ACB SSAC SCM

Technology Reports

Further Development of LTE-Advanced—Release12 Standardization Trends—

Access Class Control Technology in LTE/LTE-Advanced Systems

Fast market penetration of smartphones has caused not only rapid growth of mobile data traffic, but also changes to communications types (e.g., human to human, human to server/machine and machine to machine). These have brought demands for access control technologies to ensure robust and reliable communications in situations where networks are highly congested such as disasters. The importance of access controls to secure communications during disasters has increased, especially since the Great East Japan Earthquake. Thus, mechanisms to control mobile data traffic for different scenarios and needs have been specified and standardized in 3GPP in recent years. This article describes and explains the motivation for developing and the behaviors of these standardized access control mechanisms.

Radio Access Network Development Department — *Kenichiro Aoyagi* †
Wuri A. Hapsari
Communication Device Development Department — *Shinya Takeda*
Core Network Development Department — *Itsuma Tanaka*

1. Introduction

The advances of the smartphone and its rapid market penetration in recent years have brought about massive amounts of mobile data traffic on mobile communications networks as well as dramatic changes to the types of communications traffic, ranging from traditional peer to peer communications to communications in which applications autonomously exchange signals with servers. In high-speed, high capacity mobile communications systems, traffic congestion controls are crucial for maintaining service stability in different situations. Furthermore, during major disasters such as the Great East Japan Earthquake, mobile data traffic can increase to unanticipated levels and cause the network to malfunction, which is a major cause for concern (**Figure 1**). Therefore, mobile communications systems need mechanisms to prevent such unanticipated high traffic before it occurs. Moreover, to ensure successful communications for emergency calls (e.g. emergency numbers 110, 118, 119 in Japan) and/or disaster message boards, traffic congestion control mechanisms must reduce non-critical/non-high priority calls to make sure that network resources for critical/high-priority and emergency calls are available

† Currently Network Department

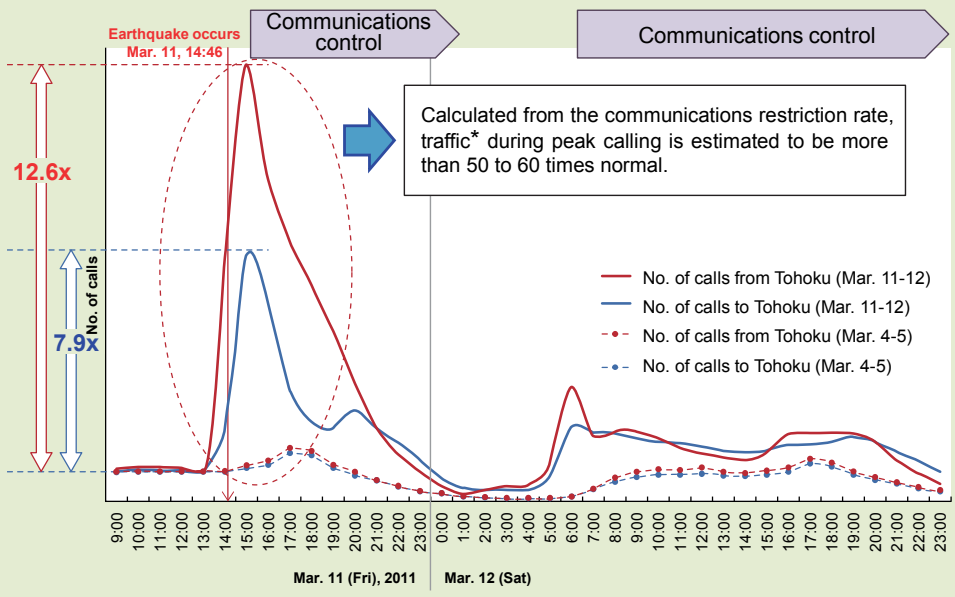

Figure 1 Example of mobile phone congestion and communication restrictions in the Tohoku region

to as many users as possible. In addition, under the law in Japan, mobile terminals must be equipped with access control functions (Telecommunications Business Law, Terminal Equipment Regulations, Article 28 stipulates that, in order to secure critical communications, in case of receiving call restriction request signal transmitted from a mobile communications facility, a mobile telephone terminals must be equipped with functions to refrain from sending a call).

3GPP has been standardizing a series of traffic congestion mechanisms to control mobile communication access to the network. One access control mechanism standardized as part of 3G (UMTS) specification and widely used in LTE is called "Access Class (AC)" control, which is a control technology that uses priority identifier data stored in terminals. Responding to the development of terminals and communications services of recent years and the dramatic changes to the types of traffic, these controls offer more detailed traffic control. This article describes an overview of the trends and mechanisms of access class control in LTE/LTE-Advanced systems.

2. Overview of Access Class Control in Traffic Congestion Control

2.1 Radio Access Barring Control

Radio access barring control refers to a traffic congestion control technology whose main purpose is to secure and ensure the success of critical communications such as emergency calls, by restricting connection request (RRC CONNECTION REQUEST) from mobile terminals to base stations. Radio access barring control can be categorized as the following two methods:

- Access Class control method (control in mobile terminals)

  Before a mobile terminal sends the connection request to the base station, the mobile terminal identifies the type of call and determines whether a connection request for the call should be barred.
- RRC CONNECTION REJECT method (control in the base station)

  The base station identifies the type of signals that triggers the connection request sent from mobile terminals, and decides whether this request should be rejected (by sending RRC CONNECTION REJECT) or

accepted.

