F-SCP D-SCP Round robin selection

Technology Reports

"F-SCP" Service Control Equipment Providing Higher Reliability Services

IPSCP provides important functions on the NTT DOCOMO mobile communications network such as subscriber information management, call sending and receiving, and providing additional services. Therefore, these systems require a high level of reliability. To improve reliability, we separated IPSCP into F-SCP, which controls IPSCP, and D-SCP, which is the DB section. By separating these sections, opposing devices such as exchange equipment can access subscriber information (in D-SCP) no matter which F-SCP the opposing devices access. Thus, higher reliability can be ensured by distributing load across F-SCPs and controlling access if an F-SCP malfunction occurs. This article describes F-SCP.

Core Network Development Department

Tomonori Kagi
Jun Kakishima
Kohei Yamamoto
Toru Hasegawa

1. Introduction

On its mobile communications network, NTT DOCOMO uses IP Service Control Point (IPSCP) to achieve Home Location Register (HLR)*1 and Home Subscriber Server (HSS)*2 functions to manage user subscriber information and location information, control call sending and receiving, and location registration. As well as the recent spread of M2M (Machine to Machine)*3 terminals that has increased subscriber numbers that must be managed, new services such as Voice over LTE (VoLTE) are also projected to increase traffic for IPSCP. For this reason, we separated DB functions from IPSCP as Database SCP (D-SCP) to efficiently scale out*4 equipment to handle subscriber increases [1].

Currently, we use IPSCP as control sections, however, we will deploy Front end SCP (F-SCP) as the successor to IPSCP to cope with future increases in traffic, and to enable processing to continue and provide users with reliable services during disasters or malfunction events (**Figure 1**).

This article describes F-SCP device configuration, load distribution and methods of improving reliability, as well as issues with separation and their countermeasures.

2. Improving Reliability by Round Robin F-SCP Selection

Up to now, all F-SCP-opposing devices selected the destination IPSCP based on subscriber telephone numbers etc. Because the F-SCP to be deployed does not store subscriber information, opposing devices do not need to select F-SCP based on subscriber information. For this reason, the signal destination F-SCP will be selected by round robin selection*5 to distribute load and risk (**Figure 2** (a)). Since the conventional

*1 **HLR:** A logical node defined by the 3GPP with functions for managing subscriber information and call processing.
*2 **HSS:** A subscriber information database on a 3GPP mobile network that manages authentication and location information.

IPSCP adopts an ACT/SBY configuration*6, if both ACT/SBY units malfunction the relevant subscriber information becomes inaccessible. However, with round robin selection, services can be continued even if a number of F-SCPs malfunction. Also, when there is an increase in signals for certain numbers due to traffic spike*7, the load can be distributed across a number of F-SCPs.

