

Pieter Schutte - Senior Technical Mainframe Specialist
18 February 2013














Smarter systems for a smarter planet:

System z[®] Forum

Secure and resilient cloud computing
for the modern enterprise

**Linux on System z Disaster Recovery
the BNZ Way**

AGENDA

-  Bank of New Zealand
-  DRP and BCP functions a closely coupled process
-  Considerations for Disaster Recovery
-  Types of disasters
-  Major discussion points
-  Customer Requirements
-  Infrastructure DR
-  Steps we follow for DR
-  Live DR
-  Summary and Learning
-  Questions

Bank of New Zealand

The National Australia Group



- Asset base of A\$685 Billion 2010
- Approximately A\$600 billion in assets under administration
- Ranked as the 17th largest bank in the world
- Represented across 4 continents and 10 countries
- Serving 9 Million consumers and business banking customers
- Over 2.3 Million wealth management customers



Bank of New Zealand

- Established 1861
- Employs 5,000+ staff
- 300+ IT Staff
- >2 million accounts
- Over 1 million customers
- ~100 retail banking products
- Acquired by NAB group in 1992
- 180 Retail stores and partner centres across NZ
- First Computer 1966 (an IBM 360/30 with 16k memory)
- Total assets 69 billion



**DRP and BCP functions a
closely coupled process**

Business Continuity Planning (BCP)

Business Continuity Planning (BCP)

Is an enterprise wide planning process used to create detailed procedures in the case of a disaster

BCP Plans take into account:

- Processes
- People
- Facilities
- Systems
- External elements which could affect an organisation to function

BCP objective

Maintain critical business processes in the event of an unplanned outage the scope of BCP involves the IT infrastructure

Disaster Recovery Planning (DRP)

Disaster Recovery Planning (DRP)

- Is an IT-centric logical subset of the BCP process
- Functions as a logical subset to the Business Continuity Planning (BCP) process
- DRP process ensures continuity of operations in the event of a wide variety of disaster scenarios
- IT operations handles DRP and BCP functions as a closely coupled Process
- Plan designed to restore operability of the target systems, applications, or computer facility at an alternate site
- May also include a significant focus on disaster prevention

Considerations for Disaster Recovery

Considerations for Disaster Recovery “DR”

Consider DR - Site

- DR- Hotsite
- DR - Warmsite
- DR - Coldsite
- Bare metal recovery
- High availability
- One active production site and one for DR
- Two active sites with production and test
- Borrowed resources for DR
- When will a DR be called

When will DR be called

Disaster Recovery is needed when?

- We are unable to continue working as per normal
- Main systems unavailable (not just production)
- Storage subsystems unavailable
- Communication infrastructure failed

Reasons for and impact of Disaster

Reasons for failures:

