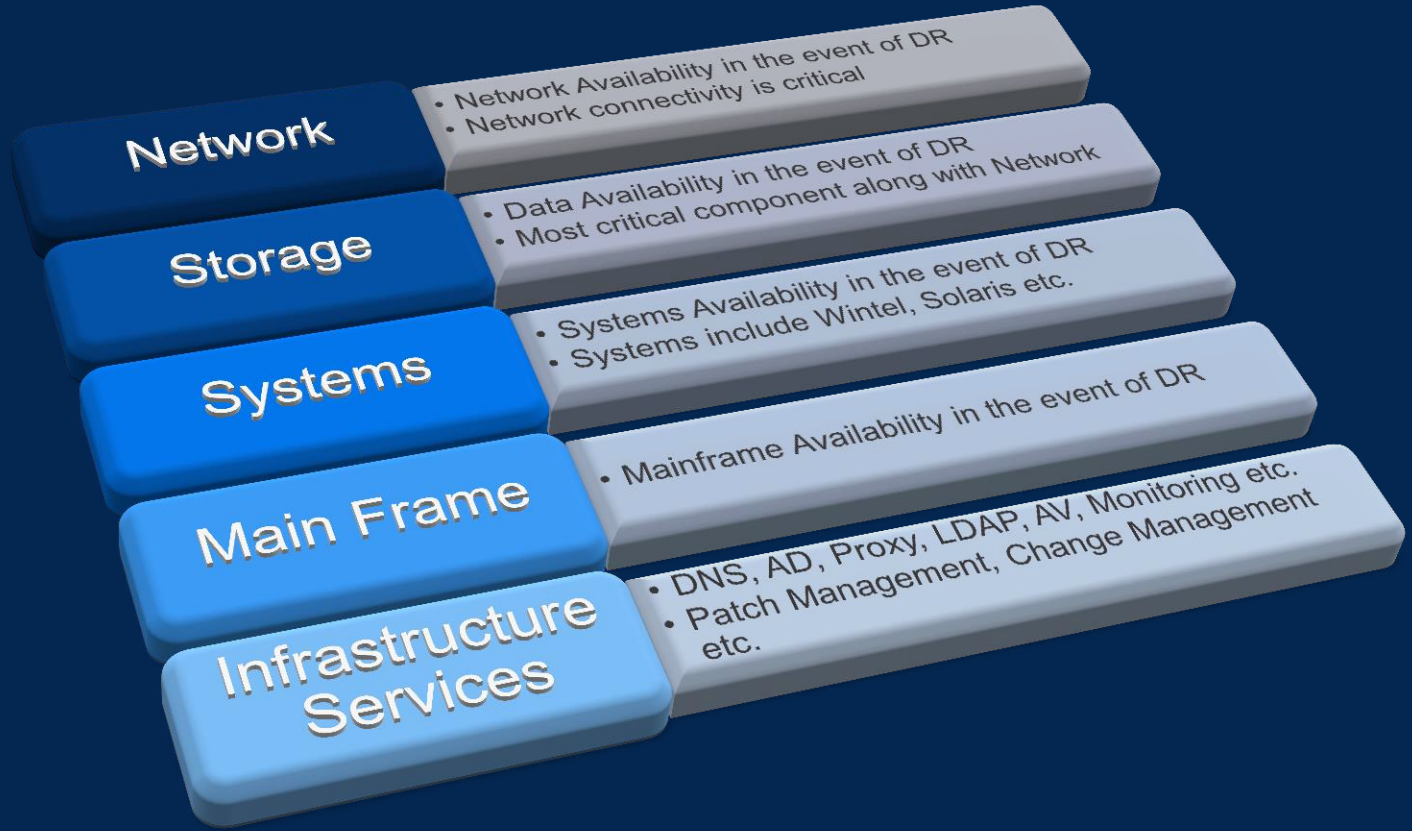
Verticals

- Healthcare
- Utilities
- K-12
- Financials
- Airline
- Retails
- Manufacturing

Business Revenue Sensitivity

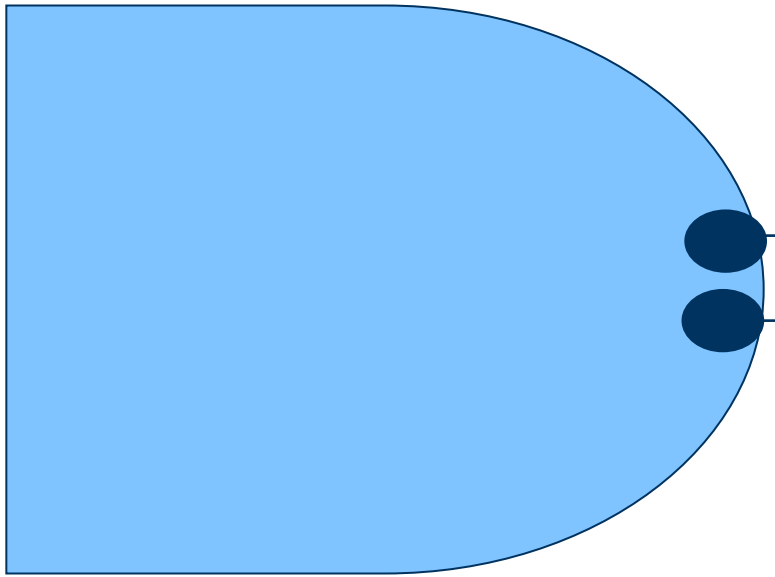
- Financials/Banking
- Retails
- Manufacturing