Furthermore, if an F-SCP malfunction occurs, each opposing device removes

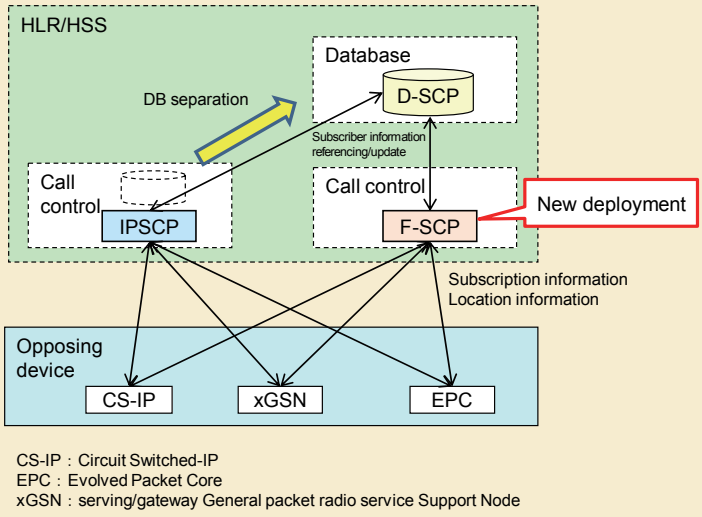


Figure 1 F-SCP and D-SCP network configuration

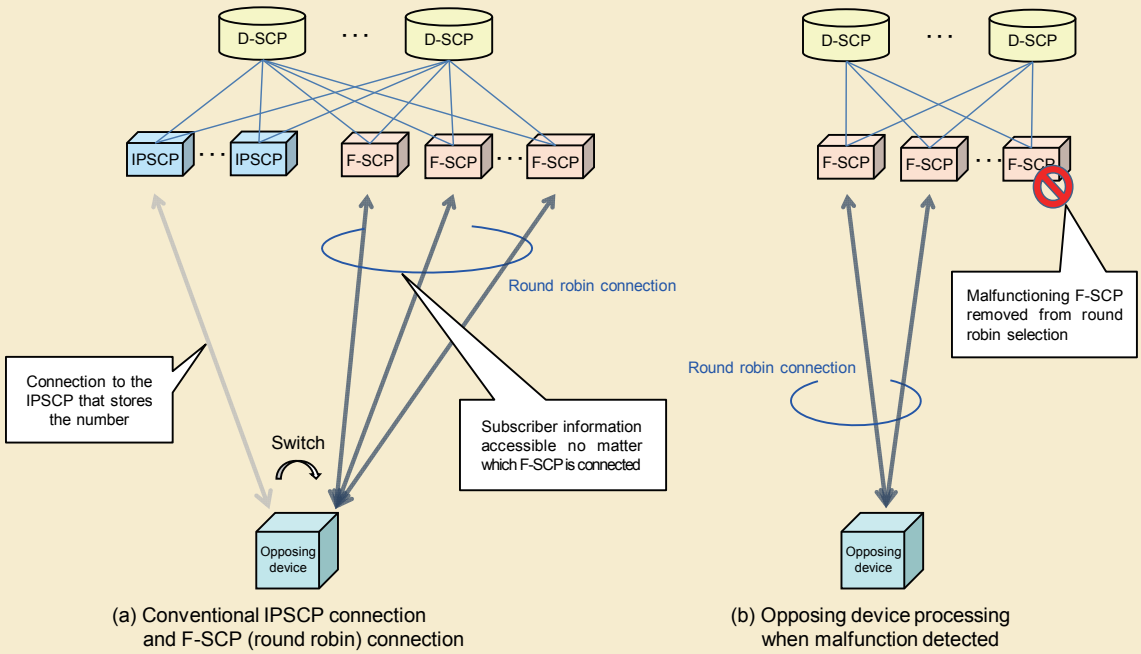


Figure 2 Round robin overview

*3 **M2M:** Machine-to-Machine Communications between machines. Systems that enable machines to communicate with each other without any human mediation.

*4 **Scale out:** Adding and assigning new resources to reinforce processing capacity when service requests increase and there is insufficient processing capacity on the network.

*5 **Round robin selection:** A selection method using a round robin. A Round robin is one way to distribute load over a network. It entails preparation of a number of devices capable of the same processing, and allocating requested processes to them in sequence.

*6 **ACT/SBY configuration:** A system configuration in which two servers perform the same function with one server in active mode (ACT) and the other in standby mode (SBY). If the ACT server malfunctions, the SBY server immediately takes over to prevent service outages. The ACT state is always retained in the SBY in readiness for switching over.

*7 **Traffic spike:** A sudden increase in traffic.

the F-SCP judged to have failed from the round robin selection, stops sending signals to it, and continues services (Figure 2 (b)).

3. F-SCP Equipment Configuration

1) Equipment Configuration

The hardware configurations of IPSCP and F-SCP are shown in **Figure 3**.

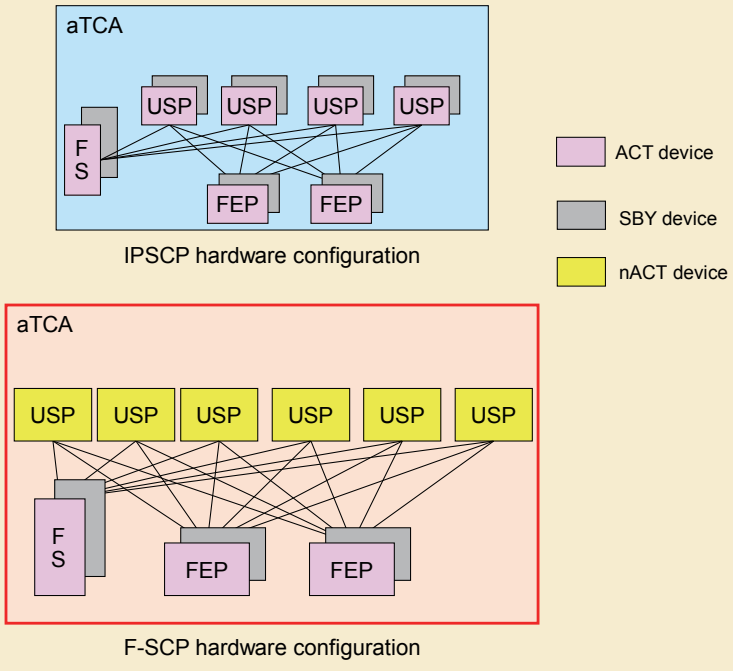
Both IPSCP and F-SCP are equipped with a Front End Processor (FEP), File Server (FS) and User Service Processor (USP).

