SMPP

The **Short Message Peer-to-Peer (SMPP)** protocol is a telecommunications industry protocol for exchanging SMS messages between SMS peer entities such as short message service centers and/or External Short Messaging Entities. It is often used to allow third parties (e.g. value-added service providers like news organizations) to submit messages, often in bulk.

SMPP was originally designed by Aldiscon, a small Irish company that was later acquired by Logica (now split off and known as Acision). In 1999, Logica formally handed over SMPP to the SMPP Developers Forum, later renamed as The SMS Forum and now disbanded. The SMPP protocol specifications are still available through the website which also carries a notice stating that it will be taken down at the end of 2007. As part of the original handover terms, SMPP ownership has now returned to Acision due to the disbanding of the SMS forum.

The protocol is based on pairs of request/response PDUs (protocol data units, or packets) exchanged over OSI layer 4 (TCP session or X.25 SVC3) connections. PDUs are binary encoded for efficiency.

The most commonly used versions of SMPP are v3.3, the most widely supported standard, and v3.4, which adds transceiver support (single connections that can send and receive messages). Data exchange may be synchronous, where each peer must wait for a response for each PDU being sent, and asynchronous, where multiple requests can be issued in one go and acknowledged in a skew order by the other peer. The latest version of SMPP is v5.0.

SNMP

Simple Network Management Protocol (**SNMP**) is a UDP-based network protocol. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.[1]

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

Overview and basic concepts

In typical SNMP use, one or more administrative computers called managers have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an *agent* which reports information via SNMP to the manager.

Essentially, SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

An SNMP-managed network consists of three key components:

- Managed device
- Agent — software which runs on managed devices
- Network management system (NMS) — software which runs on the manager

A *managed device* is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An *agent* is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP specific form.

A *network management system* (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

[edit] Management information base (MIB)

Main article: Management information base

SNMP itself does not define which information (which variables) a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by management information bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP. MIBs use the notation defined by ASN.1.

[edit] Protocol details

SNMP operates in the Application Layer of the Internet Protocol Suite (Layer 7 of the OSI model). The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response will be sent back to the source port on the manager. The manager receives notifications (*Traps* and *InformRequests*) on port 162. The agent may generate notifications from any available port.

SNMPv1 specifies five core protocol data units (PDUs). Two other PDUs, *GetBulkRequest* and *InformRequest* were added in SNMPv2 and carried over to SNMPv3.

All SNMP PDUs are constructed as follows:

IP header	UDP header	version	community	PDU-type	request-id	error-status	error-index	variable bindings

The seven SNMP protocol data units (PDUs) are as follows:

[edit] GetRequest

Retrieve the value of a variable or list of variables. Desired variables are specified in variable bindings (values are not used). Retrieval of the specified variable values is to be done as an atomic operation by the agent. A *Response* with current values is returned.

[edit] SetRequest

Change the value of a variable or list of variables. Variable bindings are specified in the body of the request. Changes to all specified variables are to be made as an atomic operation by the agent. A *Response* with (current) new values for the variables is returned.

[edit] GetNextRequest

Returns a *Response* with variable binding for the lexicographically next variable in the MIB. The entire MIB of an agent can be walked by iterative application of *GetNextRequest* starting at OID 0. Rows of a table can be read by specifying column OIDs in the variable bindings of the request.

[edit] GetBulkRequest

Optimized version of *GetNextRequest*. Requests multiple iterations of *GetNextRequest* and returns a *Response* with multiple variable bindings walked from the variable binding or bindings in the request. PDU specific *non-repeaters* and *max-repetitions* fields are used to control response behavior. *GetBulkRequest* was introduced in SNMPv2.

[edit] Response

Returns variable bindings and acknowledgement for *GetRequest*, *SetRequest*, *GetNextRequest*, *GetBulkRequest* and *InformRequest*. Error reporting is provided by *error-status* and *error-index* fields. Although it was used as a response to both gets and sets, this PDU was called *GetResponse* in SNMPv1.

[edit] Trap

Asynchronous notification from agent to manager. Includes current *sysUpTime* value, an OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed *SNMPv2-Trap*.

[edit] InformRequest

Acknowledged asynchronous notification from manager to manager. This PDU use the same format as the SNMPv2 version of *Trap*. Manager-to-manager notifications were already possible in SNMPv1 (using a *Trap*), but as SNMP commonly runs over UDP where delivery is not assured and dropped packets are not reported, delivery of a *Trap* was not guaranteed. *InformRequest* fixes this by sending back an acknowledgement on receipt. Receiver replies with *Response* parroting all information in the *InformRequest*. This PDU was introduced in SNMPv2.

SS7 Network Architecture and Protocols Introduction

The International Telecommunication Union (ITU) is the international governing body for Signaling System No. 7. More specifically, it is governed by the Telecommunication Standardization Sector of the ITU (ITU-TS or ITU-T for short). Formerly it was governed by the ITU's Consultative Committee for International Telegraph and Telephone (CCITT) subcommittee until that was disbanded in 1992 as part of a process to speed up the production of recommendations (as well as other organization changes).

Signaling System No. 7 is more commonly known by the acronyms SS7 and C7. Strictly speaking, the term C7 (or, less commonly, CCS7) refers to the international Signaling System No. 7 network protocols specified by the ITU-T recommendations as well as national or regional variants defined within the framework provided by the ITU-T. The term C7 originates from the former title found on the specifications□CCITT Signaling System No. 7. The term SS7 tends to specifically refer to the North American regional standards produced by Telcordia (formerly known as Bell Communications Research or Bellcore) and the American National Standards Institute (ANSI). The North American standards themselves are based on the ITU-T recommendations but have been tailored outside the provided framework. The differences between ITU and Telcordia/ANSI are largely subtle at the lower layers. Interaction between ANSI and ITU-T networks is made challenging by different implementations of higher-layer protocols and procedures.

For the purpose of this book, we will use the term SS7 to refer generically to any Signaling System No. 7 protocol, regardless of its origin or demographics. An overview of SS7 by the ITU-T can be found in recommendation Q.700 [111], and a similar overview of SS7 by ANSI can be found in T1.110 [112].

"The Role of SS7" provides a comprehensive list of the functions and services afforded by SS7. These can be summarized as follows:

- Setting up and tearing down circuit-switched connections, such as telephone calls made over both cellular and fixed-line.
- Advanced network features such as those offered by supplementary services (calling name/number presentation, Automatic Callback, and so on).
- Mobility management in cellular networks, which permits subscribers to move geographically while remaining attached to the network, even while an active call is in place. This is the central function of a cellular network.
- Short Message Service (SMS) and Enhanced Messaging Service (EMS), where SS7 is used not only for signaling but also for content transport of alphanumeric text.
- Support for Intelligent Network (IN) services such as toll-free (800) calling.
- Support for ISDN.
- Local Number Portability (LNP) to allow subscribers to change their service, service provider, and location without needing to change their telephone number.

SS7 Network Architecture

SS7 can employ different types of signaling network structures. The choice between these different structures can be influenced by factors such as administrative aspects and the structure of the telecommunication network to be served by the signaling system.

The worldwide signaling network has two functionally independent levels:

- International
- National

This structure makes possible a clear division of responsibility for signaling network management. It also lets numbering plans of SS7 nodes belonging to the international network and the different national networks be independent of one another.

SS7 network nodes are called signaling points (SPs). Each SP is addressed by an integer called a point code (PC). The international network uses a 14-bit PC. The national networks also use a 14-bit PC, except North America and China, which use an incompatible 24-bit PC, and Japan, which uses a 16-bit PC. The national PC is unique only within a particular operator's national network. International PCs are unique only within the international network. Other operator networks (if they exist) within a country also could have the same PC and also might share the same PC as that used on the international network. Therefore, additional routing information is provided so that the PC can be interpreted correctly that is, as an international network, as its

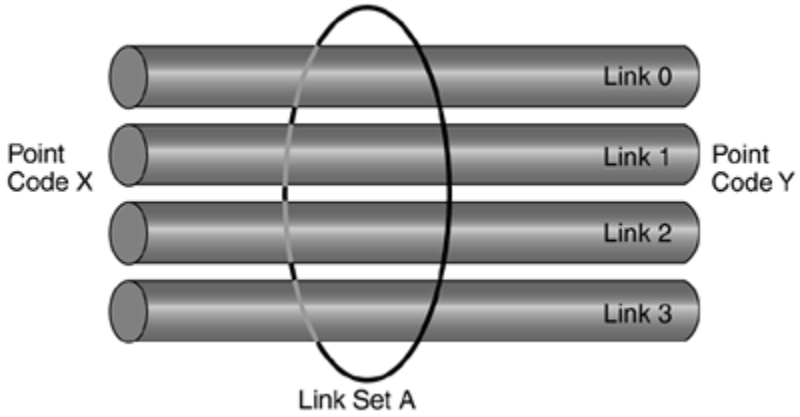
own national network, or as another operator's national network. The structure of point codes is described in Chapter 7, "Message Transfer Part 3 (MTP3)."

Signaling Links and Linksets

SPs are connected to each other by signaling links over which signaling takes place. The bandwidth of a signaling link is normally 64 kilobits per second (kbps). Because of legacy reasons, however, some links in North America might have an effective rate of 56 kbps. In recent years, high-speed links have been introduced that use an entire 1.544 Mbps T1 carrier for signaling. Links are typically engineered to carry only 25 to 40 percent of their capacity so that in case of a failure, one link can carry the load of two.

To provide more bandwidth and/or for redundancy, up to 16 links between two SPs can be used. Links between two SPs are logically grouped for administrative and load-sharing reasons. A logical group of links between two SP is called a linkset. Figure 4-2 shows four links in a linkset.

Figure 4-2. Four Links in a Linkset Between SPs



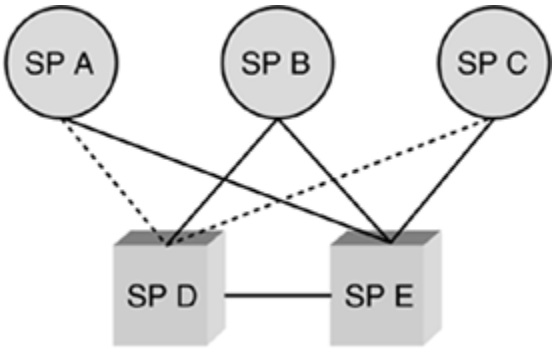
A number of linksets that may be used to reach a particular destination can be grouped logically to form a combined linkset. For each combined linkset that an individual linkset is a member of, it may be assigned different priority levels relative to other linksets in each combined linkset.

A group of links within a linkset that have the same characteristics (data rate, terrestrial/satellite, and so on) are called a link group. Normally the links in a linkset have the same characteristics, so the term link group can be synonymous with linkset.

Routes and Routesets

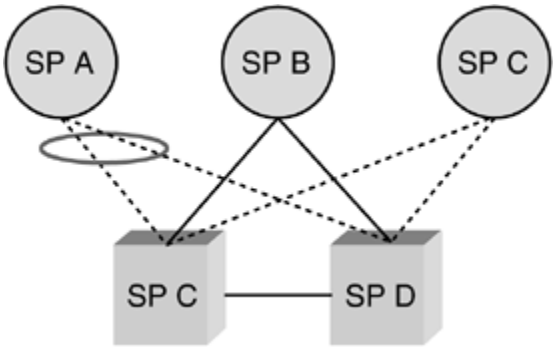
SS7 routes are statically provisioned at each SP. There are no mechanisms for route discovery. A route is defined as a preprovisioned path between source and destination for a particular relation. Figure 4-3 shows a route from SP A to SP C.

Figure 4-3. Route from SP A to SP C



All the preprovisioned routes to a particular SP destination are called the routeset. Figure 4-4 shows a routeset for SSP C consisting of two routes.

Figure 4-4. Routeset from SP A to SP C



The following section discusses the SP types.

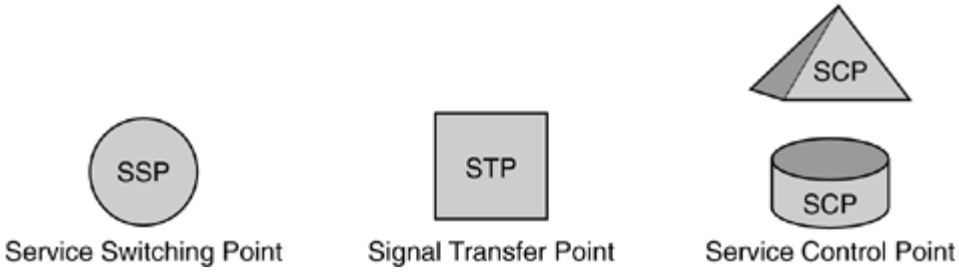
Node Types

There are three different types of SP (that is, SS7 node):

- Signal Transfer Point
- Service Switching Point
- Service Control Point

Figure 4-5 graphically represents these nodes.

Figure 4-5. SS7 Node Types



The SPs differ in the functions that they perform, as described in the following sections.

Signal Transfer Point

A Signal Transfer Point (STP) is responsible for the transfer of SS7 messages between other SS7 nodes, acting somewhat like a router in an IP network.

An STP is neither the ultimate source nor the destination for most signaling messages. Generally, messages are received on one signaling link and are transferred out another. The only messages that are not simply transferred are related to network management and global title translation. These two functions are discussed more in Chapters 7 and 9. STPs route each incoming message to an outgoing signaling link based on routing information contained in the SS7 message. Specifically, this is the information found in the MTP3 routing label, as described in Chapter 7.

Additionally, standalone STPs often can screen SS7 messages, acting as a firewall. Such usage is described in Chapter 15, "SS7/C7 Security and Monitoring."

An STP can exist in one of two forms:

- Standalone STP
- Integrated STP (SP with STP)

Standalone STPs are normally deployed in "mated" pairs for the purposes of redundancy. Under normal operation, the mated pair shares the load. If one of the STPs fails or isolation occurs because of signaling link failure, the other STP takes the full load until the problem with its mate has been rectified.

Integrated STPs combine the functionality of an SSP and an STP. They are both the source and destination for MTP user traffic. They also can transfer incoming messages to other nodes.

Service Switching Point

A Service Switching Point (SSP) is a voice switch that incorporates SS7 functionality. It processes voice-band traffic (voice, fax, modem, and so forth) and performs SS7 signaling. All switches with SS7 functionality are considered SSPs regardless of whether they are local switches (known in North America as an end office) or tandem switches.

An SSP can originate and terminate messages, but it cannot transfer them. If a message is received with a point code that does not match the point code of the receiving SSP, the message is discarded.

Service Control Point

A Service Control Point (SCP) acts as an interface between telecommunications databases and the SS7 network. Telephone companies and other telecommunication service providers employ a number of databases that can be queried for service data for the provision of services. Typically the request (commonly called a query) originates at an SSP. A popular example is freephone calling (known as toll-free in North America). The SCP provides the routing number (translates the toll-free number to a routable number) to the SSP to allow the call to be completed. For more information, see Chapter 11, "Intelligent Networks (IN)."

SCPs form the means to provide the core functionality of cellular networks, which is subscriber mobility. Certain cellular databases (called registers) are used to keep track of the subscriber's location so that incoming calls may be delivered. Other telecommunication databases include those used for calling card validation (access card, credit card), calling name display (CNAM), and LNP.

SCPs used for large revenue-generating services are usually deployed in pairs and are geographically separated for redundancy. Unless there is a failure, the load is typically shared between two mated SCPs. If failure occurs in one of the SCPs, the other one should be able to take the load of both until normal operation resumes.

Queries/responses are normally routed through the mated pair of STPs that services that particular SCP, particularly in North America.

See Chapters 10, "Transaction Capabilities Application Part (TCAP)," and 11, "Intelligent Networks (IN)," for more information on the use of SCPs within both fixed-line and cellular networks. See Chapters 12, "Cellular Networks," and 13, "GSM and ANSI-41 Mobile Application Part (MAP)," for specific information on the use of SCPs within cellular networks.

The following section introduces the concept of link types.

Link Types

Signaling links can be referenced differently depending on where they are in the network. Although different references can be used, you should understand that the link's physical characteristics remain the same. The references to link types A through E are applicable only where standalone STPs are present, so the references are more applicable to the North American market.

Six different link references exist:

- Access links (A links)

- Crossover links (C links)
- Bridge links (B links)
- Diagonal links (D links)
- Extended links (E links)
- Fully associated links (F links)

The following sections cover each link reference in more detail.

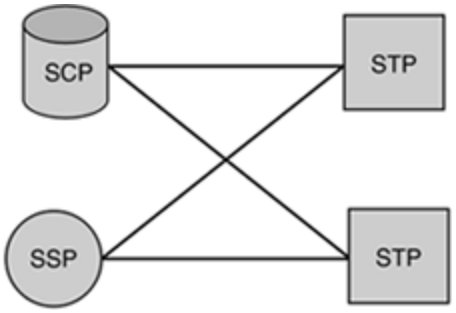
NOTE

In the figures in the sections covering the different link references, dotted lines represent the actual link being discussed, and solid lines add network infrastructure to provide necessary context for the discussion.

Access Links (A Links)

Access links (A links), shown in Figure 4-6, provide access to the network. They connect "outer" SPs (SSPs or SCPs) to the STP backbone. A links connect SSPs and SCPs to their serving STP or STP mated pair.

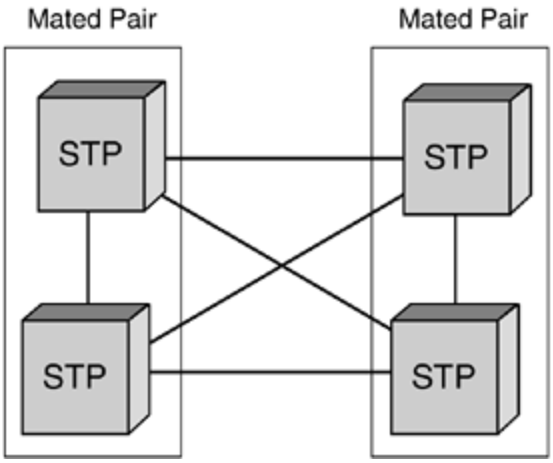
Figure 4-6. A Links



Cross Links (C Links)

Cross links (C links), shown in Figure 4-7, are used to connect two STPs to form a mated pair that is, a pair linked such that if one fails, the other takes the load of both.

Figure 4-7. C Links



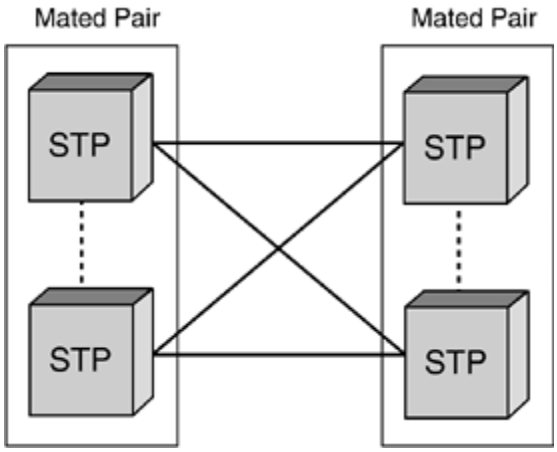
C links are used to carry MTP user traffic only when no other route is available to reach an intended destination. Under normal conditions, they are used only to carry network management messages.

Bridge Links (B Links)

Bridge links (B links) are used to connect mated pairs of STPs to each other across different regions within a network at the same hierarchical level. These links help form the backbone of the SS7 network. B links are normally deployed in link quad configuration between mated pairs for redundancy.

Figure 4-8 shows two sets of mated pairs of B links.

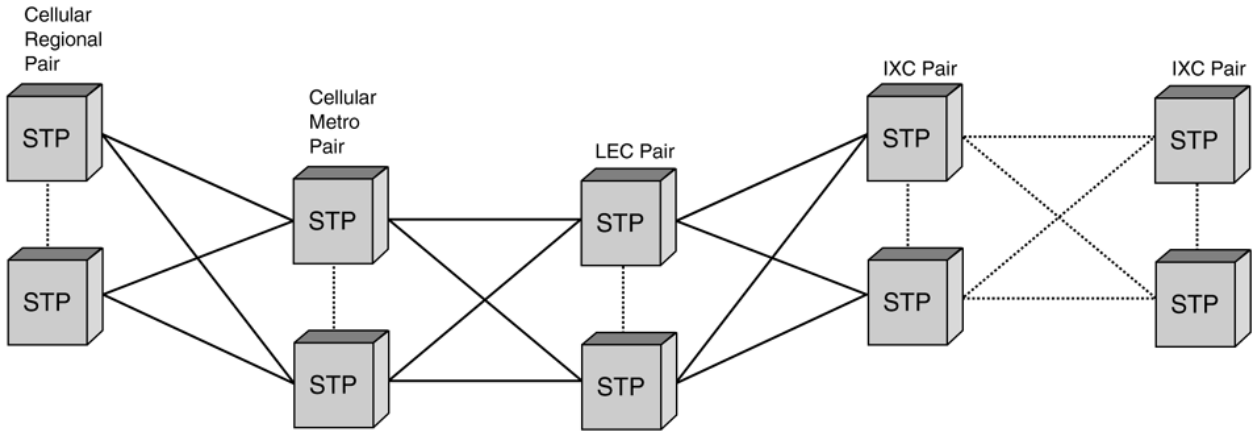
Figure 4-8. B Links



Diagonal Links (D Links)

Diagonal links (D links), shown in Figure 4-9, are the same as B links in that they connect mated STP pairs.

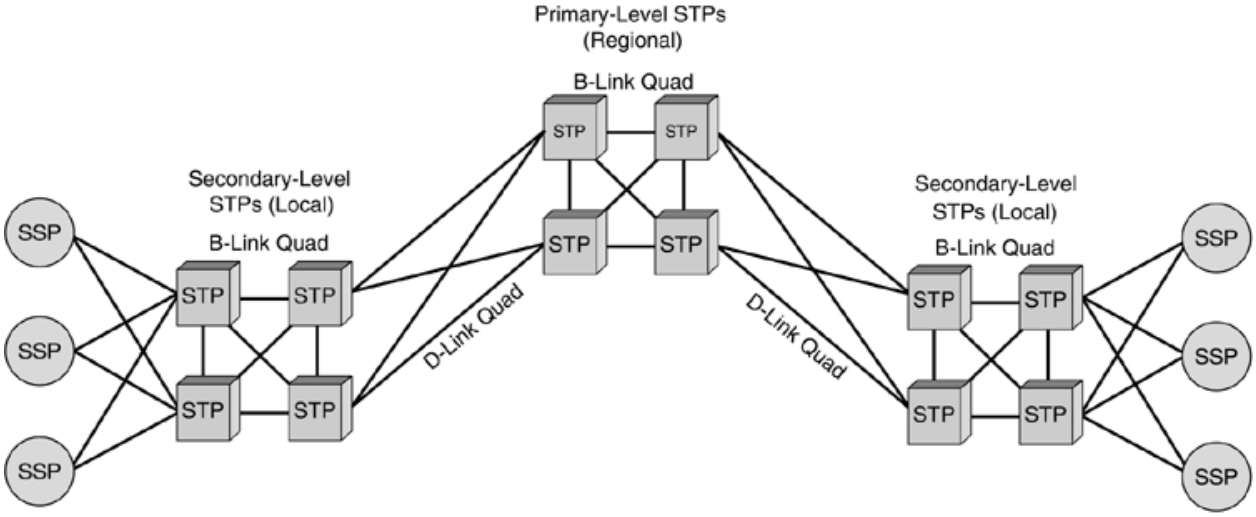
Figure 4-9. D Links



The difference is that they connect mated STP pairs that belong to different hierarchical levels or to different networks altogether. For example, they may connect an interexchange carrier (IXC) STP pair to a local exchange carrier (LEC) STP pair or a cellular regional STP pair to a cellular metro STP pair.

As mentioned, B and D links differ in that D links refer specifically to links that are used either between different networks and/or hierarchical levels, as shown in Figure 4-10.

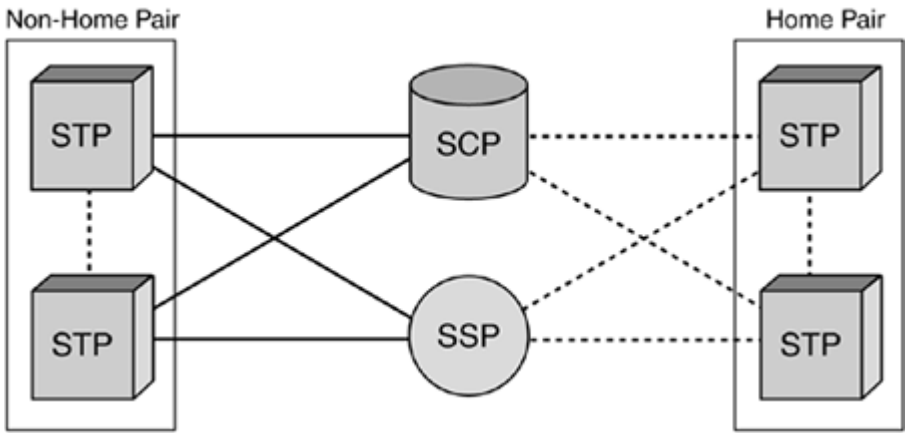
Figure 4-10. Existence of an STP Backbone and STP Hierarchy



Extended Links (E Links)

Extended links (E links), shown in Figure 4-11, connect SSPs and SCPs to an STP pair, as with A links, except that the pair they connect to is not the normal home pair. Instead, E links connect to a nonhome STP pair. They are also called alternate access (AA) links. E links are used to provide additional reliability or, in some cases, to offload signaling traffic from the home STP pair in high-traffic corridors. For example, an SSP serving national government agencies or emergency services might use E links to provide additional alternate routing because of the criticality of service.