Disaster Recovery: Technology Snapshot



This presentation is focused on Network Disaster Recovery

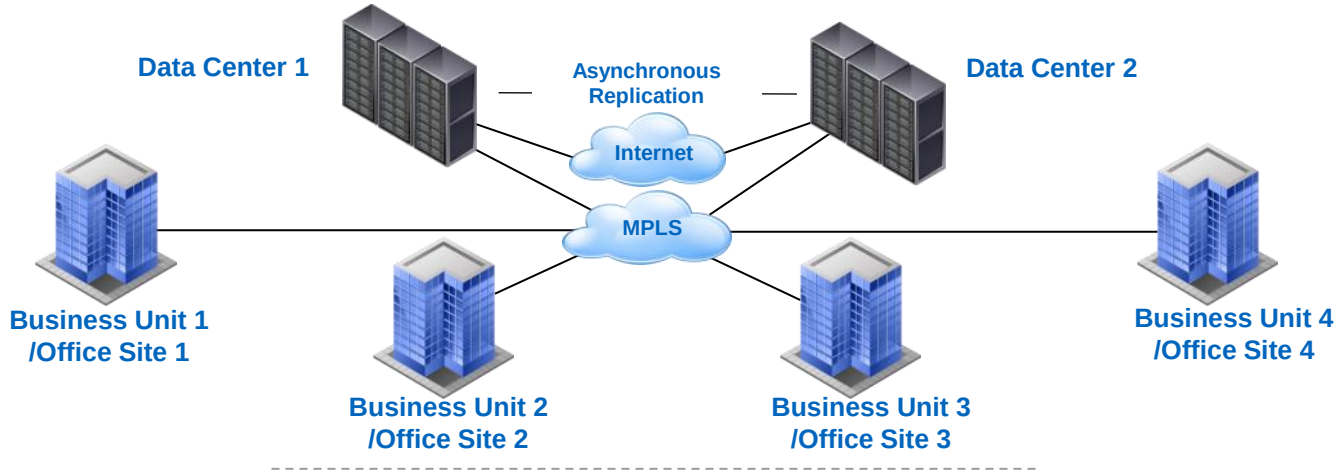
AGENDA



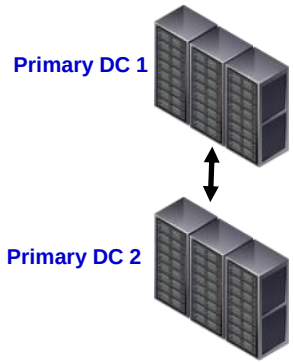
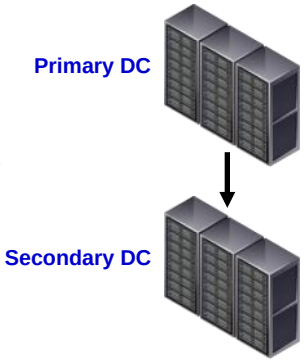
Disaster Recovery Facility Models

DR Facility Model: Two Date Center Sites

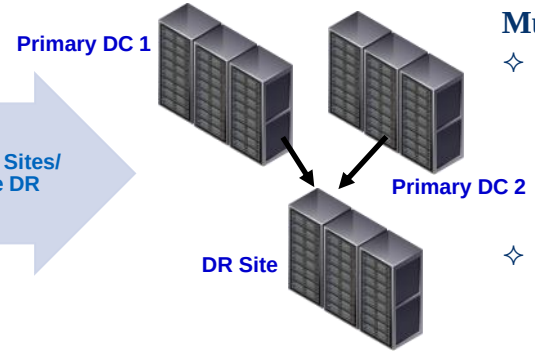
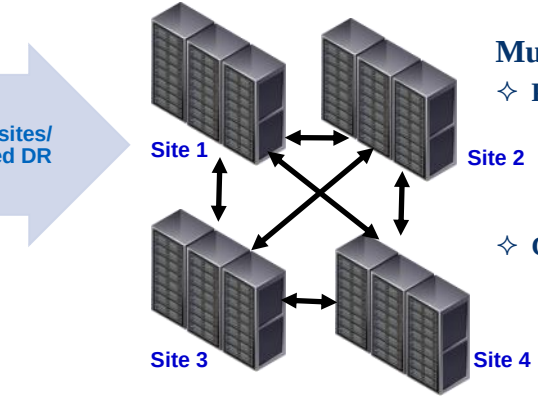
Base IT Facility Model



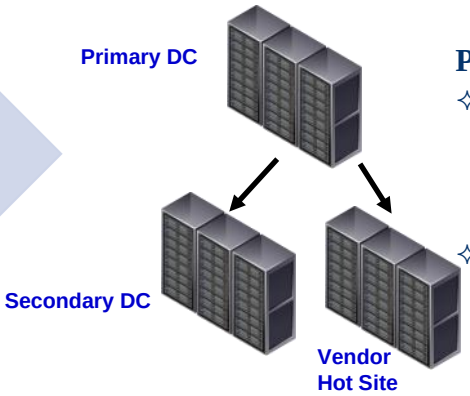
DR Facility Models

Model	Illustration	Description
Primary/ Primary (50/50)		**Two internal facilities with production balanced between both sites** ✧ **PROS: -** ✧ Full control of IT assets ✧ Reduced site loss impact (e.g. outage to only 50% of production) ✧ Support of site load-balancing for higher availability ✧ **CONS: -** ✧ Highest change management risk during DR testing ✧ Greater complexity for network infrastructure and application designs
Primary/ Secondary		**Two internal facilities with production in the primary and DR in the secondary** ✧ **PROS: -** ✧ Full control of IT assets ✧ Flexible DR test scheduling ✧ Less complex fail-over to DR ✧ Low risk of production impact during DR testing ✧ **CONS: -** ✧ Highest cost (e.g. requires more bandwidth and storage for replication ✧ Highest outage impact with all production in a single site Note: Development and testing environments can be run from secondary site