FEP is a blade*8 that has Diameter*9/GSM-MAP (Mobile Application Part)*10 protocol termination, while FS is a blade that has HTTP/SO (Service Order)*11 protocol termination and regulatory control. These functions are the same in IPSCP and F-SCP. Furthermore, to ensure high reliability, both FEP and FS are configured for ACT/SBY.

USP is a blade that resolves the address to determine D-SCP and processes calls to provide services based on subscriber information. Because IPSCP retains subscriber information in USP, user call processing must be performed in a specific USP. High reliability is ensured by configuring USP for ACT/SBY, by switching to the SBY system if there is a USP malfunction. In contrast, because F-SCPs do not retain subscriber information in USP, it's possible to switch to another USP if one malfunctions. For this reason, the nACT configuration*12 was adopted for F-SCP because processing is possible even if more than one USP fails.

2) Round Robin Selection

The opposing device selects the FEP and FS individually using round robin selection. Round robin selection is also performed for blades in F-SCP equipment for load distribution and improved reliability. The FEP or FS that receives signals from an opposing device performs USP round robin selection. An overview of USP round robin selection is shown in **Figure 4**.



aTCA : advanced Telecommunications Computing Architecture

Figure 3 IPSCP and F-SCP hardware configurations

*8 **Blade:** A device inserted into a blade server case. Mainly refers to servers equipped with a CPU and memory.

*9 **Diameter:** An extended protocol based on Remote Authentication Dial In User Service (RADIUS), and used for authentication, authorization and accounting in IMS.

*10 **GSM-MAP:** A communications protocol used between HLR and SGSN.

*11 **SO:** A protocol used for transmitting and receiving signals with customer information management systems.

*12 **nACT configuration:** Distributes the load across n number of servers operating in parallel. If a server malfunctions, its processing can be taken over by another server.

4. Isolation Control

F-SCPs must be able to handle call processing functions and continue services even when malfunctions occur. This chapter describes typical F-SCP and USP system isolation functions for service continuity.

Isolation is an opposing device or opposing blade function that disables round robin selection for the relevant F-SCP or USP.

4.1 F-SCP System Isolation

If there is an F-SCP system malfunction, F-SCP autonomously performs system isolation processing. After that, opposing devices detect that the F-SCP has been isolated, and delete it from the round robin selection.

The following describes triggers for F-SCP system isolation.

(1) Three or more USP units have malfunctioned

(2) Both FS ACT and SBY systems have malfunctioned (double-system failure*13) and restarted (service is suspended during restart (device reboot))

(3) Both FEP ACT and SBY systems have malfunctioned (double system failure) and restarted

Recovery is only possible manually using commands. This is because while the line between F-SCP and the opposing device is unstable there is a risk of repeated isolation and recovery, and because the stability of F-SCP must be confirmed.

The main criteria used to judge F-SCP isolation in an opposing device are as follows:

- The link is disconnected (GSM-MAP connection)
- When Stream Control Transmission Protocol (SCTP)*14 Association*15 is not established, Abort*16 is returned by an F-SCP for a connection request from an opposing device, or, the opposing device detects an abnormality with the F-SCP health check*17 (Diameter connection)
- The opposing device Load Balancer (LB)*18 is informed from the F-SCP that connection is not possible (HTTP connection)

An example of the malfunction detection and recovery sequence is shown in **Figure 5**.