Figure 4-11. E Links



Fully-Associated Links (F Links)

Fully-associated links (F links), shown in Figure 4-12, are used to connect network SSPs and/or SCPs directly to each other without using STPs. The most common application of this type of link is in metropolitan areas. F links can establish direct connectivity between all switches in the area for trunk signaling and Custom Local Area Signaling Service (CLASS), or to their corresponding SCPs.

Figure 4-12. F Links

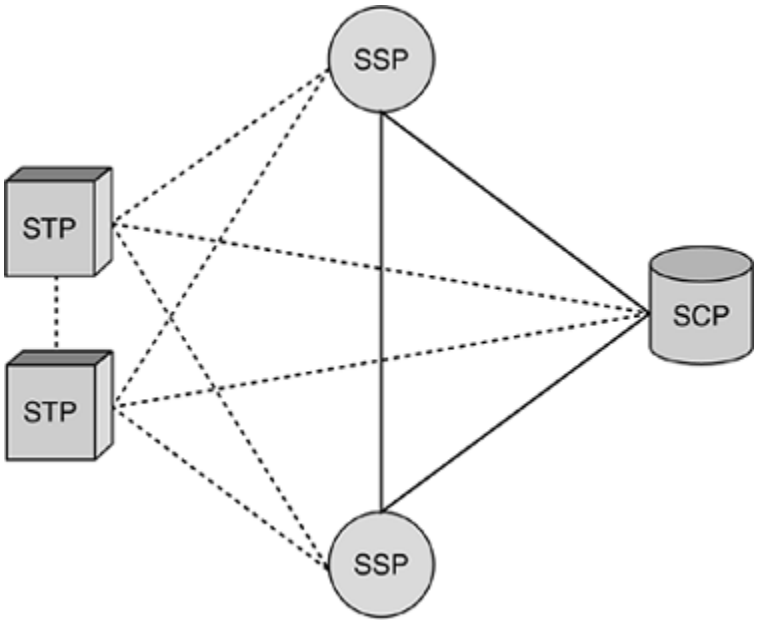
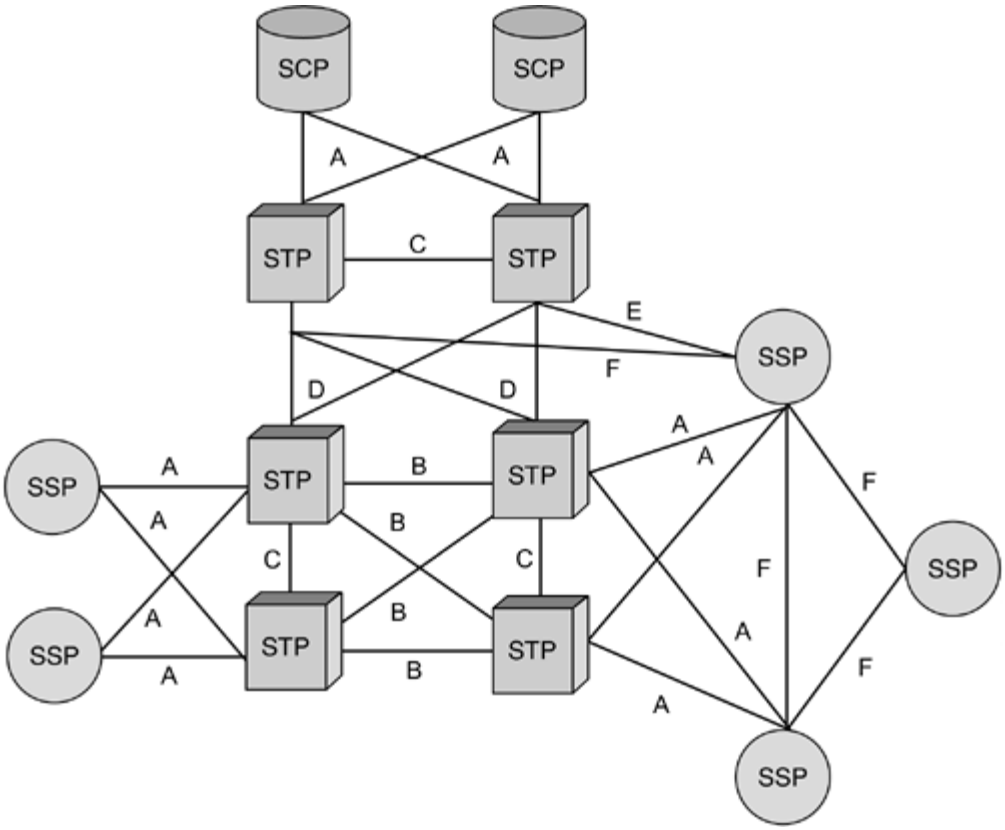


Figure 4-13 shows an SS7 network segment. In reality, there would be several factors more SSPs than STPs.

Figure 4-13. SS7 Network Segment



Signaling Modes

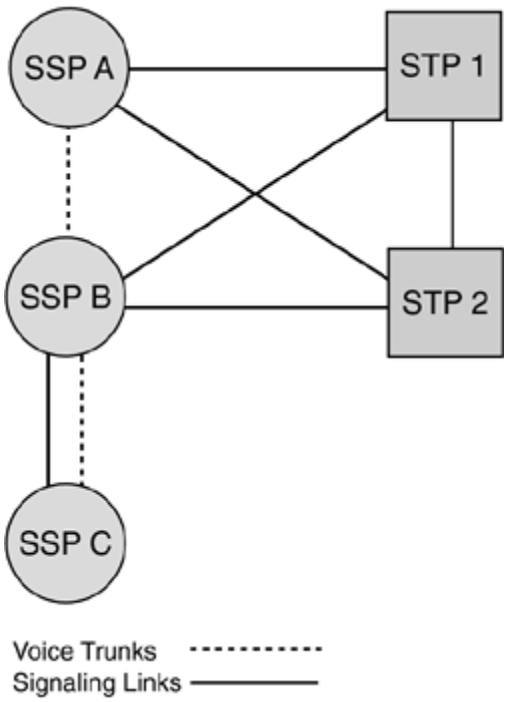
The signaling relationship that exists between two communicating SS7 nodes is called the signaling mode. The two modes of signaling are associated signaling and quasi-associated signaling. When the destination of an SS7 message is directly connected by a linkset, the associated signaling mode is being used. In other words, the source and destination nodes are directly connected by a single linkset. When the message must pass over two or more linksets and through an intermediate node, the quasi-associated mode of signaling is being used.

It's easier to understand the signaling mode if you examine the relationship of the point codes between the source and destination node. When using the associated mode of signaling, the Destination Point Code (DPC) of a message being sent matches the PC of the node at the far end of the linkset, usually referred to as the far-end PC or adjacent PC. When quasi-associated signaling is used, the DPC does not match the PC at the far end of the connected linkset. Quasi-associated signaling requires the use of an STP as the intermediate node because an SSP cannot transfer messages.

In Figure 4-14, the signaling relationships between each of the nodes are as follows:

- SSP A to SSP B uses quasi-associated signaling.
- SSP B to SSP C uses associated signaling.
- STP 1 and STP 2 use associated signaling to SSP A, SSP B, and each other.

Figure 4-14. SS7 Signaling Modes



As you can see from Figure 4-14, associated signaling is used between nodes that are directly connected by a single linkset, and quasi-associated signaling is used when an intermediate node is used. Notice that SSP C is only connected to SSP B using an F link. It is not connected to any other SS7 nodes in the figure.

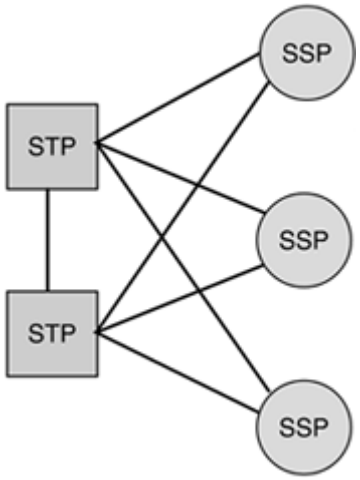
When discussing the signaling mode in relation to the voice trunks shown between the SSPs, the signaling and voice trunks follow the same path when associated signaling is used. They take separate paths when quasi-associated signaling is used. You can see from Figure 4-14 that the signaling between SSP B and SSP C follows the same path (associated mode) as the voice trunks, while the signaling between SSP A and SSP B does not follow the same path as the voice trunks.

Signaling Network Structure

Standalone STPs are prevalent in North America because they are used in this region to form the backbone of the SS7 network. Attached to this backbone are the SSPs and SCPs. Each SSP and SCP is assigned a "home pair" of STPs that it is directly connected to. The network of STPs can be considered an overlay onto the telecommunications network□a packet-switched data

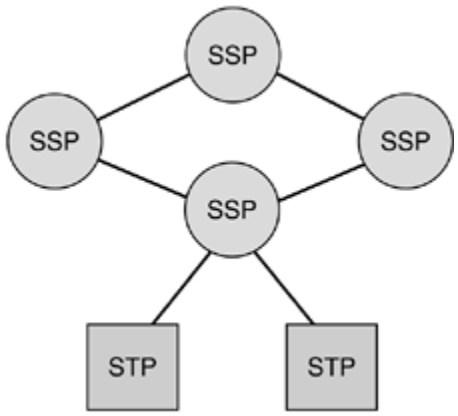
communications network that acts as the nervous system of the telecommunications network. Figure 4-15 shows a typical example of how SSPs are interconnected with the STP network in North America.

Figure 4-15. Typical Example of North American SSP Interconnections



STPs are not as common outside North America. Standalone STPs typically are used only between network operators and/or for applications involving the transfer of noncircuit-related signaling. In these regions, most SSPs have direct signaling link connections to other SSPs to which they have direct trunk connections. Figure 4-16 shows an example of this type of network with most SSPs directly connected by signaling links.

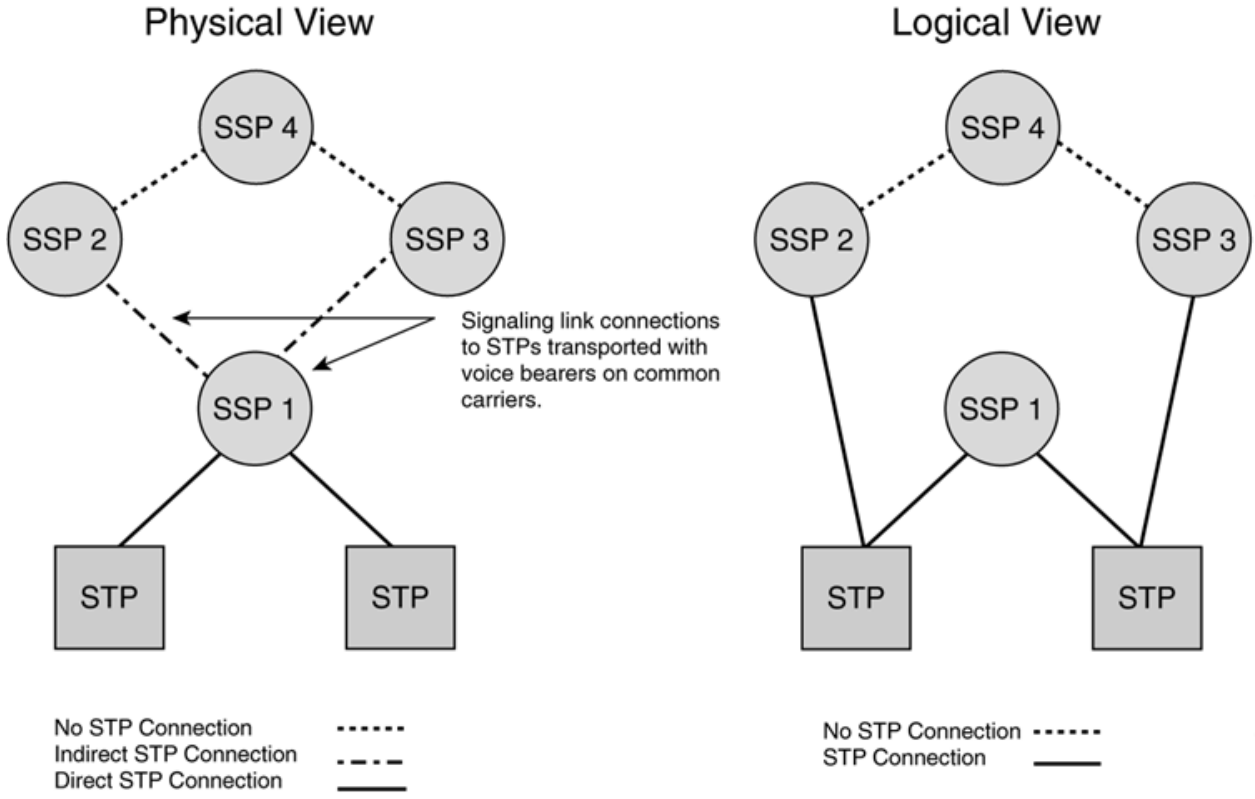
Figure 4-16. Typical Example of SSP Interconnections in Most Areas Outside North America



SSPs often have indirect physical connections to STPs, made through other SSPs in the network. These are usually implemented as nailed-up connections, such as through a Digital Access

Cross-Connect System or other means of establishing a semipermanent connection. Logically, these SSPs are directly connected to the STP. The signaling link occupies a digital time slot on the same physical medium as the circuit-switched traffic. The SSPs that provide physical interconnection between other SSPs and an STP do not "transfer" messages as an STP function. They only provide physical connectivity of the signaling links between T1/E1 carriers to reach the STP. Figure 4-17 shows an example of a network with no STP connection, direct connections, and nondirect connections. SSP 1 is directly connected to an STP pair. SSP 4 uses direct signaling links to SSP 2 and SSP 3, where it also has direct trunks. It has no STP connection at all. SSP 2 and SSP 3 are connected to the STP pair via nailed-up connections at SSP 1.

Figure 4-17. Example of Direct and Indirect SSP Interconnections to STPs



Normally within networks that do not use STPs, circuit-related (call-related) signaling takes the same path through the network as user traffic because there is no physical need to take a different route. This mode of operation is called associated signaling and is prevalent outside North America. Referring back to Figure 4-14, both the user traffic and the signaling take the same path between SSP B and SSP C.

Because standalone STPs are used to form the SS7 backbone within North America, and standalone STPs do not support user traffic switching, the SSP's signaling mode is usually quasi-associated, as illustrated between SSP A and SSP B in Figure 4-14.

In certain circumstances, the SSP uses associated signaling within North America. A great deal of signaling traffic might exist between two SSPs, so it might make more sense to place a signaling link directly between them rather than to force all signaling through an STP.

SS7 Protocol Overview

SS7 protocol suite

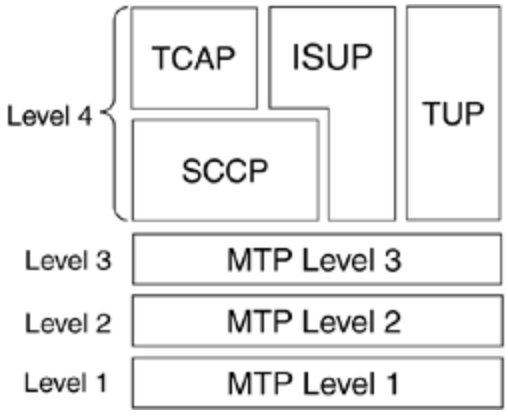
OSI Layer	SS7 Protocols
Application	INAP, MAP, IS-41... TCAP, CAP, ISUP, TUP...
Network	MTP Level 3 + SCCP
Data link	MTP Level 2
Physical	MTP Level 1

The number of possible protocol stack combinations is growing. It depends on whether SS7 is used for cellular-specific services or intelligent network services, whether transportation is over IP or is controlling broadband ATM networks instead of time-division multiplexing (TDM) networks, and so forth. This requires coining a new term "traditional SS7" to refer to a stack consisting of the protocols widely deployed from the 1980s to the present:

- Message Transfer Parts (MTP 1, 2, and 3)
- Signaling Connection Control Part (SCCP)
- Transaction Capabilities Application Part (TCAP)
- Telephony User Part (TUP)
- ISDN User Part (ISUP)

Figure 4-18 shows a common introductory SS7 stack.

Figure 4-18. Introductory SS7 Protocol Stack



Such a stack uses TDM for transport. This book focuses on traditional SS7 because that is what is implemented. Newer implementations are beginning to appear that use different transport means such as IP and that have associated new protocols to deal with the revised transport.

The SS7 physical layer is called MTP level 1 (MTP1), the data link layer is called MTP level 2 (MTP2), and the network layer is called MTP level 3 (MTP3). Collectively they are called the Message Transfer Part (MTP). The MTP protocol is SS7's native means of packet transport. In recent years there has been an interest in the facility to transport SS7 signaling over IP instead of using SS7's native MTP. This effort has largely been carried out by the Internet Engineering Task Force (IETF) SigTran (Signaling Transport) working group. The protocols derived by the SigTran working group so far are outside the scope of this introductory chapter on SS7. However, full details of SigTran can be found in Chapter 14, "SS7 in the Converged World."

TUP and ISUP both perform the signaling required to set up and tear down telephone calls. As such, both are circuit-related signaling protocols. TUP was the first call control protocol specified. It could support only plain old telephone service (POTS) calls. Most countries are replacing TUP with ISUP. Both North America and Japan bypassed TUP and went straight from earlier signaling systems to ISUP. ISUP supports both POTS and ISDN calls. It also has more flexibility and features than TUP.

With reference to the Open System Interconnection (OSI) seven-layer reference model, SS7 uses a four-level protocol stack. OSI Layer 1 through 3 services are provided by the MTP together with the SCCP. The SS7 architecture currently has no protocols that map into OSI Layers 4 through 6. TUP, ISUP, and TCAP are considered as corresponding to OSI Layer 7 [111]. SS7 and the OSI model were created at about the same time. For this reason, they use some differing terminology.

SS7 uses the term levels when referring to its architecture. The term levels should not be confused with OSI layers, because they do not directly correspond to each other. Levels was a term introduced to help in the discussion and presentation of the SS7 protocol stack. Levels 1, 2, and 3 correspond to MTP 1, 2, and 3, respectively. Level 4 refers to an MTP user. The term user refers to any protocol that directly uses the transport capability provided by the MTP□namely, TUP, ISUP, and SCCP in traditional SS7. The four-level terminology originated back when SS7 had only a call control protocol (TUP) and the MTP, before SCCP and TCAP were added.

The following sections provide a brief outline of protocols found in the introductory SS7 protocol stack, as illustrated in Figure 4-18.

MTP

MTP levels 1 through 3 are collectively referred to as the MTP. The MTP comprises the functions to transport information from one SP to another.

The MTP transfers the signaling message, in the correct sequence, without loss or duplication, between the SPs that make up the SS7 network. The MTP provides reliable transfer and delivery

of signaling messages. The MTP was originally designed to transfer circuit-related signaling because no noncircuit-related protocol was defined at the time.

The recommendations refer to MTP1, MTP2, and MTP3 as the physical layer, data link layer, and network layer, respectively. The following sections discuss MTP2 and MTP3. (MTP1 isn't discussed because it refers to the physical network.) For information on the physical aspects of the Public Switched Telephone Network (PSTN), see Chapter 5, "The Public Switched Telephone Network (PSTN)."

MTP2

Signaling links are provided by the combination of MTP1 and MTP2. MTP2 ensures reliable transfer of signaling messages. It encapsulates signaling messages into variable-length SS7 packets. SS7 packets are called signal units (SUs). MTP2 provides delineation of SUs, alignment of SUs, signaling link error monitoring, error correction by retransmission, and flow control. The MTP2 protocol is specific to narrowband links (56 or 64 kbps).

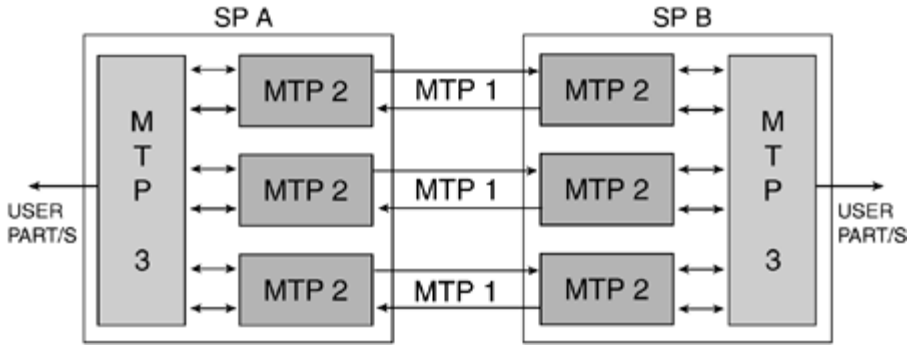
MTP3

MTP3 performs two functions:

- Signaling Message Handling (SMH)□ Delivers incoming messages to their intended User Part and routes outgoing messages toward their destination. MTP3 uses the PC to identify the correct node for message delivery. Each message has both an Origination Point Code (OPC) and a DPC. The OPC is inserted into messages at the MTP3 level to identify the SP that originated the message. The DPC is inserted to identify the address of the destination SP. Routing tables within an SS7 node are used to route messages.
- Signaling Network Management (SNM)□ Monitors linksets and routesets, providing status to network nodes so that traffic can be rerouted when necessary. SNM also provides procedures to take corrective action when failures occur, providing a self-healing mechanism for the SS7 network.

Figure 4-19 shows the relationship between levels 1, 2, and 3.

Figure 4-19. A Single MTP3 Controls Many MTP2s, Each of Which Is Connected to a Single MTP1



TUP and ISUP

TUP and ISUP sit on top of MTP to provide circuit-related signaling to set up, maintain, and tear down calls. TUP has been replaced in most countries because it supports only POTS calls. Its successor, ISUP, supports both POTS and ISDN calls as well as a host of other features and added flexibility. Both TUP and ISUP are used to perform interswitch call signaling. ISUP also has inherent support for supplementary services, such as automatic callback, calling line identification, and so on.

SCCP

The combination of the MTP and the SCCP is called the Network Service Part (NSP) in the specifications (but outside the specifications, this term is seldom used).

The addition of the SCCP provides a more flexible means of routing and provides mechanisms to transfer data over the SS7 network. Such additional features are used to support noncircuit-related signaling, which is mostly used to interact with databases (SCPs). It is also used to connect the radio-related components in cellular networks and for inter-SSP communication supporting CLASS services. SCCP also provides application management functions. Applications are mostly SCP database driven and are called subsystems. For example, in cellular networks, SCCP transfers queries and responses between the Visitor Location Register (VLR) and Home Location Register (HLR) databases. Such transfers take place for a number of reasons. The primary reason is to update the subscriber's HLR with the current VLR serving area so that incoming calls can be delivered.

Enhanced routing is called global title (GT) routing. It keeps SPs from having overly large routing tables that would be difficult to provision and maintain. A GT is a directory number that serves as an alias for a physical network address. A physical address consists of a point code and an application reference called a subsystem number (SSN). GT routing allows SPs to use alias addressing to save them from having to maintain overly large physical address tables. Centralized STPs are then used to convert the GT address into a physical address; this process is called Global Title Translation (GTT). This provides the mapping of traditional telephony addresses (phone numbers) to SS7 addresses (PC and/or SSN) for enhanced services. GTT is typically performed at STPs.

NOTE

It is important not to confuse the mapping of telephony numbers using GTT with the translation of telephony numbers done during normal call setup. Voice switches internally map telephony addresses to SS7 addresses during normal call processing using number translation tables. This process does not use GTT. GTT is used only for noncircuit-related information, such as network supplementary services (Calling Name Delivery) or database services (toll-free).

In addition to mapping telephony addresses to SS7 addresses, SCCP provides a set of subsystem management functions to monitor and respond to the condition of subsystems. These management functions are discussed further, along with the other aspects of SCCP, in Chapter 9, "Signaling Connection Control Part (SCCP)."