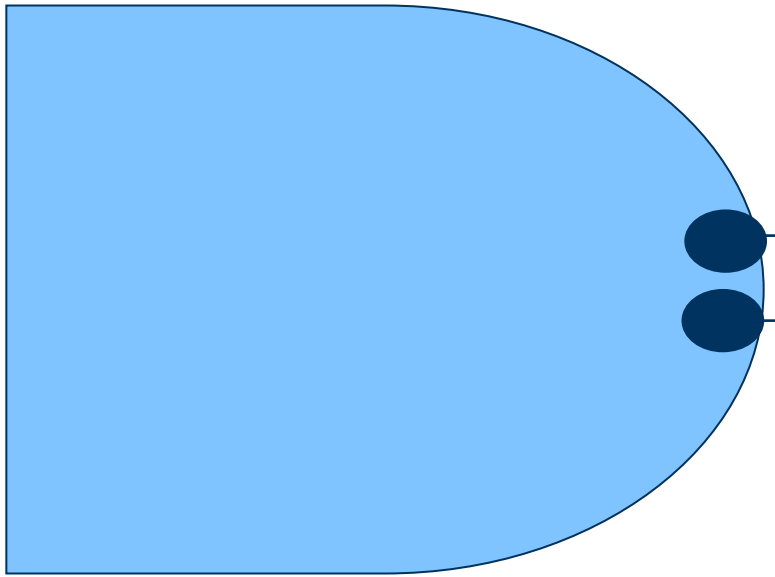
DR Facility Models

Model	Illustration	Description
Multiple Sites/ Single DR		**Multiple internal production sites with a single DR site for largest production site** ✧ **PROS: -** ✧ Full control of IT assets with all internal sites ✧ Maximize DR install and test flexibility by leveraging single DR site ✧ Simplified DR network and storage infrastructure with a single DR site ✧ Low risk of production impact during DR testing ✧ **CONS: -** ✧ Minimal use of DR site for normal operation. ✧ Only used in annual DR exercise. ✧ High cost (e.g. bandwidth and storage for one-way replication)
Multiple sites/ Integrated DR		**Multiple internal production sites with a DR services integrated between site** ✧ **PROS: -** ✧ Full control of IT assets with all internal sites ✧ Reduced site loss impact (e.g. outage to only 25% of production) ✧ Support of multi-site load-balancing for highest availability ✧ **CONS: -** ✧ Highest change management risk during DR testing ✧ Most complex model for infrastructure design and support

DR Facility Models

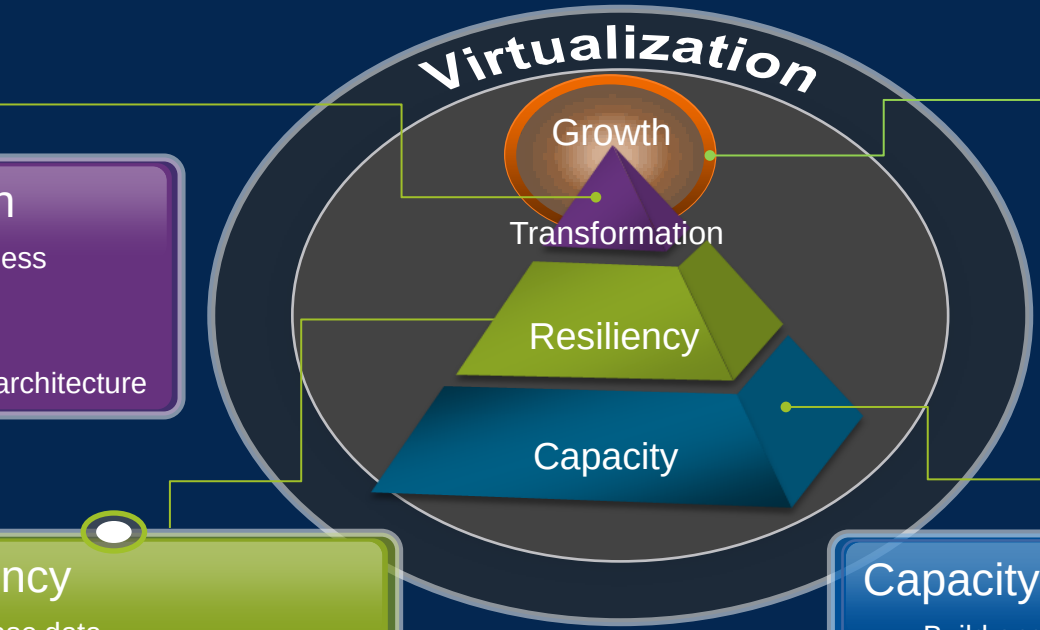
Model	Illustration	Description
Primary/ Hot Site		**One internal site for production and a vendor hot site for data recovery** ✧ **PROS: -** ✧ Lowest initial and ongoing data center facility costs ✧ IT staff augmentation available with hot site resources ✧ Data Center facilities support and equipment maintenance included ✧ Least impact to existing IT infrastructure and resources ✧ **CONS: -** ✧ Limited DR testing flexibility ✧ Limited post disaster occupancy period (e.g. can not be a permanent site) ✧ Possible 1st come, 1st server guarantee issues for preferred vendor location
Primary/ Hybrid		**Production site and two DR sites; internal for replication, hot site for lower priority** ✧ **PROS: -** ✧ Less cost then larger second internal sites for DR ✧ Flexibility to install and test DR for critical applications ✧ DR for Lower priority applications provided at lower price point ✧ **CONS: -** ✧ Greater technical support effort with two DR sites ✧ Increased IT Management and administration effort with two DR sites

AGENDA



Cisco IT: Disaster Recovery Strategy

Global Data Center Strategy



Transformation

- Run IT as a business
- Internal service provider model
- Service-oriented architecture

Growth Enablement

- New markets and business models
- Global expansion
- User experience

Resiliency

- Increase data center tiers
- Multi-site architecture
- Move out of high risk geographies

Capacity

- Build and occupy data centers
- Optimize demand
- Consolidate where appropriate

