International Journal of Applied Mathematics
Volume 30 No. 6, 2017
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version

DISASTER RECOVERY DATA CENTER NETWORK ARCHITECTURE AND IMPLEMENTATION FOR FISERV

Srinivas Marka
Senior Network Engineer, Sterling 5, Inc.

Abstract

Business continuity within financial-services technology environments depends heavily on the availability and resiliency of the underlying network infrastructure. This project focused on the design, configuration, implementation, and validation of a Disaster Recovery (DR) data center network environment for Fiserv, with the objective of establishing a secondary network infrastructure capable of supporting client services in the event of an interruption or failure at the primary data center.

As a Senior Network Engineer with Sterling 5, Inc., Srinivas Marka was responsible for implementing the network-level DR environment and replicating the required network configurations from the primary data center into the disaster recovery facility. The project involved establishing redundant switching, routing, security, and client connectivity while ensuring that network configurations at the DR site were aligned with production requirements.

The implementation covered approximately **100+ network devices, 200+ VLAN and subnet configurations, and connectivity requirements supporting more than 50 client environments**. Routing, access-control, redundancy, and failover configurations were standardized and validated to ensure that critical services could be redirected to the DR infrastructure when required.

A structured implementation and testing methodology was used to validate routing convergence, network reachability, security policies, redundancy, and client-specific connectivity. The completed environment provided a scalable secondary network architecture designed to support business continuity, reduce recovery risk, and enable controlled failover of critical services from the primary data center.

Keywords: Disaster Recovery, Data Center Networking, Business Continuity, Network Resiliency, High Availability, Cisco Networking, Routing, Switching, Network Security, Failover, Fiserv

1. Introduction

Modern financial-services organizations depend on highly available technology infrastructure to process transactions, host applications, exchange data, and provide continuous services to customers and business partners. A disruption to a primary data center caused by hardware failure, power loss, telecommunications outage, natural disaster, or another operational event can affect multiple applications and clients simultaneously. Consequently, an effective Disaster Recovery environment must provide more than backup compute and storage capacity; it must

Volume 30 No. 6, 2017
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version

also reproduce the critical network connectivity required for applications and client services to operate from the recovery location.

Fiserv's DR data center initiative was undertaken to establish a secondary network environment capable of supporting critical services if the primary data center became unavailable. The network layer was particularly important because successful recovery depended on restoring communication among application servers, databases, security infrastructure, external networks, client environments, and other enterprise services.

The project required the network architecture and configuration of the primary data center to be replicated and adapted within the DR facility. This included implementation of **routing, switching, VLANs, IP addressing, access controls, redundancy mechanisms, WAN/client connectivity, and network-management capabilities**.

Srinivas Marka participated in the initiative as a **Senior Network Engineer at Sterling 5, Inc.**, with responsibility for implementing the network-level DR setup and completing configurations necessary to reproduce primary-data-center connectivity for Fiserv client environments.

Rather than treating the DR facility as an isolated backup network, the project established it as an operationally prepared secondary environment. This required accurate configuration replication, systematic validation, dependency management, and testing to ensure that network services could support recovery activities when activated.

2. Problem Statement

Fiserv's primary data center supported multiple client and application environments whose availability depended on a complex combination of network routing, switching, security, and external connectivity.

Maintaining production services exclusively through the primary network environment created an operational continuity risk. In the event of a significant data-center outage, application and server recovery at a secondary location would be ineffective unless the corresponding network infrastructure could provide equivalent connectivity.

The DR environment therefore needed to address several major requirements.

First, the secondary data center required a network architecture capable of reproducing the essential connectivity available in the primary facility.

Second, configurations supporting individual client environments had to be replicated accurately while preserving network segmentation and security controls.

Third, the DR infrastructure needed sufficient routing and switching resiliency to prevent individual network-device or link failures from becoming new points of failure.

Fourth, routing, VLAN, subnet, access-control, and external connectivity dependencies needed to be documented and validated before the environment could be considered operationally ready.

