Database | Scale Out | High Reliability

Technology Reports

Enhanced Service Control Equipment Supporting Diverse NTT DOCOMO Services

To deal with the increasing number of subscribers accompanying the provision of smartphones and machine communications, the NTT DOCOMO mobile communications network is expanding with the deployment of new networks such as IMS and LTE. To facilitate this expansion, we are separating the database function and call-processing function in the existing IPSCP and constructing a new system (D-SCP) to handle the database function.

Core Network Development Department
Keiichiro Otsuka
Tomonori Kagi
Haiyan Zheng
Core Network Division, DOCOMO Technology, Inc.
Atsuhiko Ochiai

1. Introduction

Recent years have seen a dramatic increase in the use of smartphones, an increase in machine communications via communication modules embedded in vending machines, automobiles and other equipment, and an increase in the number of subscribers to the LTE-based "Xi" (Crossy) service. As a result, subscriber information and location-registration data managed by the network and traffic generated by call-processing signals for location registration and incoming/outgoing calls have been increasing and diversifying.

In the NTT DOCOMO network, an IP Service Control Point (IPSCP)[*1] has been used to manage user subscriber information and to control location registration and incoming/outgoing calls. However, the recent increase in subscribers and traffic described above has been pushing the limits of IPSCP database capacity and CPU processing power making it necessary to increase the number of IPSCP units in the network.

Considering further increases in number of subscribers and further diversification of services in the years to come, the need is felt for constructing a flexible IPSCP that can strike an optimal balance between database capacity and traffic while keeping facility costs down instead of simply increasing the number of IPSCP units.

The current IPSCP configuration, however, incorporates a database and a CPU for controlling call-processing signals in the same unit of equipment. This means that either a tightening situation in database capacity or one in CPU processing power because of increased traffic will make it necessary to add more IPSCP units. This measure, though, results in wasted facility spending. For this reason, dividing the IPSCP into two units of equipment—one for a Database Service Control Point (D-SCP) corresponding to the database function and the other for a Frontend Service Control Point (F-SCP) corresponding to the call-processing function—is seen as a flexible scheme for increasing facilities in a more efficient manner.

*1 **IPSCP**: A node with functions to manage subscriber service information (contract and configuration information) and for service control.

This article first presents the configuration and respective functions of F-SCP and D-SCP equipment. It then describes the D-SCP functions for achieving high data integrity and robustness to disaster made possible by this separation of database and call-processing functions.

2. Separation of Database Function and Call-processing Function

The separation of the database function and call-processing function is shown in **Figure 1**. To achieve this separation, we migrate only the database function from the IPSCP and construct a new D-SCP. The F-SCP is achieved by directly appropriating the IPSCP call-processing function and equipment.

The F-SCP controls call-processing signals with other nodes such as switches as performed in the existing IPSCP and also accesses data on the D-SCP (i.e., references subscriber information and issues update requests). The D-SCP, in turn, updates data and returns subscriber information in response to data access from the F-SCP.

Separation of the database function and call-processing function in this way has the three effects described below.

1) Flexible Capacity Expansion

It is now possible to increase database capacity (D-SCP) independently of increasing CPU processing power (F-SCP) for handling service traffic.

2) Flexible Access from Other Nodes

The present IPSCP scheme distributes subscriber information among multiple units of equipment as a countermeasure to any fallout from a system failure. As a result, a node that accesses IPSCP requires a function for determining which unit accommodates the target subscriber. In contrast, separating F-SCP and D-SCP means that D-SCP is given the task of managing subscriber information while F-SCP holds no subscriber information at all. In this case, only F-SCP needs to be concerned about subscriber-information accommodation while an outside node can access any one of a number of F-SCPs without having to care about the whereabouts of subscriber information. This has the effect of keeping development costs down.

In addition, the adoption of a round-robin[*2] or similar access method raises reliability while distributing load.