DC 3.0 – A Transformational Journey

Location Freedom

HW Freedom

Provisioning Freedom

Business Process Freedom

Consolidation

Virtualization

Automation

Utility

Market

Inter-Cloud

Enterprise-Class Clouds

Unified Computing

Unified Fabric

Data Center Networking

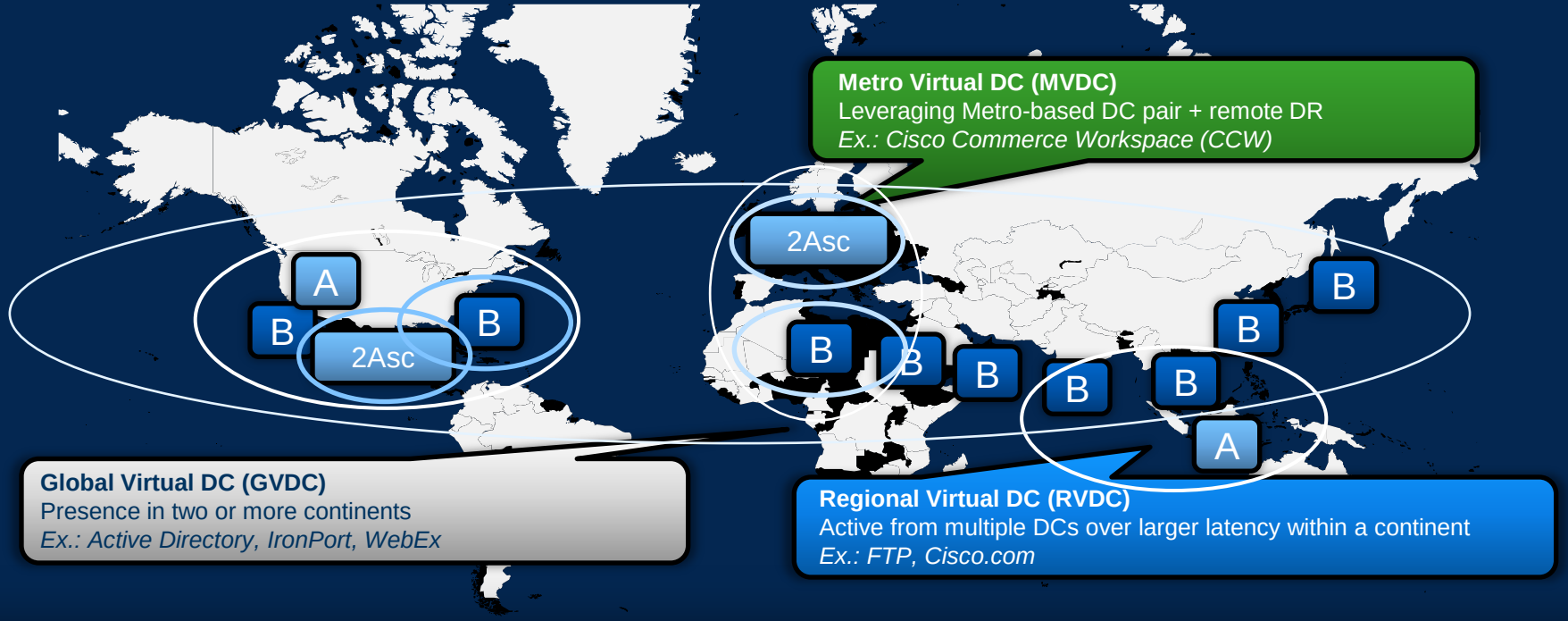
GDCP

DeVirt

Cisco IT Elastic Infrastructure Service

Global Data Center Presence—Target State

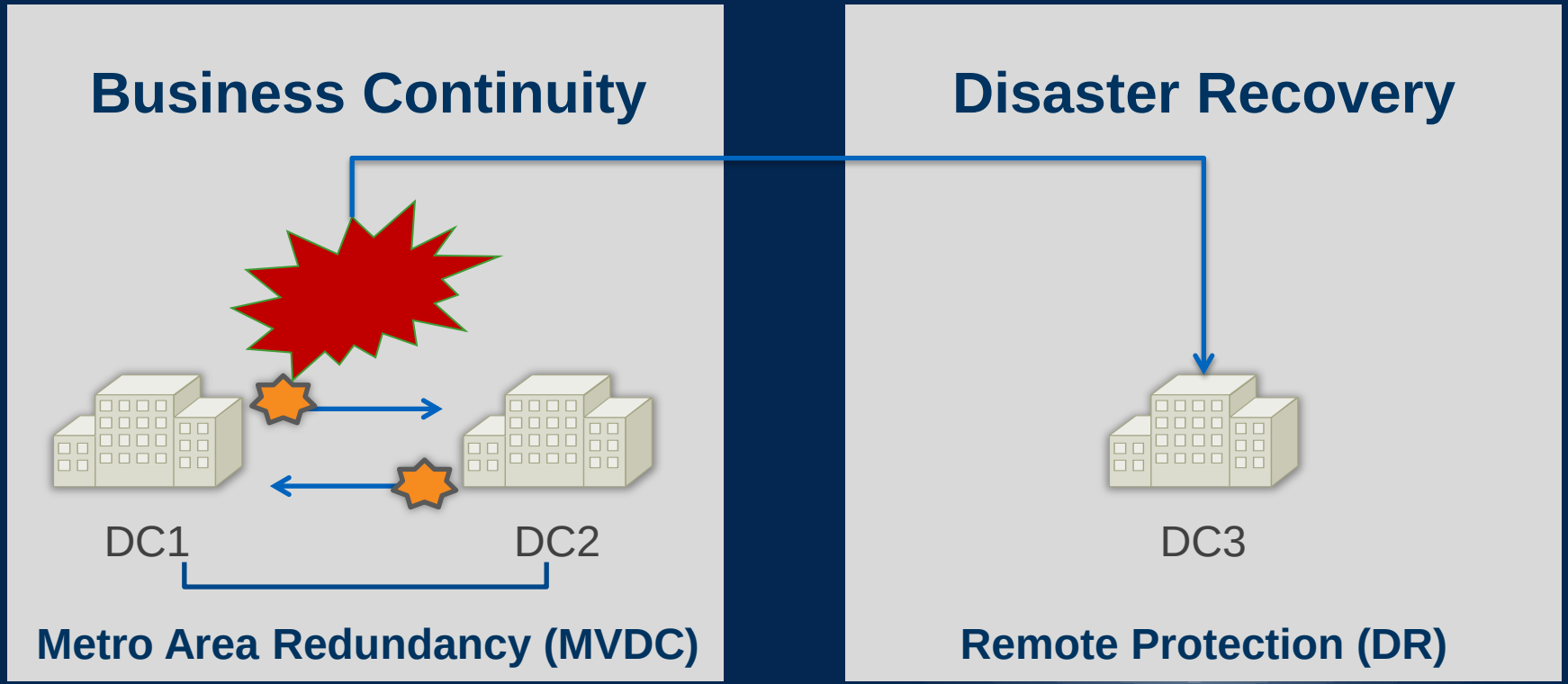
Shared Resilient Infrastructure Enables Diversified Business Growth