TCAP

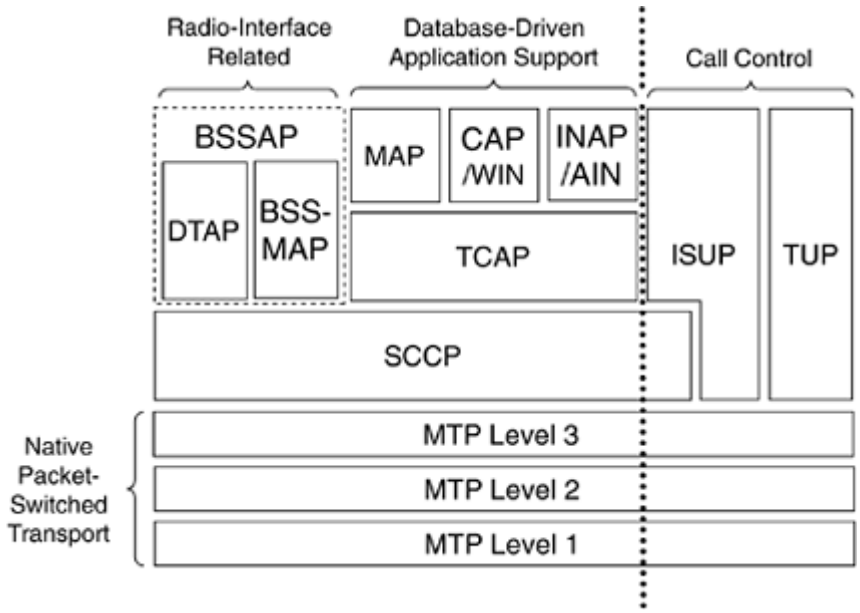
TCAP allows applications (called subsystems) to communicate with each other (over the SS7 network) using agreed-upon data elements. These data elements are called components. Components can be viewed as instructions sent between applications. For example, when a subscriber changes VLR location in a global system for mobile communication (GSM) cellular network, his or her HLR is updated with the new VLR location by means of an UpdateLocation component. TCAP also provides transaction management, allowing multiple messages to be associated with a particular communications exchange, known as a transaction.

There are a number of subsystems; the most common are

- Toll-free (E800)
- Advanced Intelligent Network (AIN)
- Intelligent Network Application Protocol (INAP)
- Customizable Applications for Mobile Enhanced Logic (CAMEL)
- Mobile Application Part (MAP)

Figure 4-20 illustrates these subsystems as well as another protocol that uses SCCP, the Base Station Subsystem Application Part. It is used to control the radio-related component in cellular networks.

Figure 4-20. Some Protocols That Might Exist on Top of the SCCP, Depending on the Application



It is highly unlikely that a protocol such as the one shown in Figure 4-20 would exist at any one SP. Instead, protocol stacks vary as required by SP type. For example, because an STP is a routing device, it has only MTP1, MTP2, MTP3, and SCCP. A fixed-line switch without IN support might have only MTP1, MTP2, MTP3, and ISUP, and so forth. A diagram showing how the SS7 protocol stack varies by SP can be found in Chapter 13.

MAP

The **Mobile Application Part** (**MAP**) is an SS7 protocol which provides an application layer for the various nodes in GSM and UMTS mobile core networks and GPRS core networks to communicate with each other in order to provide services to mobile phone users. The Mobile Application Part is the application-layer protocol used to access the Home Location Register, Visitor Location Register, Mobile Switching Center, Equipment Identity Register, Authentication Centre, Short message service center and Serving GPRS Support Node.

Facilities provided

The primary facilities provided by MAP are:

- Mobility Services: location management (roaming), authentication, managing service subscription information, fault recovery,
- Operation and Maintenance: subscriber tracing, retrieving a subscriber's IMSI
- Call Handling: routing, managing calls whilst roaming, checking that a subscriber is available to receive calls
- Supplementary Services
- Short Message Service
- Packet Data Protocol (PDP) services for GPRS: providing routing information for GPRS connections
- Location Service Management Services: obtaining the location of subscribers

Published specification

The Mobile Application Part specifications were originally defined by the GSM Association, but are now controlled by ETSI/3GPP. MAP is defined by two different standards, depending upon the mobile network type:

- MAP for GSM (prior to Release 4) is specified by 3GPP TS 09.02
- MAP for UMTS ("3G") and GSM (Release 99 and later) is specified by 3GPP TS 29.002

Implementation

MAP is a Transaction Capabilities Application Part (TCAP) user, and as such can be transported using 'traditional' SS7 protocols or over IP using *Transport Independent Signalling Connection Control Part (TI-SCCP)*;[1] or using SIGTRAN.

MAP Signaling

In mobile cellular telephony networks like GSM and UMTS the SS7 application MAP is used. Voice connections are Circuit Switched (CS) and data connections are Packet Switched (PS) applications.

Some of the **GSM/UMTS Core Switched interfaces** in the Mobile Switching Center (MSC) transported over SS7 include the following:

B -> VLR (uses MAP/B). Most MSCs are associated with a Visitor Location Register (VLR), making the B interface "internal".

C -> HLR (uses MAP/C) Messages between MSC to HLR handled by C Interface

D -> HLR (uses MAP/D) for attaching to the CS network and location update

E -> MSC (uses MAP/E) for inter-MSC handover

F -> EIR (uses MAP/F) for equipment identity check

H -> SMS-G (uses MAP/H) for Short Message Service (SMS) over CS

There are also several **GSM/UMTS PS interfaces** in the Serving GPRS Support Node (SGSN) transported over SS7:

Gr -> HLR for attaching to the PS network and location update

Gd -> SMS-C for SMS over PS

Gs -> MSC for combined CS+PS signaling over PS

Ge -> Charging for Customised Applications for Mobile networks Enhanced Logic (CAMEL) prepaid charging

Gf -> EIR for equipment identity check

INAP

The **Intelligent Network Application Part** (**INAP**) is a signalling protocol used in the intelligent network architecture. It is part of the SS7 protocol suite, typically layered on top of TCAP.It can also be termed as logic for controlling telecommunication services migrated from traditional switching points to computer based service independent platform

SIGTRAN

SIGTRAN is the name, derived from *signaling transport*, of the Internet Engineering Task Force (IETF) working group that produced specifications for a family of protocols that provide reliable datagram service and user layer adaptations for Signaling System 7 (SS7) and ISDN communications protocols. The SIGTRAN protocols are an extension of the SS7 protocol family. It supports the same application and call management paradigms as SS7 but uses an Internet Protocol (IP) transport called Stream Control Transmission Protocol (SCTP).[1] Indeed, the most significant protocol defined by the SIGTRAN group is SCTP, which is used to carry PSTN signaling over IP.

The SIGTRAN group was significantly influenced by telecommunications engineers intent on using the new protocols for adapting VoIP networks to the PSTN with special regard to signaling applications.[2] Recently, SCTP is finding applications beyond its original purpose wherever reliable datagram service is desired.

SIGTRAN has been published in RFC 2719, under the title *Architectural Framework for Signaling Transport*. RFC 2719 also defines the concept of a Signaling gateway (SG), which converts CCS messages from SS7 to SIGTRAN. Implemented in a variety of network elements including softswitches, the SG function can provide significant value to existing common channel signaling networks, leveraging investments associated with SS7 and delivering the cost/performance values associated with IP transport.

SIGTRAN protocols

The SIGTRAN family of protocols includes:

- Stream Control Transmission Protocol (SCTP), RFC 3873, RFC 4166, RFC 4960.
- ISDN User Adaptation (IUA), RFC 4233, RFC 5133.
- Message Transfer Part 2 (MTP) User Peer-to-Peer Adaptation Layer (M2PA), RFC 4165.
- Message Transfer Part 2 User Adaptation Layer (M2UA), RFC 3331.
- Message Transfer Part 3 User Adaptation Layer (M3UA), RFC 4666.
- Signalling Connection Control Part (SCCP) User Adaptation (SUA), RFC 3868.
- V5 User Adaptation (V5UA), RFC 3807.

The Stream Control Transmission Protocol provides the transport protocol for SIGTRAN user adaptation layer messages across an IP network. It is described in RFC 3873, RFC 4166 and RFC 4960.

IUA provides an SCTP adaptation layer for the seamless backhaul of Q.921 user messages and service interface across an IP network. Some users that it supports are Q.931 and QSIG.[3] It is specified in RFC 4233.

V5UA provides an SCTP adaptation layer for the seamless backhaul of V5.2 user messages and service interface across an IP network. It is a variation of *IUA* and is specified in RFC 3807.

M2PA provides an SCTP adaptation layer for providing an SS7 MTP signaling link over an IP network. It is specified in RFC 4165.

M2UA provides an SCTP adaptation layer for the seamless backhaul of MTP Level 2 user messages and service interface across an IP network. It is specified in RFC 3331.

M3UA provides an SCTP adaptation layer for the seamless backhaul or peering of MTP Level 3 user messages and service interface across an IP network. It is specified in RFC 4666.

SUA provides an SCTP adaptation layer for the seamless backhaul or peering of Signalling Connection Control Part user messages and service interface across an IP network. It is specified in RFC 3868.

UCP

External Machine Interface (**EMI**), an extension to **Universal Computer Protocol** (**UCP**), is a protocol primarily used to connect to short message service centres (SMSCs) for mobile telephones. The protocol was developed by CMG Wireless Data Solutions, now part of Acision.

Syntax

A typical EMI/UCP exchange looks like this :

```
^B01/00045/O/30/66677789///1//////68656C6C6F/CE^C
^B01/00041/R/30/A//66677789:180594141236/F3^C
```

The start of the packet is signaled by ^B (STX, hex 02) and the end with ^C (ETX, hex 03). Fields within the packet are separated by / characters.

The first four fields form the mandatory header. the third is the *operation type* (O for operation, R for result), and the fourth is the *operation* (here 30, "short message transfer").

The subsequent fields are dependent on the operation. In the first line above, '66677789' is the recipient's address (telephone number) and '68656C6C6F' is the content of the message, in this case the ASCII string "hello". The second line is the response with a matching transaction reference number, where 'A' indicates that the message was successfully acknowledged by the SMSC, and a timestamp is suffixed to the phone number to show time of delivery.

The final field is the checksum, calculated simply by summing all bytes in the packet (including slashes) and taking the 8 least significant bits from the result.

The full specification is available on the LogicaCMG website developers' forum, but registration is required.

Technical Limitations

The two digit *transaction reference number* means that an entity sending text messages can only have 100 outstanding messages; this can limit performance.

The destination *AdC* phone number cannot contain * or # characters, although the originator *OAdC* can, in which case the text message could not be replied to.

The default alphabet is not ASCII compatible and is missing the characters: apostrophe ' (only Grave Accent `), Underscore and Tab.

As the protocol is itself text, the text of the SMS message must be encoded twice (characters packed to 7 bits, then encoded as hex), and can not be read from a dump of a message. This also applies to GSM MAP.

Alternatives

- Short message peer-to-peer protocol (SMPP) also provides SMS over TCP/IP.
- Computer Interface for Message Distribution (CIMD) developed by Nokia

IVR

Interactive Voice Response (**IVR**) is a technology that allows a computer to detect voice and dual-tone multi-frequency signaling (DTMF) keypad inputs. IVR technology is used extensively in telecommunication, but is also being introduced into automobile systems for hands-free operation. Current deployment in automobiles revolves around satellite navigation, audio and mobile phone systems. In telecommunications, IVR allows customers to access a company's database via a telephone keypad or by speech recognition, after which they can service their own inquiries by following the instructions. IVR systems can respond with pre-recorded or dynamically generated audio to further direct users on how to proceed. IVR systems can be used to control almost any function where the interface can be broken down into a series of simple menu choices. In telecommunications applications, such as customer support lines, IVR systems generally scale well to handle large call volumes.

It has become common in industries that have recently entered the telecommunications industry to refer to an Automated Attendant as an IVR. The terms **Automated Attendant** and **IVR** are distinct and mean different things to traditional telecommunications professionals, whereas emerging telephony and VoIP professionals often use the term **IVR** as a catch-all to signify any kind of telephony menu, even a basic automated attendant. The term **VRU**, for **Voice Response Unit**, is sometimes used as well.[1]

Entertainment and information

The largest installed IVR platforms are used for applications such as tele-voting on television game shows, such as *Pop Idol* and *Big Brother*, which can generate enormous call spikes. Often, the network provider will have to deploy *call gapping* in the public network to prevent network overload.

The following are some of the more common uses of an IVR:

- Mobile — Pay-As-You-Go account funding
- Telephone banking — balance, payments, and transfers
- Mobile purchases — particularly for mobile content, such as ring tones and logos
- Caller identification and routing
- Order placements — credit card payments
- Airline — ticket booking, flight arrivals, flight departures, check-in
- Adult entertainment — dating, chat line, etc.
- Weather forecasts

Outbound calling

IVR systems can be used for outbound calls, as IVR systems are more intelligent than dialer systems and can recognize different line conditions as follows:

- RNA — Ring No Answer
- Answered by voice mail or answering machine (In this circumstances they can leave a message)
- Fax tone (IVR can leave a TIFF image fax message)
- Answer (IVR can tell the customer who is calling and ask them to wait for an agent)
- Recognize divert messages and abandon call.

IVR uses Call Progress Detection to monitor line conditions, and report to the IVR database.

Technologies used

DTMF signals (entered via the telephone keypad) and natural language speech recognition interpret the caller's response to voice prompts.

Other technologies include the ability to speak complex and dynamic information, such as an e-mail, news report or weather information using Text-To-Speech (TTS). TTS is computer generated synthesized speech that is no longer the robotic voice generally associated with computers. Real voices create the speech in fragments (phonemes) that are spliced together (concatenated) before being played to the caller.

An IVR can be utilized in several different ways:

1. Equipment installed on the customer premise
2. Equipment installed in the PSTN (Public Switched Telephone Network)
3. Application service provider (ASP).
4. Hosted IVR
5. A simple voice mail system is different from IVR in that it is person-to-person, whereas an IVR is person to computer. IVR voice forms can be used to provide a more complex voice mail experience to the caller. For example, the IVR could ask if the caller wishes to hear, edit, forward or remove a message that was just recorded.
6. An automatic call distributor (ACD) is often the first point of contact when calling many larger businesses. An ACD uses digital storage devices to play greetings or announcements, but typically routes a caller without prompting for input. An IVR can play announcements and request an input from the caller. This information can be used to profile the caller and route the call to an agent with a particular skill set. (A skill set is a function applied to a group of call-center agents with a particular skill.)
7. Interactive voice response can be used to front-end a call center operation by identifying the needs of the caller. Information can be obtained from the caller such as account numbers. Answers to simple questions such as account balances or pre-recorded information can be provided without operator intervention. Account numbers from the IVR are often compared to caller ID data for security reasons and additional IVR responses are required if the caller ID data do not match the account record.
8. IVR call flows are created in a variety of ways. A traditional IVR depended upon proprietary programming or scripting languages, whereas modern IVR applications are structured similar to Web pages, using VoiceXML[2], CCXML[3], SRGS[4], SALT or T-XML languages. The ability to use XML developed applications allows a Web server to act as an application server, freeing the developer to focus on the call flow. It was widely believed that developers would no longer require specialized programming skills, however this has been proven to be misguided as IVR applications need to understand the human reaction to the application dialog. This is the difference between a good user experience and IVR hell[*citation needed*].
9. Higher level IVR development tools are available in recent years to further simplify the application development process. A call flow diagram can be drawn with a GUI tool and the application code (VoiceXML or SALT) can be automatically generated. In addition, these tools normally provide extension mechanisms for software integration, such as HTTP interface to Web site and Java interface for connecting to a database.
10. In telecommunications, an **audio response unit** (ARU) is a device that provides synthesized voice responses to DTMF keypresses by processing calls based on (a) the call-originator input, (b) information received from a database, and (c) information in the incoming call, such as the time of day.
11. ARUs increase the number of information calls handled and to provide consistent quality in information retrieval.

VoIP

The increased usage of VoIP in voice networks is likely to affect how IVR will be used in voice networks, this is due to the introduction of protocols such as Session Initiation Protocol (SIP). The introduction of SIP means that point to point communications is no longer restricted to voice calls but can now be extended to multimedia technologies such as video. This will bring a new meaning to automated services as IVR extends its reach to video calls. Many IVR manufacturers are currently working on IVVR (Interactive Voice and Video Response) systems, especially for the mobile phone networks. The use of video will give IVR systems the ability to use graphical and video information to assist the caller.

The introduction of video IVR may allow systems in the future the ability to read emotions and facial expressions. It may be used to identify the caller, using technology such as Iris scan or other biometric means. Recordings of the caller may be stored to monitor certain transactions, and may be used to reduce identity fraud.

[edit] Unified communications in the SIP contact center

With the introduction of SIP contact centers, automation has finally come of age. Calls arriving at a SIP contact center must now be queued against a SIP IVR system. Call control in a SIP contact center is controlled by VXML scripting which is an extension of the language used to write modern IVR Applications. As calls are queued in the SIP contact center, the IVR system can provide treatment, automation, wait for a fixed period, or play music. Inbound calls to a SIP contact center must be queued or terminated against a SIP end point. In addition SIP IVR systems can be used to replace agents directly by the use of BBUA (Back to Back User Agents).

[edit] Interactive Messaging Response (IMR)

As communications have migrated to multimedia so has Automation. The introduction of Instant Messaging (IM) in Contact Centers is starting to take off. Agents can handle up to 6 different IM conversations at the same time and so agent productivity is increasing. IVR systems are now starting to handle IM conversations using existing Speech Recognition Technology. This is different from email handling as email automated response is based on key word spotting. IM conversations are different to email as IM is conversational. The use of text messaging abbreviations and smilies requires different grammars than those currently used for speech recognition. IM is also starting to replace text messaging on Multimedia Mobile handsets and is expected to become more widely used.

[edit] Hosted vs. on-premise IVR

With the introduction of Web services into the Contact Center, integration has been simplified. The use of Web based applications allow IVR applications to be hosted remotely from the contact center. This allows the use of hosted IVR applications using speech to be made available to smaller Contact Centers across the globe and is likely to lead to an expansion of ASP (Application Service Providers).

IVR applications can also be hosted in the public network, which do not require contact center integration. This will include public announcement messages or message services for small business. It is also possible to use two prong IVR services where the initial IVR application is used to route the call to the appropriate contact center. This can be used to balance loading across multiple contact centers or provide business continuity in the event of system outage.

XML

XML (**Extensible Markup Language**) is a set of rules for encoding documents in machine-readable form. As of 2009, hundreds of XML-based languages have been developed,[7] including RSS, Atom, SOAP, and XHTML. XML-based formats have become the default for most office-productivity tools, including Microsoft Office (Office Open XML), OpenOffice.org (OpenDocument), and Apple's iWork.

Key terminology

The material in this section is based on the XML Specification. This is not an exhaustive list of all the constructs which appear in XML; it provides an introduction to the key constructs most often encountered in day-to-day use.

(Unicode) Character
: By definition, an XML document is a string of characters. Almost every legal Unicode character may appear in an XML document.

Processor and Application
: The *processor* analyzes the markup and passes structured information to an *application*. The specification places requirements on what an XML processor must do and not do, but the application is outside its scope. The processor (as the specification calls it) is often referred to colloquially as an *XML parser*.

Markup and Content
: The characters which make up an XML document are divided into *markup* and *content*. Markup and content may be distinguished by the application of simple syntactic rules. All strings which constitute markup either begin with the character "<" and end with a ">", or begin with the character "&" and end with a ";". Strings of characters which are not markup are content.

Tag
: A markup construct that begins with "<" and ends with ">". Tags come in three flavors: *start-tags*, for example `<section>`, *end-tags*, for example `</section>`, and *empty-element tags*, for example `<line-break/>`.

Element
: A logical component of a document which either begins with a start-tag and ends with a matching end-tag, or consists only of an empty-element tag. The characters between the start- and end-tags, if any, are the element's *content*, and may contain markup, including other elements, which are called *child elements*. An example of an element is `<Greeting>Hello, world.</Greeting>` (see hello world). Another is `<line-break/>`.

Attribute

A markup construct consisting of a name/value pair that exists within a start-tag or empty-element tag. In the example (below) the element *img* has two attributes, *src* and *alt*: `<img src="madonna.jpg" alt='by Raphael'/>`. Another example would be `<step number="3">Connect A to B.</step>` where the name of the attribute is "number" and the value is "3".

XML Declaration

XML documents may begin by declaring some information about themselves, as in the following example.

```
<?xml version="1.0" encoding="UTF-8" ?>
```

[edit] Example

Here is a small, complete XML document, which uses all of these constructs and concepts.

```
<?xml version="1.0" encoding="UTF-8" ?>
<painting>
  <img src="madonna.jpg" alt='Foligno Madonna, by Raphael'/>
  <caption>This is Raphael's "Foligno" Madonna, painted in
    <date>1511</date>-<date>1512</date>.
  </caption>
</painting>
```

There are five elements in this example document: `painting`, `img`, `caption`, and two `date`s. The `date` elements are children of `caption`, which is a child of the root element `painting`. `img` has two attributes, `src` and `alt`.

USSD

Unstructured Supplementary Service Data is a capability of all GSM phones. It is generally associated with real-time or instant messaging type phone services. There is no store-and-forward capability, such as is typical of other short-message protocols (in other words, an SMSC is not present in the processing path). Response times for interactive USSD-based services are generally quicker than those used for SMS.

USSD Phase 1, specified in GSM 02.90, only supports mobile initiated operation (pull operation). In the core network the message is delivered over MAP. USSD Phase 2, specified in GSM 03.90, supports network-initiated operation (pulls and push operation).

USSD is typically used as a 'trigger' to invoke independent calling services that don't require the overhead and additional usage costs of an SMSC, such as a callback service (e.g. cheaper phone charges while roaming), or interactive data service (e.g. stock quotes, sports results).

USSD is a standard for transmitting information over GSM signaling channels. It is mostly used as a method to query the available balance and other similar information in pre-paid GSM services. The function that is triggered when sending USSD is network-dependent and depends on the specific services the operator is offering.

Example USSD codes:

- *101#
- *109*72348937857623#

After entering a USSD code on your GSM handset, the reply from the GSM operator is displayed within a few seconds.

USSD is the base of some payment methods such as SharEpay, SWAP Mobile in South Africa, Mobipay in Spain, M-Pesa in Tanzania (but not in Kenya, where M-Pesa menus are provided by STK rather than USSD), and mPay in Poland.

IN

The **Intelligent Network**, typically stated as its acronym IN, is a network architecture intended both for fixed as well as mobile telecom networks. It allows operators to differentiate themselves by providing value-added services in addition to the standard telecom services such as PSTN, ISDN and GSM services on mobile phones.

The intelligence is provided by network nodes on the service layer, distinct from the switching layer of the core network, as opposed to solutions based on intelligence in the core switches or telephone equipments. The IN nodes are typically owned by telecommunications operators (Telecommunications Service Providers).

IN is based on the Signaling System #7 (SS7) protocol between telephone network switching centers and other network nodes owned by network operators.

Examples of such services are:

- Televoting
- Call screening
- Telephone number portability
- Toll free calls / Freephone
- Prepaid calling
- Account card calling
- Virtual private networks (eg : Family group calling)
- Centrex service (Virtual PBX)
- Private-number plans (with numbers remaining unpublished in directories)
- Universal Personal Telecommunication service (a universal personal telephone number)
- Mass-calling service
- Prefix free dialing from cellphones abroad
- Seamless MMS message access from abroad.
- Reverse charging
- Home Area Discount
- Premium Rate calls
- Call distribution based on various criteria associated with the call

    - Location Based Routing
    - Time based routing
    - Proportional call distribution (eg between two or more call centres or offices).
- Call Queueing
- Call transfer

The main concepts (functional view) surrounding IN services or architecture are connected with SS7 architecture:

- **Service Switching Function (SSF)** or **Service Switching Point (SSP)** This is co-located with the telephone exchange itself, and acts as the trigger point for further services to be invoked during a call. The SSP implements the *Basic Call State Machine (BCSM)* which is a Finite state machine that represents an abstract view of a call from beginning to end (off hook, dialing, answer, no answer, busy, hang up, etc.). As each state is traversed, the exchange encounters *Detection Points (DPs)* at which the SSP may invoke a query to the SCP to wait for further instructions on how to proceed. This query is usually called a trigger. Trigger criteria are defined by the operator and might include the subscriber calling number or the dialled number. The SSF is responsible for entertaining calls requiring value added services.

- **Service Control Function (SCF)** or **Service Control Point (SCP)** This is a separate set of platforms that receive queries from the SSP. The SCP contains service logic which implements the behaviour desired by the operator, i.e., the services. During service logic processing, additional data required to process the call may be obtained from the SDF. The logic on the SCP is created using the SCE.

- **Service Data Function (SDF)** or **Service Data Point (SDP)** This is a database that contains additional subscriber data, or other data required to process a call. For example, the subscribers prepaid credit which is remaining may be an item stored in the SDF to be queried in real time during the call. The SDF may be a separate platform, or is sometimes co-located with the SCP.

- **Service Creation Environment (SCE)** This is the development environment used to create the services present on the SCP. Although the standards permit any type of environment, it is fairly rare to see low level languages like C used. Instead, proprietary graphical languages have been used to enable telecom engineers to create services directly. The languages usually belong to 4G languages, the user can use Graphical Interface to manipulate between different functions to formulate a service.