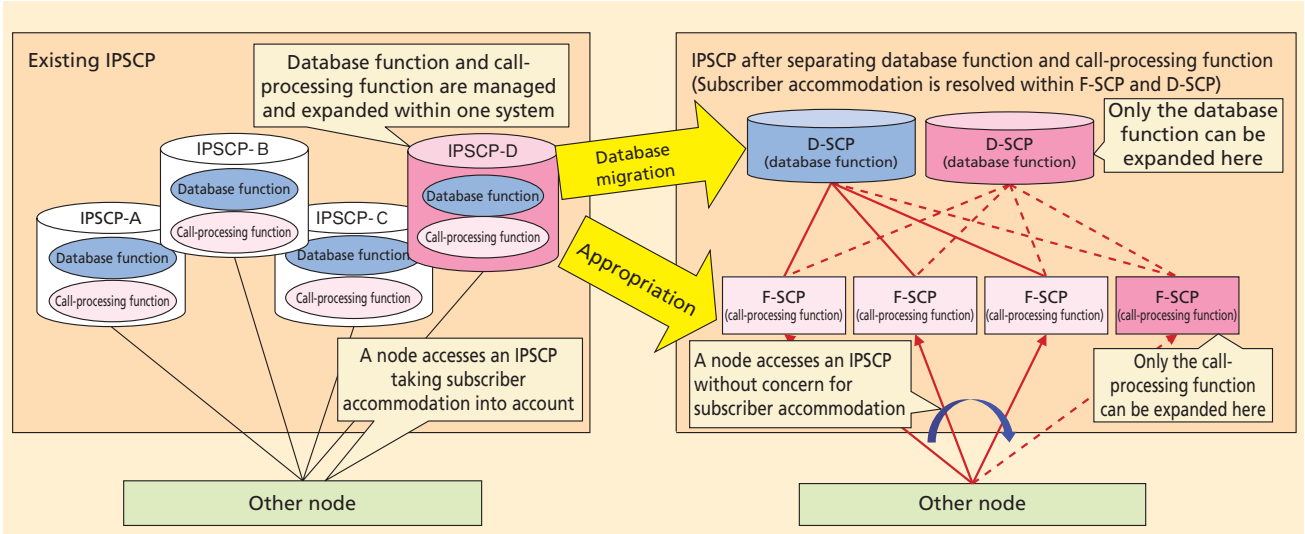

Figure 1 Separation of database function and call-processing function

*2 **Round-robin**: One of the techniques of load distribution in networks. A number of devices capable of performing the same function are prepared and the requested process is allocated to them in turn.

3) Flexible D-SCP Configuration

In the new separated scheme, only F-SCP connects with D-SCP, which means that measures for enhancing the data integrity of D-SCP can be adopted without affecting other nodes.

3. System Configuration

1) Network Configuration

The network configuration of F-SCP and D-SCP is shown in **Figure 2**. The F-SCP section connects to core network[*3] equipment consisting of Circuit Switched-IP (CS-IP)[*4], serving/gateway General packet radio service Support Node (xGSN)[*5], and Evolved Packet Core (EPC)[*6], to operation equipment consisting of the Element Management System (EMS), and to customer management systems consisting of ALl Around DOCOMO INformation systems (ALADIN).

Here, F-SCP receives call-processing signals for location registration and other purposes from CS-IP, xGSN and EPC and service orders from ALADIN, and accesses data on D-SCP.

2) Hardware Configuration

The hardware configuration of D-SCP is shown in **Figure 3**. In this configuration, a Data Base Processor (DBP) holds data and database functions for processing subscriber information. These data and functions are loaded in memory to ensure high-speed, real-time access, but because data in memory always runs the risk of being corrupted or lost, data will be backed up periodically to a Redundant Array of Independent Disks (RAID)[*7] device (specifically, Data Base Fiber Channel RAID (DB-FRAID)[*8]) as a precautionary measure. Moreover, as a countermeasure to the loss of backup files, the system adopts backup-data management for two or more generations of data and a redundant configuration. The DBP blocks connect to RAID by a Fiber Channel SWitch (FCSW). The D-SCP also includes a File Server (FS) having an interface function for equipment monitoring and maintenance. It holds data for maintaining and operating the system and managing equipment and also connects to RAID (File Server Fiber Channel RAID (FS-FRAID)[*9]) for backup purposes.