Distributed Virtual Data Center (DVDC) Architecture

Three Variations Reflecting Varying Latency Constraints and Performance Requirements

Resiliency Strategy

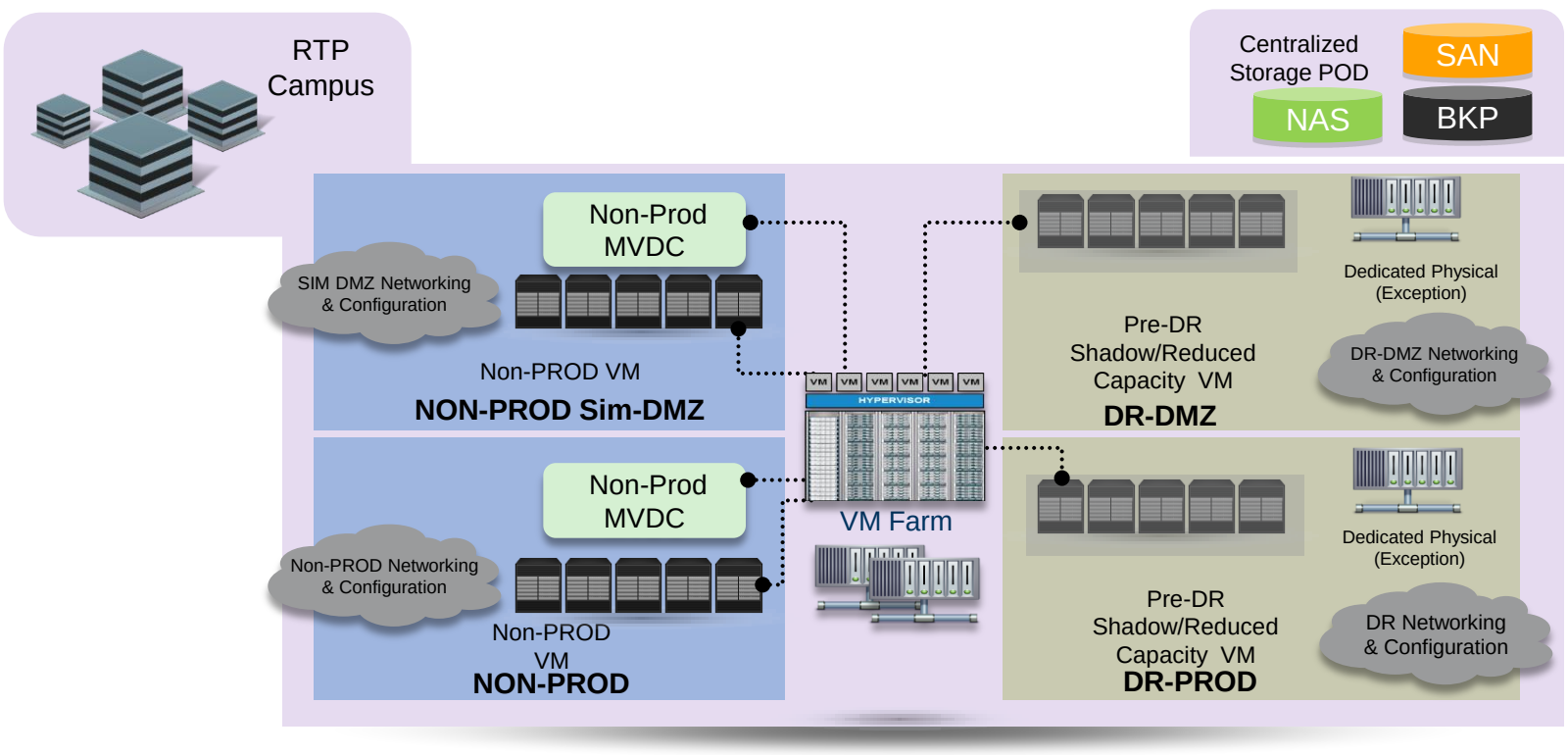


DR Strategy Key Tenets

- Make DR prioritization less prohibitive
- Drive cost efficiencies through reuse of infrastructure and processes
- Integrate DR into day to day operations
- Make capacity growth sustainable through repurposed infrastructure and shared resources leveraging virtualization