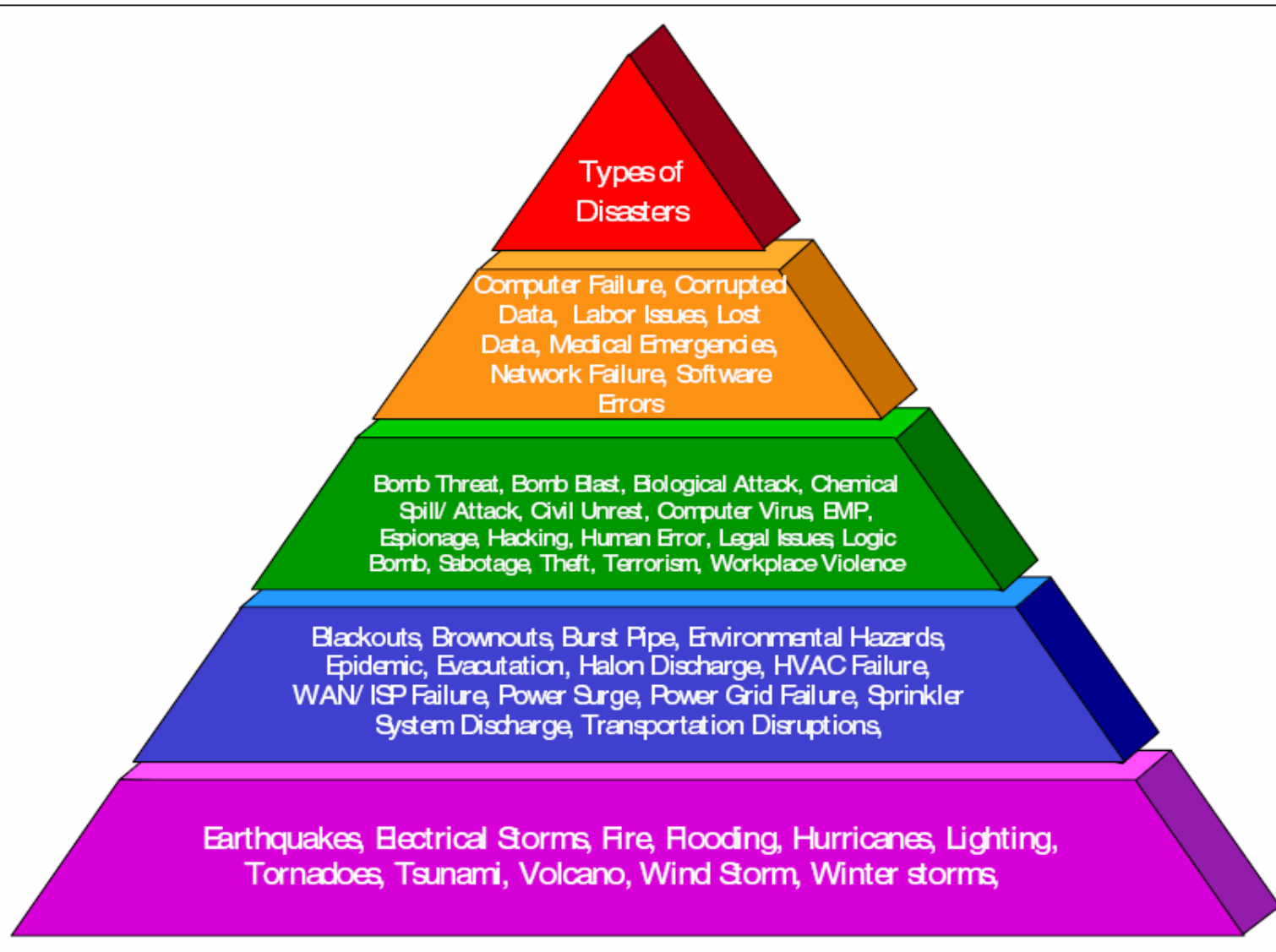
- Outage of power planed or unplanned
- Natural catastrophe (water, wind, earthquake ...)
- Technical failures
- Human error
- Hardware errors and outages
- Political (terror)

Impact:

- Inability to be productive - loss of money
- Once you are in DR this becomes your Production site
- Need to plan for a DR to switch back to Prime production site

Types of disasters

Types of disasters



Major discussion points

Major discussion points

Possible Systems affected

- Type of systems, relation, how many systems participate in the DR scenario

System positions - Geographically

- Distance between them for data mirroring

Connectivity and attachments

- Ability to replace each other w/o application/user adjustments

Separation of Data Stores

- Logical connected data should reside on same side

Network topology

- Types of networks to be interconnected

Operating Systems and application Landscape

- Application execution based on operating systems

Major discussion points (continued)

The Business impact analysis (BIA)
 IT Resource relation and priorities for DR
 Consider all environments
 Prioritise based on business importance