- **Specialized Resource Function (SRF)** or **Intelligent Peripheral (IP)** This is a node which can connect to both the SSP and the SCP and delivers additional special resources into the call, mostly related to voice data, for example play voice announcements or collect DTMF tones from the user.

Call screening

Call screening is the process of evaluating the characteristics of a telephone call before deciding how or whether to answer it.

Some methods may include:

- listening to the message being recorded on an answering machine or voice mail
- checking a caller ID display to see who or where the call is from
- checking the time or date which a call or message was received
- prescreening callers to a request line at a radio station or call-in talk show before they are allowed on the air

In addition, in the US and Canada, **Call Screen** is the name of a calling feature offered by the telephone companies that allows a customer to establish a list of numbers; anyone calling the customer from those numbers will receive an automatic message indicating that the call is not being accepted. Another name, not usually used for marketing purposes, is "Selective Call Rejection".

MSISDN

MSISDN is a number uniquely identifying a subscription in a GSM or a UMTS mobile network. Simply put, it is the telephone number of the SIM card in a mobile/cellular phone. This abbreviation has several interpretations, the most common one being "Mobile Subscriber Integrated Services Digital Network Number".[1]

The MSISDN together with IMSI are two important numbers used for identifying a mobile subscriber. The latter identifies the SIM, i.e. the card inserted in to the mobile phone, while the former is used for routing calls to the subscriber. IMSI is often used as a key in the HLR ("subscriber database") and MSISDN is the number normally dialed to connect a call to the mobile phone. A SIM is uniquely associated to an IMSI, while the MSISDN can change in time (e.g. due to number portability), i.e. different MSISDNs can be associated to the SIM.

Abbreviation

Depending on source or standardization body, the abbreviation MSISDN can be written out in several different ways. These are today the most widespread and common in use.

Organization	Meaning	Source
3GPP ITU OMA	Mobile Subscriber ISDN Number	Vocabulary for 3GPP Specifications (new)[2] ITU-T Rec. Q.1741-4 (10/2005)[3] Dictionary for OMA Specifications [4]
3GPP ITU	Mobile Station International ISDN Number(s)	GSM 03.03 (old)[5] ITU-T Rec. Q.1741-4 (10/2005)[3]

GSMA		Mobile Terms & Acronyms[6]
ITU	Mobile International ISDN Number	Vocabulary of Switching and Signalling Terms [7]
	Mobile Station International Subscriber Directory Number	

[edit] MSISDN Format

An MSISDN is limited to 15 digits, prefixes not included (e.g., 00 prefixes an international MSISDN when dialing from Sweden).

MSISDN - Mobile Station International Subscriber Directory Number

In GSM and its variant DCS 1800, MSISDN is built up as

```
MSISDN = CC + NDC + SN
CC = Country Code
NDC = National Destination Code, identifies one or part of a PLMN
SN = Subscriber Number
```

In the GSM variant *PCS 1900*, MSISDN is built up as

```
MSISDN = CC + NPA + SN
CC = Country Code
NPA = Number Planning Area
SN = Subscriber Number
```

[edit] Example

MSISDN: 79261234567

CC	7	Russia
NDC	926	MegaFon
SN	1234567	Subscriber's number

CAMEL

Customised Applications for Mobile networks Enhanced Logic, or CAMEL (ETSI TS 123 078) for short, is a set of standards designed to work on either a GSM core network or UMTS

network. They allow an operator to define services over and above standard GSM services/ UMTS services. The CAMEL architecture is based on the Intelligent network (IN) standards, and uses the CAP protocol.

Many services can be created using CAMEL, and it is particularly effective in allowing these services to be offered when a subscriber is roaming, like, for instance, no-prefix dialing (the number the user dials is the same no matter the country where the call is placed) or seamless MMS message access from abroad.

CAMEL entities

- gsmSCF: GSM Service Control Function
- gsmSSF: GSM Service Switching Function
- gsmSRF: GSM Specialized Resource Function
- gprsSSF: GPRS Service Switching Function

[edit] Phases

CAMEL was always intended to be specified in phases.[1] As of 2007, there have been 4 phases specified, each building on the previous phase.[2] Phases 1 and 2 were defined before 3G networks were specified, and as such support adding IN services to a GSM network, although they are equally applicable to 2.5G and 3G networks. Phase 3 was defined for 3GPP Releases 99 and 4, and hence is a GSM and UMTS common specification, while Phase 4 was defined as part of 3GPP Release 5.

In line with other GSM specifications, later phases should be fully backwards compatible with earlier phases; this is achieved by means of the Transaction Capabilities Application Part (TCAP) Application Context (AC) negotiation procedure, with each CAMEL phase being allocated its own AC version.[3]

[edit] Phase 1

CAMEL Phase 1 defined only very basic call control services, but introduced the concept of a CAMEL Basic call state model (BCSM) to the Intelligent Network (IN). Phase 1 gave the gsmSCF the ability to bar calls (release the call prior to connection), allow a call to continue unchanged, or to modify a limited number of call parameters before allowing it to continue. The gsmSCF could also monitor the status of a call for certain events (call connection and disconnection), and take appropriate action on being informed of the event.[1]

Phase 1 was defined as part of Release 96 in 1997.

[edit] Phase 2

CAMEL Phase 2 enhanced the capabilities defined in Phase 1. In addition to supporting the facilities of Phase 1, Phase 2 included the following:

- Additional event detection points
- Interaction between a user and a service using announcements, voice prompting and information collection via in-band interaction or Unstructured Supplementary Service Data (USSD) interaction
- Control of call duration and transfer of Advice of Charge Information to the mobile station;
- The ability to inform the gsmSCF about the invocation of the supplementary services Explicit Call Transfer (ECT), Call Deflection (CD) and Multi-Party Calls (MPTY)
- The ability, for easier post-processing, of integrating charging information from a serving node in normal call records[1]

Phase 2 was defined as part of 3GPP Releases 97 and 98, in 1998, although it is referenced in the stage 1 specification of Release 96.

[edit] Phase 3

The third phase of CAMEL enhanced the capabilities of phase 2. The following capabilities were added:

- Support of facilities to avoid overload
- Capabilities to support Dialed Services
- Capabilities to handle mobility events, such as (Not-)reachability and roaming;
- Control of GPRS sessions and PDP contexts
- Control of Mobile Originated SMS through both circuit-switched and packet-switched serving network entities
- Interworking with SoLSA (Support of Localised Service Area). Support for this interworking is optional;
- The gsmSCF can be informed about the invocation of the supplementary service Call Completion to Busy Subscriber (CCBS)[2]

Phase 3 was released as part of 3GPP Releases 99 and 4 in 1999.

[edit] Phase 4

The fourth phase of CAMEL built on the capabilities of phase 3. The following features were defined:

- CAMEL support for Optimal Routing of circuit-switched mobile-to-mobile calls
- The capability for the gsmSCF to create additional parties in an existing call (Call Party Handling)
- The capability for the gsmSCF to create a new call unrelated to any other existing call (Call Party Handling - new call)
- Capabilities for the enhanced handling of call party connections (Call Party Handling)
- Control of Mobile Terminated SMS through both circuit-switched and packet-switched serving network entities
- The capability for the gsmSCF to control sessions in the IP Multimedia Subsystem (IMS)[2]
- The gsmSCF can request the gsmSSF to play a fixed or a variable sequence of tones

With CAMEL Phase 4, it is possible that only a limited subset of the new functionalities is supported, in addition to the complete support of CAMEL Phase 3.

Phase 4 was released as part of 3GPP Release 5 in 2002.

Basic call state model

From Wikipedia, the free encyclopedia

In Intelligent Network and CAMEL switching, a **BCSM** is a Basic Call State Model

Types

- O-BCSM (Originating BCSM)
- T-BCSM (Terminating BCSM)

A fundamental concept for IN control is the basic call state model (BCSM). When a call is processed by an exchange, the call goes through a number of pre-defined phases. These phases of the call are described in the BCSM. The BCSM generally follows the ISUP signalling of a call

State machine description

In the following IN BCSMs, bold Detection Points and Points In Call are also present in the CAMEL Ph1 subset.

TODO: Expand to Ph2,3,4

[edit] O-BCSM

[edit] Points in call

- 1. **O_Null & Authorize Origination Attempt**
- 2. **Collect_info** (Merged with 1. in CAMEL Ph1)
- 3. **Analyze_Info**
- 4. **Routing & Alerting** (Merged with 3. in CAMEL Ph1)
- 5. **O_Active**
- 6. **O_Exception**

[edit] Detection Points

- 1 Origination_Attempt_Authorized
- 2 **Collected_Info**
- 3 Analyzed_Info (this is the only Statically armed DP, others are dynamically armed using "Request Report BCSM (RRBE)" message by the SCP)
- 4 Route_Select_Failure

- 5 O_Called_Party_Busy
- 6 O_No_Answer
- 7 **O_Answer**
- 8 O_Mid_Call
- 9 **O_Disconnect**
- 10 O_Abandon

[edit] T-BCSM

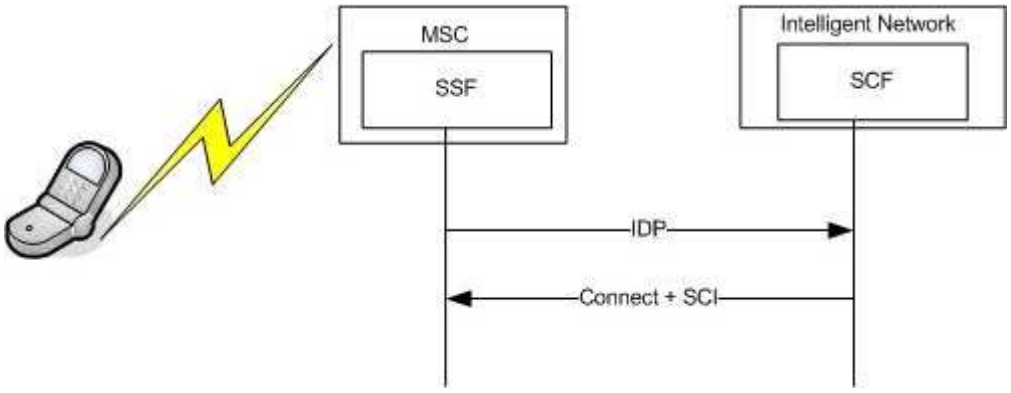
[edit] Points in call

- 7. **T_Null & Authorize Termination_Attempt**
- 8. **Select_Facility & Present_Call**
- 9. **T_Alerting** (Merged with 8. in CAMEL Ph1)
- 10. **T_Active**
- 11. **T_Exception**

[edit] Detection Points

- 12 **Termination_Attempt_Authorized**
- 13 T_Called_Party_Busy
- 14 T_No_Answer
- 15 **T_Answer**
- 16 T_Mid_Call
- 17 **T_Disconnect**
- 18 T_Abandon

[edit] Messages



basic INAP call example

- Initial Detection Point (IDP)
- RRB (Request Report BCSM)
- Event Report BCSM (ERB)
- Connect (CONN)

- Send Charging Information (SCI)
- AC (Apply Charging)

IMSI

An **International Mobile Subscriber Identity** or **IMSI** (pronounced /□□mzi/) is a unique number associated with all GSM and UMTS network mobile phone users. It is stored in the SIM inside the phone and is sent by the phone to the network. It is also used for acquiring other details of the mobile in the Home Location Register (HLR) or as locally copied in the Visitor Location Register. To prevent eavesdroppers identifying and tracking the subscriber on the radio interface, the IMSI is sent as rarely as possible and a randomly-generated TMSI is sent instead.

The IMSI is used in *any* mobile network that interconnects with other networks, in particular CDMA and EVDO networks as well as GSM networks. This number is provisioned in the phone directly or in the R-UIM card (a CDMA analogue equivalent to a SIM card in GSM).

An IMSI is usually 15 digits long, but can be shorter (for example MTN South Africa's old IMSIs that are still being used in the market are 14 digits). The first 3 digits are the Mobile Country Code (MCC), and is followed by the Mobile Network Code (MNC), either 2 digits (European standard) or 3 digits (North American standard). The remaining digits are the mobile station identification number (MSIN) within the network's customer base.

Examples

IMSI: 429011234567890

MCC 429 Nepal

MNC 01 Nepal Telecom

MSIN 1234567890

IMSI: 310150123456789

MCC 310 USA

MNC 150 AT&T Mobility

MSIN 123456789

MML (language)

A **man-machine language** or *MML* is a specification language. MML typically are defined to standardize the interfaces for managing a telecommunications or network device from a console.

API

An **application programming interface** (**API**) is an interface implemented by a software program which enables it to interact with other software. It facilitates interaction between different software programs similar to the way the user interface facilitates interaction between humans and computers. An API is implemented by applications, libraries, and operating systems to determine their vocabularies and calling conventions, and is used to access their services. It may include specifications for routines, data structures, object classes, and protocols used to communicate between the consumer and the implementer of the API

Concept

An API is an abstraction that describes an interface for the interaction with a set of functions used by components of a software system. The software providing the functions described by an API is said to be an *implementation* of the API.

An API can be:

- general, the full set of an API that is bundled in the libraries of a programming language, e.g. Standard Template Library in C++ or Java API.
- specific, meant to address a specific problem, e.g. Google Maps API or Java API for XML Web Services.
- language-dependent, meaning it is only available by using the syntax and elements of a particular language, which makes the API more convenient to use.
- language-independent, written so that it can be called from several programming languages. This is a desirable feature for a service-oriented API that is not bound to a specific process or system and may be provided as remote procedure calls or web services. For example, a website that allows users to review local restaurants is able to layer their reviews over maps taken from Google Maps, because Google Maps has an API that facilitates this functionality. Google Maps' API controls what information a third-party site can use and how they can use it.

API may be used to refer to a complete interface, a single function, or even a set of APIs provided by an organization. Thus, the scope of meaning is usually determined by the context of usage.

Advanced explanation

An API may describe the ways in which a particular task is performed. For example, in Unix systems, the `math.h` include file for the C language contains the definition of the mathematical functions available in the C language library for mathematical processing (usually called `libm`). This file would describe how to use these functions and the expected result. For example, on a

Unix system the command `man 3 sqrt` will present the signature of the function `sqrt` in the form:

```
SYNOPSIS
            #include <math.h>
            double sqrt(double X);
            float  sqrtf(float X);
DESCRIPTION
       DESCRIPTION
       sqrt computes the positive square root of the argument. ...
RETURNS
       On success, the square root is returned. If X is real and positive...
```

that means that the function returns the square root of a positive floating point number (`single` or `double` precision) as another floating point number. Hence the API in this case can be interpreted as the collection of the included files used by the C language and its human readable description provided by the man pages.

In object oriented languages, an API usually includes a description of a set of class definitions, with a set of behaviours associated with those classes. A *behaviour* is the set of rules for how an object, derived from that class, will act in a given circumstance. This abstract concept is associated with the real functionalities exposed, or made available, by the classes that are implemented in terms of class methods.

The API in this case can be conceived as the totality of all the methods publicly exposed by the classes (usually called the class *interface*). This means that the API prescribes the methods by which one handles the objects derived from the class definitions.

More generally, one can see the API as the collection of all the kind of objects one can derive from the class definitions, and their associated possible behaviours. The use again is mediated by the public methods, but in this interpretation, the methods are seen as a technical detail of how the behaviour is implemented.

For instance: a class representing a `Stack` can expose publicly two methods `push()` (to add a new item to the stack), and `pop()` (to extract the last item, ideally placed on top of the stack).

The API in this case can be interpreted as the two methods `pop()` and `push()`, or more generally as the idea that one can use an item of type `Stack` that implements the behaviour of a stack (a pile *exposing* its top to add/remove elements).

This concept can be carried to the point where a class interface in an API has no methods at all, but only behaviours associated with it. For instance, the Java language API includes the interface `Serializable`, which is an interface that requires the class that implements it to behave in a serialized fashion. This does not require it to have any public method, but rather requires that the class permit it to have a representation that can be saved at any time. This is typically true for any class containing simple data and no link to external resources, like an open connection to a file, a remote system, or an external device.

In this sense, in object oriented languages, the API defines a set of behaviors, possibly mediated by a set of class methods. In such languages, the API is still distributed as a library. For example, the Java language libraries include a set of APIs that are provided in the form of the JDK used by the developers to build new Java programs. The JDK includes the documentation of the API in Javadoc notation. The quality of the documentation associated to an API is often a factor determining its success in terms of ease of use.

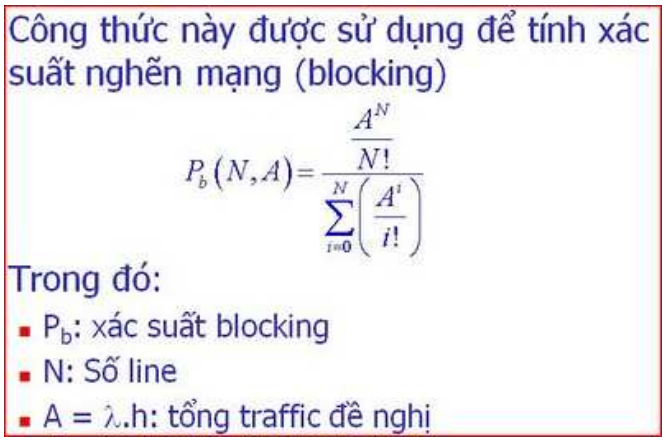
Erlang

Erlang (Erl): là đ□n v□ đo c□a l□u l□□ng (Traffic) (b□n c□ hi□u là 1Erl là 1 thuê bao đ□□c chi□m kênh(full) trong su□t th□i gian 1gi□) được tính nh□ sau:

A = (n x t)/ T
Trong đó: A là l□u l□□ng đo b□ng Erl, n là s□ cu□c g□i, t là độ dài trung bình của mỗi cuộc gọi, T là th□i gian đo (th□□ng T=1h = 3600s)
Từ Erl ta có thể biết được số phút gọi: số phút gọi = lưu lượng (Erl) *60 (phút)

Công th□c trên dùng đ□ tính l□u l□□ng trung bình c□a 1 thuê bao. Erlang tối đa c□a h□ th□ng d□a vào b□ng Erlang B khi bi□t đ□□c c□u hình c□a tr□m và GoS c□a h□ th□ng. Lưu lượng cell có khả năng phục vụ được tra bảng bảng Erlang B theo số kênh TCH với GoS (th□□ng thì GoS = 2%.) *V*du: 1 cell cấu hình 4, có 24 kênh TCH. Tra bảng Erlang B với GoS = 2%, thì lưu lượng cell có khả năng phục vụ là 16,63 Erl

Trong th□c t□, Erlang còn đ□i di□n cho kh□ năng chuy□n m□ch c□a 1 t□ng đài. Xác su□t b□ ngh□n m□ch ph□ thu□c vào Erlang c□a t□ng đài và t□ng Erlang c□a subscriber vào 1 th□i gian nào đó Ngoài ra, các operator dùng Erl hi□n t□i c□a tr□m đ□ d□ trù cho l□u l□□ng c□a khu v□c dân c□ mà BTS đó ph□c v□ nh□ b□ nâng gi□m c□u hình, HR, cosite, b□ sung tr□m, và quan tr□ng nh□t là 1 operator dùng Erl đ□ tính ra ti□n, hehe



Offered traffic (in erlangs) is related to the **call arrival rate**, λ, and the **average call-holding time**, *h*, by:

$$E = \lambda h$$

provided that *h* and λ are expressed using the same units of time (seconds and calls per second, or minutes and calls per minute).

Erlang B formula

Erlang-B (sometimes also written without the hyphen **Erlang B**), also known as the **Erlang loss formula**, is a formula for the **blocking probability** derived from the Erlang distribution to describe the probability of call loss on a group of circuits (in a circuit switched network, or equivalent). It is, for example, used in planning telephone networks. The formula was derived by Agner Krarup Erlang and is not limited to telephone networks, since it describes a probability in a queuing system (albeit a special case with a number of servers but no buffer spaces for incoming calls to wait for a free server). Hence, the formula is also used in certain inventory systems with lost sales.

The formula applies under the condition that an unsuccessful call, because the line is busy, is not queued or retried, but instead really lost forever. It is assumed that call attempts arrive following a Poisson process, so call arrivals are independent. Further it is assumed that message length (holding times) are exponentially distributed (Markovian system) although the formula turns out to apply under general holding time distributions.

Erlangs are a dimensionless quantity calculated as the average arrival rate, λ, multiplied by the average call length, *h*. (see Little's Law) The Erlang B formula assumes an infinite population of sources (such as telephone subscribers), which jointly offer traffic to *N* servers (such as links in a trunk group). The rate of arrival of new calls (birth rate) is equal to λ and is constant, *not* depending on the number of active sources, because the total number of sources is assumed to be infinite. The rate of call departure (death rate) is equal to the number of calls in progress divided by *h*, the mean call holding time. The formula calculates blocking probability in a loss system, where if a request is not served immediately when it tries to use a resource, it is aborted.

Requests are therefore not queued. Blocking occurs when there is a new request from a source, but all the servers are already busy. The formula assumes that blocked traffic is immediately cleared.

The formula provides the GoS (grade of service) which is the probability P_b that a new call arriving at the circuit group is rejected because all servers (circuits) are busy: $B(E, m)$ when E Erlang of traffic are offered to m trunks (communication channels).

$$P_b = B(E,m) = \frac{\frac{E^m}{m!}}{\sum_{i=0}^{m} \frac{E^i}{i!}}$$

where:

- P_b is the probability of blocking
- m is the number of resources such as servers or circuits in a group
- $E = \lambda h$ is the total amount of traffic offered in erlangs

This may be expressed recursively as follows, in a form that is used to simplify the calculation of tables of the Erlang B formula:

$$B(E,0) = 1.$$

$$B(E,j) = \frac{EB(E,j-1)}{EB(E,j-1)+j} \quad \forall j = 1,2,...,m$$

Typically, instead of $B(E, m)$ the inverse $1/B(E, m)$ is calculated in numerical computation in order to ensure numerical stability:

$$\frac{1}{B(E,0)} = 1$$

$$\frac{1}{B(E,j)} = 1 + \frac{j}{E}\frac{1}{B(E,j-1)} \quad \forall j = 1,2,...,m$$

```
Function ErlangB (E as Double, m As Integer) As Double
Dim InvB As Double
Dim j As Integer

  InvB = 1.0
  For j = 1 To m
    InvB = 1.0 + j / E * InvB
  Next j
  ErlangB = 1.0 / InvB
End Function
```

The Erlang B formula applies to loss systems, such as telephone systems on both fixed and mobile networks, which do not provide traffic buffering, and are not intended to do so. It assumes that the call arrivals may be modeled by a Poisson process, but is valid for any statistical distribution of call holding times with finite mean. Erlang B is a trunk sizing tool for voice switch to voice switch traffic. The Erlang B formula is decreasing and convex in m.[2]

[edit] Extended Erlang B

Extended Erlang B is an iterative calculation, rather than a formula, that adds an extra parameter, the Recall Factor, which defines the recall attempts[3].

The steps in the process are as follows[4]:

1. Calculate

$$P_b = B(E, m)$$

as above for Erlang B.

2. Calculate the probable number of blocked calls

$$B_e = EP_b$$

3. Calculate the number of recalls, R assuming a Recall Factor, R_f:

$$R = B_e R_f$$

4. Calculate the new offered traffic

$$E_{i+1} = E_0 + R$$

where E_0 is the initial (baseline) level of traffic.

5. Return to step 1 and iterate until a stable value of E is obtained.

[edit] Erlang C formula

The **Erlang C formula** expresses the waiting probability in a queuing system. Just as the Erlang B formula, Erlang C assumes an infinite population of sources, which jointly offer traffic of A erlangs to N servers. However, if all the servers are busy when a request arrives from a source, the request is queued. An unlimited number of requests may be held in the queue in this way simultaneously. This formula calculates the probability of queuing offered traffic, assuming that blocked calls stay in the system until they can be handled. This formula is used to determine the number of agents or customer service representatives needed to staff a call centre, for a specified desired probability of queuing.

$$P_W = \frac{\frac{A^N}{N!}\frac{N}{N-A}}{\sum_{i=0}^{N-1}\frac{A^i}{i!} + \frac{A^N}{N!}\frac{N}{N-A}}$$

where:

- A is the total traffic offered in units of erlangs
- N is the number of servers
- P_W is the probability that a customer has to wait for service

It is assumed that the call arrivals can be modeled by a Poisson process and that call holding times are described by a negative exponential distribution. A common use for Erlang C is modeling and dimensioning call center agents in a call center environment.

Technical details

Engset's equation is similar to the Erlang-B formula; however it contains one major difference: Erlang's equation assumes an infinite source of calls, yielding a Poisson arrival process, while Engset specifies a finite number of callers[5] [6]. Thus Engset's equation should be used when the source population is small (say less than 200 users, extensions or customers).

$$P_b(N, A, S) = \frac{A^N \binom{S}{N}}{\sum_{i=0}^{N} A^i \binom{S}{i}}$$

where

A = offered traffic intensity in erlangs, from all sources

S = number of sources of traffic

N = number of circuits in group

P(b) = probability of blocking or congestion

In practice, like Erlang's equations, Engset's formula requires recursion to solve for the blocking or congestion probability. There are several recursions that could be used[6]. One way to determine this probability, one first determines an initial estimate. This initial estimate is substituted into the equation and the equation then is solved. The answer to this initial calculation is then substituted back into the equation, resulting in a new answer which is again substituted. This iterative process continues until the equation converges to a stable result.[5][7].