Disaster Recovery Architecture

Virtual Routing and Forwarding and Virtualization for Re-Purpose Based DR



Disaster Recovery Drives Transformation

Existing Capabilities

Metro level protection for applications

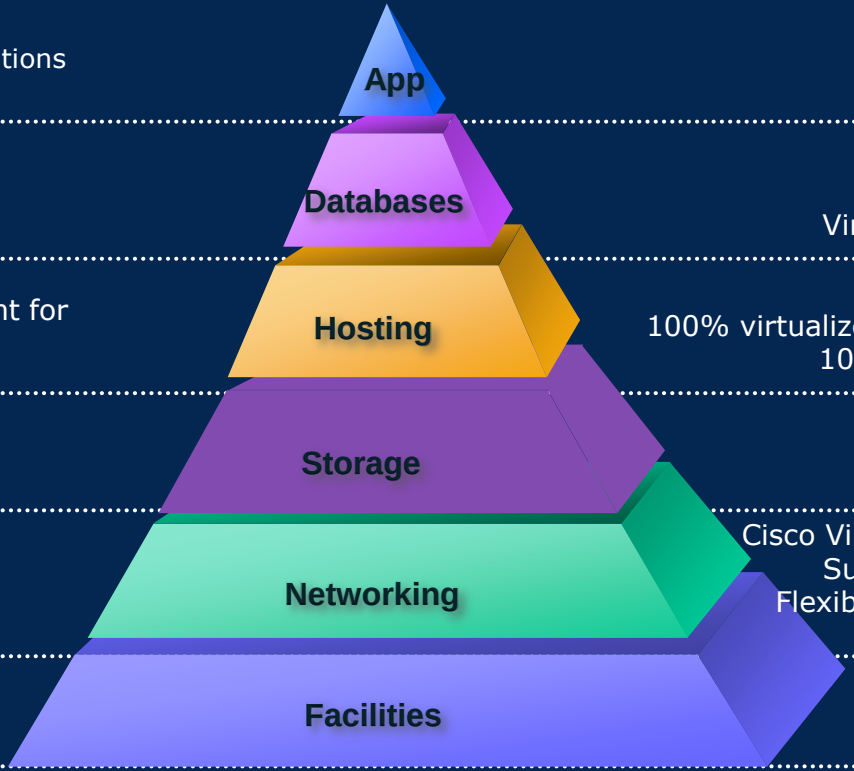
Oracle RAC with Data Guard
Standalone DB Virtualization

Physical and virtual environment for Non-Prod

SAN and NAS Pools

Multiple Physical PODS
Physical network segregation

Tier II DC



New Capabilities

Regional level protection for applications and services

Oracle Data Guard with
Async Replication (A-P-P)
Virtualization of RAC databases

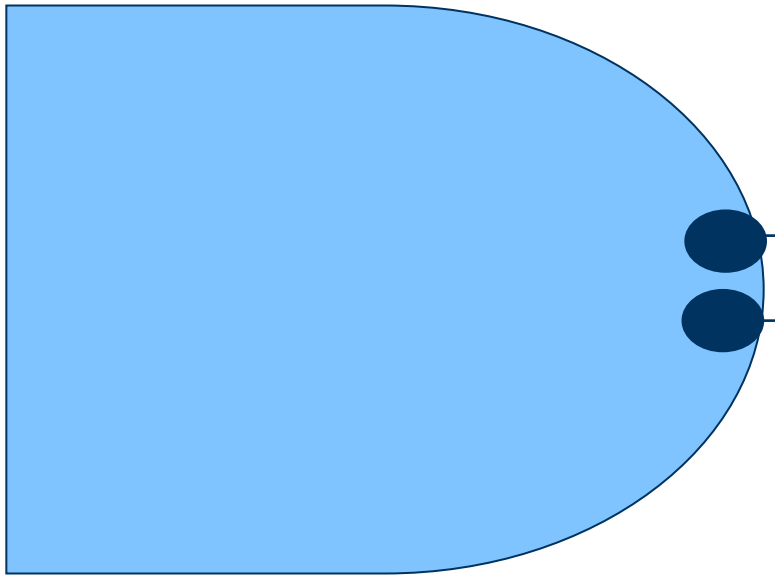
Repurpose Capacity for DR
100% virtualized environment for Non-Prod
100% UCS hosted environment

Centralized storage POD
SAN snapshot for refresh

Cisco Virtual Routing and Forwarding
Super POD – Greater Efficiency
Flexible host migration to different security zones

Tier II Data Center
Hardened Facility

AGENDA



ABC Corporation: Case Study

ABC Corporation: Overview

- ABC Corporation Size: 2000 Employees, 10 Office Location, 2 DCs
- ABC Corporation Vertical: Transportation
- ABC Corporation Revenue: 3 Billion
- ABC Corporation IT Budget: 60 Million/Year (2%)
- ABC Corporation Revenue Sensitivity: HIGH

ABC Corporation: Network DR Design

1. Overview

Objectives, Assumptions, Current State

2. DR-Network Design Requirements

Guiding Principles, NAD, WAN Link Analysis, Network DR requirements List

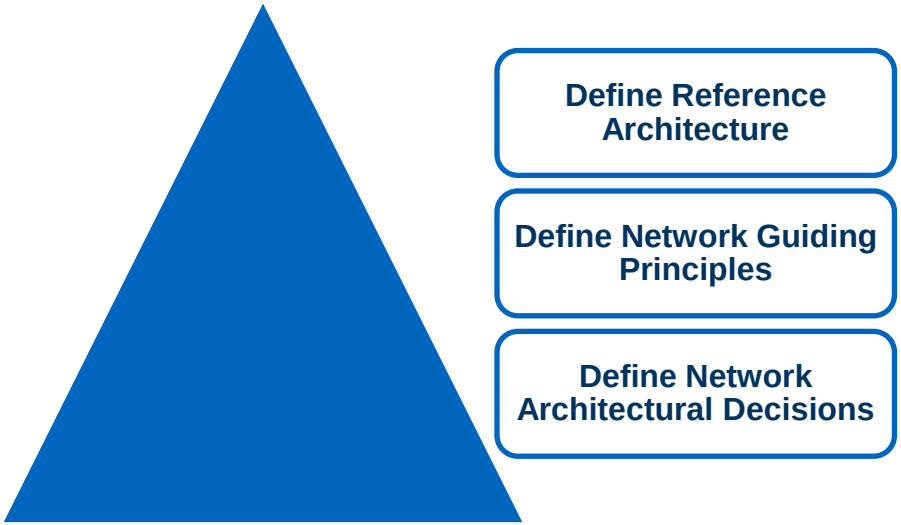
3. DR-Network Design

Proposed LAN/ WAN/ DCI Design & Recommendation

1. ABC Corporation Overview: Objectives

Full DC-1 failure: All production to be recovered in DC-2:

- Design DR Network Solutions for the recovery of ABC Corporation's Production systems running in Site-1 to Site-2 in the event of a full Site-1 data center failure.