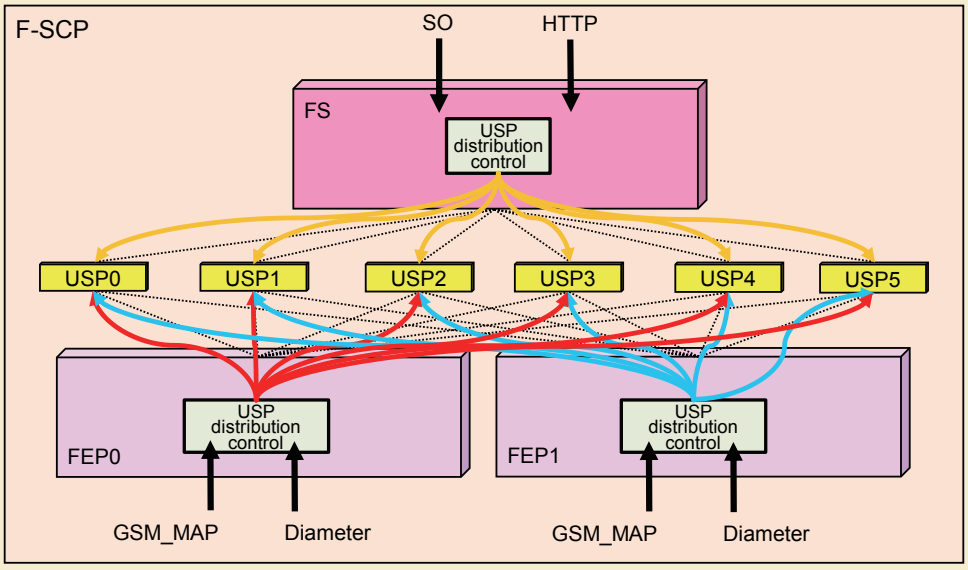


Figure 4 USP round robin overview

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

*14 **SCTP:** A transport layer protocol created to transmit telephone network protocols over IP.

*15 **Association:** A communications route established between a client and server with SCTP.

*16 **Abort:** Refusal of a request signal or suspension of communications.

When F-SCP automatically performs isolation, SCTP communications are instantly cut to prevent opposing device signal buffer overflow and impacts on resources.

4.2 USP Isolation

If a USP is malfunctioning, FEP/FS delete it from the round robin selection to ensure service continuity.

FEP/FS use the following detection triggers. If services are judged not to be continuous, they isolate the relevant USP.

(1) USP restart event

(2) USP malfunctions and errors in communications with USP detected periodically

The USP isolates itself with any of the following detection triggers:

(3) All health checks abnormal between D-SCPs (DBP: Data Base Processor*19)

Recovery triggers are as follows:

- USP restart has finished
- USP communications status is normal for a certain amount of time
- At least one health check possible between D-SCPs (DBP)

It is also possible to isolate/recover a specific USP manually with commands.

5. Issues with Round Robin Selection

1) Issues

If call processing becomes concentrated on a number range stored in a particular D-SCP when performing round robin selection with separated F-SCPs and D-SCPs, there is a possibility of signals from multiple F-SCPs converging on one D-SCP, which could cause the D-SCP to become congested*20. To solve this issue, F-SCPs are equipped with functions control flow to D-SCPs.

2) Flow Control

An overview of flow control is shown in **Figure 6**. With a D-SCP, the amount of traffic is periodically notified to FS from each DBP. Monitoring is performed in FS in D-SCP so that the amount of DBP traffic does not exceed its threshold. If the amount of traffic exceeds the threshold per unit time, the D-SCP FS notifies of the congestion to all F-SCP

