International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

Network Migration Strategies

Vaishali Nagpure
BE, Industrial Electronics,
Pune University,
Maharashtra, India

***Abstract* - Technology is always changing and providing new solutions to address current as well as future needs of IT Infrastructure. Network Infrastructure is crucial part in any kind of IT Infrastructure. Network Infrastructure provides communication path between users and applications. Network Infrastructure refers to Hardware Devices that enable network connectivity. Network Infrastructure means end-to-end communication, operations and management of devices involved in communication. After certain time span there is always a need to migrate existing network infrastructure. There are various reasons for migration like: requirement of centralized repository instead of distributed environment, need for converged network with voice, video and data traffic, devices used are either EOL (End of Life) or EOS (End of Sale) and may be there are some advanced techniques available best suited for current or future environment. Detailed step by step approach is required to carry out any migration. First step is detailed survey of existing Infrastructure. Then next step is to document these details which will be helpful for migration process. Then most important step is planning migration steps with multiple phases along with documentation. Perfect planning is a key to successful migration. After planning next step is first phase implementation and testing. Testing will cover some key points like performance and high availability testing for every application. Then move to next migration phase and repeat all steps from planning till testing. This paper presents one migration case study. It will consider migration of existing network with distributed environment to centralized architecture like Data Centre along with high availability and security. This will cover LAN and WAN migration with CISCO environment. It will cover some useful tips and strategies that would help for migration process. Ii will mention configuration examples on CISCO devices which can be done in certain scenarios. It will present some useful design techniques in certain routing protocol deployments as well as some redundancy techniques useful for optimized performance. It will cover each step in detail for planning; implementation and testing in each phase and will suggest best design techniques. It will also mention commands that can be used on CISCO devices for testing each implementation phase.**

Key Words: Network Infrastructure, Migration, Data Center, CISCO

1. INFRASTRUCTURE DETAILS

This will consider details of existing and new infrastructure. It covers connectivity and configuration details for end-to-end communication.

1.1 Existing Network Infrastructure

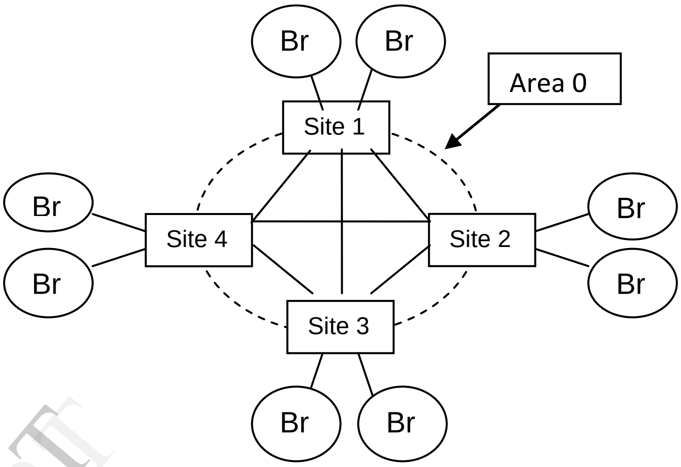

Fig -1: Existing Network Infrastructure logical diagram

There are four major sites connected via routers with leased lines and having redundant links. Branch routers are connected to these four sites via leased lines as shown in Fig-1. Application/Database servers are distributed among these four sites LAN. Users are spread among all branches LAN.

Design of Routing Protocol [2] -

Static default route is configured on each branches pointing towards major sites and static route is configured on site routers for particular branch LAN connected to the site router. OSPF Area 0 is configured between four major sites. There is redistribution configured on site routers for end to end connectivity.

1.2 Proposed Network Architecture

New proposed architecture is for centralized repository. All application/database servers, storage will be placed in one place called Data Center. While designing this infrastructure following parameters will be taken into consideration such as security, high availability and scalability. Network Architecture will be hierarchical in nature called 3-tier consists of Core, Distribution and Access layer [1]. IP addressing and routing protocol design best suited for this hierarchical design will be decided. Following is the distribution at each layer as shown in Fig-2

1. Branches will be at access layer (B1, B2, B3, B4… and so on). Branches will have redundant links which will serve as backup links. Backup links can be ISDN, VSAT, CDMA, 3G or even PSTN links.
2. All Sites will be at Distribution Layer.
3. Core Layer will contain core/aggregation Routers (R1, R2) at Data Center (DC) and Disaster Recovery Center (DR).