Mobile network operators may use one or both of the above two radio access barring controls depending on network congestion and traffic conditions. This article focuses on the former method, i.e., the Access Class control. Access Class control enables controlling traffic from all terminals simultaneously in a given area by setting barring information for each AC in the system broadcast information *1 sent continuously by base stations. Also, this method does not cause network processing load because connection request are restricted/barred, i.e., are not being sent to the base station, by each terminal. Therefore, this control is suitable for application in overload scenarios such as spikes in signal processing that occur in base stations, since this control can be implemented quickly over a wide area.

Also, compared to the RRC CONNECTION REJECT method performed by base stations, since Access Class control is performed by identifying the types of calls or services to be restricted in the mobile terminals, the control of radio access restriction for different type of call (e.g. voice, applications) can be done much more precisely and with better flexibility. Thus, in 3GPP standards, Access Class controls have been gradually enhanced in different 3GPP Releases to meet the needs of network operators and the market. These enhancements are described in **Figure 2** and explained as follows.

(1) Access Class Barring (ACB)

Firstly, because all services in LTE/LTE-Advanced network architecture including voice utilize the Packet Switch (PS) domain*2, ACB was defined in 3GPP Release 8 as a basic access class control mechanism for all packet transmissions (see Chapter 3).

(2) Service Specific Access Control (SSAC) and ACB for Circuit Switch FallBack (CSFB)

SSAC was standardized to handle communications during large scale disasters, because people tend to use voice services to confirm the safety of family and friends since voice services are known to have higher reliability than other packet services. This tendency results in sudden increases in voice traffic. Thus, to satisfy the above service requirements, voice services in these circumstances need to be restricted. For this purpose, SSAC access class control for Voice over LTE (VoLTE) services and ACB for CSFB access class control for CSFB voice services were defined in Releases 9 and 10 respectively (see Section 4.1).

(3) Smart Congestion Mitigation (SCM)

In addition to the data communications done intentionally by users,

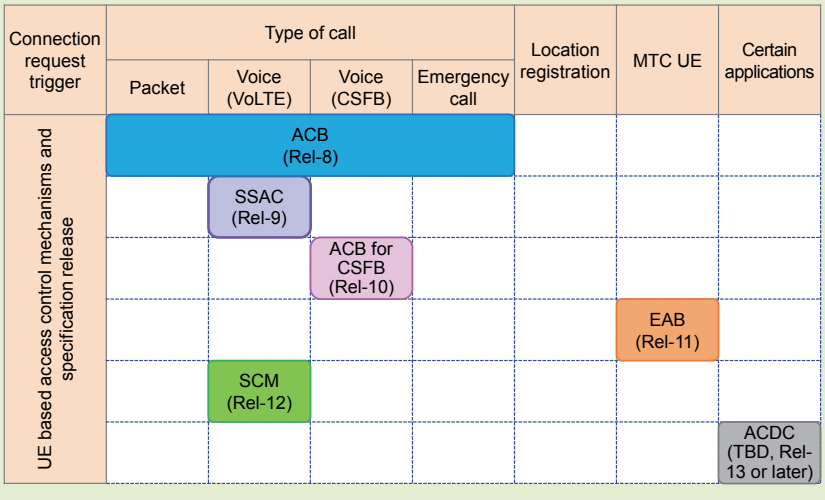

Figure 2 Access class control in LTE/LTE-Advanced systems

*1 **Broadcast information:** Information necessary for a mobile terminal to connect to a cell, which includes call restriction and barring information. This information is unique to each cell.

*2 **PS domain:** A network domain that provides services based on packet switching.

most smartphones run background applications that regularly send connection request to the network for exchanging data with application servers. For these reasons, in public festivity scenarios such as fireworks displays or concerts where many users come together in the same place, smartphone data communications can trigger network congestion*3. The ACB controls mentioned above prevent network congestion caused by smartphones by restricting all packet data transmissions including voice calls, which lowers the success rate of voice services. Therefore, there have been demands to enable prioritizing voice data above packet data (non-voice data). To satisfy these demands, SCM, an access control for prioritizing voice services (VoLTE) while restricting other packet data services, was defined in Release 12 (see Section 4.2). Combinations of SCM and other access class controls such as ACB and SSAC enable independent control of packet and voice data.

(4) Extended Access Barring (EAB)

There has also been ongoing study and implementation of Machine-to-Machine (M2M) communications technologies and services in recent years. There are a range of businesses that could utilize M2M terminals such as automatic vending machines and smart meters, hence a huge number of access from these terminals is foreseen. To accommodate both M2M terminals and typical smartphone terminals on the same network, the network needs to ensure that access from M2M terminals does not impede access from typical smartphone terminals. To achieve this, EAB access control that enables differentiation between the two types of terminal was defined in Release 11 (see Section 5.3).

(5) Access Control for general Data Connectivity (ACDC)

There are also discussions about requirements for emergency situations such as natural disasters, where packet data for "disaster message boards" (message board services where people can post whether they are safe so that relatives and friends can confirm that information via the Internet) should be given priority compared to other smartphone applications. To satisfy these requirements, new access class controls are being considered for Release 13 called "Access Control for general Data Connectivity (ACDC)" (see Section 5.1).