Engset's equation follows[5]:

$$P(b) = \frac{\left[\frac{(S-1)!}{N!\cdot(S-1-N)!}\right] \cdot M^N}{\sum_{X=1}^{N}\left[\frac{(S-1)!}{X!\cdot(S-1-X)!}\right] \cdot M^X}$$

$$M = \frac{A}{S - A \cdot (1 - P(b))}$$

GT

A **Global Title** (GT) is an address used in the SCCP protocol for routing signaling messages on telecommunications networks. In theory, a global title is a unique address which refers to only one destination, though in practice destinations can change over time.

DRM

*D*ata *R*esponse *M*anagement

IVVR

*I*nteractive *V*oice and *V*ideo *R*esponse

Portal

In **computing**:

- Enterprise portal, a framework to provide a single point of access to a variety of information and tools
- Intranet portal, a gateway that unifies access to all enterprise information and applications
- Portal rendering, an optimization technique in 3D computer graphics
- Web portal, a site that functions as a point of access to information on the Internet
- Portals network programming API, a high-performance networking programming interface for massively parallel supercomputers

BICC

The **Bearer Independent Call Control** (**BICC**) is a signaling protocol based on N-ISUP that is used for supporting narrowband ISDN service over a broadband backbone network. BICC is designed to interwork with existing transport technologies

BICC signaling messages are nearly identical to those in ISUP; the main difference being that the narrowband Circuit Identification Code (CIC) has been removed from the header. The BICC architecture consists of interconnected Serving Nodes that provide the Call Service Function and the Bearer Control Function. The Call Service Function uses BICC signaling for call setup and may also interwork with ISUP. The Bearer Control Function receives directives from the Call

Service Function via BICC Bearer Control Protocol (ITU-T recommendation Q.1950) and is responsible for setup and teardown of bearer paths on a set of physical transport links. Transport links are most commonly TDM, ATM or IP.

According to the ITU, the completion of the BICC protocols is a historic step toward broadband multimedia networks because it enables the seamless migration from circuit-switched TDM networks to high-capacity broadband multimedia networks.

The Third Generation Partnership Project (3GPP) has included BICC CS 2 in the Universal Mobile Telecommunications Service (UMTS) release 4

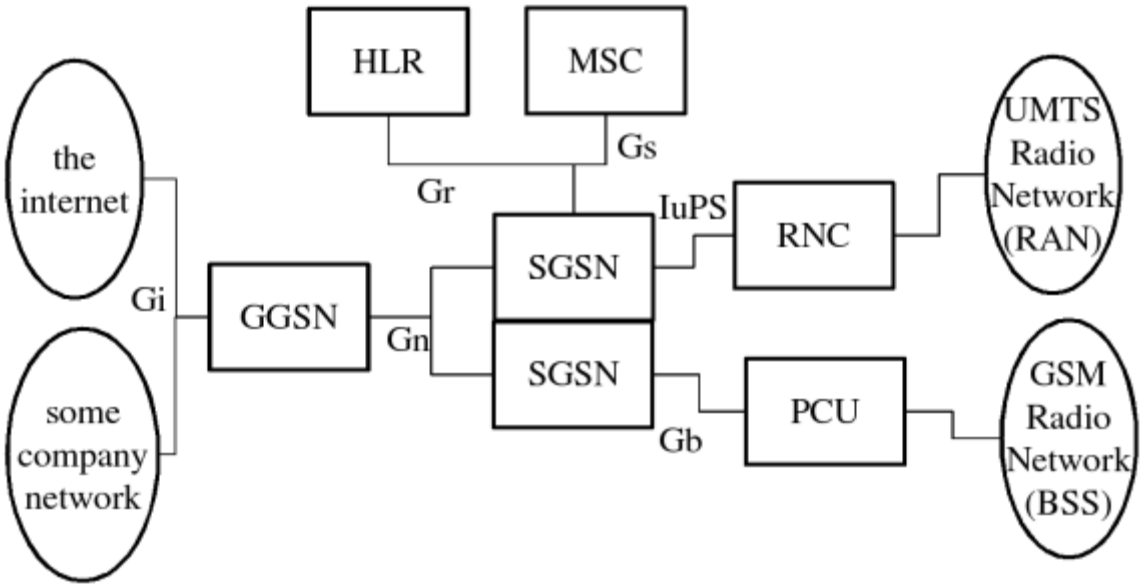
Stream (computing), succession of data elements supplied over time

Streaming media, multimedia data transferred in a stream of packets that are interpreted and rendered, in real-time, by a software application as the packets arrive

GPRS Core Network

The General Packet Radio Service (GPRS) system is used by GSM mobile phones, the most common mobile phone system in the world, for transmitting IP packets. The **GPRS core network** is the centralized part of the GPRS system. It also provides support for WCDMA based 3G networks. The GPRS core network is an integrated part of the GSM network switching subsystem.

General support functions



GPRS core structure

The GPRS core network provides mobility management, session management and transport for Internet Protocol packet services in GSM and WCDMA networks. The core network also provides support for other additional functions such as billing and lawful interception. It was also proposed, at one stage, to support packet radio services in the US D-AMPS TDMA system, however, in practice, all of these networks have been converted to GSM so this option has become irrelevant.

Like GSM in general, GPRS module is an open standards driven system. The standardization body is the 3GPP.

GPRS tunnelling protocol (GTP)

GPRS tunnelling protocol is the defining IP protocol of the GPRS core network. Primarily it is the protocol which allows end users of a GSM or WCDMA network to move from place to place while continuing to connect to the Internet as if from one location at the Gateway GPRS Support Node (GGSN). It does this by carrying the subscriber's data from the subscriber's current Serving GPRS Support Node (SGSN) to the GGSN which is handling the subscriber's session. Three forms of GTP are used by the GPRS core network.

GTP-U

for transfer of user data in separated tunnels for each Packet Data Protocol (PDP) context

GTP-C

for control reasons including:

- setup and deletion of PDP contexts
- verification of GSN reachability
- updates; e.g., as subscribers move from one SGSN to another.

GTP'

for transfer of charging data from GSNs to the charging function.

GGSNs and SGSNs (collectively known as GSNs) listen for GTP-C messages on UDP port 2123 and for GTP-U messages on port 2152. This communication happens within a single network or may, in the case of international roaming, happen internationally, typically across a GPRS roaming exchange (GRX).

The *Charging Gateway Function* (CGF) listens to GTP' messages sent from the GSNs on TCP or UDP port 3386. The core network sends charging information to the CGF, typically including PDP context activation times and the quantity of data which the end user has transferred. However, this communication which occurs within one network is less standardized and may, depending on the vendor and configuration options, use proprietary encoding or even an entirely proprietary system.

GPRS support nodes (GSN)

A GSN is a network node which supports the use of GPRS in the GSM core network. All GSNs should have a *Gn* interface and support the GPRS tunnelling protocol. There are two key variants of the GSN, namely Gateway and Serving GPRS Support Node.

Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node (GGSN) is a main component of the GPRS network. The GGSN is responsible for the interworking between the GPRS network and external packet switched networks, like the Internet and X.25 networks.

From an external network's point of view, the GGSN is a router to a sub-network, because the GGSN ‘hides’ the GPRS infrastructure from the external network. When the GGSN receives data addressed to a specific user, it checks if the user is active. If it is, the GGSN forwards the data to the SGSN serving the mobile user, but if the mobile user is inactive, the data is discarded. On the other hand, mobile-originated packets are routed to the right network by the GGSN.

The GGSN is the anchor point that enables the mobility of the user terminal in the GPRS/UMTS networks. In essence, it carries out the role in GPRS equivalent to the Home Agent in Mobile IP.

It maintains routing necessary to tunnel the Protocol Data Units (PDUs) to the SGSN that service a particular MS (Mobile Station).

The GGSN converts the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format (e.g., IP or X.25) and sends them out on the corresponding packet data network. In the other direction, PDP addresses of incoming data packets are converted to the GSM address of the destination user. The readdressed packets are sent to the responsible SGSN. For this purpose, the GGSN stores the current SGSN address of the user and his or her profile in its location register. The GGSN is responsible for IP address assignment and is the default router for the connected user equipment (UE). The GGSN also performs authentication and charging functions.

Other functions include subscriber screening, IP Pool management and address mapping, QoS and PDP context enforcement.

With LTE scenario the GGSN functionality moves to SAE gateway (with SGSN functionality working in MME).

Serving GPRS Support Node (SGSN)

A Serving GPRS Support Node (SGSN) is responsible for the delivery of data packets from and to the mobile stations within its geographical service area. Its tasks include packet routing and transfer, mobility management (attach/detach and location management), logical link management, and authentication and charging functions. The location register of the SGSN stores location information (e.g., current cell, current VLR) and user profiles (e.g., IMSI, address(es) used in the packet data network) of all GPRS users registered with this SGSN.

Common SGSN Functions

- Detunnel GTP packets from the GGSN (downlink)
- Tunnel IP packets toward the GGSN (uplink)
- Carry out mobility management as Standby mode mobile moves from one Routing Area to another Routing Area
- Billing user data

GSM/EDGE specific SGSN functions

Enhanced Data Rates for GSM Evolution (EDGE) specific SGSN functions and characteristics are:

- Maximum data rate of approx. 60 kbit/s (150 kbit/s for EDGE) per subscriber
- Connect via frame relay or IP to the Packet Control Unit using the Gb protocol stack
- Accept uplink data to form IP packets
- Encrypt down-link data, decrypt up-link data
- Carry out mobility management to the level of a cell for connected mode mobiles

WCDMA specific SGSN functions

- Carry up to about 42 Mbit/s traffic downlink and 5.8 Mbit/s traffic uplink (HSPA+)
- Tunnel/detunnel downlink/uplink packets toward the radio network controller (RNC)
- Carry out mobility management to the level of an RNC for connected mode mobiles

These differences in functionality have led some manufacturers to create specialist SGSNs for each of WCDMA and GSM which do not support the other networks, whilst other manufacturers have succeeded in creating both together, but with a performance cost due to the compromises required.

Access point

Main article: Access point name

An access point is:

- An IP network to which a mobile can be connected
- A set of settings which are used for that connection
- A particular option in a set of settings in a mobile phone

When a GPRS mobile phone sets up a PDP context, the access point is selected. At this point an access point name (APN) is determined

Example: aricent.mnc012.mcc345.gprs

Example: Internet

Example: mywap

This access point is then used in a DNS query to a private DNS network. This process (called APN resolution) finally gives the IP address of the GGSN which should serve the access point. At this point a PDP context can be activated.

PDP Context

The packet data protocol (PDP; e.g., IP, X.25, FrameRelay) context is a data structure present on both the *Serving GPRS Support Node* (SGSN) and the *Gateway GPRS Support Node* (GGSN) which contains the subscriber's session information when the subscriber has an active session. When a mobile wants to use GPRS, it must first attach and then *activate a PDP context*. This allocates a PDP context data structure in the SGSN that the subscriber is currently visiting and the GGSN serving the subscriber's access point. The data recorded includes

- Subscriber's IP address
- Subscriber's IMSI
- Subscriber's

- Tunnel Endpoint ID (TEID) at the GGSN
- Tunnel Endpoint ID (TEID) at the SGSN

The Tunnel Endpoint ID (TEID) is a number allocated by the GSN which identifies the tunnelled data related to a particular PDP context.

Several PDP contexts may use the same IP address. The Secondary PDP Context Activation procedure may be used to activate a PDP context while reusing the PDP address and other PDP context information from an already active PDP context, but with a different QoS profile.[1] Note that the procedure is called secondary, not the resulting PDP contexts that have no such relationship with the one the PDP address of which they reused.

A total of 11 PDP contexts (with any combination of primary and secondary) can co-exist. NSAPI are used to differentiate the different PDP context.

Reference Points and Interfaces

Within the GPRS core network standards there are a number of interfaces and reference points (logical points of connection which probably share a common physical connection with other reference points). Some of these names can be seen in the network structure diagram on this page.

Interfaces in the GPRS network

Ga

The interface servers the CDRs (accounting records) which are written in the GSN and sent to the charging gateway (CG). This interface uses a GTP-based protocol, with modifications that supports CDRs (Called *GTP'* or *GTP prime*).

Gb

Interface between the base station subsystem and the SGSN the transmission protocol could be Frame Relay or IP.

Gd

Interface between the SGSN and the SMS Gateway. Can use MAP1, MAP2 or MAP3.

Ge

The interface between the SGSN and the service control point (SCP); uses the CAP protocol.

Gf

The interface between the SGSN and the Equipment Identity Register (EIR), used for checking the mobile's equipment identity number (IMEI) against a list of reported stolen mobile phones.

Gi

IP based interface between the GGSN and a public data network (PDN) either directly to the Internet or through a WAP gateway.

Gmb

The interface between the GGSN and the Broadcast-Multicast Service Center (BM-SC), used for controlling MBMS bearers.

Gn

IP Based interface between SGSN and other SGSNs and (internal) GGSNs. DNS also shares this interface. Uses the GTP Protocol.

Gp

IP based interface between internal SGSN and external GGSNs. Between the SGSN and the external GGSN, there is the border gateway (which is essentially a firewall). Also uses the GTP Protocol.

Gr

Interface between the SGSN and the HLR. Messages going through this interface uses the MAP3 protocol.

Gs

Interface between the SGSN and the MSC (VLR). Uses the BSSAP+ protocol. This interface allows paging and station availability when it performs data transfer. When the station is attached to the GPRS network, the SGSN keeps track of which routing area (RA) the station is attached to. An RA is a part of a larger location area (LA). When a station is paged this information is used to conserve network resources. When the station performs a PDP context, the SGSN has the exact BTS the station is using.

Gx

The on-line policy interface between the GGSN and the charging rules function (CRF). It is used for provisioning service data flow based charging rules. Uses the diameter protocol.

Gy

The on-line charging interface between the GGSN and the online charging system (OCS). Uses the diameter protocol (DCCA application).

Gz

The off-line (CDR-based) charging interface between the GSN and the CG. Uses GTP'.

Lg

The interface between the SGSN and the Gateway Mobile Location Center (GMLC), used for location based services.

MGW

A **Media gateway** is a translation device or service that converts digital media streams between disparate telecommunications networks such as PSTN, SS7, Next Generation Networks (2G, 2.5G and 3G radio access networks) or PBX. Media gateways enable multimedia communications across Next Generation Networks over multiple transport protocols such as Asynchronous Transfer Mode (ATM) and Internet Protocol (IP).

Because the media gateway connects different types of networks, one of its main functions is to convert between different transmission and coding techniques (see also Transcode). Media streaming functions such as echo cancellation, DTMF, and tone sender are also located in the media gateway.

Media gateways are often controlled by a separate Media Gateway Controller which provides the call control and signaling functionality. Communication between media gateways and Call Agents is achieved by means of protocols such as MGCP or Megaco(H.248) or Session Initiation Protocol (SIP). Modern media gateways used with SIP are often stand-alone units with their own call and signaling control integrated and can function as independent, intelligent SIP end-points.

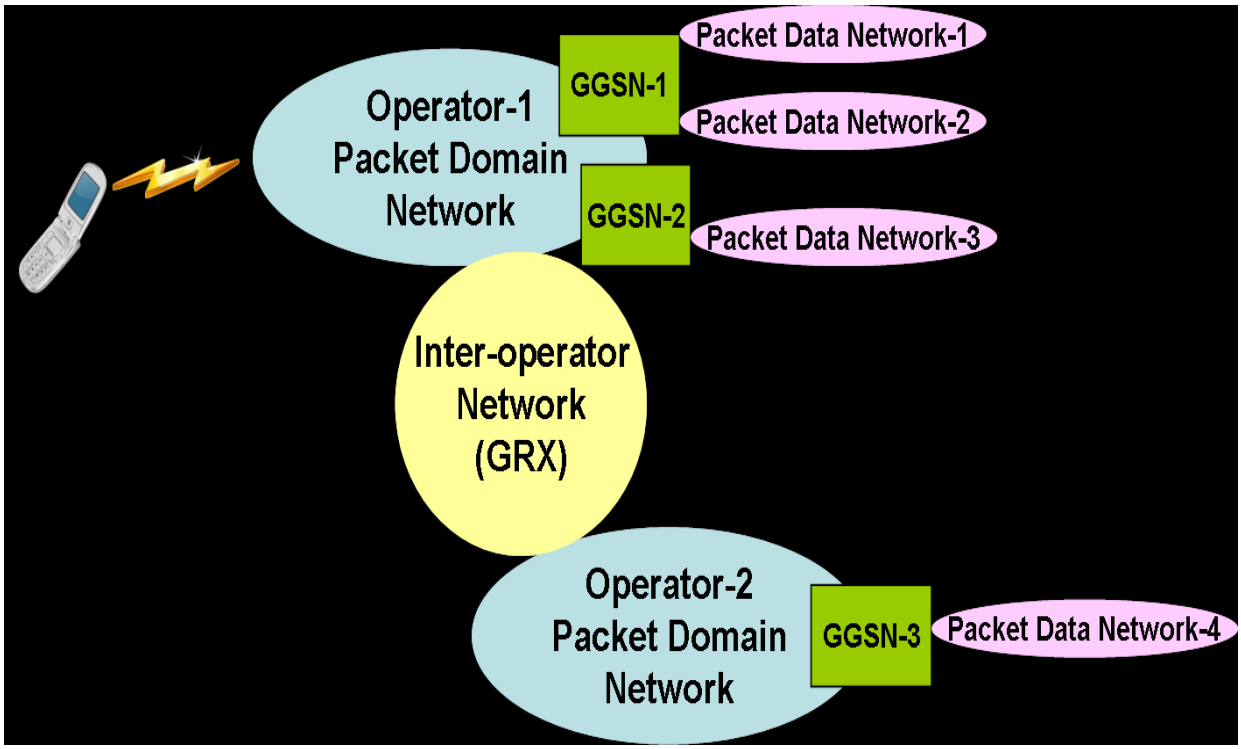
Voice over Internet Protocol (VoIP) media gateways perform the conversion between TDM voice to a media streaming protocol (usually Real-time Transport Protocol, RTP), as well as a signaling protocol used in the VoIP system.

Mobile access Media Gateways connect the radio access networks of a public land mobile network PLMN to a Next Generation Core network. 3GPP standards define the functionality of CS-MGW and IMS-MGW for UTRAN and GERAN based PLMNs.

APN

Access point name (APN) identifies an IP packet data network (PDN), that a mobile data user wants to communicate with. In addition to identifying a PDN, an APN may also be used to define the type of service, (eg connection to wireless application protocol (WAP) server, multimedia messaging service (MMS)), that is provided by the PDN. APN is used in 3GPP data access networks, eg general packet radio service (GPRS), evolved packet core (EPC).

Packet Data Network



The concept of Packet Data Network[1] in 3GPP accesses is illustrated in the accompanying figure. The operator's packet domain network is responsible for providing data connectivity to the mobile user. The user accesses one or more packet data networks (PDN), that either belongs to the operator or is an external network eg internet, corporate intranet, etc. The GGSN separates the operator's packet domain network from packet data networks (PDN). A GGSN may provide connectivity to one or more PDNs. A user may access a PDN either via a GGSN in the visited operator's network VPLMN or via a GGSN in its home operator's network HPLMN. Inter-operator network (GRX)[2] provides IP connectivity between different operators packet domain networks.

Examples of PDNs are:

- Public Internet
- Operator's private IP network which provides wireless application protocol (WAP) service
- Operator's private IP network which provides multimedia messaging service (MMS) service
- Corporate intranet.

An APN is used to identify the PDN from which to provide the user's IP address. It is also used to select a GGSN from which the PDN is accessible.

Structure of an APN

network id. mnc<MNC>.mcc<MCC>.gprs

Network Identifier Operator Identifier

Access Point Name Structure

An APN consists of two parts[3] as shown in the accompanying figure.

- *Network Identifier*: Defines the external network to which the GGSN is connected. Optionally, it may also include the service requested by the user. This part of the APN is mandatory
- *Operator Identifier*: Defines the specific operator's packet domain network in which the GGSN is located. This part of the APN is optional. The MCC is the Mobile Country Code and the MNC is the Mobile Network Code which together uniquely identify a mobile network operator.

Examples of APN are:

Example: internet.mnc012.mcc345.gprs

Example: internet (NOTE: This APN example does not contain an operator identifier part)

APN Resolution

APN resolution[2] is the process of DNS look up to determine the IP address of the GGSN that provides connectivity to the PDN identified by the APN. When a GPRS mobile phone sets up a data connection (which in technical terms is called setting up a primary PDP context), it provides the APN to which it wants to connect to. APN resolution is then used to select the GGSN and provide an IP address.

BCCS

Server chứa cơ sở dữ liệu cho mọi thuê bao (nghe thấy bảo thế!)

MCU

A **Multipoint Control Unit** (MCU) is a device commonly used to bridge videoconferencing connections.

The Multipoint Control Unit is an endpoint on the LAN that provides the capability for 3 or more terminals and gateways to participate in a multipoint conference. The MCU consists of a mandatory Multipoint Controller (MC) and optional Multipoint Processors (MPs).

3G-324M

3G-324M is the 3GPP umbrella protocol for video telephony in 3G mobile networks.

The 3G-324M protocol operates over an established circuit switched connection between two communicating peers. 3G-324M is an umbrella specification to enable conversational multimedia communication over Circuit Switched (CS) networks and has been adopted by the

3GPP. 3G-324M is based on the ITU-T H.324 specification for multimedia conferencing over Circuit switched networks. 3G-324M is composed of the following sub-protocols:

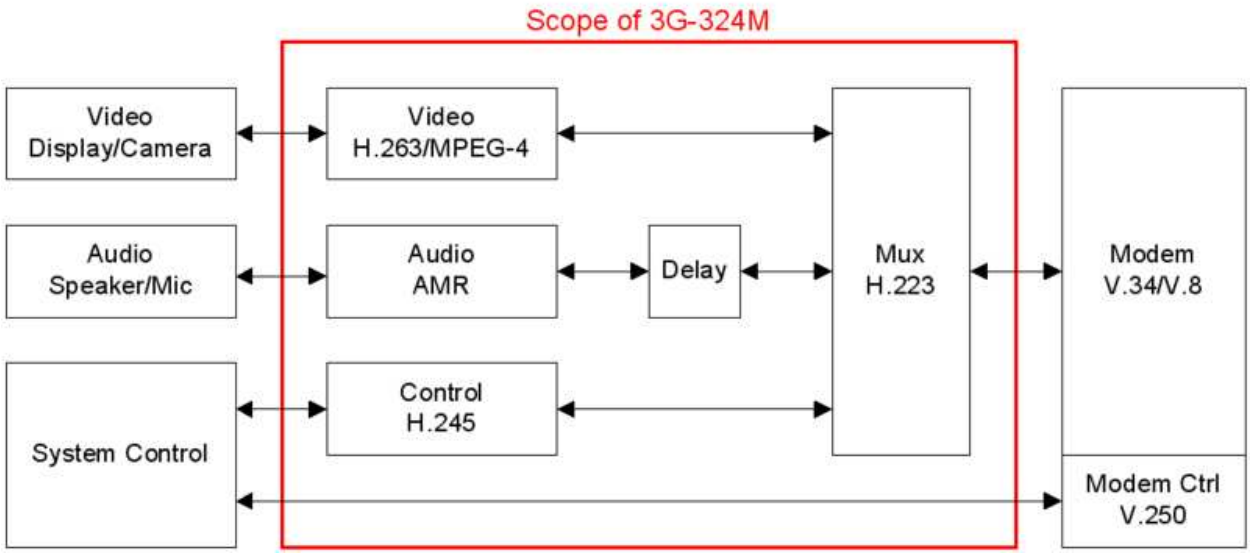
- ITU-T H.245 for call control
- ITU-T H.223 for bit streams to data packets multiplexer/demultiplexer
- ITU-T H.223 Annex A and B for error handling of low and medium BER detection, correction and concealment
- ITU-T H.324 with Annexes A and C for operating in wireless environment

The 3G-324M specification using the Circuit switched network allows delay sensitive conversational multimedia services such as:

- Video Conferencing for personal and business use
- Multimedia entertainment services
- Telemedicine
- Surveillance
- Live Video Broadcasting– Cable TV On-the-Go
- Video-on-demand (movies, news clips)

3G-324M is agnostic to the actual Circuit switched network that uses it. It can run as easily over UMTS as well as TD-SCDMA networks.

3G-324M is a proven solution for conversational multimedia based services that packet-based wireless networks cannot deliver because of inherent overhead, BER sensitivity, and variant routing delays. 3G-324M operating over a circuit switched channel between two communication peers guarantees the fixed-delay quality of service for multimedia communications. Combining Circuit switched 3G-324M services with packet-based SIP services such as presence can leverage the strength of both networks to enable new types of differentiated and innovative mobile 3G services.