1. ABC Corporation Overview: Assumptions

See Reference Architecture Diagram for Reference:

- Used average peak utilization for GigaMAN, MIS, EVPN and DCI for DR WAN sizing requirements
- Future State 2x1GE (Premium 1GE circuit with 500M CDR) connection to AWS in DC-1 will be backed up by VPN tunnel in DR Site. 20% of 500M CDR has been assumed for DR design MIS sizing
- This DR design provides Connectivity/Access to external vendor clouds (AWS) for DR Event support.
- Dual Data Center Application Model Assumptions. Current model in use is Primary/Secondary with Active/Active components in Secondary site.
- All Extranet/B2B connections are via internet using VPN tunnels
- No Assumption for Routers, switches, firewalls, IPS, LBs (Virtualization Compliant)
- DR Testing will be performed using controlled network access to the DR site i.e. DR-Lab and pre-defined WAN test cases

1. ABC Corporation Overview: Current State

i – Current State (Findings) for LAN:

- Recover existing production DC-1-IP Addresses for DR in DC-2
- Active-Active for some applications i.e. DC-1/DC-2: Email, AD

ii - Current State (Findings) for WAN

- Current State: WAN Components
  - DC-1 Data Center has 4-Paths to the rest of the ABC Network
- AWS Cloud Connectivity are VPN tunnels: from DC-1 for production and from DC-2 for development on existing MIS-DS3 circuits

iii. Current State (Findings) for DCI *DCI= Data Center Interconnect

- 2 x OC-12s between DC-1 – DC-2

1. ABC Corp. Overview: Alternate Routing Scenarios

- Alternate Routing Scenarios can be configured as follows (Refer to figure 2):
  - Internet (MIS) Failure → DNS redirect. All traffic comes to DC-2 and over EVPN to DC-1
  - DC-1-EVPN Failure → DCI as alternative. All Traffic traverses GigaMAN to DC-1
  - GigaMAN failure → All traffic comes to DC-1 via EVPN as backup, controlled by BGP
  - DCI failure → All traffic traverses via EVPN to DC-2
  - Some additional configuration required for alternate routing

2. ABC Corporation: DR-Network Design Requirements

a. Network Guiding Principles (NGPs)

- LAN Guiding Principles (Core, Distribution, Access, Firewalls, IPS, LB)
- WAN Guiding Principles (internet, Intranet, DCI)

b. Network Architectural Decisions (NADs)

- LAN Architectural Decisions (Core, Distribution, Access, Firewalls, IPS, LB)
- WAN Architectural Decisions (MIS, EVPN)
- DCI Architectural Decisions

c. WAN Link Analysis

- MIS (internet) Link Analysis
  - Utilization, Sizing, Costing, Recommendation
- EVPN (Intranet) Link Analysis
  - Utilization, Sizing, Costing, Recommendation
- DCI (Data Center Interconnect) Link Analysis
  - Utilization, Sizing, Costing, Recommendation

2. ABC Corporation: Network Guiding Principles (NGPs)

NGP#1 Applications have hard-coded IP Addresses.

NGP#2 Leverage the existing Network architecture and equipment at DC-2 to reduce component costs.

NGP#3 Network Resilience for the DR environment should be equivalent to the production systems i.e. Dual network devices, Dual Server NICs, dual HBAs per Server, Redundant IP connections etc.

NGP#4 DR Solutions should be scalable to accommodate new applications, technology and growth

NGP#5 The DR Site must have facility capacity to support build out of 100% and beyond

NGP#6 Cross data center active/active or active/passive solutions are considered for production systems and can be used in a DR event but should not be disrupted for DR testing because it could potentially corrupt data

NGP#7 The external perimeter (internet) and internal perimeter (intranet) firewall devices MUST be from different security vendors, i.e. Use Cisco ASA 5520 for internet and Checkpoint FCS-20s for intranet

2. ABC Corporation: Network Architectural Decisions (NADs)

NAD # 1 DR-Fence will be required at DC-2. It will provide isolation from production during DR testing and support Recovery of application of hard-coded IP addresses.

NAD # 2 Isolated DR network (a.k.a. DR Fence) will utilize virtualization for all components i.e. Routers, Switches, Firewall, IPS, LB.

NAD # 3 ISP-1 Retail to procure and implement DR Fence Convergence firewalls ASA-5520 for the DR Normal State Fence Solution.
ISP-1 wholesale to implement a 4 GE ether-channel (8-ports) connectivity for the DR Event Convergence solution.

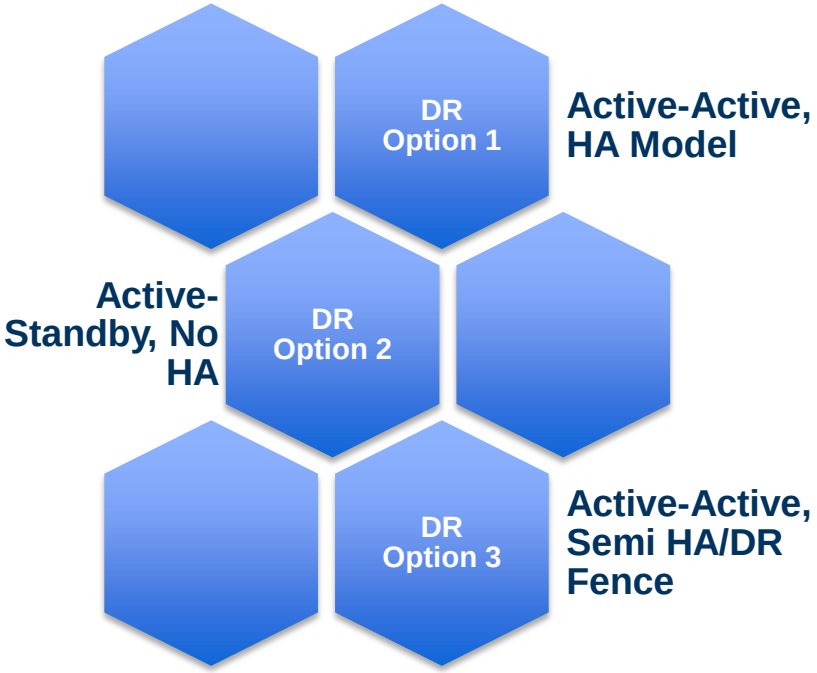
NAD # 4 ISP-1 Retail to replace the DC-2 MIS/EVPN links from 2-DS3 to 2-OC3 to support combined ISP bandwidth from DC-1 & DC-2 in a DR Event

NAD # 5 ISP-1 Retail to replace the HQ & HQ EVPN links from 1-DS3 to 1-OC3 to provide production system support by developers in a DR event

NAD # 6 ISP-1 Wholesale to replace the DC-2 DCI links from 2-OC12 to 3-OC12s using existing DCI design to support additional replication bandwidth requirements

DR Options Presented

- Based on the Reference Architecture, Business Requirements, and Budget Analysis following three DR options were presented to the customer.