2.2 Access Class Control Features

AC is an identifier assigned by operator to each user to indicate its access priority and is stored in the Subscriber Identity Module (SIM)*4. As standardized in 3GPP, AC 0 to 9 is assigned to general users, AC 10 is assigned for emergency calls (e.g., emergency numbers 110, 118, 119 in Japan), while AC 11 to 15 are assigned for special or high priority users such as the users in public institutions or authorities such as police, fire departments and users/terminals belonging to network operators for maintenance purposes [1].

In access class control, the base station sends broadcast information containing control data (e.g. barring rate) set for each AC so that all terminals in its coverage area can receive the information simultaneously and promptly perform the access control (**Figure 3**). Thus, this mechanism is effective in reducing the amount of traffic accessing the network shortly after the broadcast (**Figure 4**). Appropriate adjustment of these control data settings enables optimized access restriction for different levels of network congestion. For example, when the network congestion level is high, the broadcast information can be updated to increase the barring rate (meaning reduce the successful call establishment rate). When a terminal attempts to perform a connection request, it reads the control data set in the broadcast information. Then, if the terminal's AC is subject to barring, based on the set parameter in the control data, the terminal will refrain from sending the connection request for a certain period of time.

In general, the purpose of applying access class control to AC 0 to 9 is to protect network equipment and to optimize communications traffic, while applying access class control to AC 10 and 11 to 15 such that no barring is applied, is to achieve secure communication for

*3 **Congestion:** A state in which the load (e.g., processing capabilities, resources, etc.) on a network entity exceeds a certain threshold per unit time due to traffic burst. This state can degrade services provided by the mobile network operator.

*4 **SIM:** An IC card which stores mobile phone subscriber information.

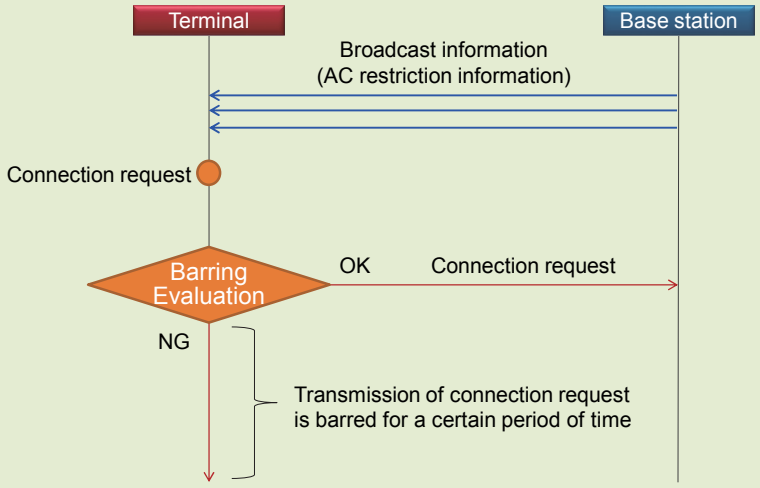

Figure 3 Access class control flow

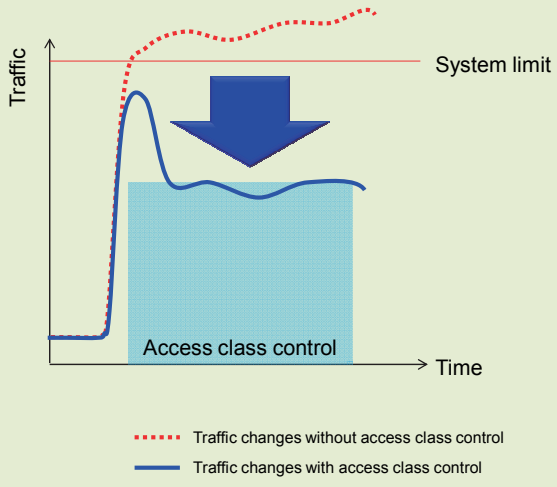

Figure 4 Traffic changes with and without access class control

emergency and high priority communications.

3. Access Class Control (ACB)

3.1 Packet Data Barring

As discussed above, ACB is applied to all packet data traffic originating in the LTE terminal traffic including VoLTE, because in LTE/LTE-Advanced network architecture, all packet data communications including voice services (VoLTE) are enabled by the PS domain.

In 3G, because 3G network architecture consists of two domains - the Circuit Switching (CS) domain that processes voice service and the PS domain that provides packet data service - Domain Specific Access Control (DSAC) was defined [1] to enable separate evaluation of access class control to each domain to enable independent and separate traffic control for voice/packet services. **Figure 5** describes how ACB is achieved for the different LTE and 3G architectures.

ACB is performed in the terminal RRC layer [2]. Based on the barring rate information broadcasted by the network, the terminal determines whether the connection request is allowed to be transmitted based on its AC. Furthermore, there are two types of packet data transmissions controllable with ACB - transmission of the connection request for general packet calls and emergency calls. For emergency calls, AC 10 is used.