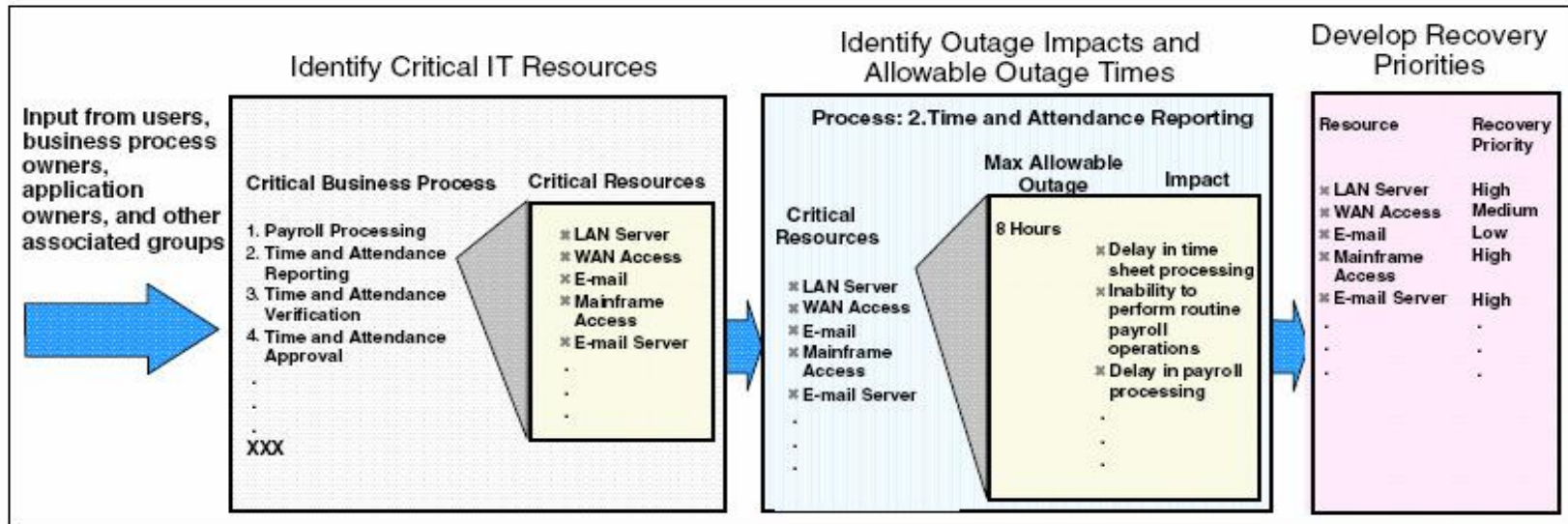


Figure 3-2 Example of the Business Impact Analysis process

Major discussion points (continued)

Risk Analysis

A risk analysis identifies important functions and assets that are critical to a firm's operations, then subsequently establishes the probability of a disruption to those functions and assets.

Once the risk is established, objectives and strategies to eliminate avoidable risks and minimise impacts of unavoidable risks can be set.

A list of critical business functions and assets should first be compiled and prioritised.

Following this, determine the probability of specific threats to business functions and assets. For example, a certain type of failure may occur once in 10 years.

From a risk analysis, a set objectives and strategies to prevent, mitigate, and recover from disruptive threats should be developed.

Major discussion points (continued)

Disaster Tolerance

Disaster tolerance defines an environment's ability to withstand major disruptions to systems and related business processes.

Disaster tolerance at various levels should be built into an environment and can take the form of hardware redundancy, high availability/clustering solutions, multiple data centers, eliminating single points of failure, and distance solutions.

Objectives for Disaster Recovery

Following Objectives are the same for System, Storage and Network infrastructure failures

- Minimize time of outage
- Minimize affected systems in case of a disaster
- Minimize effort for a restart
- Required knowledge in case of a DR:
- Special Communication hardware for the DR case - to avoid busy lines from users
- Documentation of DR Process

Customer Requirements

Identify the following before designing DR sellution

Recovery Time Objective (RTO)

What time difference can be between failure and a total up run level?

Business Resiliency Plan

Last Backup time

Recovery Point Objective (RPO)

What is the toleration for data loss?

RPO = “0” means, NULL data loss acceptable

RPO = “5” means, data loss in last 5 min acceptable

TREND: RPO = 0

Network Recovery Objective (NRO)

Time requirements for network availability

System environment Agreements for DR

For the 'warm' situation - "Doing Work", includes:

- Production
- Development
- Program maintenance
- Testing
- Mirroring of transactions
- Updating of files
- Synchronisation of programs, data or other resources (eg. active
- Linking with another machine, program, data base or other resource, etc.).

Any activity or configurability that would allow an active hot-switch or other synchronised switch-over between programs, data bases, or other resources to occur.

System environment Agreements for DR

(continued)

A scheduled hardware outage, such as preventive maintenance or installation of upgrades, is NOT considered a backup situation.

Preparation for emergency backup situations requires periodic tests - based on the requirements of system availability.

No extra program charges apply for these tests if:

- The number is appropriate (eg. 1-3 tests per year)
- The duration is adequate, (eg. 2 to 3 days per test).

For more frequent tests required (eg. for on-line systems running 24x7 critical customer business operation).

A shorter duration without exceeding the total hours of above guidelines.