In addition, the Open Flow SWitch (OFSW) incorporates a function for

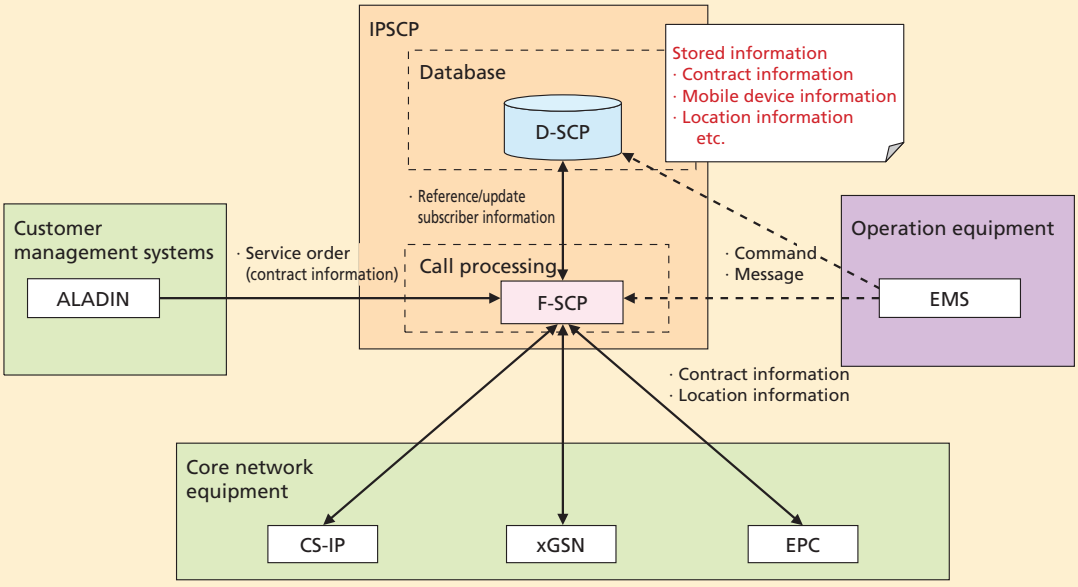

Figure 2 F-SCP and D-SCP network configuration

*3 **Core network**: A network comprising switching equipment, subscriber information management equipment, etc. A mobile terminal communicates with the core network via a radio access network.

*4 **CS-IP**: An IP-based core network for controlling and transmitting voice traffic using the IP Multimedia Subsystem (IMS) standardized by 3GPP.

*5 **xGSN**: A packet communication processing device in the FOMA network. It has both the SGSN function and the GGSN function specified by 3GPP.

*6 **EPC**: A core network that can accommodate diverse radio access systems including LTE.

*7 **RAID**: A device that manages multiple hard disks at the same time.

*8 **DB-FRAID**: RAID equipment for DBP use. Functions as external storage equipment for backing up the DBP database via a fiber channel.

directing data-access requests from F-SCP to the DBP blocks accommodating subscriber information. Meanwhile, the server group consisting of the Chassis Management Module (CMM) performing management functions within the chassis[*10], the Shelf SWitch (SSW) acting as an internal switch blade between FS and DBP, and the FS described above adopts the aTCA[*11] standard.

This D-SCP configuration also allows for the construction of one master unit and two backup centers. In the backup process, HS3[*12] backup storage transfers backup files of master subscriber information using a replication[*13] function thereby improving the reliability of backed up subscriber data. The flow of backup files to the backup centers from the master D-SCP is shown in **Figure 4**.