Codecs

Audio Codec

- GSM Adaptive Multi-Rate, mandatory
- AMR-WB (G.722.2), optional
- ITU-T G.723.1, optional

Video Codec

- ITU-T H.263, mandatory
- ITU-T H.261, optional
- MPEG-4 part 2 simple profile 1 level 0, optional
- ITU-T H.264, optional

H.324 is an ITU-T recommendation for voice, video and data transmission over regular analog phone lines. It uses a regular 33,600 bit/s modem for transmission, the H.263 codec for video encoding and G.723.1 for audio.

H.324 standard is formally known as *Terminal for low bit-rate multimedia communication*. H.324 covers the technical requirements for very low bit-rate multimedia telephone terminals operating over the General Switched Telephone Network (GSTN). H.324 terminals provide real-time video, audio, or data, or any combination, between two multimedia telephone terminals over a GSTN voice band network connection.

H.324 terminals offering audio communication shall support the G.723.1 audio codec. H.324 terminals offering video communication shall support the H.263 and H.261 video codecs. G.722.1 may be used for wideband audio applications. Annex G of H.324 specification defines usage of ISO/IEC 14496-1 (MPEG-4 Systems) generic capabilities in H.324 terminals. H.324/I terminals shall support interoperation with voice telephones using G.711 speech coding, if the connected network supports transmission and reception of G.711. Other modes such as G.722 audio may optionally be supported as well.[1]

H.324 was adapted by 3GPP to form 3G-324M.

LBS

A **location-based service** (LBS) is an information and entertainment service, accessible with mobile devices through the mobile network and utilizing the ability to make use of the geographical position of the mobile device [1] [2] [3].

LBS services can be used in a variety of contexts, such as health, work, personal life, etc. [4]. LBS services include services to identify a location of a person or object, such as discovering the nearest banking cash machine or the whereabouts of a friend or employee. LBS services include parcel tracking and vehicle tracking services. LBS can include mobile commerce when taking the form of coupons or advertising directed at customers based on their current location. They

include personalized weather services and even location-based games. They are an example of telecommunication convergence.

Locating methods

Control Plane Locating

Sometimes referred to as positioning, with control plane locating the service provider gets the location based on the radio signal delay of the closest cell-phone towers (for phones without GPS features) which can be quite slow as it uses the 'voice control' channel.[3] In the UK, networks do not use trilateration; LBS services use a single base station, with a 'radius' of inaccuracy, to determine a phone's location. This technique was the basis of the E-911 mandate and is still used to locate cellphones as a safety measure. Newer phones and PDAs typically have an integrated A-GPS chip.

In order to provide a successful LBS technology the following factors must be met:

- Coordinates accuracy requirements that are determined by the relevant service;
- Lowest possible cost;
- Minimal impact on network and equipment.

Several categories of methods can be used to find the location of the subscriber.[1][11] The simple and standard solution is GPS-based LBS. Sony Ericsson's "NearMe" is one such example. It is used to maintain knowledge of the exact location, however can be expensive for the end-user, as they would have to invest in a GPS-equipped handset. GPS is based on the concept of trilateration, a basic geometric principle that allows finding one location if one knows its distance from other, already known locations.

GSM Localization

GSM localization is the second option. Finding the location of a mobile device in relation to its cell site is another way to find out the location of an object or a person. It relies on various means of multilateration of the signal from cell sites serving a mobile phone. The geographical position of the device is found out through various techniques like time difference of arrival (TDOA) or Enhanced Observed Time Difference (E-OTD).

Others

Another example is Near LBS (NLBS), in which local-range technologies such as Bluetooth, WLAN, infrared and/or RFID/Near Field Communication technologies are used to match devices to nearby services. This application allows a person to access information based on their surroundings; especially suitable for using inside closed premises, restricted/ regional areas.

Another alternative is an operator- and GPS-independent location service based on access into the deep level telecoms network (SS7). This solution enables accurate and quick determination

of geographical coordinates of mobile phone numbers by providing operator-independent location data and works also for handsets that are not GPS-enabled.

Many other Local Positioning Systems are available, especially for indoor use. GPS and GSM don't work very well indoors, so other techniques are used, including Bluetooth, UWB, RFID and Wi-Fi. But which technique provides the best solution for a specific LBS problem? A general model for this problem has been constructed at the Radboud University of Nijmegen [12].

Further information: Mobile phone tracking

LBS applications

Some examples of location-based services are [1]:

- Requesting the nearest business or service, such as an ATM or restaurant
- Turn by turn navigation to any address
- Locating people on a map displayed on the mobile phone
- Receiving alerts, such as notification of a sale on gas or warning of a traffic jam
- Location-based mobile advertising
- Asset recovery combined with active RF to find, for example, stolen assets in containers where GPS wouldn't work

More examples are listed in [1].

For the carrier, location-based services provide added value by enabling services such as:

- *Resource tracking with dynamic distribution*. Taxis, service people, rental equipment, doctors, fleet scheduling.
- *Resource tracking*. Objects without privacy controls, using passive sensors or RF tags, such as packages and train boxcars.
- *Finding someone or something*. Person by skill (doctor), business directory, navigation, weather, traffic, room schedules, stolen phone, emergency calls.
- *Proximity-based notification (push or pull)*. Targeted advertising, buddy list, common profile matching (dating), automatic airport check-in.
- *Proximity-based actuation (push or pull)*. Payment based upon proximity (EZ pass, toll watch).

In the U.S. the FCC requires that all carriers meet certain criteria for supporting location-based services (FCC 94-102). The mandate requires 95% of handsets to resolve within 300 meters for network-based tracking (e.g. triangulation) and 150 meters for handset-based tracking (e.g. GPS). This can be especially useful when dialling an emergency telephone number - such as enhanced 9-1-1 in North America, or 112 in Europe - so that the operator can dispatch emergency services such as Emergency Medical Services, police or firefighters to the correct location. CDMA and iDEN operators have chosen to use GPS location technology for locating emergency callers. This led to rapidly increasing penetration of GPS in iDEN and CDMA handsets in North America and other parts of the world where CDMA is widely deployed. Even though no such rules are yet in place in Japan or in Europe the number of GPS-enabled

GSM/WCDMA handset models is growing fast. According to the independent wireless analyst firm Berg Insight the attach rate for GPS is growing rapidly in GSM/WCDMA handsets, from less than 8 percent in 2008 to 15 percent in 2009[13].

European operators are mainly using Cell-ID for locating subscribers. This is also a method used in Europe by companies such as Podsystem that are using cell based LBS as part of systems to recover stolen assets. In the US companies such as Rave Wireless in New York are using GPS and triangulation to enable college students to notify campus police when they are in trouble. Rave Wireless and other companies with location based offerings are powered by a variety of companies, including Skyhook Wireless and Xtify.

Mobile messaging

Mobile messaging plays an essential role in LBS. Messaging, especially SMS, has been used in combination with various LBS applications, such as location-based mobile advertising. SMS is still the main technology carrying mobile advertising / marketing campaigns to mobile phones. A classic example of LBS applications using SMS is the delivery of mobile coupons or discounts to mobile subscribers who are near to advertising restaurants, cafes, movie theatres. The Singaporean mobile operator MobileOne carried out such an initiative in 2007 that involved many local marketers, what was reported to be a huge success in terms of subscriber acceptance.

Companies offering location-based messaging (sometimes referred to as 'geo-messaging') include The Coupons App [1](US), Centrl [2](International), Zhiing (international), BluePont (US)[14], Loopt (US), Dodgeball (US) and GeoMe [3](Spain).

NFS

Network File System (**NFS**) is a network file system protocol originally developed by Sun Microsystems in 1984,[1] allowing a user on a client computer to access files over a network in a manner similar to how local storage is accessed. NFS, like many other protocols, builds on the Open Network Computing Remote Procedure Call (ONC RPC) system. The Network File System is an open standard defined in RFCs, allowing anyone to implement the protocol. NFS is often used with Unix operating systems such as Solaris, AIX, HP-UX, FreeBSD and Unix-like operating systems (such as Linux). It is also available to operating systems such as the classic Mac OS, OpenVMS, Microsoft Windows, Novell NetWare, and IBM AS/400

Network switching subsystem

Network switching subsystem (**NSS**) (or **GSM core network**) is the component of a GSM system that carries out call switching and mobility management functions for mobile phones roaming on the network of base stations. It is owned and deployed by mobile phone operators and allows mobile devices to communicate with each other and telephones in the wider Public Switched Telephone Network or (PSTN). The architecture contains specific features and functions which are needed because the phones are not fixed in one location.

The NSS originally consisted of the circuit-switched core network, used for traditional GSM services such as voice calls, SMS, and circuit switched data calls. It was extended with an overlay architecture to provide packet-switched data services known as the GPRS core network. This allows mobile phones to have access to services such as WAP, MMS, and the Internet.

All mobile phones manufactured today have both circuit and packet based services, so most operators have a GPRS network in addition to the standard GSM core network.

Mobile switching center (MSC)

Description

The **mobile switching center** (MSC) is the primary service delivery node for GSM/CDMA, responsible for routing voice calls and SMS as well as other services (such as conference calls, FAX and circuit switched data).

The MSC sets up and releases the end-to-end connection, handles mobility and hand-over requirements during the call and takes care of charging and real time pre-paid account monitoring.

In the GSM mobile phone system, in contrast with earlier analogue services, fax and data information is sent directly digitally encoded to the MSC. Only at the MSC is this re-coded into an "analogue" signal (although actually this will almost certainly mean sound encoded digitally as PCM signal in a 64-kbit/s timeslot, known as a DS0 in America).

There are various different names for MSCs in different contexts which reflects their complex role in the network, all of these terms though could refer to the same MSC, but doing different things at different times.

The **gateway MSC** (G-MSC) is the MSC that determines which visited MSC the subscriber who is being called is currently located. It also interfaces with the PSTN. All mobile to mobile calls and PSTN to mobile calls are routed through a G-MSC. The term is only valid in the context of one call since any MSC may provide both the gateway function and the Visited MSC function, however, some manufacturers design dedicated high capacity MSCs which do not have any BSSs connected to them. These MSCs will then be the Gateway MSC for many of the calls they handle.

The **visited MSC** (V-MSC) is the MSC where a customer is currently located. The VLR associated with this MSC will have the subscriber's data in it.

The **anchor MSC** is the MSC from which a handover has been initiated. The **target MSC** is the MSC toward which a Handover should take place. A mobile switching centre server is a part of the redesigned MSC concept starting from 3GPP Release 4.

Mobile switching centre server (MSCS)

Main article: Mobile switching centre server

The **mobile switching centre server** is a soft-switch variant of the mobile switching centre, which provides circuit-switched calling, mobility management, and GSM services to the mobile phones roaming within the area that it serves. MSS functionality enables split between control (signalling) and user plane (bearer in network element called as media gateway/MG), which guarantees more optimal placement of network elements within the network.

MSS and MGW media gateway makes it possible to cross-connect circuit switched calls switched by using IP, ATM AAL2 as well as TDM. More information is available in 3GPP TS 23.205.

Other GSM core network elements connected to the MSC

The MSC connects to the following elements:

- The home location register (HLR) for obtaining data about the SIM and mobile services ISDN number (MSISDN; i.e., the telephone number).
- The base station subsystem which handles the radio communication with 2G and 2.5G mobile phones.
- The UMTS terrestrial radio access network (UTRAN) which handles the radio communication with 3G mobile phones.
- The visitor location register (VLR) for determining where other mobile subscribers are located.
- Other MSCs for procedures such as handover.

Procedures implemented

Tasks of the MSC include:

- Delivering calls to subscribers as they arrive based on information from the VLR.
- Connecting outgoing calls to other mobile subscribers or the PSTN.
- Delivering SMSs from subscribers to the short message service centre (SMSC) and vice versa.
- Arranging handovers from BSC to BSC.
- Carrying out handovers from this MSC to another.
- Supporting supplementary services such as conference calls or call hold.
- Generating billing information.

Home location register (HLR)

The **home location register** (HLR) is a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network. There can be several logical, and physical, HLRs per public land mobile network (PLMN), though one international mobile subscriber identity (IMSI)/MSISDN pair can be associated with only one logical HLR (which can span several physical nodes) at a time.

The HLRs store details of every SIM card issued by the mobile phone operator. Each SIM has a unique identifier called an IMSI which is the primary key to each HLR record.

The next important items of data associated with the SIM are the MSISDNs, which are the telephone numbers used by mobile phones to make and receive calls. The primary MSISDN is the number used for making and receiving voice calls and SMS, but it is possible for a SIM to have other secondary MSISDNs associated with it for fax and data calls. Each MSISDN is also a primary key to the HLR record. The HLR data is stored for as long as a subscriber remains with the mobile phone operator.

Examples of other data stored in the HLR against an IMSI record is:

- GSM services that the subscriber has requested or been given.
- GPRS settings to allow the subscriber to access packet services.
- Current location of subscriber (VLR and serving GPRS support node/SGSN).
- Call divert settings applicable for each associated MSISDN.

The HLR is a system which directly receives and processes MAP transactions and messages from elements in the GSM network, for example, the location update messages received as mobile phones roam around.

Other GSM core network elements connected to the HLR

The HLR connects to the following elements:

- The G-MSC for handling incoming calls
- The VLR for handling requests from mobile phones to attach to the network
- The SMSC for handling incoming SMS
- The voice mail system for delivering notifications to the mobile phone that a message is waiting
- The AUC for authentication and ciphering and exchange of data (triplets)

Procedures implemented

The main function of the HLR is to manage the fact that SIMs and phones move around a lot. The following procedures are implemented to deal with this:

- Manage the mobility of subscribers by means of updating their position in administrative areas called 'location areas', which are identified with a LAC. The action of a user of moving from one LA to another is followed by the HLR with a Location area update procedure.
- Send the subscriber data to a VLR or SGSN when a subscriber first roams there.
- Broker between the G-MSC or SMSC and the subscriber's current VLR in order to allow incoming calls or text messages to be delivered.
- Remove subscriber data from the previous VLR when a subscriber has roamed away from it.

Authentication centre (AUC)

Description

The **authentication centre** (AUC) is a function to authenticate each SIM card that attempts to connect to the GSM core network (typically when the phone is powered on). Once the authentication is successful, the HLR is allowed to manage the SIM and services described above. An encryption key is also generated that is subsequently used to encrypt all wireless communications (voice, SMS, etc.) between the mobile phone and the GSM core network.

If the authentication fails, then no services are possible from that particular combination of SIM card and mobile phone operator attempted. There is an additional form of identification check performed on the serial number of the mobile phone described in the EIR section below, but this is not relevant to the AUC processing.

Proper implementation of security in and around the AUC is a key part of an operator's strategy to avoid SIM cloning.

The AUC does not engage directly in the authentication process, but instead generates data known as *triplets* for the MSC to use during the procedure. The security of the process depends upon a shared secret between the AUC and the SIM called the K_i. The K_i is securely burned into the SIM during manufacture and is also securely replicated onto the AUC. This K_i is never transmitted between the AUC and SIM, but is combined with the IMSI to produce a challenge/response for identification purposes and an encryption key called K_c for use in over the air communications.

Other GSM core network elements connected to the AUC

The AUC connects to the following elements:

- the MSC which requests a new batch of triplet data for an IMSI after the previous data have been used. This ensures that same keys and challenge responses are not used twice for a particular mobile.

Procedures implemented

The AUC stores the following data for each IMSI:

- the K_i
- Algorithm id. (the standard algorithms are called A3 or A8, but an operator may choose a proprietary one).

When the MSC asks the AUC for a new set of triplets for a particular IMSI, the AUC first generates a random number known as *RAND*. This *RAND* is then combined with the K_i to produce two numbers as follows:

- The K_i and *RAND* are fed into the A3 algorithm and the signed response (SRES) is calculated.
- The K_i and *RAND* are fed into the A8 algorithm and a session key called K_c is calculated.

The numbers (*RAND*, SRES, K_c) form the triplet sent back to the MSC. When a particular IMSI requests access to the GSM core network, the MSC sends the *RAND* part of the triplet to the SIM. The SIM then feeds this number and the K_i (which is burned onto the SIM) into the A3 algorithm as appropriate and an SRES is calculated and sent back to the MSC. If this SRES matches with the SRES in the triplet (which it should if it is a valid SIM), then the mobile is allowed to attach and proceed with GSM services.

After successful authentication, the MSC sends the encryption key K_c to the base station controller (BSC) so that all communications can be encrypted and decrypted. Of course, the mobile phone can generate the K_c itself by feeding the same RAND supplied during authentication and the K_i into the A8 algorithm.

The AUC is usually collocated with the HLR, although this is not necessary. Whilst the procedure is secure for most everyday use, it is by no means crack proof. Therefore a new set of security methods was designed for 3G phones.

Visitor location register (VLR)

Description

The **visitor location register** is a temporary database of the subscribers who have roamed into the particular area which it serves. Each base station in the network is served by exactly one VLR, hence a subscriber cannot be present in more than one VLR at a time.

The data stored in the VLR has either been received from the HLR, or collected from the MS. In practice, for performance reasons, most vendors integrate the VLR directly to the V-MSC and, where this is not done, the VLR is very tightly linked with the MSC via a proprietary interface.

Data stored include:

- IMSI (the subscriber's identity number).
- Authentication data.
- MSISDN (the subscriber's phone number).
- GSM services that the subscriber is allowed to access.
- access point (GPRS) subscribed.
- The HLR address of the subscriber.

Other GSM core network elements connected to the VLR

The VLR connects to the following elements:

- The V-MSC to pass needed data for its procedures; e.g., authentication or call setup.
- The HLR to request data for mobile phones attached to its serving area.
- Other VLRs to transfer temporary data concerning the mobile when they roam into new VLR areas. For example, the temporal mobile subscriber identity (TMSI).

Procedures implemented

The primary functions of the VLR are:

- To inform the HLR that a subscriber has arrived in the particular area covered by the VLR.
- To track where the subscriber is within the VLR area (location area) when no call is ongoing.
- To allow or disallow which services the subscriber may use.
- To allocate roaming numbers during the processing of incoming calls.
- To purge the subscriber record if a subscriber becomes inactive whilst in the area of a VLR. The VLR deletes the subscriber's data after a fixed time period of inactivity and informs the HLR (e.g., when the phone has been switched off and left off or when the subscriber has moved to an area with no coverage for a long time).
- To delete the subscriber record when a subscriber explicitly moves to another, as instructed by the HLR.

Equipment identity register (EIR)

The **equipment identity register** is often integrated to the HLR. The EIR keeps a list of mobile phones (identified by their IMEI) which are to be banned from the network or monitored. This is designed to allow tracking of stolen mobile phones. In theory all data about all stolen mobile phones should be distributed to all EIRs in the world through a Central EIR. It is clear, however, that there are some countries where this is not in operation. The EIR data does not have to change in real time, which means that this function can be less distributed than the function of the HLR. The EIR is a database that contains information about the identity of the mobile equipment that prevents calls from stolen, unauthorized or defective mobile stations. Some EIR also have the capability to log Handset attempts and store it in a log file.

Other support functions

Connected more or less directly to the GSM core network are many other functions.

Billing centre (BC)

The **billing centre** is responsible for processing the toll tickets generated by the VLRs and HLRs and generating a bill for each subscriber. It is also responsible for generating billing data of roaming subscriber.

Short message service centre (SMSC)

The **short message service centre** supports the sending and reception of **text messages**.

Multimedia messaging service centre (MMSC)

The **multimedia messaging service centre** supports the sending of multimedia messages (e.g., images, audio, video and their combinations) to (or from) MMS-enabled Handsets.

Voicemail system (VMS)

The **voicemail system** records and stores voicemails.

Lawful interception functions

According to U.S. law, which has also been copied into many other countries, especially in Europe, all telecommunications equipment must provide facilities for monitoring the calls of selected users. There must be some level of support for this built into any of the different elements. The concept of *lawful interception* is also known, following the relevant U.S. law, as CALEA. Generally Lawful Interception implementation is similar to the implementation of conference call. While A and B is talking with each other, C can join the call and listens silently.

Báo hiệu (viễn thông)

Trong viễn thông, **báo hiệu** là quá trình trao đổi thông tin về để thiết lập và điều khiển một kết nối hoặc để quản lí mạng.

Người ta phân loại hệ thống báo hiệu dựa trên một số đặc điểm như sau:

Báo hiệu trong băng và báo hiệu ngoài băng

Trong mạng chuyển mạch công cộng (PSTN), **báo hiệu trong băng** là tín hiệu có tần số trong khoảng 0,3 --> 3,4 Khz, nếu nằm ngoài khoảng trên được gọi là báo hiệu ngoài băng.

Báo hiệu kênh riêng (CAS) và báo hiệu kênh chung (CCS)

Báo hiệu kênh riêng: dùng một kênh báo hiệu riêng cho từng kênh thoại.

Báo hiệu kênh chung như tên gọi, dùng một kênh chung để truyền thông tin điều khiển liên quan đến nhiều cuộc gọi. Những kênh thoại này do đó sẽ có một kênh báo hiệu chung.

Báo hiệu Compelled

Báo hiệu compelled là báo hiệu trong đó bản tin phải được xác nhận trước khi gửi bản tin mới. Hầu hết các dạng của báo hiệu R2 là báo hiệu compelled, báo hiệu R1 đa tần thì ngược lại.

Báo hiệu kênh người dùng và báo hiệu trung kế

Báo hiệu thuê bao là giữa thuê bao và tổng đài điện thoại. **Báo hiệu trung kế** là giữa các tổng đài với nhau.

Ví dụ

Một hệ thống báo hiệu có thể là nhiều trong các loại báo hiệu trên đây tùy theo cách phân loại. Sau đây là vài ví dụ:

Lưỡng âm đa tần (DTMF) là báo hiệu trong băng, kênh riêng, không compelled.

Báo hiệu số 7 (SS7) là báo hiệu ngoài băng, kênh chung, bao gồm cả báo hiệu đường dây và báo hiệu địa chỉ.

Báo hiệu bằng xung (tùy thuộc vào từng quốc gia, có thể là 50Hz, 12kHz, 16kHz) là báo hiệu ngoài băng và kênh chung, còn được xem là báo hiệu đường dây. Báo hiệu E&M là báo hiệu ngoài băng, kênh riêng, thường được dùng chung với báo hiệu địa chỉ DTMF.

Báo hiệu L1 (thường dùng tone 2280Hz với các độ dài khác nhau) là báo hiệu trong băng, kênh riêng. Ví dụ như SF 2600 Hz trong Bell System.

Loop start, Ground start, Reverse Battery và Revertive Pulse là những tín hiệu một chiều, cho nên là báo hiệu ngoài băng, kênh riêng.

Mặc dù báo hiệu kênh chung được xem là báo hiệu ngoài băng và báo hiệu trong băng là báo hiệu kênh riêng, nhưng báo hiệu bằng xung ở trên là báo hiệu kênh riêng mà là báo hiệu ngoài băng.

The DTMF keypad is laid out in a 4×4 matrix, with each row representing a *low* frequency, and each column representing a *high* frequency. Pressing a single key (such as '1') will send a sinusoidal tone for each of the two frequencies (697 and 1209 hertz (Hz)). The original keypads had levers inside, so each button activated two contacts. The multiple tones are the reason for calling the system multifrequency. These tones are then decoded by the switching center to determine which key was pressed.

DTMF keypad frequencies (with sound clips)

	1209 Hz	**1336 Hz**	**1477 Hz**	**1633 Hz**
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Special tone frequencies

National telephone systems define additional tones to indicate the status of lines, equipment, or the result of calls with special tones. Such tones are standardized in each country and may consist of single or multiple frequencies. Most European countries use a single frequency, where the United States uses a dual frequency system, presented in the following table.

Event	Low frequency	High frequency
Busy signal	480 Hz	620 Hz
Ringback tone (US)	440 Hz	480 Hz
Dial tone	350 Hz	440 Hz

The tone frequencies, as defined by the Precise Tone Plan, are selected such that harmonics and intermodulation products will not cause an unreliable signal. No frequency is a multiple of another, the difference between any two frequencies does not equal any of the frequencies, and the sum of any two frequencies does not equal any of the frequencies. The frequencies were initially designed with a ratio of 21/19, which is slightly less than a whole tone. The frequencies may not vary more than ±1.8% from their nominal frequency, or the switching center will ignore the signal. The high frequencies may be the same volume or louder as the low frequencies when sent across the line. The loudness difference between the high and low frequencies can be as large as 3 decibels (dB) and is referred to as "twist." The minimum duration of the tone should be at least 70 ms, although in some countries and applications DTMF receivers must be able to reliably detect DTMF tones as short as 45ms.

WAP

Wireless Application Protocol (WAP) is an open international standard[1] for application-layer network communications in a wireless-communication environment. Most use of WAP involves accessing the mobile web from a mobile phone or from a PDA.