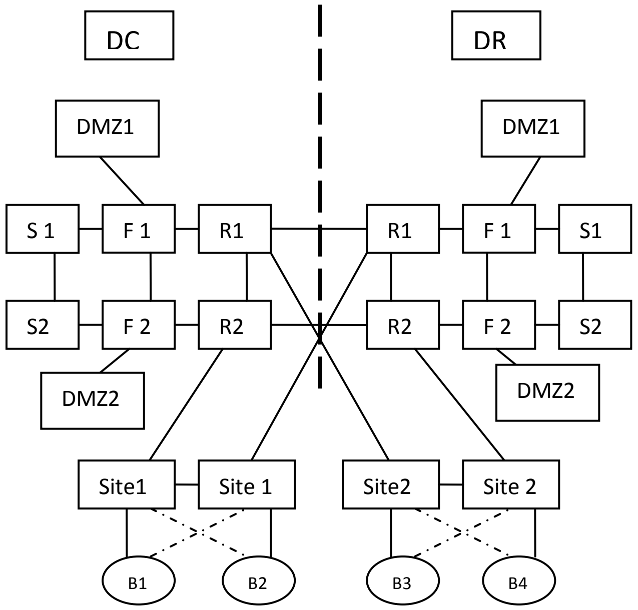

Fig -2: Proposed Network Architecture logical diagram

DC and DR are two geographically separated locations. DC is primary and DR is secondary location for all applications and database. All devices at DC and DR are connected in redundant fashion for high availability as shown in Fig-2. All servers are distributed on Core Switches (S1, S2) and on DMZ switches connected to firewall (F1, F2) at DC and DR.
Critical servers are placed in high security zone. Now instead of previous distributed applications and database architecture, there will be centralized application and database environment. Branches will access application and database servers at DC after migration.
WAN links connectivity will be as follows-
1. At core level, Core routers at DC and DR are connected with each other with two WAN links as shown in Fig-2. Core routers will have WAN links from different service providers (SP) like R1 will have links from SP1 and R2 will have links from SP2 at DC and DR.
2. At Distribution level, sites are connected to DC as well as DR through WAN links. Sites will have two routers connected back to back and if one router is having connectivity to DC R1 (SP1), other router will have connectivity to DR R2 (SP2). Sites distribution will be such that few sites will have DC connectivity through SP1 (R1) and others through SP2 (R2).
3. At access level, there are branches connected to site routers through WAN links. Branches will have primary WAN link connected to one site router and redundant link connected to other router. Branches distribution will be such that some branches will have primary link on one router and others will have primary links on other router.
Thus redundancy is maintained at device as well as service provider level.

2. MIGRATION PROCESS STEP-1 - SURVEY

Migration process will start with the survey of existing infrastructure. Then next stages are planning, implementation and testing. Each stage will be documented with detailed information.

2.1 Detailed Survey of existing Infrastructure
In this step following details will be considered and documented-
1. Physical connectivity details of all devices like on which switch port particular device or server is connected.
2. Device details such as model, IOS versions, RAM, FLASH, license information and so on.
2. Technical details such as configurations of all devices, IP addressing and technologies used for routing.
IP addressing details include class and subnet information. It will also include IP addresses given to each interface of each device as well as servers.
Existing routing protocol information and its design is studied in detail which will be useful for migration.

3. MIGRATION PROCESS STEP-2 - PLANNING

Planning is the most crucial phase in any migration. If planning is done with careful consideration of all minute details, migration can be carried out successfully.

3.1 DC/DR implementation planning
Planning of DC and DR setup will include following steps
1. Plan for connectivity details of all devices considering redundancy of each device.
2. Then plan IP addressing design for DC and DR devices. Once IP addressing design for DC devices is ready same can be replicated at DR with another IP subnet.
3. Plan for configuration of all devices along with routing protocol configuration so that branch can be able to communicate with Servers behind Firewall

3.2 Planning at sites and branches for installation of new hardware
At branches and sites following points are taken into consideration for new setup architecture-
1. Branches should have additional interface to terminate additional backup links. At sites new router will be installed along with old router.
2. All devices should have enough resources such as RAM, Flash and IOS version to support new routing protocol design.
If resources or devices are not supporting new architecture, detailed plan should be ready to upgrade existing devices

3.3 Planning for configuration of devices

After planning for physical connectivity of all new devices is done, second step is planning configuration of all devices.

Configuration includes following steps-
1. Configuration of IP addresses on each interface as per new IP addressing design. IP addressing design should be such that it should be scalable and summarization can be done at distribution level.
2. Routing protocol configuration for 3-tier architecture.
Routing protocol design should be best suitable for 3-tier architecture.
For example OSPF routing protocol can be used for 3-tier architecture [2].
OSPF design can be as follows-
1. Branches will be divided in separate areas. Each site can have multiple branch areas depending upon number of branches connected to the site.
2. Core routers at DC, DR and site routers are configured for Area 0(Backbone Area).