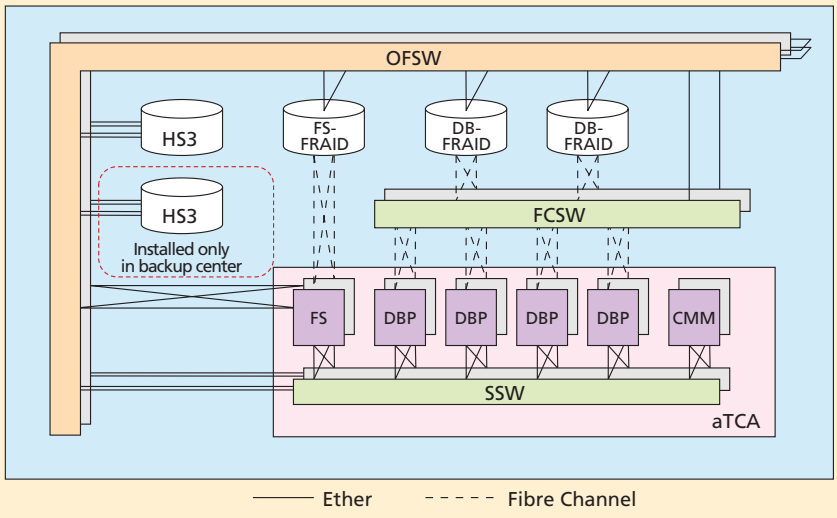

Figure 3 D-SCP hardware configuration (master and backup center)

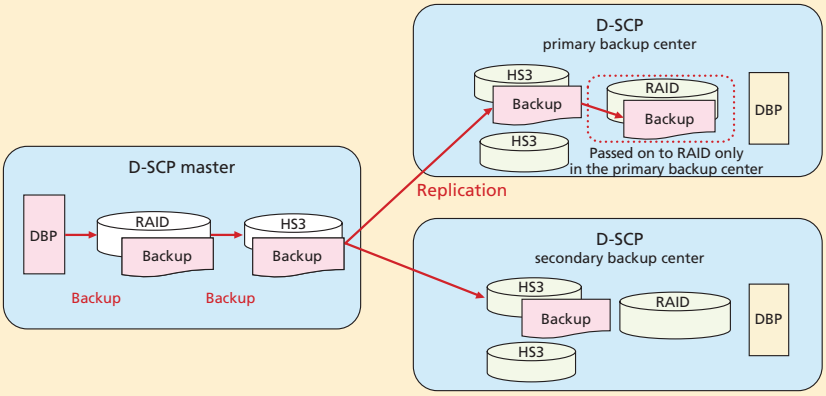

Figure 4 Configuration of D-SCP master and backup centers and backup-file flow

4. Measures for Improving D-SCP System Reliability

As a vitally important system for managing subscriber information, the D-SCP requires measures to ensure reliability in the face of a system failure. We here introduce relocation[*14] and backup center switching as representative of these measures.

4.1 Relocation Method

The D-SCP implements a relocation method for improving network reliability at the time of a system failure. An overview of this method is presented in **Figure 5**. In the event that a DBP double-system failure[*15] occurs preventing service from being provided to the subscribers accommodated by that DBP, the method relocates the subscriber information held by the failed DBP to other DBPs thereby ensuring service continuity.

The relocation method is activated when FS, which monitors the state of DBPs, judges that a double-system failure has occurred. It selects the DBPs for relocating the subscriber information depending on the number of subscribers involved and traffic volume.

In more detail, FS expands subscriber information to memory in the

*9 **FS-FRAID**: RAID equipment for FS use. Functions as external storage equipment for backing up data related to system maintenance/operations and equipment management via a fiber channel.
*10 **Chassis**: Housing that accepts a blade server and mounts on a rack.
*11 **aTCA**: Industrial standard specifications for operator-oriented next-generation communication equipment defined by the PCI Industrial Computer Manufacturers Group (PICMG).
*12 **HS3**: BacKup SToraGe (BKSTG) within a unit. External storage equipment used to store backed up data within a unit and to perform replication with backup centers. Also used to store backed up data from multiple units through replication with D-SCPs.