DR Option 1 – Details

Two sites, internally (owned) facilities with production balanced between both sites.

Normal State
Site-1 = ACTIVE (DC 1 – IP)
Site-2 = ACTIVE (DC 2 – IP)
External traffic shared to both sites
Intranet traffic shared to both sites

DR Event State
Site-1 = DOWN
Site-2 = ACTIVE (DC 2 – IP)
All external traffic goes through Site-2
All internal traffic goes through Site-2

DR Option 2 – Details

Two sites, internal facilities with production in the primary and DR in the secondary

Normal State	
	Site-1 = ACTIVE (DC 1 – IP)
	Site-2 = STANDBY-DR (DC 2 – IP)
	All external traffic goes through Site-1
	All intranet traffic goes through Site-1

DR Event State	
	Site-1 = DOWN
	Site-2 = ACTIVE (DC 2 – IP)
	All external traffic goes through Site-2
	All internal traffic goes through Site-2

DR Option 3 – Details

Two sites, internal facilities with production in the primary and DR in the secondary

Normal State	Site-1 = ACTIVE (DC 1 – IP)
	Site-2 = DR (DC 1 - IP, DOWN) + ACTIVE (DC 2 – IP)
	All external traffic goes through Site-1
	All intranet traffic goes through Site-1

DR Event State	Site-1 = DOWN
	Site-2 = DR (DC 1 - IP, ACTIVE) + ACTIVE (DC 2 – IP)
	All traffic goes through Site-2 in the DR event
	Only critical applications

ABC Corp. Overview: DR Network Recommendations

- For the Isolated DR Network, LAN Virtualization Option-1
  - ✧ Option-1: Most Expensive: A duplicate DR environment with a separate address space in DC-2.
  - ✧ Option-2: Middle price: Dedicated Core and access switches at DR in DC-2.
  - ✧ Option-3: Cheapest: Virtualize all Access, Core, Distribution.

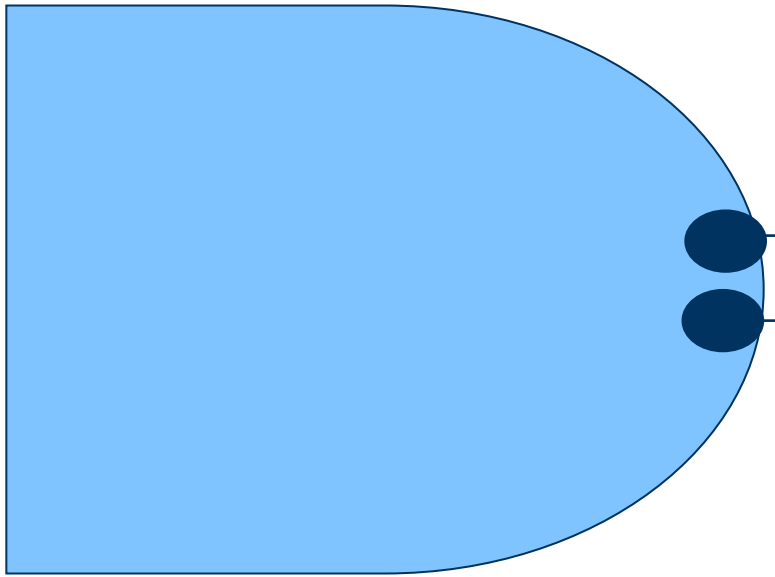
- Increase Link Bandwidths for MIS, EVPN, DCI at DC-2
  - ✧ Increase the DCI bandwidth with an added OC-12 to provision for additional data replication requirements.
    - ✓ Implement PBR and QoS to prioritize replication traffic
  - ✧ Increase EVPN (Intranet) bandwidth at DC-2, HQ1 and HQ2 by replacing DS3s with OC3s to provision for DR-Event intranet traffic
  - ✧ Increase the MIS (internet) bandwidth by replacing the 2-DS3s with 2-OC3s with CDR to provision for DR-Event internet traffic
    - ✓ Use VPN Tunnel from DC-2 to the production Cloud at AWS as a backup to the 500 Mbps (2x1GE planned connection) at DC-1

Proposed DR Network Design

a. Proposed LAN Design

- Isolated DR network: The “DR Fence”
  - Virtualize Layer-2/3 components i.e. Firewalls (internet, intranet, restricted zones), IPS, LB (Fig-1)
  - Create DR-DC-1 VRF in Core, Distribution, ID and SD switches
  - For access L2 switches, create DR-DC-1 VLANs and trunk to dist. Switch
  - Virtualize existing DC-2 Firewalls and add DR-DC-1 context firewalls
  - Virtualize existing IPS
  - Virtualize existing Load balancers
- DR Convergence Point: Normal State Solution (Fig-3,4)
  - Add new Firewall pair in DR-Fence to isolate DR-network from production DC-2 network
- DR Convergence Point: Event State Solution (Fig-4)
  - In DC-2 Core switch, use dedicated layer-3 ports with DC-1-address space for DR VRF to be used for manual convergence in the case of DR event
  - Use static routing to switch DR event traffic to DR-DC-1-VRF for convergence

AGENDA



Conclusion


CISCO
TM