3.4 Planning of configuration for optimized performance and redundancy

Following guidelines can be followed for optimized performance-
1. OSPF stub area feature can be configured for optimized performance of OSPF routing protocol.
Site routers will function as ABR (Area Border Router) and will have connectivity to backbone area as well as to Branch area.
2. Summarization can be done on ABR for all branches. Hence core routers will have only summarized routes in routing table.
3. Following redundancy techniques can be used to avoid down times in case of either Link or device failure.
LAN redundancy techniques such as HSRP (Cisco Proprietary) or VRRP (Open Standard) can be used at sites [3] where site LAN is connected. Site router connected to DC will act as HSRP active router whiles other will act as standby router. If load balancing is required GLBP can be configured instead of HSRP/VRRP.
Firewall can be configured in either Active/Active or Active/Standby configuration in case of CISCO based on the requirement [4].

3.5 Planning for first branch Migration

Now first branch migration plan can be decided and scheduled. First branch migration plan will include following steps-
1. Connectivity from branch router to DC. This will include connectivity from branch to site and site to DC and DR. As per design, branch can be connected to either old or new site router.
2. Change of IP addressing of WAN as well as LAN links.
3. Change of Routing protocol configuration on Branch and site router

4. MIGRATION PROCESS STEP-3 - IMPLEMENTATION

Phase wise implementation will be done. In first phase of implementation, first branch will be configured so that it can access application at DC. After successful testing of first phase implementation all other branches are migrated for new application access.
Implementation will include following steps-
1. Physical connectivity of all devices along with all WAN as well as LAN links
2. Configuration of all devices which includes IP address configuration and routing protocol configuration.

4.1 Implementation of DC and DR setup

Following steps are carried out for DC and DR implementation-
1. Installation of Core routers, Firewalls and Switches (Core, DMZ).
2. Configuration of IP addresses on every interface of each device as per DC/DR IP addressing design plan.
3. Configuration of OSPF routing protocol on core routers for backbone area
4. Static routing can be configured on Core routers pointing towards firewall to obtain connectivity to all servers behind firewall. Default routing can be configured from Firewall pointing towards core router for all sites as well as branches communication. Redistribution is configured on Core routers at DC/DR for end-to-end communication.
5. Firewalls will be configured for active/active or active/standby configuration [4].
6. HSRP/GLBP can be configured for Core routers LAN wherever possible for redundancy purpose.

4.2 Implementation at Site

Following steps are carried out at Site-
1. Additional router will be connected in site LAN with existing router. Connect WAN links on both routers at site which are connected to DC and DR. After configuration of all IP addresses, HSRP will be configured on Site LAN interfaces such that router having WAN link connected to DC will become HSRP active router[3].
2. Site router will be configured as ABR (Area Border Router) such that WAN link connected to DC/DR will be in Area 0 (Backbone Area) and link connected to branch will be in branch Area [2].
3. Link between two site routers will be in Area 0
4. Branch Area will be configured as Totally-Stub Area
Following is the OSPF configuration command configured on site router to make branch area as totally-stub area

```
Router (conf-router) # area <area-id> no-summary
```

OSPF summarization can be configured on site routers with following command [2]

```
Router# area <area-id> range <summarized subnet>
```

4.3 Implementation at Branch

Following steps are carried out at branch-

1. Additional card will be installed in branch router to connect backup link.
2. Configure IP addresses on branch router interfaces. Configure secondary IP address on branch Ethernet interface.
3. Remove static default routing from branch router and respective static route from site router. Configure OSPF routing protocol with stub area configuration as shown below [2]

```
Router (conf-router) # area <area-id> stub
```

Advertise both LAN subnets under OSPF.

4. Host in branch LAN can be configured with new IP address one by one. Both old and new branch LAN IP addresses will be able to communicate with servers at DC or DR. When all hosts in LAN are configured with new IP addresses, make new IP subnet as primary and remove old from Ethernet segment of branch router.

5. MIGRATION PROCESS STEP-4 - TESTING

After first phase implementation, step by step testing can be done as follows-

1. Check WAN links on DC/DR core routers, both site routers and branch router with following command

```
Router# show interface <Interface details>
```

After configuration of IP addresses on WAN links, connectivity can be checked with following command

```
Router# ping <next-hop IP address>
```

Next-hop IP address is the address of the next hop router where other end of point to point link is connected.

Success rate should be 100 percent.

2. HSRP can be verified with following command on site routers [3]

```
Router# show standby
```

Make sure that site router connected to DC is HSRP active router. Also make sure Standby router information is correct.