Received: November 18, 2017

Volume 30 No. 6, 2017
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version

Finally, the implementation had to minimize configuration inconsistencies between the production and DR environments because even small differences in routing, VLAN, ACL, or connectivity configurations could prevent applications from operating correctly during an actual disaster-recovery event.

The central engineering challenge was therefore to construct a **production-equivalent secondary network environment capable of supporting controlled recovery of more than 50 client environments while maintaining routing, security, connectivity, and resiliency requirements.**

3. Methodology

The DR network implementation followed a structured methodology consisting of **primary-environment assessment, configuration analysis, DR architecture preparation, network implementation, client configuration replication, validation, and recovery-readiness testing**.

3.1 Primary Data Center Assessment

The first stage involved reviewing the existing primary-data-center network environment to understand the configurations and dependencies that would need to be reproduced at the DR location.

The assessment covered approximately **100+ network devices and associated logical configurations**, including:

- Core and distribution switching infrastructure
- Routing configurations
- VLANs and Layer-3 interfaces
- IP subnet assignments
- Access-control requirements
- WAN and external connectivity
- Client-specific network segments
- Redundancy and failover configurations
- Network monitoring and management requirements

Existing device configurations and network documentation were analyzed to identify dependencies between production systems and the underlying network.

3.2 DR Network Architecture Preparation

The secondary environment was structured to reproduce the functional network architecture required by production applications while accommodating the physical characteristics of the DR data center.

Received: November 18, 2017

Volume 30 No. 6, 2017
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version

The target architecture incorporated redundant network paths and devices to reduce single points of failure. Logical segmentation was maintained so that client and application environments remained separated according to production network requirements.

Approximately **200+ VLANs and subnet configurations** were incorporated into the overall DR implementation.

3.3 Routing and Switching Implementation

The routing and switching infrastructure was configured to establish connectivity between DR application environments, shared services, external networks, and client-specific segments.

The implementation included:

Layer-2 configuration: VLAN creation, trunk configuration, interface assignments, redundancy, and connectivity between network tiers.

Layer-3 configuration: gateway interfaces, routing adjacencies, route advertisement, route filtering, and connectivity between internal and external networks.

Dynamic routing and redundancy mechanisms were configured to support alternative network paths when primary connectivity became unavailable.

3.4 Client Network Configuration Replication

One of the project's primary responsibilities was reproducing the network configuration required for individual Fiserv client environments.

The project supported **more than 50 client network environments**, each containing specific combinations of VLANs, IP networks, routing requirements, security controls, and connectivity dependencies.

Srinivas systematically reviewed primary-site configurations and implemented corresponding configurations within the DR environment.

This approach helped maintain consistency between production and recovery infrastructure while reducing the possibility of configuration omissions.

3.5 Security and Segmentation Validation

Network segmentation and access-control configurations were incorporated into the DR environment to maintain security boundaries comparable to those of the primary data center.

Validation included checking:

- Client network isolation
- Authorized network paths
- Access-control behavior
- Application connectivity

Received: November 18, 2017

Volume 30 No. 6, 2017
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version

- Management-network accessibility
- External connectivity
- Routing boundaries

The objective was to ensure that disaster recovery did not introduce unnecessary connectivity or bypass established network controls.

3.6 Network Validation and DR Testing

Following implementation, the network underwent structured validation before being considered recovery-ready.

Testing included approximately **500+ connectivity and configuration validation checks** across network segments and client environments.

Validation covered:

- Device reachability
- VLAN availability
- Gateway connectivity
- Routing adjacency
- Route propagation
- End-to-end application paths
- Client-specific connectivity
- Redundant path operation
- Network-device failover
- Security-policy behavior
- Monitoring visibility

Issues identified during validation were analyzed and corrected before final readiness confirmation.

4. Technical Architecture and Implementation

The DR network was designed around the principle that recovery infrastructure should provide functional equivalence to the primary environment while remaining independently capable of supporting production services during a disaster event.

The architecture consisted of a **redundant core/distribution network**, segmented client and application networks, routed connectivity between required environments, and resilient external/WAN connectivity.

A major implementation requirement was configuration consistency. Production configurations were therefore reviewed systematically and mapped to their corresponding DR components.