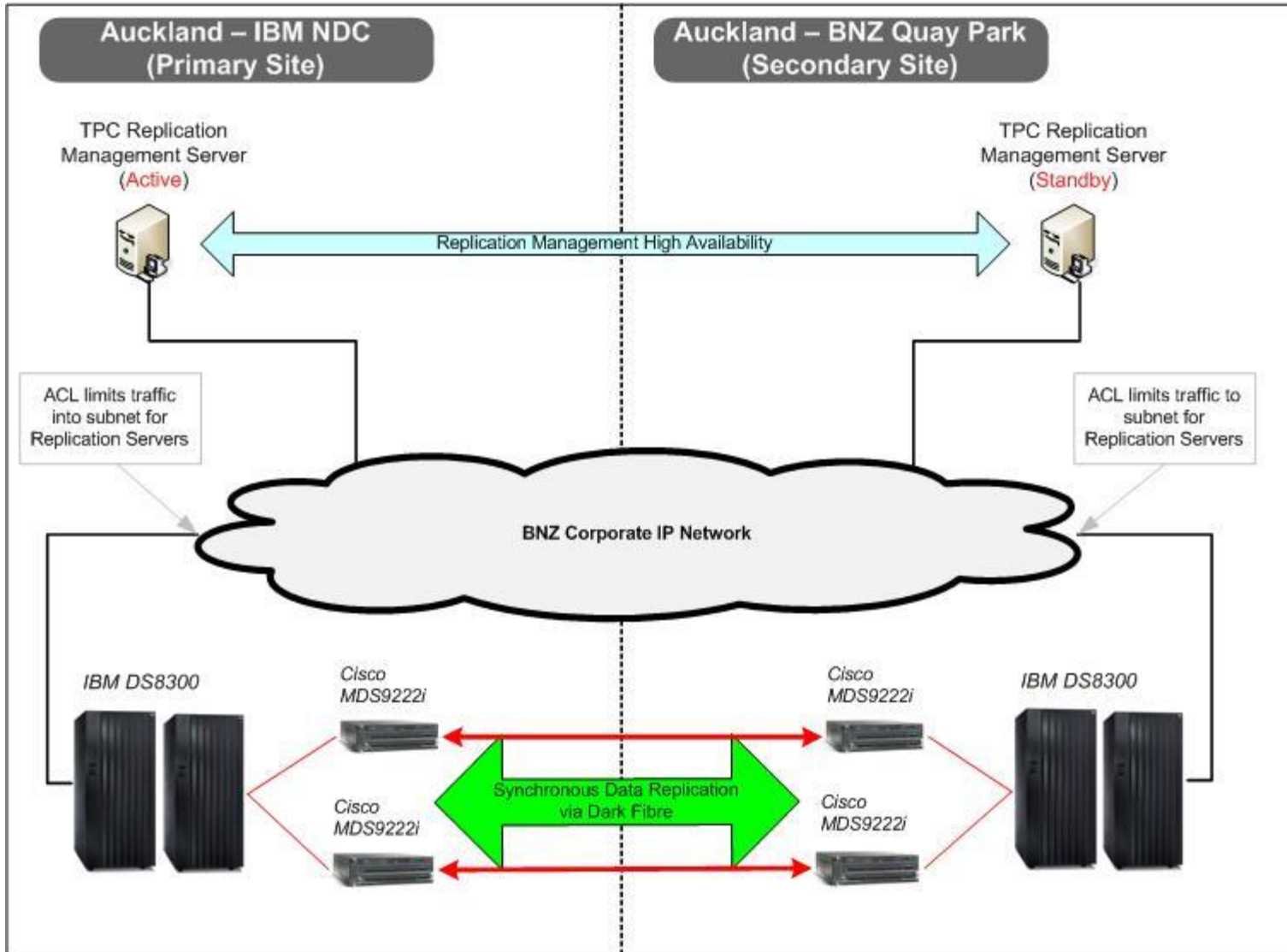
System environment Agreements for DR

(continued)