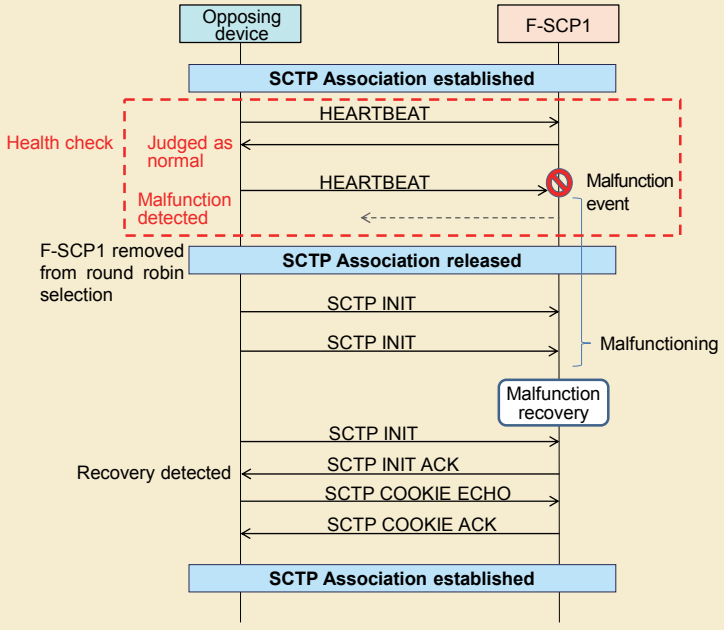


Figure 5 Malfunction detection and recovery sequence example (link disconnected)

*17 **Health check:** A periodic check of the operation of adjacent devices to detect abnormalities if they occur.

*18 **LB:** A device that distributes the load of request signals from clients across a number of servers, and detects malfunctions.

*19 **DBP:** The blade that stores subscriber information in a D-SCP. Notifies subscriber information to an F-SCP for reference requests from the F-SCP, and updates subscriber information for update requests.

*20 **Congestion:** Impediments to communications services due to communications requests being concentrated in a short period of time and exceeding the processing capabilities of the communications control server.

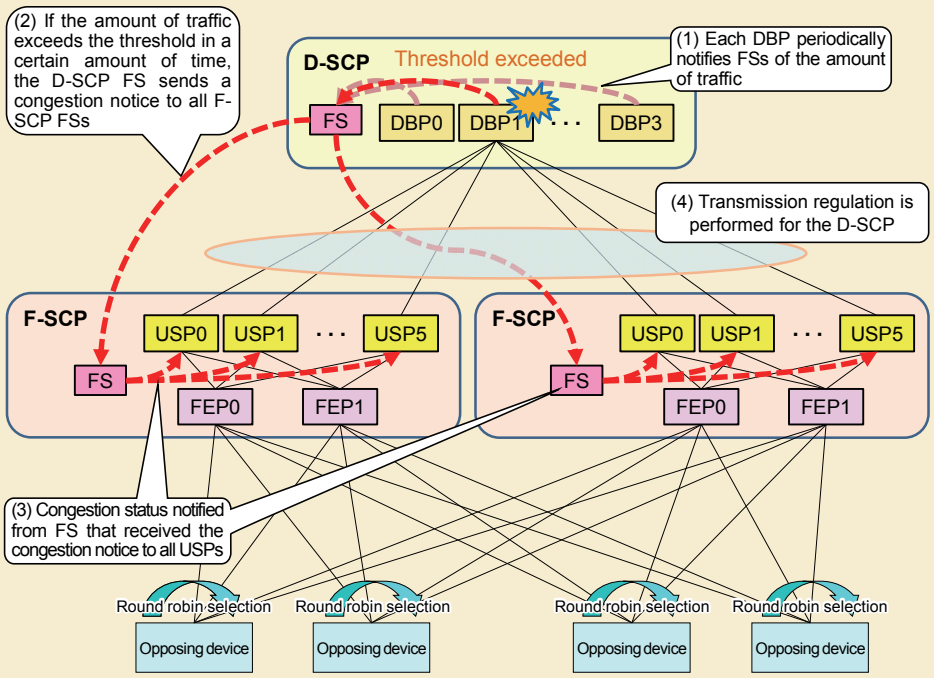


Figure 6 Overview of flow control

FSs. The F-SCP FSs then notify all USPs in the system of the congestion and control transmission to the D-SCP.

6. Conclusion

With F-SCP positioned as successor technology to IPSCP, this article has described related round robin selection functions between opposing devices, device configurations, round robin selection functions in devices, isolation control functions and flow control functions for D-SCP congestion. Deploying F-SCPs and D-SCPs will enable the quick response and flexibility needed to handle future increases in subscribers and traffic. These systems will also enable NTT DOCOMO to provide users with uninterrupted services when there are malfunctions such as during disasters.

We plan to move all opposing device connections from IPSCP to F-SCP to further improve performance and add more functionality.

Reference

[1] K.Otsuka, et al.: "Enhanced Service Control Equipment Supporting Diverse NTT DOCOMO Services," NTT DOCOMO Technical Journal, Vol. 14, No. 4, pp. 37-42, Apr. 2013.