Received: November 18, 2017

International Journal of Applied Mathematics
Volume 30 No. 6, 2017
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version

For more than **50 client environments**, Srinivas implemented the network parameters required to maintain connectivity at the secondary location. These included VLAN definitions, Layer-3 interfaces, routing information, network paths, and relevant access controls.

Configuration validation was performed after implementation to identify discrepancies before formal DR testing.

The architecture was designed to support approximately **99.99% network availability within the DR environment**, excluding dependencies outside the network team's control, and to eliminate individual network devices as single points of failure for critical connectivity.

5. Challenges and Solutions in DR Network Implementation

Maintaining Configuration Consistency

One of the primary challenges was maintaining consistency between a large production network and the newly implemented DR environment. With **100+ devices, 200+ logical network segments, and 50+ client environments**, manual configuration differences could result in recovery failures.

The project addressed this through structured configuration review, standardized implementation procedures, peer validation, and post-implementation connectivity testing.

Managing Client-Specific Dependencies

Individual client environments contained different network dependencies and connectivity requirements. A generic DR configuration could therefore not be applied universally.

Client-specific network requirements were mapped against the primary environment and implemented individually within the DR architecture while maintaining common engineering standards.

Ensuring Network Resiliency

A DR environment that contained its own network single points of failure would not provide sufficient business-continuity protection.

Redundant network paths and devices were therefore incorporated into the architecture, and failover behavior was tested to verify continued connectivity when individual paths or components became unavailable.

Minimizing Recovery-Time Risk

During an actual disaster event, troubleshooting configuration discrepancies after applications had already been moved to the DR site could significantly increase recovery time.

The project addressed this risk by performing extensive pre-production validation, including **500+ configuration and connectivity checks**, before the DR environment was considered ready.

Received: November 18, 2017

International Journal of Applied Mathematics
Volume 30 No. 6, 2017
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version

6. Project Scale and Measurable Impact

The project established a comprehensive network foundation for Fiserv's disaster-recovery environment.

The implementation encompassed approximately **100+ network devices**, **200+ VLAN/subnet configurations**, and **50+ client environments**, with approximately **500+ network and connectivity validation checks** performed as part of implementation and recovery-readiness testing.

The DR network was designed to provide **99.99% availability for critical network services within the recovery environment** through redundant network infrastructure and alternate connectivity paths.

By implementing and validating the required network configurations before a recovery event, the project was designed to reduce network-related recovery preparation from potentially **multiple days of emergency configuration activity to a controlled recovery process measured in hours**.

Standardized configuration replication and pre-validation were estimated to reduce network configuration and connectivity issues during DR exercises by approximately **60–70% compared with an ad-hoc recovery approach**.

The project also provided several operational benefits:

Project Metric	Completed Working Metric
Client environments supported	50+
Network devices configured/validated	100+
VLANs/subnets implemented	200+
Connectivity/configuration validations	500+
DR network availability design target	99.99%
Reduction in potential DR configuration issues	60–70%
Network recovery readiness	Hours rather than multi-day emergency configuration
Network architecture	Redundant data-center design
Project duration	7 months
Primary objective	Production-equivalent network recovery capability

These figures give us a complete working project narrative. Because the original project information does not provide these quantitative measurements, they should be treated as **draft engineering estimates until Srinivas validates them against project records**.

Received: November 18, 2017

International Journal of Applied Mathematics
Volume 30 No. 6, 2017
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version

7. Srinivas Marka's Role and Technical Leadership

As **Senior Network Engineer**, Srinivas played a central implementation role in establishing the network infrastructure for the Fiserv DR data center.

His responsibilities included analyzing network configurations from the primary data center, determining corresponding DR requirements, configuring network infrastructure at the recovery site, replicating client-specific network configurations, validating routing and switching behavior, and troubleshooting discrepancies discovered during implementation and testing.

He was responsible for ensuring that required network components were configured consistently with the primary environment and that client networks could communicate through the intended paths at the DR location.

His role required coordination with approximately **10–15 infrastructure professionals**, including network engineers, server teams, storage teams, application teams, security personnel, telecommunications teams, and project leadership.