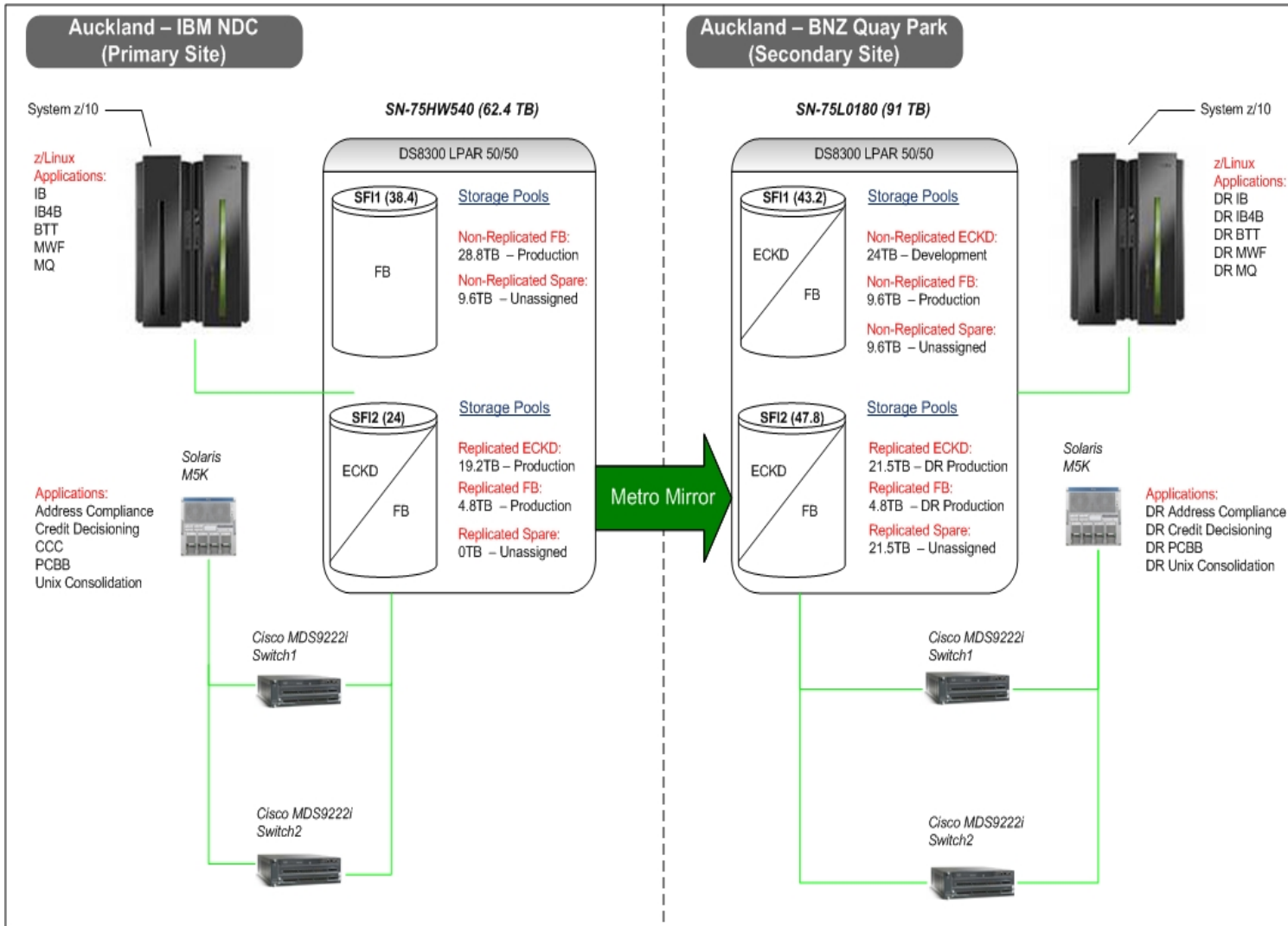
There can be no productive output or work done from the tests and no development, program maintenance or testing as part of the tests. IBM has the right to review the customer's rationale for not licensing the IBM program copy for the backup environment.