3.2 Mobile Terminating Access Permission

When access control in 3G was first studied, connection requests for both "mobile-originating calls" from terminals and "mobile-terminating calls" as responses to paging sent from the network to terminals, were seen by the network as the same type of signal and thus handled in the same way, which meant that barring controls were applied to those signals in the same way.

During disasters, there are cases such that public authorities (police or fire department) call back victims who have already called an authority in an emergen-

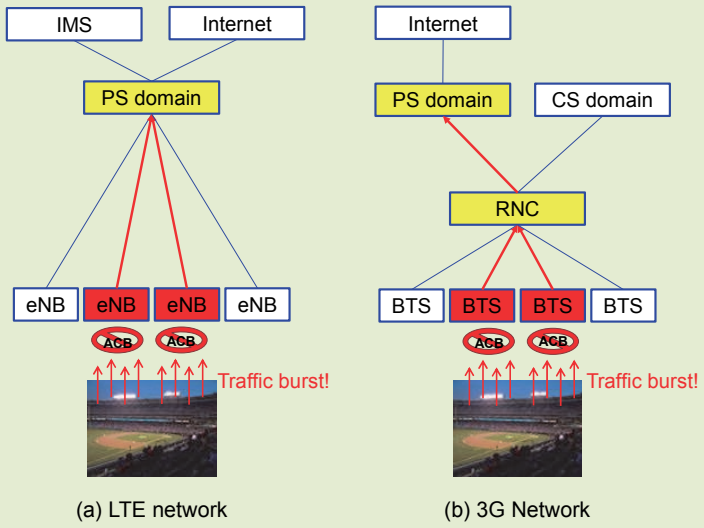

Figure 5 Different ACB mechanism for LTE and 3G architectures

cy to confirm their safety. In this case, the mobile-terminating call as a response to paging should not be barred. If the network decides to minimize the mobile-terminating call, the network will refrain from sending paging messages to UE. This mechanism was considered for LTE, and mobile-terminating access permission was standardized as part of the ACB functions. This is because paging response for voice services are also considered to be part of critical communications [3].

In 3G, this mechanism realized by defining a function called Paging Permission Access Control (PPAC), which was standardized in 3GPP Release 8 [1].

3.3 Access Control for Location Registration (Mobile Originating Signal)

Tracking Area Update (TAU)*5 (location registration in a service area) is required by terminals to receive incoming calls (paging) as described in Section 3.2. However, because it was not possible to separately set barring information for location registration signaling separate from packet data and voice data in 3G, connection requests for location registration were also barred in terminals. Therefore, if terminals move into new location registration areas, location registration cannot be performed because connection request to perform location registration is barred. In this case, the network cannot send paging to such a terminal because the network does not recognize where the terminal is camping and incoming calls cannot be received. To solve this issue, an AC to allow location registration was required. Barring of location registration signals is required for scenarios in which many terminals could send location registration signals simultaneously when crossing the border of a location registration area, which can lead to network congestion. For this reason, a barring parameter of location registration signaling (ac-Barring For MO-Signaling) separate from the barring parameter for ordinary data signaling (ac-Barring For MO-Data) is defined for ACB in LTE [1] [3]. Barring control for location registration signaling is performed in the same way as for barring evaluation performed by packet data connection establishment signaling described in Section 3.1 above. This function enables control of location registration traffic in different kinds of operational scenarios. For example, restricting packet data but allowing location registration means terminals can receive incoming calls during a disaster. The function can also prevent network congestion due to mobile terminals sending simultaneous location registration signals when buses or trains pass through location registration border areas during situations such as rush hour.

As mentioned, separate restriction functions for location registration have been standardized in 3G since Release 8 [1] as a part of PPAC.

4. Enhancements of Access Class Controls for Voice Services

4.1 Voice Service Restriction Controls

In large-scale disasters, traffic bursts

*5 **TAU:** A procedure for updating location registration in LTE.

occur due to signaling generated by people trying to contact friends and family to check their safety. When a traffic burst causes congestion on a network, simultaneously providing access for all types of communications and for all traffic is problematic. Generally in such cases, network resources for critical communications are secured by restricting traffic such as voice and video that use large amounts of resources while giving priority to services such as email and disaster message boards so that services are available to the largest number of users possible. The needs for these kinds of controls have become even more pronounced with the increase in communications with the various applications such as social networking accompanying the recent popularization of smartphones. For this reason, mechanisms to restrict voice services are specified in 3GPP, and described below. Emergency calls can be set so such that they are not subject to barring with any of these controls.

1) VoLTE Access Barring Controls (SSAC, SSAC in Connected)

(1) SSAC

In LTE, real time voice and video call services are provided in the PS domain as VoLTE using the IP Multimedia Subsystem (IMS)*6. In 3G, independent access restrictions known as DSAC are available for each CS domain that provides voice service and PS domain that provides packet data services. Unlike 3G, access restrictions only for voice services were not possible in LTE. Therefore, SSAC was defined to enable access restriction for IMS-based voice and video [1]. SSAC has also been designed to enable independent restriction of Video over LTE (ViLTE). NTT DOCOMO considers this functionality critical to ensure successful critical/emergency communications during disasters, and has provided it since the VoLTE service rollout in June 2014.