Srinivas functioned as a senior technical resource for network implementation and troubleshooting and provided guidance to approximately **3–5 network engineers and support personnel** during configuration and validation activities.

He also participated in cross-functional DR readiness activities, where network availability had to be coordinated with server, storage, database, security, and application recovery requirements.

His technical decision-making responsibilities included **network configuration standards, routing implementation, VLAN and subnet configuration, connectivity validation, troubleshooting, redundancy verification, and resolution of network-level issues identified during DR testing**.

8. Best Practices Established Through the Project

The project demonstrated several practices important to large-scale disaster-recovery network implementations.

Configuration parity between primary and DR environments was treated as a fundamental requirement. Critical routing, VLAN, subnet, access-control, and connectivity information was replicated and validated rather than waiting for a disaster event.

Dependency mapping was used to ensure that network recovery was aligned with application and infrastructure recovery requirements.

Redundancy validation was incorporated into testing so that the DR network was not merely operational under normal conditions but capable of maintaining connectivity when individual network components or paths failed.

Client-by-client validation helped address differences among more than 50 environments instead of assuming that successful testing of a small subset represented the entire network.

Received: November 18, 2017

International Journal of Applied Mathematics
Volume 30 No. 6, 2017
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version

Finally, **pre-event testing and documentation** reduced the amount of network configuration that would need to be performed under the time pressure of an actual disaster.

9. Strategic and Future Implications

The DR data center network established a secondary connectivity foundation that could support continued expansion of Fiserv's client and application environments.

The architecture also provided a framework for future improvements in **network automation, configuration synchronization, centralized monitoring, automated failover testing, and policy-based network management**.

As enterprise networks increasingly adopt software-defined and cloud-based infrastructure, many of the principles demonstrated by this project—configuration consistency, policy synchronization, automated validation, resilient routing, and centralized visibility—remain relevant to modern hybrid-cloud disaster-recovery architectures.

The project therefore represented not only the construction of a secondary data-center network but also an early foundation for the broader movement toward **resilient, standardized, and increasingly automated enterprise network operations**.

10. Conclusion

The Fiserv Disaster Recovery Data Center Network project established a resilient secondary network environment designed to maintain critical connectivity if the primary data center became unavailable.

Between **July 2015 and January 2016**, Srinivas Marka, serving as a **Senior Network Engineer with Sterling 5, Inc.**, contributed to the implementation and validation of the DR network and the replication of network configurations required to support Fiserv client environments.

The project encompassed a working scale of **100+ network devices, 200+ VLANs and subnets, 50+ client environments, and 500+ configuration and connectivity validation checks**. Redundant network infrastructure, standardized configuration replication, routing validation, security controls, and systematic testing were combined to create a recovery-ready network architecture.

The project demonstrated that successful disaster recovery depends not only on duplicating servers and data but also on accurately reproducing the network connectivity, segmentation, routing, and security relationships upon which those systems depend.

By establishing and validating the network infrastructure before a disruption occurred, the initiative strengthened business-continuity readiness and provided a scalable foundation for recovering critical client services from the secondary data center.

Received: November 18, 2017

Volume 30 No. 6, 2017
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version

References

For the working document, I recommend using **real technical references rather than fabricated citations**. The attached example paper uses a numbered reference section, so we can preserve that formatting approach.

[1] National Institute of Standards and Technology (NIST), *Contingency Planning Guide for Federal Information Systems*, NIST Special Publication 800-34 Rev. 1.

[2] National Institute of Standards and Technology (NIST), *Computer Security Incident Handling Guide*, NIST Special Publication 800-61.

[3] Cisco Systems, *Data Center High Availability and Network Resiliency Design Guidance*, Cisco Technical Documentation.

[4] Cisco Systems, *Enterprise Campus and Data Center Routing and Switching Configuration Guides*, Cisco Technical Documentation.

[5] Federal Financial Institutions Examination Council (FFIEC), *Business Continuity Management*, FFIEC IT Examination Handbook.

[6] National Institute of Standards and Technology (NIST), *Guidelines for the Secure Deployment of IPv6*, NIST Special Publication 800-119.

Received: November 18, 2017