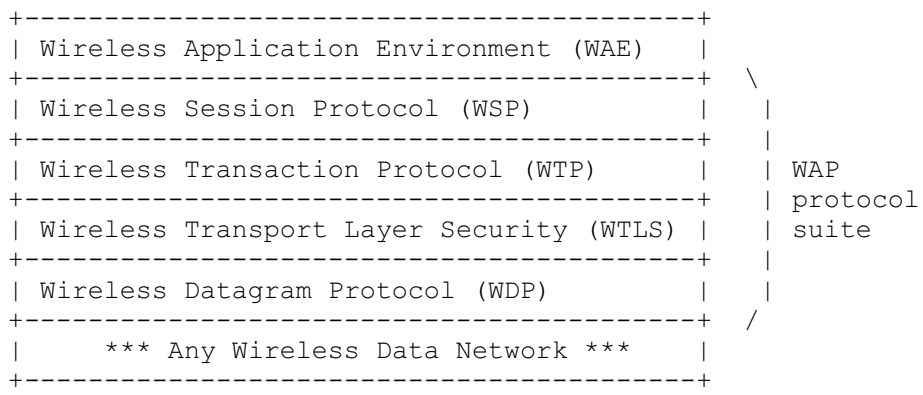
A WAP browser provides all of the basic services of a computer-based web browser but simplified to operate within the restrictions of a mobile phone, such as its smaller view screen. Users can connect to **WAP sites**: websites written in, or dynamically converted to, WML (Wireless Markup Language) and accessed via the WAP browser.

Before the introduction of WAP, service providers had extremely limited opportunities to offer interactive data services, but needed interactivity to support now-commonplace activities such as:

- Email by mobile phone
- Tracking of stock-market prices
- Sports results
- News headlines
- Music downloads

Technical specifications

- The WAP standard describes a protocol suite allowing the interoperability of WAP equipment and software with many different network technologies, thus allowing the building of a single platform for competing network technologies such as GSM and IS-95 (also known as CDMA) networks.



- The bottom-most protocol in the suite, the WAP Datagram Protocol (WDP), functions as an adaptation layer that makes every data network look a bit like UDP to the upper layers by providing unreliable transport of data with two 16-bit port numbers (origin and destination). All the upper layers view WDP as one and the same protocol, which has several "technical realizations" on top of other "data bearers" such as SMS, USSD, etc. On native IP bearers such as GPRS, UMTS packet-radio service, or PPP on top of a circuit-switched data connection, WDP is in fact exactly UDP.

- WTLS, an optional layer, provides a public-key cryptography-based security mechanism similar to TLS.

- WTP provides transaction support (reliable request/response) adapted to the wireless world. WTP supports more effectively than TCP the problem of packet loss, which occurs commonly in 2G wireless technologies in most radio conditions, but is misinterpreted by TCP as network congestion.

- Finally, one can think of WSP initially as a compressed version of HTTP.

This protocol suite allows a terminal to transmit requests that have an HTTP or HTTPS equivalent to a WAP gateway; the gateway translates requests into plain HTTP.

Wireless Application Environment (WAE)

The WAE space defines application-specific markup languages.

For WAP version 1.X, the primary language of the WAE is WML. In WAP 2.0, the primary markup language is XHTML Mobile Profile.

History

The WAP Forum dates from 1997. It aimed primarily to bring together the various wireless technologies in a standardised protocol.[2]

In 2002 the WAP Forum was consolidated[*by whom?*] (along with many other forums of the industry) into OMA (Open Mobile Alliance)[3], which covers virtually everything in future development[*citation needed*] of wireless data services.

WAP 1.X

The WAP 1.0 standard, released in April 1998, described a complete software stack for mobile internet access.[4].

WAP version 1.1 came out in 1999.[5]. WAP 1.2, the final update of the 1.X series was released in June 2000.[6]. The most important addition in version 1.2 was WAP push.[7]

WAP Push

WAP Push has been incorporated into the specification to allow WAP content to be pushed to the mobile handset with minimum user intervention. A WAP Push is basically a specially encoded message which includes a link to a WAP address.[8]

WAP Push is specified on top of WDP; as such, it can be delivered over any WDP-supported bearer, such as GPRS or SMS.[9] Most GSM networks have a wide range of modified processors, but GPRS activation from the network is not generally supported, so WAP Push messages have to be delivered on top of the SMS bearer.

On receiving a WAP Push, a WAP 1.2 or later enabled handset will automatically give the user the option to access the WAP content. This is also known as WAP Push SI (Service Indication).[9]

The network entity that processes WAP Pushes and delivers them over an IP or SMS Bearer is known as a Push Proxy Gateway (PPG).[9]

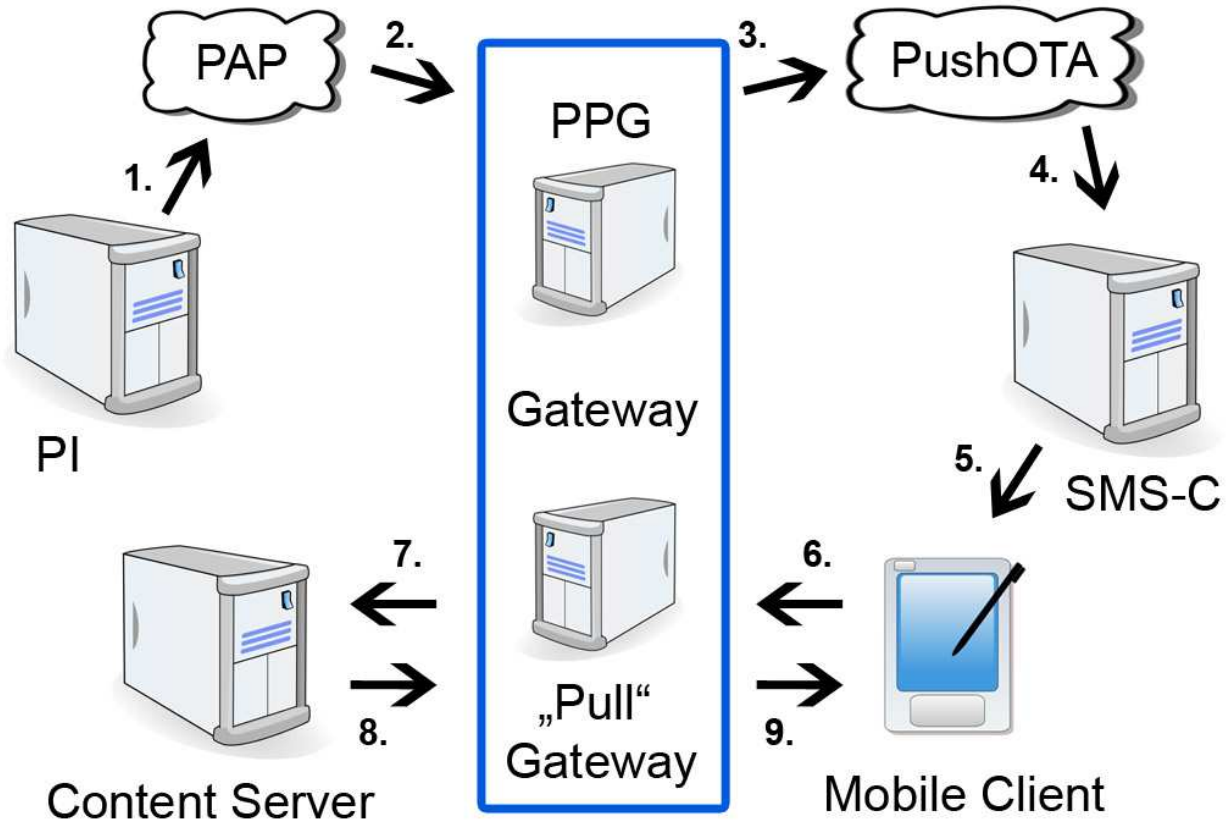
WAP 2.0

WAP 2.0[1], released in 2002, a re-engineered WAP, uses a cut-down version of XHTML with end-to-end HTTP (i.e., dropping the gateway and custom protocol suite used to communicate with it). A WAP gateway can be used in conjunction with WAP 2.0; however, in this scenario, it is used as a standard proxy server. The WAP gateway's role would then shift from one of translation to adding additional information to each request. This would be configured by the operator and could include telephone numbers, location, billing information, and handset information.

Mobile devices process XHTML Mobile Profile (XHTML MP), the markup language defined in WAP 2.0. It is a subset of XHTML and a superset of XHTML Basic. A version of cascading style sheets (CSS) called WAP CSS is supported by XHTML MP.

PPG

A **Push Proxy Gateway** is a component of WAP Gateways that pushes URL notifications to mobile handsets. Notifications typically include MMS, email, IM, ringtone downloads, and new device firmware notifications. Most notifications will have an audible alert to the user on the device. The notification will typically be a text string with a URL link. Note that only a notification is pushed to the device; the device must do something with the notification in order to download or view the content associated with it.

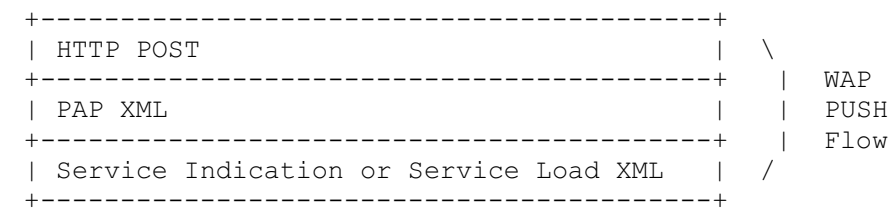


WAP Push Process

Technical specifications

PUSH to PPG

A push message is sent as an HTTP POST to the Push Proxy Gateway. The POST will be a multipart XML document, with the first part being the PAP (Push Access Protocol) Section and the second part being either a Service Indication or a Service Load.



POST

The POST contains at a minimum the URL being posted to (this is not standard across different PPG vendors), and the content type.

An example of a PPG POST:

```
 POST /somelocation HTTP/1.1
 Host: ppg.somecarrier.com
 Content-Type:          multipart/related;          boundary=someboundarymesg;
type="application/xml"
```

PAP

The PAP XML contains at the minimum, a <pap> element, a <push-message> element, and an <address> element.

An example of a PAP XML:

```
 --someboundarymesg
 Content-Type: application/xml

 <?xml version="1.0"?>
 <!DOCTYPE      pap      PUBLIC      "-//WAPFORUM//DTD      PAP      1.0//EN"
"http://www.wapforum.org/DTD/pap_1.0.dtd">
 <pap>
 <push-message push-id="some_push_id">
 <address   address-value="WAPPUSH=+12065551212/TYPE=PLMN@ppg.somecarrier.com"
/>
 </push-message>
 </pap>
```

The important parts of this PAP message are the address value and type. The value is typically a MSISDN and type indicates whether to send to an MSISDN (typical case) or to an IP Address. The TYPE is almost always MSISDN as the Push Initiator (PI) will not typically have the Mobile Station's IP address - which is generally dynamic. In the case of IP Address:

```
 TYPE=USER@a.b.c.d
```

Additional capability of PAP can be found in the PAP article.

Service Indication

A PUSH Service Indication (SI) contains at a minimum an <si> element and a <indication> element.

An example of a Service Indication:

```
--someboundarymesg
Content-Type: text/vnd.wap.si

<?xml version="1.0"?>
<!DOCTYPE si PUBLIC "-//WAPFORUM//DTD SI 1.0//EN"
"http://www.wapforum.org/DTD/si.dtd">
<si>
<indication si-id=345532 href="http://mmsc.somecarrier.com/CFJIOJF43F">
A new MMS has been received, download?
</indication>
</si>
```

Short code

Short codes (also known as **short numbers**) are special telephone numbers, significantly shorter than full telephone numbers, that can be used to address SMS and MMS messages from mobile phones or fixed phones. There are two types of short codes: dialing and messaging.

Short codes are designed to be easier to read and remember than normal telephone numbers. Like telephone numbers, short codes are unique to each operator at the technological level. Even so, providers generally have agreements to avoid overlaps. In some countries, such as the United States, some classes of numbers are inter-operator (U.S. inter-operator numbers are called **Common Short Codes**).

Short codes are widely used for value-added services such as television voting, ordering ringtones, charity donations and mobile services. Messages sent to short code can be billed at a higher rate than a standard SMS and may even subscribe a customer to a reoccurring monthly service that will be added to their mobile phone bill until they text e.g. the word "STOP" to terminate the service.

Technology

Normal telephone numbers (following the E.164 standard) may be of any length, and so when dialed from landline telephones, the network must apply heuristics to determine when dialing is complete — in the US, for example, dialed numbers are generally seven or ten digits long, with an optional prefix of "1" (the country code for the US and Canada). On mobile phones, numbers are terminated with the "Send" or "Call" key and sent all at once over the network, so the

network knows the end of the dialed number, and thus one can use short numbers without clashing with longer numbers.

For instance, on a land-line phone, one could not use the short code 12345, since then one could not dial the phone number 1-234-555-4626 begin_of_the_skype_highlighting 1-234-555-4626 end_of_the_skype_highlighting (or any other number that shared the prefix 12345), but on a mobile phone there is no such ambiguity.

Short codes and service identifiers (prefix)

Short codes are often associated with automated services. An automated program can handle the response and typically requires the sender to start the message with a command word or prefix. The service then responds to the command appropriately.

In ads or in other printed material where a provider has to inform about both the prefix and the short code number, the advertisement will typically follow this format:

Example 1 - Long version: Text Football to 72404 for latest football news. Example 2 - Short version: football@72404

IIS

Internet Information Services (**IIS**) – formerly called **Internet Information Server** – is a web server application and set of feature extension modules created by Microsoft for use with Microsoft Windows. It is the world's second most popular web server in terms of overall websites behind the industry leader Apache HTTP Server. As of March 2010, it served 24.47% of all websites on the Internet according to Netcraft.[1] The protocols supported in IIS 7 include: FTP, FTPS, SMTP, NNTP, and HTTP/HTTPS.

IIS features

IIS 7 is built on a modular architecture. Modules, also called extensions, can be added or removed individually so that only modules required for specific functionality have to be installed. IIS 7 includes native modules as part of the full installation. These modules are individual features that the server uses to process requests and include the following:

- HTTP modules – Used to perform tasks specific to HTTP in the request-processing pipeline, such as responding to information and inquiries sent in client headers, returning HTTP errors, and redirecting requests.

- Security modules – Used to perform tasks related to security in the request-processing pipeline, such as specifying authentication schemes, performing URL authorization, and filtering requests.

- Content modules – Used to perform tasks related to content in the request-processing pipeline, such as processing requests for static files, returning a default page when a client does not specify a resource in a request, and listing the contents of a directory.

- Compression modules – Used to perform tasks related to compression in the request-processing pipeline, such as compressing responses, applying Gzip compression transfer coding to responses, and performing pre-compression of static content.

- Caching modules – Used to perform tasks related to caching in the request-processing pipeline, such as storing processed information in memory on the server and using cached content in subsequent requests for the same resource.

- Logging and Diagnostics modules – Used to perform tasks related to logging and diagnostics in the request-processing pipeline, such as passing information and processing status to HTTP.sys for logging, reporting events, and tracking requests currently executing in worker processes.

IIS 5.0 and higher support the following authentication mechanisms:

- Basic access authentication
- Digest access authentication
- Integrated Windows Authentication
- .NET Passport Authentication (not supported in Windows Server 2008 and above)

IIS 7.5 includes the following additional security features:

- Client Certificate Mapping
- IP Security
- Request Filtering
- URL Authorization

Authentication changed slightly between IIS 6.0 and IIS 7, most notably in that the anonymous user which was named "IUSR_{machinename}" is a built-in account in Vista and future operating systems and named "IUSR". Notably, in IIS 7, each authentication mechanism is isolated into its own module and can be installed or uninstalled.

IIS extensions

IIS releases new feature modules between major version releases to add new functionality. The following extensions are available for IIS 7:

- **FTP Publishing Service** – Lets Web content creators publish content securely to IIS 7 Web servers with SSL-based authentication and data transfer.

- **Administration Pack** – Adds administration UI support for management features in IIS 7, including ASP.NET authorization, custom errors, FastCGI configuration, and request filtering.

- **Application Request Routing** – Provides a proxy-based routing module that forwards HTTP requests to content servers based on HTTP headers, server variables, and load balance algorithms.

- **Database Manager** – Allows easy management of local and remote databases from within IIS Manager.

- **Media Services** – Integrates a media delivery platform with IIS to manage and administer delivery of rich media and other Web content.

- **URL Rewrite Module** – Provides a rule-based rewriting mechanism for changing request URLs before they are processed by the Web server.

- **WebDAV** – Lets Web authors publish content securely to IIS 7 Web servers, and lets Web administrators and hosters manage WebDAV settings using IIS 7 management and configuration tools.

- **Web Deployment Tool** – Synchronizes IIS 6.0 and IIS 7 servers, migrates an IIS 6.0 server to IIS 7, and deploys Web applications to an IIS 7 server.

MSRN

MSRN - Mobile Station Roaming Number

The Mobile Station Roaming Number is an E.164 defined telephone number used to route telephone calls in a mobile network from a GMSC (Gateway Mobile Switching Centre) to the target MSC (see Network Switching Subsystem). It can also be defined as a directory number temporarily assigned to a mobile for a mobile terminated call. A MSRN is assigned for every mobile terminated call, not only the calls where the terminating MS lives on a different MSC than the originating MS. Although this seems unnecessary since many vendors' VLR's are integrated with the MSC, the GSM specification indicates that the MSC and VLR (Visitor Location Register) do not need to reside on the same switch. They are considered two different nodes as they have their own routing addresses. i.e.the MSRN is one of the returned parameters into SRI_ACK message. In particular the MSRN is used into an MNP scenario (in this case it can be modified as 'RgN + MSISDN').

Another temporary address that hides the identity of a subscriber. The VLR generates this address on request from the MSC,and the address is also stored in the HLR. MSRN contains the current visitor country code(VCC),the visitor national destination code(VNDC),the identification of the current MSC together with the suscriber number. If we have all the MSC working as a GMSC like the latest technologies so what would be the states of the MSRN ? we can use it only for test to route the calls to a specific MSC otherwise we don't need it to use it.

Diameter (protocol)

Internet Protocol Suite

Application Layer

BGP · DHCP · DNS · FTP · HTTP · IMAP · IRC · LDAP · MGCP · NNTP · NTP · POP · RIP · RPC · RTP · SIP · SMTP · SNMP · SSH · Telnet · TLS/SSL · XMPP ·

(more)

Transport Layer

TCP · UDP · DCCP · SCTP · RSVP · ECN ·

(more)

Internet Layer

IP (IPv4, IPv6) · ICMP · ICMPv6 · IGMP · IPsec ·

(more)

Link Layer

ARP/InARP · NDP · OSPF · Tunnels (L2TP) · PPP · Media Access Control (Ethernet, DSL, ISDN, FDDI) ·

(more)

Diameter is a AAA protocol, a type of computer networking protocol for authentication, authorization and accounting, and is a successor to RADIUS. Diameter controls communication between the authenticator (Secure Ticket Authority, STA) and any network entity requesting authentication.

Diameter Applications extend the base protocol by adding new commands and/or attributes, such as those for use of the Extensible Authentication Protocol (EAP).

Comparison with RADIUS

The name is a pun on the RADIUS protocol, which is the predecessor (a diameter is twice the radius). Diameter is not directly backwards compatible, but provides an upgrade path for RADIUS. The main differences are as follows:

- Reliable transport protocols (TCP or SCTP, not UDP)
- Network or transport layer security (IPsec or TLS)
- Transition support for RADIUS, although Diameter is not fully compatible with RADIUS
- Larger address space for attribute-value pairs (AVPs) and identifiers (32 bits instead of 8 bits)
- Client–server protocol, with exception of supporting some server-initiated messages as well
- Both stateful and stateless models can be used
- Dynamic discovery of peers (using DNS SRV and NAPTR)
- Capability negotiation
- Supports application layer acknowledgements, defines failover methods and state machines (RFC 3539)
- Error notification
- Better roaming support
- More easily extended; new commands and attributes can be defined
- Aligned on 32-bit boundaries
- Basic support for user-sessions and accounting

Applications

A *Diameter Application* is not a software application, but a protocol based on the Diameter base protocol (defined in RFC 3588). Each application is defined by an application identifier and can add new command codes and/or new mandatory AVPs. Adding a new optional AVP does not require a new application.

Examples of Diameter applications :

- Diameter Mobile IPv4 Application (MobileIP, RFC 4004)
- Diameter Network Access Server Application (NASREQ, RFC 4005)
- Diameter Extensible Authentication Protocol Application (RFC 4072)
- Diameter Credit-Control Application (DCCA, RFC 4006)
- Diameter Session Initiation Protocol Application (RFC 4740)
- Various applications in the 3GPP IP Multimedia Subsystem

  Both the HSS and the SLF communicate using the Diameter protocol.

Protocol description

The Diameter base protocol is defined by RFC 3588, and defines the minimum requirements for an AAA protocol. *Diameter Applications* can extend the base protocol, by adding new commands and/or attributes. Diameter security is provided by IPSEC or TLS, both well-regarded protocols. The IANA has assigned TCP and SCTP port number 3868 to Diameter.

Packet format

The packet comprises of a Diameter header and a variable number of Attribute-Value Pairs, or AVPs, for encapsulating information relevant to the Diameter message.

Diameter Header

Bit offset	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
0	version message length
32	R P E T command code
64	application ID
96	hop-by-hop ID
128	end-to-end ID
160	AVPs
...	...

Commands

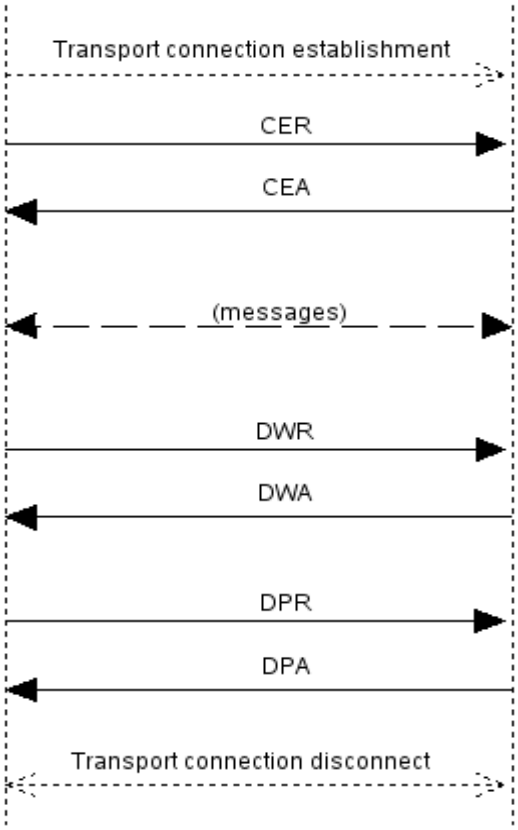
Each command is assigned a command code, which is used for both Requests and Answers.

Command-Name	**Abbr.**	**Code**
AA-Answer	AAA	265
AA-Request	AAR	265
Abort-Session-Answer	ASA	274
Abort-Session-Request	ASR	274
Accounting-Answer	ACA	271
Accounting-Request	ACR	271
Bootstrapping-Info-Answer	BIA	310
Bootstrapping-Info-Request	BIR	310
Capabilities-Exchange-Answer	CEA	257

Capabilities-Exchange-Request	CER	257
Credit-Control-Answer	CCA	272
Credit-Control-Request	CCR	272
Device-Watchdog-Answer	DWA	280
Device-Watchdog-Request	DWR	280
Diameter-EAP-Answer	DEA	268
Diameter-EAP-Request	DER	268
Disconnect-Peer-Answer	DPA	282
Disconnect-Peer-Request	DPR	282
Location-Info-Answer	LIA	302
Location-Info-Request	LIR	302
Message-Process-Answer	MPA	311
Message-Process-Request	MPR	311
Multimedia-Auth-Answer	MAA	303
Multimedia-Auth-Request	MAR	303
Profile-Update-Answer	PUA	307
Profile-Update-Request	PUR	307
Push-Notification-Answer	PNA	309
Push-Notification-Request	PNR	309
Push-Profile-Answer	PPA	305
Push-Profile-Request	PPR	305
Re-Auth-Answer	RAA	258

Re-Auth-Request	RAR	258
Registration-Termination-Answer	RTA	304
Registration-Termination-Request	RTR	304
Server-Assignment-Answer	SAA	301
Server-Assignment-Request	SAR	301
Session-Termination-Answer	STA	275
Session-Termination-Request	STR	275
Subscribe-Notifications-Answer	SNA	308
Subscribe-Notifications-Request	SNR	308
User-Authorization-Answer	UAA	300
User-Authorization-Request	UAR	300
User-Data-Answer	UDA	306
User-Data-Request	UDR	306

Message flows



The communication between two diameter peers starts the establishment of a transport connection (TCP or SCTP). The initiator then sends a Capabilities-Exchange-Request (CER) to the other peer, which responds with a Capabilities-Exchange-Answer (CEA). After that, TLS may optionally be negotiated.

The connection is then ready for exchanging application messages.

If no messages have been exchanged for some time either side may send a Device-Watchdog-Request (DWR) and the other peer must respond with Device-Watchdog-Answer.