(2) SSAC in connected

Typically, smartphones applications have settings to regularly synchronize with servers. This results into frequent connection to the network and increasingly more time spent in the RRC connected state (the state in which a terminal is connected to the network, not in the IDLE state). Since the main purpose of access class control is to restrict the transmission of connection requests to the network, restrictions do not apply to terminals in the RRC connected state, because they are already connected. Due to concerns that traffic burst (generated by both background synchronization traffic or the foreground actual traffic) during disasters may impact the core network*7 equipment such as IMS nodes as well as base stations, SSAC should ideally be similarly applicable to terminals in the RRC connected state. For this reason, an access control function for IMS-based voice and video calls applicable to terminals in the RRC connected state called "SSAC in connected" was defined in 3GPP Release 12 [1]. Basically, SSAC is similar in functionality to ACB, but in SSAC, the barring control/evaluation is performed in the IMS layer instead of the RCC layer as it is in ACB. Here, AC barring information for SSAC broadcast by the network is used by the terminal to determine whether a VoLTE call is allowed or barred.

2) Access Control for CSFB Call (ACB for CSFB)

For LTE terminals that do not support the aforementioned VoLTE functions, voice services are provided with a mechanism called CSFB. CSFB is a mechanism that allows the network to transition an LTE terminal firstly connecting to an LTE network to a 3G CS domain to provide voice services on the 3G network. With CSFB, regardless of whether access class control is applied in LTE, terminals that have successfully transitioned to 3G from LTE apply access class controls broadcast by the 3G network. This means after successful CSFB transition, terminals making connection requests to the CS domain apply the 3G access class controls such as DSAC and PPAC, as described in Chapter 3. On the other hand, ACB for CSFB was defined to restrict connection request for CSFB calls when the terminal is still camping on the LTE network [1]. ACB for CSFB access class control works in similar man-

*6 **IMS:** A subsystem that provides IP multimedia services (e.g., VoIP, messaging, presence) on a 3GPP mobile communications network. SIP is used for the calling control protocol.

*7 **Core network:** A network consisting of switching equipment and subscriber information management equipment, etc. A mobile terminal communicates with the core network via a radio access network.

ner as the ACB restriction control. In this case, whether CSFB call is barred is determined by the ACB for CSFB access class control information broadcast by the network.

4.2 VoLTE Prioritization Mechanism

As explained in previous chapters, background data from applications in smartphones result in frequent attempts to connect to the network. In addition to that, there may be situations in which many users occupy the same coverage area (such as public events) or are simultaneously moving from one coverage area to another (such as on trains or busses). In these situations, since traffic burst due burst to smartphone application background and foreground date and also due to location registration can be expected, services such as VoLTE calls that are deliberately generated by the user should be prioritized over other traffic. Therefore, a mechanism that enables prioritization of voice services was defined and standardized in 3GPP. The following describes this priority control mechanism for voice services (**Figure 6**).

1) VoLTE Priority Control (SCM)

SCM is a mechanism newly defined in 3GPP Release 12 for UE to prioritize voice service so that even when ACB has been invoked by the network, ACB is not applied to VoLTE calls [1]. In other words, ACB evaluation is skipped for VoLTE calls. Service types to which ACB need not be applied are included in broadcast information. In addition to VoLTE, ViLTE and SMS are also defined as services that can be prioritized with SCM. The terminal decides which services to prioritize based on the broadcast information from the network indicating the service types for which ACB is to be skipped. In previous releases, prioritization by allowing access (not applying barring mechanisms) to a particular service was not possible, because the modem part of terminal where access control evaluation is performed cannot distinguish different kind of service types - i.e. whether it is a VoLTE call or some other packet data call. However, as part of SCM standardization, a function to notify the type of service of a packet (whether the packet is VoLTE, ViLTE or SMS) from the terminal IMS layer to the modem has been defined. This enables the modem to identify the type of service of a packet, and enables the terminal to skip ACB and allow the transmission of connection requests for VoLTE calls even when ACB is applied, thus enabling priority handling (Fig. 6 (a) bottom). Furthermore, SCM is designed so that it can be combined with SSAC described in Section 4.1. Hence, the combination of SSAC, ACB and SCM

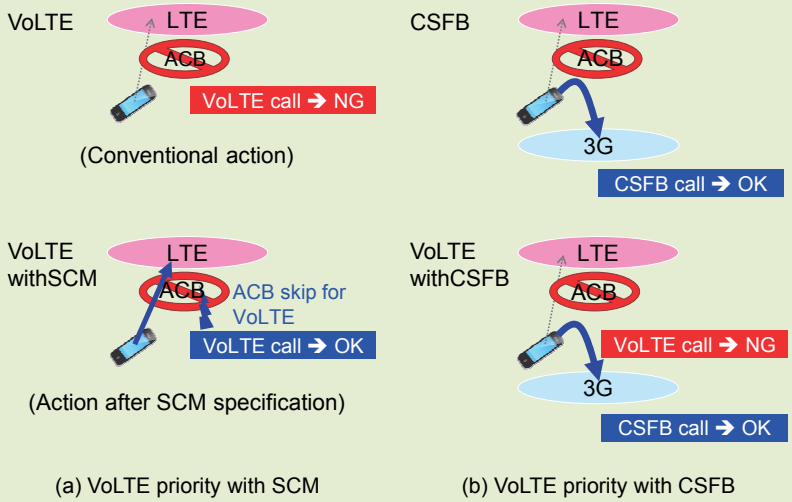

Figure 6 VoLTE priority control using SCM and CSFB

enables separate and independent access class controls for voice data and packet data. In other words, barring evaluation for voice calls will be governed only by SSAC, while in previous releases voice calls are always barred again by ACB after SSAC barring evaluation. These mechanisms enable LTE access barring capabilities comparable with 3G, since separate restriction controls for CS and PS domains are also available in 3G.