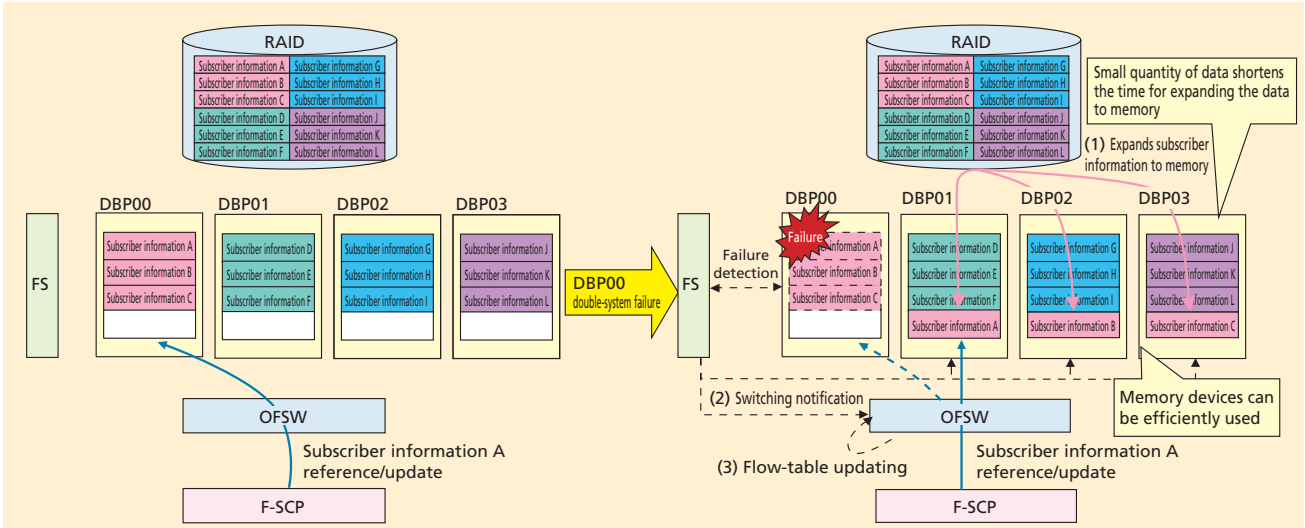

Figure 5 Overview of relocation method

destination DBPs from the RAID storing the latest data backup (Fig. 5(1)) and notifies OFSW of this DBP switching (Fig. 5(2)). The OFSW, in turn, updates the flow table to reflect those destination DBPs (Fig. 5(3)). This redirection to different DBPs by OFSW makes relocation transparent to F-SCP. In addition, subscriber information placed in DBPs is subdivided according to RAID partitions, and the relocation of subscriber information is dispersed among multiple DBPs to shorten the time needed to expand that data to memory.

A manual relocation function for execution by maintenance personnel is also provided to enable relocation of accommodated subscribers with the aim of achieving efficient facility utilization.

4.2 Backup Center Switching Method

Service continuity may be affected by an inability to restore service through relocation or by an equipment or network failure. In such a situation, a D-SCP master running during normal times activates switching to a backup center, which is then operated as an alternative master to prevent the customer from being impacted by such a failure.

An overview of the backup center switching method is presented in **Figure 6**. In this method, the D-SCP master sends a standby request to a backup center on detecting a single-system equipment failure that may require backup center switching. On receiving this standby request, the backup center expands RAID backup data to memory, constructs a subscriber information database, and places itself in a standby state ready for backup switching. Doing this beforehand enables high-speed, automatic switching when an actual switching request is later received from the master.

Switching to a backup center may be accomplished automatically by either of two methods. In one method, the master detects a failure within the system on its own and sends a switching request to the backup center (Fig. 6(a)). In the other method, the primary backup center performs a health check[*16] on the master to monitor its state of operation (Fig. 6(b)). Manual switching may also be performed by maintenance personnel.