Infrastructure DR

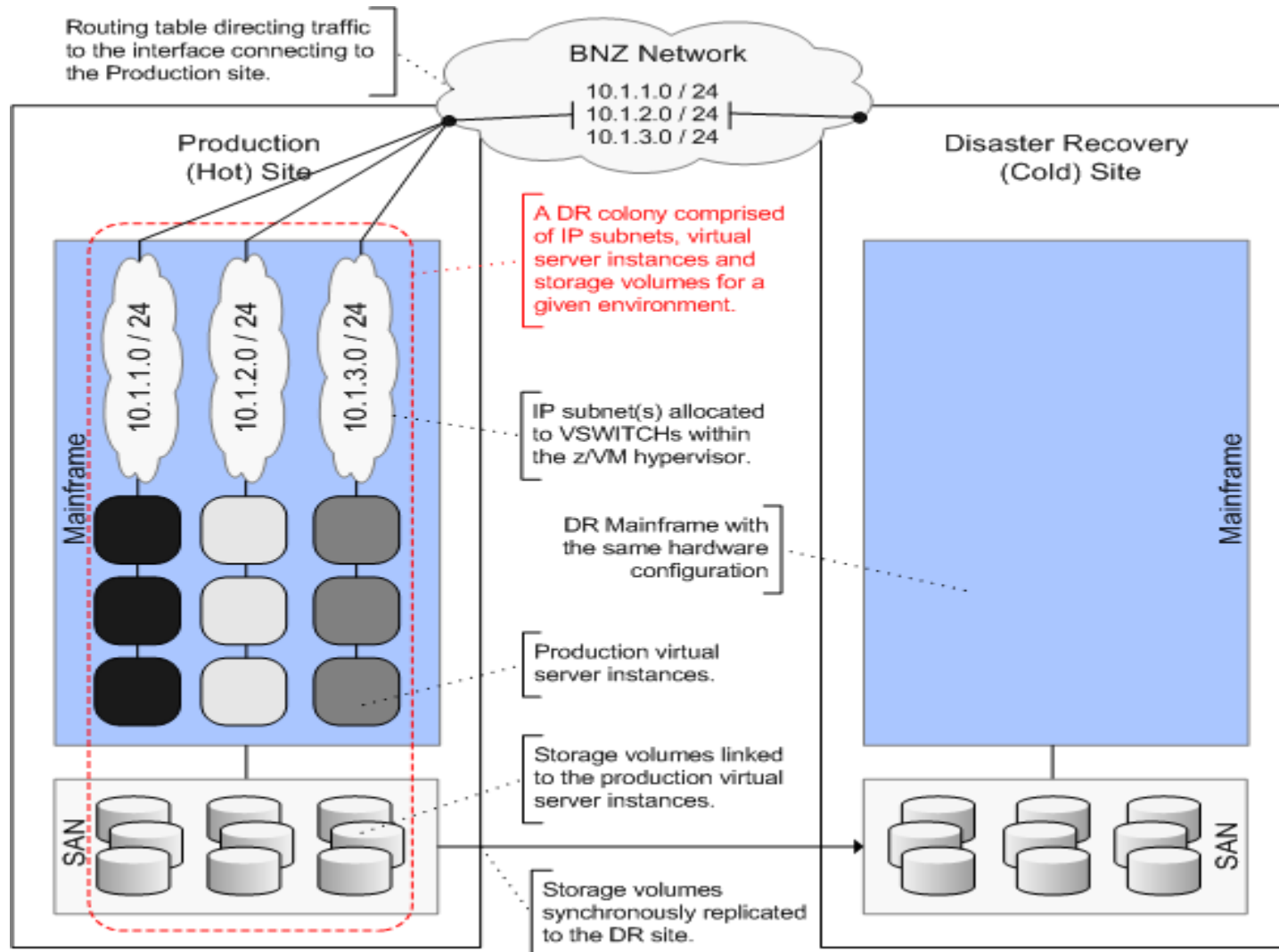
Storage Replication Setup for DR



Detailed Storage Replication View



Network Setup for DR - Colony Model



Steps we follow for DR

Planned DR Invocation Process

- Shutdown Prod
- Shutdown and deactivate PPTE and STRESS lpars running on DR z10
- Update Network switches so VLANS now active at secondary site
- Storage ownership is switched to DR site
- Add CBU's (**Capacity Backup Upgrade**)
- Activate and Start-up Production DR lpars
- IPL Guests keeping their existing IP addresses
- Checks and balances
- Open systems to customer (DR site now becomes Prod site)
- Establish copies to now DR site

Unplanned DR Invocation Process

- Decide DR or NOT
- Shutdown and deactivate PPTE and STRESS lpars
- Update Network switches so VLANS now active at secondary site
- Storage ownership is switched to DR site
- Add CBU's
- Activate and Start-up DR Lpars
- IPL Guests IPL keeping their existing IP addresses
- Checks and balances
- Open systems to customer (DR site now becomes Prod site again)
- If disaster site restored Establish copies to now DR site

Live DR

Live DR - TEST

We will swap our Sysprog lpar running on our Production z10 to our DR-z10

- Shutdown at Prod site
- Show TPCR actions
- Activate and Start system at DR-site
- Shutdown at DR-site
- Show TPCR actions.
- Start-up at Production site again

Summary and Learning

Summary and Learning

- Understand Customer requirements (timings and systems available)
- Understand what you want to achieve with DR
- Plan and document all processes and procedures well
- Staff training and staff to understand procedures
- Testing, testing and more testing.
- Good luck with your next DR - Test

Questions