2) CSFB Priority Control (CSFB behavior when ACB is applied)

When ACB is applied in LTE, all mobile-originating calls are subject to ACB including CSFB calls. However, the standard specifies that if a CSFB call is barred as a result of ACB barring evaluation, the connection request for CSFB call not be transmitted in LTE, the terminal autonomously switch to the 3G network (by means of cell selection), and the CS connection request be sent in 3G [3] (Fig. 6 (b) top). In other words, in practice this action enables priority control of voice services by enabling CS calls in 3G even when CSFB calls are barred by ACB. The reasons for this specification are as follows: (1) a connection request for a CSFB call does not necessarily have to be sent to the LTE network because the main purpose of CSFB is to enable connection to the 3G CS domain, and (2) based on the concept of access class control, ideally a radio access network (in this case LTE) should not control the access barring of another system (in this case 3G). This is because after moving from LTE to 3G, access controls such as DSAC can be applied to handle 3G network congestions, as described in Section 4.1.

In contrast, bearing in mind that all packet data is subject to access control by ACB, voice calls from terminals that support VoLTE cannot be prioritized if the terminal or network does not support SCM described in Section 4.2 (Fig. 6 (a) top). Thus, from the user experience perspective, non-VoLTE CSFB terminals could access voice services more easily than VoLTE terminals if the LTE network is more congested than the 3G network, which is an issue in terms of the fairness of radio access barring controls. To prevent this situation, when VoLTE call is subject to ACB restrictions, standard specifications allow those terminals to switch to CSFB call autonomously to make a call request on the relevant voice service [4]. Hence, with this mechanism, voice services using VoLTE can be provided with behavior and performance comparable to CSFB when ACB is invoked. NTT DOCOMO has enabled this function since the VoLTE service rollout in June 2014.

5. Further Enhancement of Radio Access Barring Control and Future Developments

5.1 Access Class Control for Individual Applications (ACDC)

As a future access class control development, discussion on Access Control for general Data Connectivity (ACDC) is ongoing as part of 3GPP Release 13. The purpose of ACDC is to allow priority handling for individual applications [1]. In ACDC, data for categorizing applications is stored in terminals, and the network broadcasts barring information for the application categories subject to access control. Then, when a call from a certain application is generated, the terminal determines whether to allow the connection request for the call by referencing the barring information for the relevant application category in the broadcast. If ACDC standardization is completed and implemented in terminals and networks, application-based access control (i.e., allowing or barring connection requests for certain applications) will be possible. As a result, more precise access class control tailored to particular services will also be possible (**Figure 7**).

5.2 Network Sharing Support for Access Class Controls

Network sharing is technology that allows two or more telecommunication carriers to share the same network equipment. Different mobile network operators have different policies about the Quality of Experience (QoE) of the services they provide and set different values for their ACB restriction rates for the level of congestion on shared network equipment based on their own policies. Also, when networks are shared, access class controls by a telecommuni-