The backup center constructs a database to hold the master's subscriber information and notifies F-SCP of backup center switching. On receiving

*13 **Replication**: A data-copy process between file systems performed on a one-to-one basis (HS3 creates a file system and controls its access). Defines pairs of replication sets between file systems. Copies data sets not stored in the transfer destination and copies just differences if data sets have already been stored.

*14 **Relocation**: Switching communications equipment such as area switches during communication.

*15 **Double-system failure**: A failure that occurs in both the active and standby systems in a redundant configuration.

*16 **Health check**: A method for detecting abnormalities by having equipment periodically check the operational state of neighboring equipment.

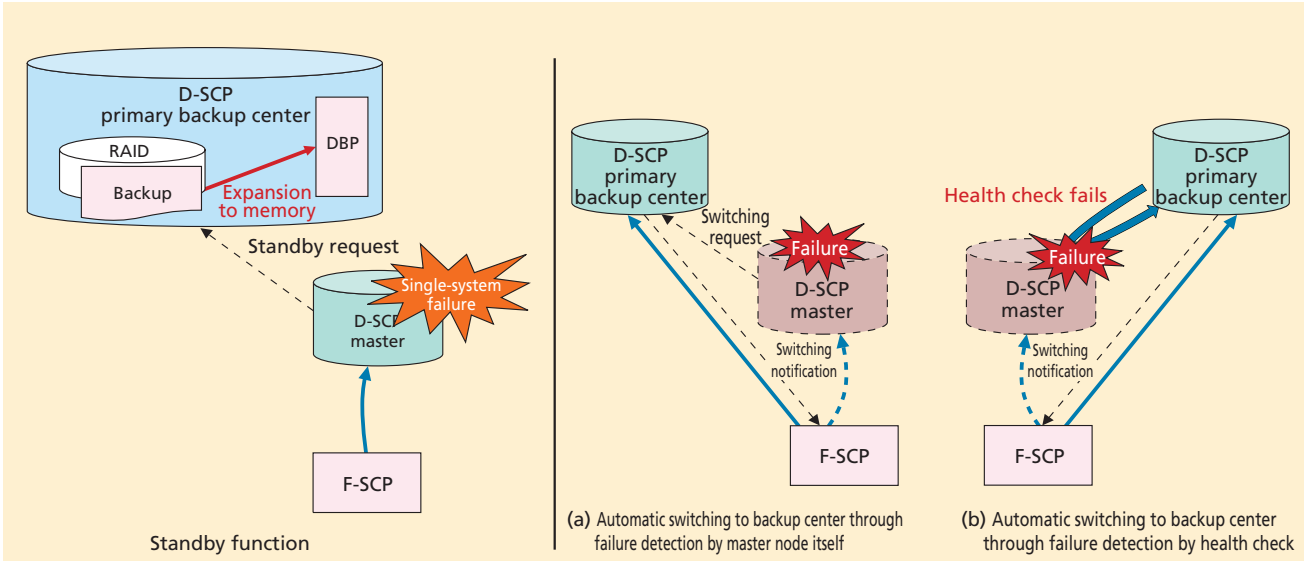

Figure 6 Overview of backup center switching method

notification of this switching, F-SCP changes the data-access destination from the master to that backup center.

Reliability is further ensured by constructing two backup centers—a primary and secondary one—so that the D-SCP can switch to the secondary backup center as a means of restoring service in the event that it is unable to switch to the primary backup center.

5. Conclusion

In this article, we described the effects of dividing up the IPSCP into F-SCP and D-SCP sections with different functions and introduced the system configuration of the newly constructed D-SCP focusing on its distinguishing functions. Looking forward, we plan to migrate all IPSCP-accommodated subscribers to D-SCP, improve reliability even further, and increase the functionality and functional extendibility of the network.