3. Check OSPF neighbor relationship with following command on all routers where OSPF is configured [2] -

```
Router# show ip ospf neighbor
```

OSPF neighbor relationship should be in FULL state on point-to-point links.

4. Check application server connectivity with PING command from host in branch LAN.
5. Check all applications from any branch LAN host. Connection state of application can be checked on Firewall with following command

```
Firewall# show conn
```

Check output of this command especially flags. Established session will show flag as UIOB [4].

While troubleshooting any connection with any server, firewall policies should also be verified. Whether connection is allowed or denied is based on firewall policy configuration.

6. MIGRATION PROCESS STEP-4 - REDUNDANCY TESTING

Redundancy testing is required for high availability. This will ensure availability in case of Links or Device failures

6.1 Device Redundancy testing at DC and DR

DC and DR setup is having all devices connected in redundant fashion as shown in Fig-2

Hence in each pair of devices, one device can be shutdown.

For example end-to-end connectivity is tested with shutting down following devices at DC and DR

S1, DMZ1, R1 and F1

Also technologies used such as HSRP/GLBP and Active/Active or Active/Standby failover of Firewalls will be tested.

6.2 DR testing (DR-DRILL)

In any infrastructure DR testing is the crucial part. DR testing requires very detailed planning. Co-ordination between all teams is required to carry out DR DRILL activity.

Down time planning is required for DR testing.

DR testing will include following steps-

1. Applications at DC will be in down state and at DR will be in running and active state
2. Database at DR will be in sync with DC database and Database at DC will be down
3. Firewall policies are changed accordingly such that branches could get access to DR servers.
4. Devices at DC are kept in power down state
5. If branches will be accessing applications with same DC IP address, NAT and routing will be configured at DR.

Scheduled and planned DR-DRILL activity is carried out at every organization having DC/DR setup.

6.3 Redundancy testing at sites

At sites, WAN links and routers are installed for redundancy.

WAN link redundancy can be tested with shutting down primary and secondary links one at a time.

Router redundancy is checked by shutting down one router at a time.

HSRP can be tested with either WAN link or Router failure.

6.4 Redundancy testing at branches

Branch is having WAN link redundancy. Branch router is configured for backup link connected to it.

Branch backup link can be tested by shutting down WAN link from site router.

Do not shut down link from branch router. If backup command is configured on primary WAN interface of branch router, it will not function if is in shutdown state.

7. MIGRATION PROCESS STEP-6 - DOCUMENTATION

Documentation at each stage is required. Make sure that every migration stage is well documented.
Documentation will cover all following details-
1. Physical connectivity details. Description is given to all devices interfaces for identification and troubleshooting purpose.
2. All network diagrams will be maintained mentioning connectivity details. Diagrams include DC LAN, DR LAN, and OSPF detailed diagram mentioning 3-tier architecture.
3. Documents will cover IP addressing design details and assignment of IP addresses to all devices at DC, DR, site and branches.
4. Routing design consideration along with its configuration details on all devices will be documented.
5. Running configuration of all devices will be saved for further reference.

8. MIGRATION PROCESS – FINAL PHASE

After successful implementation and testing of first branch migration, next phase is migration of all remaining branches and sites. Migration of each branch is carried out with all steps right from planning to documentation as given in the first phase.
When all branches under single site are migrated, old configuration can be removed from site and branch routers and old links can be disconnected.
Considering security aspect, hardening of all devices is carried out along with migration.

9. CONCLUSIONS

Step by step planning is required for Network Migration. For centralized environment such as Data Center (DC) and Disaster Recovery Center (DR), detailed study of existing network infrastructure is required. Then DC and DR setup with redundancy and security is planned and implemented. Next step is migration of existing setup considering redundancy with planned changes on existing and new devices .With proper planning and documentation, Network Migration can be carried out smoothly with minimized down time.

REFERENCES

1. Advanced IP Network Design (CCIE Professional Development), Alvaro Retana, Don Slice, Russ White Publisher: Cisco Press, First Edition June 17, 1999
2. CCIE Professional Development: Routing TCP/IP, Volume I, Jeff Doyle, Copyright© 1998 by Macmillan Technical Publishing
3. CCIE Routing and Switching Certification Guide, Fourth Edition, Wendell Odom, Rus Healy, Denise Donohue, Copyright © 2010 Pearson Education, Inc
4. Cisco ASA and PIX Firewall Handbook by Dave Hucaby, Publisher: Cisco Press, Pub Date: June 07, 2005

BIOGRAPHIES

B.E (Industrial Electronics) from Pune University. Having 15.5 yrs of experience from IT industry with specialization in Networking.

CCIE (R & S) No. 25600