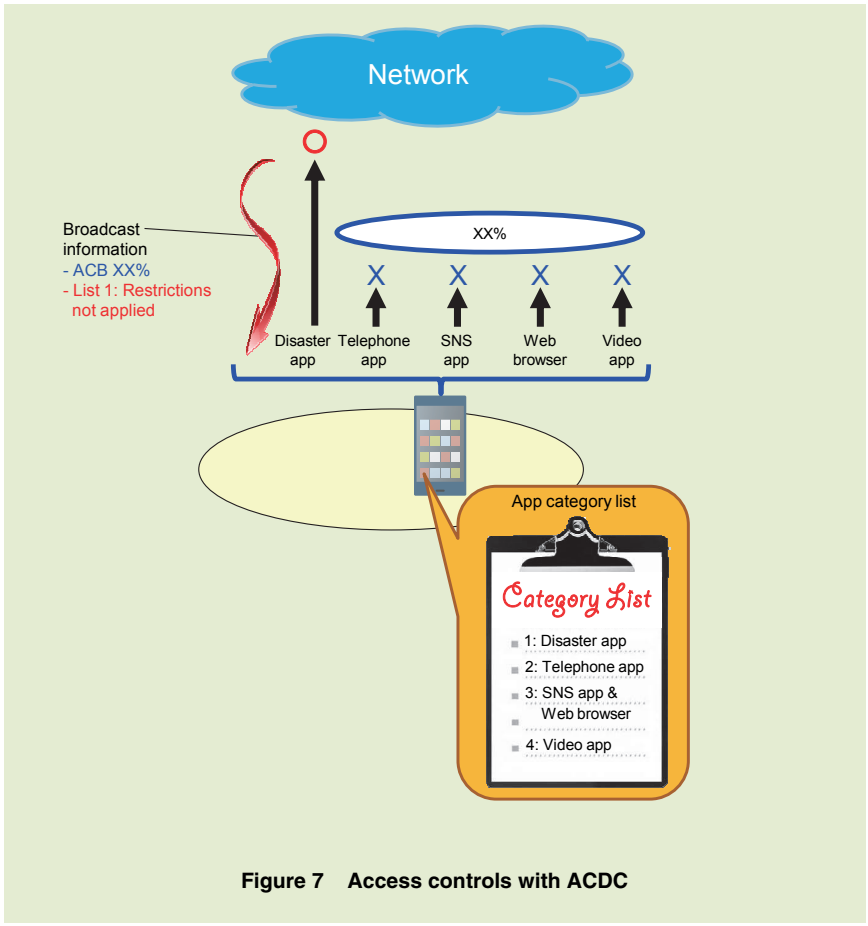

Figure 7 Access controls with ACDC

cation carrier due to their traffic must be prevented if it can dramatically affect the quality of another telecommunication carrier's services. For this reason, suitable methods for each mobile network operator to apply access class controls must be implemented in shared network environments.

Support of access control functionality for network sharing is defined for LTE in 3GPP Release 12 [1], and is achieved by allowing separate access control parameters to be set for each Public Land Mobile Network (PLMN)*8 ID that identifies the mobile network operator sharing the network equipment. When the network broadcasts access control parameters for a specific PLMN, the terminals that are registered to that PLMN apply and evaluate restrictions using the relevant parameters in the broadcast. If a broadcast does not contain any PLMN access restriction parameters, but contains common access restriction parameters, those common restriction parameters are applied.

5.3 Radio Access Barring Controls for M2M and MTC

In recent years, there have been extensive and popular studies on the so-called Internet of Things (IoT), a form of Internet communications between devices such as automatic vending machines, home appliances and smart meters. These communications could be used to address different kinds of business needs and purposes, such as IoT module-equipped vending machine, stock control, electricity usage management with smart meters, management of public transport with IoT terminal-equipped buses displaying the exact time buses will arrive at bus stops, etc.

To realize these systems using mobile communications networks, studies of M2M communications and Machine Type Communications (MTC) between devices and servers are ongoing [5]. However, as these businesses expand and applications of these technologies become more common and varied, the number of MTC (IoT) modules and communications traffic will increase dramatically, which could seriously affect the mobile communications networks.

In particular, there are concerns about traffic bursts triggered by MTC terminals sending connection requests all at once because they become disconnected from the network in the case of a server failure. Thus, Releases 10 and 11 included studies of access controls specifically for MTC terminals (**Figure 8**). Similar to normal traffic (non-MTC) control methods described in Chapter 2.1, access barring control for MTC terminals can be performed using (1) terminal-based access control mechanisms (EAB) that operate with the same concepts as the Ac-

*8 **PLMN:** An operator that provides services using a mobile communications system.

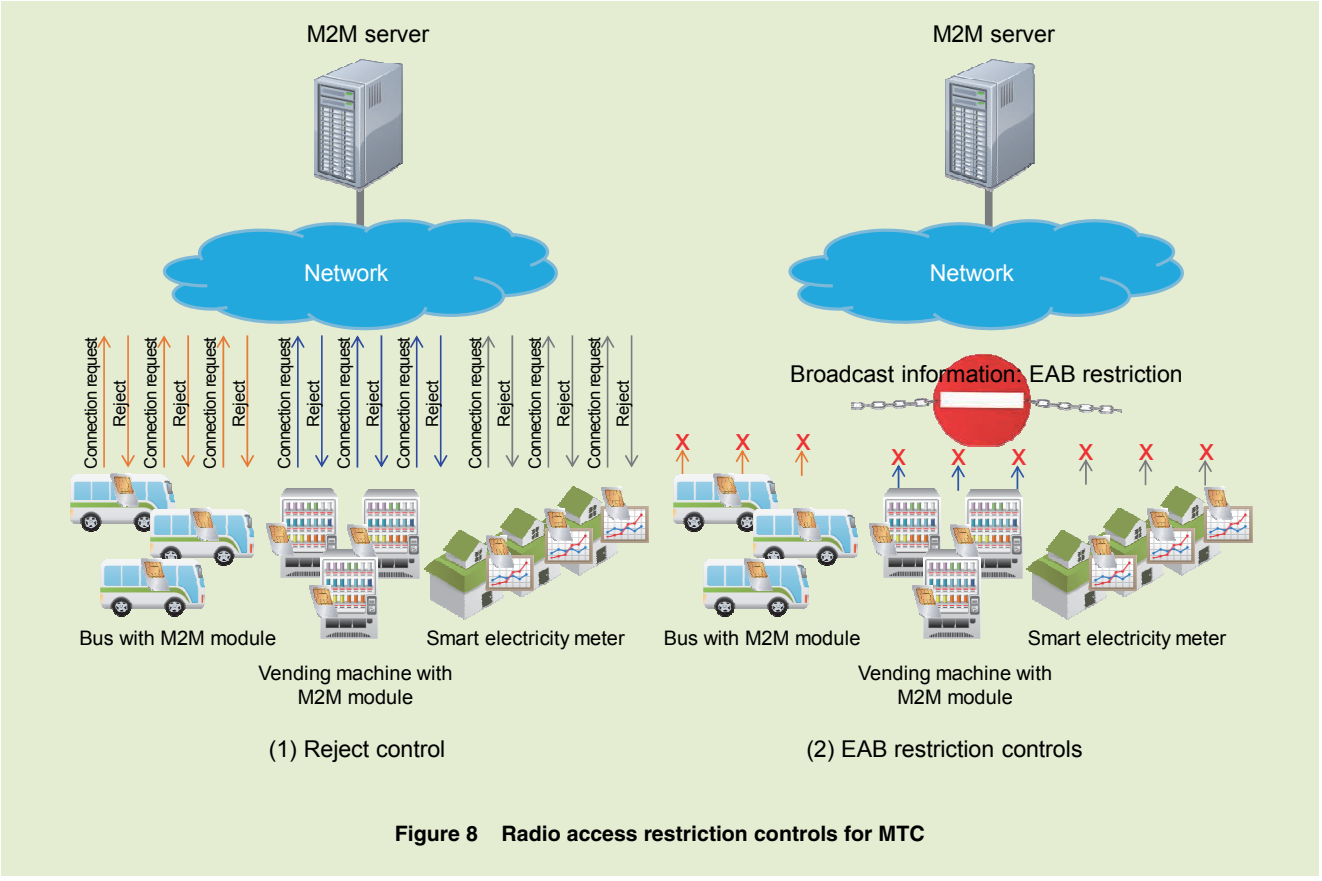

Figure 8 Radio access restriction controls for MTC

cess Class control mechanisms and (2) network-based controls, i.e., the RRC CONNECTION REJECT control mechanism. The network-based reject mechanism is performed using Delay Tolerant Access identification received in the connection request. This section describes both mechanisms to provide a clear overview of access restriction controls for MTC.

1) Reject Controls for Connection Requests Performed by Base Stations Using Delay Tolerant Access Identification

In the mechanism defined in Release 8, depending on the network congestion level, network equipment can reject connection requests from different call types (e.g., mobile originating calls (mo-Data), mobile terminating calls (mt-Access), and mobile originating signaling (mo-signaling) such as connection requests for location registration, and emergency calls) included in the RRC CONNECTION REQUEST message. However, it is not possible to distinguish MTC terminals using the above data identifiers.

For this reason, "Delay Tolerant Access" was defined in Release 10 to identify MTC terminals in the RRC CONNECTION REQUEST message. Network equipment identifies MTC terminals using Delay Tolerant Access, and performs controls such as rejecting access from MTC terminals in response to network congestion. Since most MTC communications are expected to be generated autonomously from ubiquitous devices, the requirements for connection latency and data speeds are not as demanding as conventional packet data services typically used by people such as Internet browsing or online gaming. Therefore, the above reject mechanisms can be used to delay MTC connection requests and spread out an MTC access burst over time [5].

2) EAB

On a network where MTC modules are used in different kinds of businesses, traffic bursts due to many MTC terminals simultaneously sending connection re-

quests can occur. Simultaneous connection requests from MTC terminals could happen during server outages or the simultaneous movement of large numbers of MTC-equipped mobile terminals from one coverage area to another. In such scenarios, access controls to stop terminals sending connection requests (such as ACB) are effective at reducing traffic congestion. For this reason, EAB access control that uses barring parameters for MTC terminals sent in broadcast information was defined in Release 11 [1]. One of the differences between EAB and ACB is how the terminal is differentiated/identified. In EAB, in addition to AC explained in Chapter 2, EAB categories are used to distinguish terminals and determine whether to bar access. EAB categories can also identify whether MTC terminals are roaming and whether terminals are registered to a mobile operator sharing the relevant network. Network can indicate whether EAB is supported during the Attach*9 procedure for instance, so that networks can set whether terminals are subject to EAB based on terminal capabilities and subscription data, etc.

6. Conclusion

This article has described an overview of access class control mechanisms defined for LTE/LTE-Advanced systems.

Progressing from LTE to LTE-Advanced and onwards to 5G, mobile communication systems will provide higher capacity and higher data speeds. At the same time, the need for dynamic, flexible and precise traffic congestion controls that can be applied in a wide variety of traffic situations will increase. R&D for real-time communications traffic congestion control during disasters or sudden events is regarded as a challenging aspect of raising reliability for the mobile communications networks of the future. Traffic congestion control mechanisms described in this article and their future enhancements play a critical role in maintaining the reliability of mobile communications networks. Into the future, NTT DOCOMO will continue to research, develop and enhance these technologies.

References

[1] 3GPP TS22.011 V13.1.0: "Technical Specification Group Services and System Aspects; Service accessibility," (Release 13), 2014.
[2] 3GPP TS36.331 V12.5.0: "Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification," (Release 13), 2015.
[3] 3GPP TS24.301 V13.1.0: "Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3," (Release 13), 2015.
[4] 3GPP TS24.229 V13.1.0: "Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3," (Release 13), 2015.
[5] 3GPP TS22.368 V13.1.0: "Technical Specification Group Services and System Aspects; Service requirements for Machine-Type Communications (MTC); Stage 1," (Release 13), 2014.

*9 **Attach:** The procedure of registering a mobile terminal to a mobile network when the terminal's power is turned on, etc.