Either side may terminate the communication by sending a Disconnect-Peer-Request (DPR) which the other peer must respond to with Disconnect-Peer-Answer. After that the transport connection can be disconnected.

Node B

Node B is a term used in UMTS equivalent to the BTS (base transceiver station) description used in GSM. It is the hardware that is connected to the mobile phone network that communicates directly with mobile handsets. In contrast with GSM base stations, Node B uses WCDMA/TD-SCDMA as the air interface technology. As in all cellular systems, such as UMTS and GSM, the Node B contains radio frequency transmitter(s) and the receiver(s) used to communicate directly

with mobile devices, which move freely around it. In this type of cellular network, the mobile devices cannot communicate directly with each other but have to communicate with the Node B.

Functionality

Traditionally, the Node Bs have minimum functionality, and are controlled by an RNC (Radio Network Controller). However, this is changing with the emergence of High Speed Downlink Packet Access (HSDPA), where some logic (e.g. retransmission) is handled on the Node B for lower response times.

Differences between a Node B and a GSM base station

Frequency use

The utilization of WCDMA technology allows cells belonging to the same or different Node Bs and even controlled by different RNC to overlap and still use the same frequency (in fact, the whole network can be implemented with just one frequency pair). The effect is utilized in soft handovers.

Power requirements

Since WCDMA often operates at higher frequencies than GSM (2100MHz as opposed to 900Mhz for GSM), the cell radius can be considerably smaller when compared to GSM cells due to the effect of path loss being frequency dependant.

WCDMA now has networks operating in the 850-900MHz band, and at these frequencies the coverage is considered better than the equivalent GSM network.

Unlike in GSM, the cells' size is not constant (a phenomenon known as "cell breathing"). This requires a larger number of Node Bs and careful planning in 3G (UMTS) networks. Power requirements on Node Bs and user equipment (UE) are much lower.

Node B setup

A full setup contains a cabinet, an antenna mast and actual antenna. An equipment cabinet contain e.g. power amplifiers, digital signal processors and back-up batteries. What you can see by the side of a road or in a city center is just an antenna. However, the tendency nowadays is to camouflage the antenna (paint it the color of the building or put it into an RF-transparent enclosure). Smaller indoor solutions may have a built-in antenna on the cabinet door.

A Node B can serve several cells, also called sectors, depending on the configuration and type of antenna. Common configuration include omni cell (360°), 3 sectors (3x120°) or 6 sectors (3 sectors 120° wide overlapping with 3 sectors of different frequency).

List of HTTP status codes

The following is a list of **HyperText Transfer Protocol (HTTP) response status codes**. This includes codes from IETF internet standards as well as unstandardised RFCs, other specifications and some additional commonly used codes. The first digit of the status code specifies one of five classes of response; the bare minimum for an HTTP client is that it recognises these five classes. Microsoft IIS may use additional decimal sub-codes to provide more specific information,[1] but these are not listed here. The phrases used are the standard examples, but any human-readable alternative can be provided. Unless otherwise stated, the status code is part of the HTTP/1.1 standard.

1xx Informational

Request received, continuing process.[2]

This class of status code indicates a provisional response, consisting only of the Status-Line and optional headers, and is terminated by an empty line. Since HTTP/1.0 did not define any 1xx status codes, servers *must not* send a 1xx response to an HTTP/1.0 client except under experimental conditions.

100 Continue

> This means that the server has received the request headers, and that the client should proceed to send the request body (in the case of a request for which a body needs to be sent; for example, a POST request). If the request body is large, sending it to a server when a request has already been rejected based upon inappropriate headers is inefficient. To have a server check if the request could be accepted based on the request's headers alone, a client must send `Expect: 100-continue` as a header in its initial request[2] and check if a `100 Continue` status code is received in response before continuing (or receive `417 Expectation Failed` and not continue).[2]

101 Switching Protocols

> This means the requester has asked the server to switch protocols and the server is acknowledging that it will do so.[2]

102 Processing (WebDAV) (RFC 2518)

> As a WebDAV request may contain many sub-requests involving file operations, it may take a long time to complete the request. This code indicates that the server has received and is processing the request, but no response is available yet.[3] This prevents the client from timing out and assuming the request was lost.

2xx Success

This class of status codes indicates the action requested by the client was received, understood, accepted and processed successfully.

200 OK

Standard response for successful HTTP requests. The actual response will depend on the request method used. In a GET request, the response will contain an entity corresponding to the requested resource. In a POST request the response will contain an entity describing or containing the result of the action.[2]

201 Created

The request has been fulfilled and resulted in a new resource being created.[2]

202 Accepted

The request has been accepted for processing, but the processing has not been completed. The request might or might not eventually be acted upon, as it might be disallowed when processing actually takes place.[2]

203 Non-Authoritative Information (since HTTP/1.1)

The server successfully processed the request, but is returning information that may be from another source.[2]

204 No Content

The server successfully processed the request, but is not returning any content.[2]

205 Reset Content

The server successfully processed the request, but is not returning any content. Unlike a 204 response, this response requires that the requester reset the document view.[2]

206 Partial Content

The server is delivering only part of the resource due to a range header sent by the client. The range header is used by tools like wget to enable resuming of interrupted downloads, or split a download into multiple simultaneous streams.[2]

207 Multi-Status (WebDAV) (RFC 4918)

The message body that follows is an XML message and can contain a number of separate response codes, depending on how many sub-requests were made.[4]

3xx Redirection

The client must take additional action to complete the request.[2]

This class of status code indicates that further action needs to be taken by the user agent in order to fulfil the request. The action required *may* be carried out by the user agent without interaction with the user if and only if the method used in the second request is GET or HEAD. A user agent *should not* automatically redirect a request more than five times, since such redirections usually indicate an infinite loop.

300 Multiple Choices

> Indicates multiple options for the resource that the client may follow. It, for instance, could be used to present different format options for video, list files with different extensions, or word sense disambiguation.[2]

301 Moved Permanently

> This and all future requests should be directed to the given URI.[2]

302 Found

> This is the most popular redirect code[*citation needed*], but also an example of industrial practice contradicting the standard.[2] HTTP/1.0 specification (RFC 1945) required the client to perform a temporary redirect (the original describing phrase was "Moved Temporarily"),[5] but popular browsers implemented 302 with the functionality of a 303 See Other. Therefore, HTTP/1.1 added status codes 303 and 307 to distinguish between the two behaviours. However, the majority of Web applications and frameworks still use the 302 status code as if it were the 303[6].

303 See Other (since HTTP/1.1)

> The response to the request can be found under another URI using a GET method. When received in response to a PUT, it should be assumed that the server has received the data and the redirect should be issued with a separate GET message.[2]

304 Not Modified

> Indicates the resource has not been modified since last requested.[2] Typically, the HTTP client provides a header like the If-Modified-Since header to provide a time against which to compare. Utilizing this saves bandwidth and reprocessing on both the server and client, as only the header data must be sent and received in comparison to the entirety of the page being re-processed by the server, then sent again using more bandwidth of the server and client.

305 Use Proxy (since HTTP/1.1)

> Many HTTP clients (such as Mozilla[7] and Internet Explorer) do not correctly handle responses with this status code, primarily for security reasons.[2]

306 Switch Proxy

No longer used.[2]

307 Temporary Redirect (since HTTP/1.1)

In this occasion, the request should be repeated with another URI, but future requests can still use the original URI.[2] In contrast to 303, the request method should not be changed when reissuing the original request. For instance, a POST request must be repeated using another POST request.

4xx Client Error

The 4xx class of status code is intended for cases in which the client seems to have erred. Except when responding to a HEAD request, the server *should* include an entity containing an explanation of the error situation, and whether it is a temporary or permanent condition. These status codes are applicable to any request method. User agents *should* display any included entity to the user. These are typically the most common error codes encountered while online.

400 Bad Request

The request cannot be fulfilled due to bad syntax.[2]

401 Unauthorized

Similar to *403 Forbidden*, but specifically for use when authentication is possible but has failed or not yet been provided.[2] The response must include a WWW-Authenticate header field containing a challenge applicable to the requested resource. See Basic access authentication and Digest access authentication.

402 Payment Required

Reserved for future use.[2] The original intention was that this code might be used as part of some form of digital cash or micropayment scheme, but that has not happened, and this code is not usually used. As an example of its use, however, Apple's MobileMe service generates a 402 error ("httpStatusCode:402" in the Mac OS X Console log) if the MobileMe account is delinquent.

403 Forbidden

The request was a legal request, but the server is refusing to respond to it.[2] Unlike a *401 Unauthorized* response, authenticating will make no difference.[2]

404 Not Found

The requested resource could not be found but may be available again in the future.[2] Subsequent requests by the client are permissible.

405 Method Not Allowed

A request was made of a resource using a request method not supported by that resource;[2] for example, using GET on a form which requires data to be presented via POST, or using PUT on a read-only resource.

406 Not Acceptable

The requested resource is only capable of generating content not acceptable according to the Accept headers sent in the request.[2]

407 Proxy Authentication Required[2]

408 Request Timeout

The server timed out waiting for the request.[2] According to W3 HTTP specifications: "The client did not produce a request within the time that the server was prepared to wait. The client MAY repeat the request without modifications at any later time."

409 Conflict

Indicates that the request could not be processed because of conflict in the request, such as an edit conflict.[2]

410 Gone

Indicates that the resource requested is no longer available and will not be available again.[2] This should be used when a resource has been intentionally removed; however, it is not necessary to return this code and a *404 Not Found* can be issued instead. However, despite the most common status code for such a page being *404 Not Found*, *410 Gone* is still used by some servers, including Geocities. Upon receiving a 410 status code, the client should not request the resource again in the future. Clients such as search engines should remove the resource from their indices.

411 Length Required

The request did not specify the length of its content, which is required by the requested resource.[2]

412 Precondition Failed

The server does not meet one of the preconditions that the requester put on the request.[2]

413 Request Entity Too Large

The request is larger than the server is willing or able to process.[2]

414 Request-URI Too Long

The URI provided was too long for the server to process.[2]

415 Unsupported Media Type

The request entity has a media type which the server or resource does not support.[2] For example the client uploads an image as image/svg+xml, but the server requires that images use a different format.

416 Requested Range Not Satisfiable

The client has asked for a portion of the file, but the server cannot supply that portion.[2] For example, if the client asked for a part of the file that lies beyond the end of the file.

417 Expectation Failed

The server cannot meet the requirements of the Expect request-header field.[2]

418 I'm a teapot

This code was defined as one of the traditional IETF April Fools' jokes, in RFC 2324, *Hyper Text Coffee Pot Control Protocol*, and is not expected to be implemented by actual HTTP servers.

422 Unprocessable Entity (WebDAV) (RFC 4918)

The request was well-formed but was unable to be followed due to semantic errors.[4]

423 Locked (WebDAV) (RFC 4918)

The resource that is being accessed is locked[4]

424 Failed Dependency (WebDAV) (RFC 4918)

The request failed due to failure of a previous request (e.g. a PROPPATCH).[4]

425 Unordered Collection (RFC 3648)

Defined in drafts of "WebDAV Advanced Collections Protocol",[8] but not present in "Web Distributed Authoring and Versioning (WebDAV) Ordered Collections Protocol".[9]

426 Upgrade Required (RFC 2817)

The client should switch to a different protocol such as TLS/1.0.[10]

449 Retry With

A Microsoft extension. The request should be retried after doing the appropriate action.[11]

450 Blocked by Windows Parental Controls

A Microsoft extension. This error is given when Windows Parental Controls are turned on and are blocking access to the given webpage.[12]

5xx Server Error

The server failed to fulfill an apparently valid request.[2]

Response status codes beginning with the digit "5" indicate cases in which the server is aware that it has encountered an error or is otherwise incapable of performing the request. Except when responding to a HEAD request, the server *should* include an entity containing an explanation of the error situation, and indicate whether it is a temporary or permanent condition. Likewise, user agents *should* display any included entity to the user. These response codes are applicable to any request method.

500 Internal Server Error

A generic error message, given when no more specific message is suitable.[2]

501 Not Implemented

The server either does not recognise the request method, or it lacks the ability to fulfill the request.[2]

502 Bad Gateway

The server was acting as a gateway or proxy and received an invalid response from the upstream server.[2]

503 Service Unavailable

The server is currently unavailable (because it is overloaded or down for maintenance).[2] Generally, this is a temporary state.

504 Gateway Timeout

The server was acting as a gateway or proxy and did not receive a timely response from the upstream server.[2]

505 HTTP Version Not Supported

The server does not support the HTTP protocol version used in the request.[2]

506 Variant Also Negotiates (RFC 2295)

Transparent content negotiation for the request, results in a circular reference.[13]

507 Insufficient Storage (WebDAV) (RFC 4918)[4]

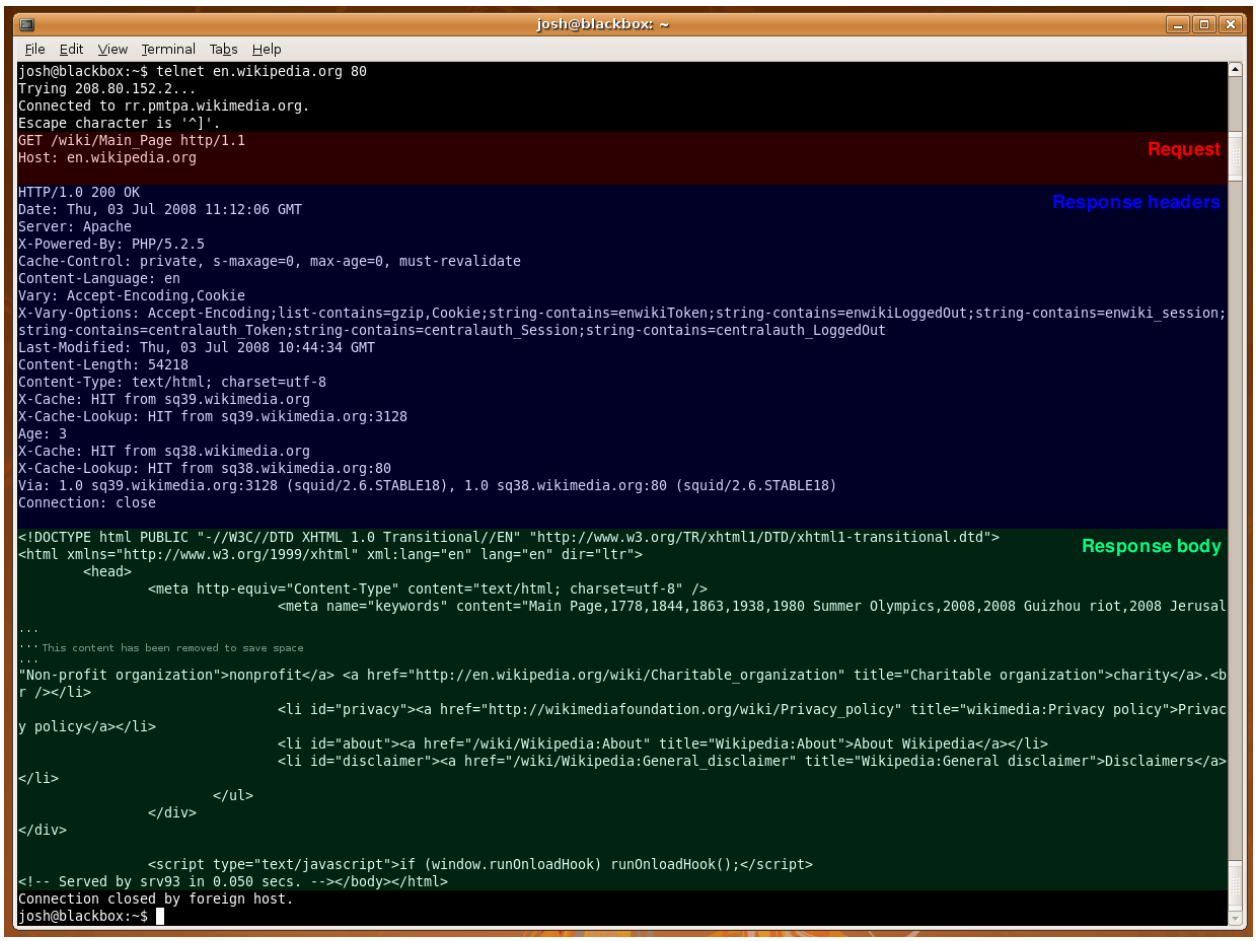
509 Bandwidth Limit Exceeded (Apache bw/limited extension)

This status code, while used by many servers, is not specified in any RFCs.

510 Not Extended (RFC 2774)

Further extensions to the request are required for the server to fulfill it.[14]

Request methods



An HTTP request made using telnet. The request, response headers and response body are highlighted.

HTTP defines nine methods (sometimes referred to as "verbs") indicating the desired action to be performed on the identified **resource**. What this resource represents, whether pre-existing data or data that is generated dynamically, depends on the implementation of the server. Often, the resource corresponds to a file or the output of an executable residing on the server.

HEAD

Asks for the response identical to the one that would correspond to a GET request, but without the response body. This is useful for retrieving meta-information written in response headers, without having to transport the entire content.

GET

Requests a representation of the specified resource. Note that GET should not be used for operations that cause side-effects, such as using it for taking actions in web applications. One reason for this is that GET may be used arbitrarily by robots or crawlers, which should not need to consider the side effects that a request should cause. See safe methods below.

POST

Submits data to be processed (e.g., from an HTML form) to the identified resource. The data is included in the body of the request. This may result in the creation of a new resource or the updates of existing resources or both.

PUT

Uploads a representation of the specified resource.

DELETE

Deletes the specified resource.

TRACE

Echoes back the received request, so that a client can see what (if any) changes or additions have been made by intermediate servers.

OPTIONS

Returns the HTTP methods that the server supports for specified URL. This can be used to check the functionality of a web server by requesting '*' instead of a specific resource.

CONNECT

Converts the request connection to a transparent TCP/IP tunnel, usually to facilitate SSL-encrypted communication (HTTPS) through an unencrypted HTTP proxy.[7]

PATCH

Is used to apply partial modifications to a resource.[8]

HTTP servers are required to implement at least the GET and HEAD methods[9] and, whenever possible, also the OPTIONS method.

E-carrier

In digital telecommunications, where a single physical wire pair can be used to carry many simultaneous voice conversations by time-division multiplexing, worldwide standards have been created and deployed. The European Conference of Postal and Telecommunications Administrations (CEPT) originally standardized the **E-carrier** system, which revised and improved the earlier American T-carrier technology, and this has now been adopted by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T). This is now widely used in almost all countries outside the USA, Canada and Japan.

The E-carrier standards form part of the Plesiochronous Digital Hierarchy (PDH) where groups of E1 circuits may be bundled onto higher capacity E3 links between telephone exchanges or countries. This allows a network operator to provide a private end-to-end E1 circuit between customers in different countries that share single high capacity links in between.

In practice, only E1 and E3 versions are used. Physically E1 is transmitted as 32 timeslots and E3 512 timeslots, but one is used for framing and typically one allocated for signalling call setup and tear down. Unlike Internet data services, E-carrier systems permanently allocate capacity for a voice call for its entire duration. This ensures high call quality because the transmission arrives with the same short delay (latency) and capacity at all times.

E1 circuits are very common in most telephone exchanges and are used to connect to medium and large companies, to remote exchanges and in many cases between exchanges. E3 lines are used between exchanges, operators and/or countries, and have a transmission speed of 34.368 Mbit/s.

E1

An E1 link operates over two separate sets of wires, usually twisted pair cable. A nominal 3 Volt peak signal is encoded with pulses using a method that avoids long periods without polarity changes. The line data rate is 2.048 Mbit/s (full duplex, i.e. 2.048 Mbit/s downstream and 2.048 Mbit/s upstream) which is split into 32 timeslots, each being allocated 8 bits in turn. Thus each timeslot sends and receives an 8-bit PCM sample, usually encoded according to A-law algorithm, 8000 times per second (8 x 8000 x 32 = 2,048,000). This is ideal for voice telephone calls where the voice is sampled into an 8 bit number at that data rate and reconstructed at the other end. The timeslots are numbered from 0 to 31.

One timeslot (TS0) is reserved for framing purposes, and alternately transmits a fixed pattern. This allows the receiver to lock onto the start of each frame and match up each channel in turn. The standards allow for a full Cyclic Redundancy Check to be performed across all bits transmitted in each frame, to detect if the circuit is losing bits (information), but this is not always used.

One timeslot (TS16) is often reserved for signalling purposes, to control call setup and teardown according to one of several standard telecommunications protocols. This includes Channel Associated Signaling (CAS) where a set of bits is used to replicate opening and closing the

circuit (as if picking up the telephone receiver and pulsing digits on a rotary phone), or using tone signalling which is passed through on the voice circuits themselves. More recent systems used Common Channel Signaling (CCS) such as ISDN or Signalling System 7 (SS7) which send short encoded messages with more information about the call including caller ID, type of transmission required etc. ISDN is often used between the local telephone exchange and business premises, whilst SS7 is almost exclusively used between exchanges and operators. In theory, a single SS7 signaling timeslot can control up to 4096 circuits per signalling channel using a 12-bit Channel Identification Code (CIC)[3], thus allowing slightly more efficient use of the overall transmission bandwidth because additional E1 links would use all 31 voice channels. ANSI uses a larger 14-bit CIC and so can accommodate up to 16,384 circuits. In most environments, multiple signalling channels would be used to provide redundancy in case of faults or outages.

Unlike the earlier T-carrier systems developed in North America, all 8 bits of each sample are available for each call. This allows the E1 systems to be used equally well for circuit switch data calls, without risking the loss of any information.

While the original CEPT standard G.703 specifies several options for the physical transmission, almost exclusively HDB3 format is used.

Definition

Link An unidirectional channel residing in one timeslot of a E1 or T1 Line, carrying 64 kbit/s (64'000 bit/s) raw digital data.

Line An unidirectional E1 or T1 physical connection.

Trunk A bidirectional E1 or T1 physical connection.

Hierarchy levels

The PDH based on the E0 signal rate is designed so that each higher level can multiplex a set of lower level signals. Framed E1 is designed to carry 30 E0 data channels + 1 signalling channel, all other levels are designed to carry 4 signals from the level below. Because of the necessity for overhead bits, and justification bits to account for rate differences between sections of the network, each subsequent level has a capacity greater than would be expected from simply multiplying the lower level signal rate (so for example E2 is 8.448 Mbit/s and not 8.192 Mbit/s as one might expect when multiplying the E1 rate by 4).

Note, because bit interleaving is used, it is very difficult to demultiplex low level tributaries directly, requiring equipment to individually demultiplex every single level down to the one that is required.

Signal Rate

E0 64 kbit/s

E1 2.048 Mbit/s

E2 8.448 Mbit/s

E3 34.368 Mbit/s

E4 139.264 Mbit/s

E5 564.992 Mbit/s

T-carrier

Two Network Interface Units. On the left with a single card, the right with two

In telecommunications, **T-carrier**, sometimes abbreviated as *T-CXR*, is the generic designator for any of several digitally multiplexed telecommunications carrier systems originally developed by Bell Labs and used in North America, Japan, and South Korea.

The basic unit of the T-carrier system is the DS0, which has a transmission rate of 64 kbit/s, and is commonly used for one voice circuit.

The **E-carrier** system, where 'E' stands for European, is incompatible with the T-carrier (though cross compliant cards exist) and is used in most locations outside of North America, Japan, and Korea. It typically uses the **E1** line rate and the E3 line rate. The E2 line rate is less commonly used. See the table below for bit rate comparisons.

T1

Main article: Digital Signal 1

Existing frequency-division multiplexing carrier systems worked well for connections between distant cities, but required expensive modulators, demodulators and filters for every voice channel. For connections within metropolitan areas, Bell Labs in the late 1950s sought cheaper terminal equipment. Pulse-code modulation allowed sharing a coder and decoder among several voice trunks, so this method was chosen for the T1 system introduced into local use in 1961. In later decades, the cost of digital electronics declined to the point that an individual codec per voice channel became commonplace, but by then the other advantages of digital transmission had become entrenched.

The most common legacy of this system is the line rate speeds. "**T1**" now means any data circuit that runs at the original 1.544 Mbit/s line rate. Originally the T1 format carried 24 pulse-code modulated, time-division multiplexed speech signals each encoded in 64 kbit/s streams, leaving 8 kbit/s of framing information which facilitates the synchronization and demultiplexing at the receiver. T2 and T3 circuit channels carry multiple T1 channels multiplexed, resulting in transmission rates of 6.312 and 44.736 Mbit/s, respectively.

Supposedly, the 1.544 Mbit/s rate was chosen because tests done by AT&T Long Lines in Chicago were conducted underground. To accommodate loading coils, cable vault manholes were physically 2000 meter (6,600 ft) apart, and so the optimum bit rate was chosen empirically — the capacity was increased until the failure rate was unacceptable, then reduced to leave a margin. Companding allowed acceptable audio performance with only seven bits per PCM sample in this original T1/D1 system. The later D3 and D4 channel banks had an extended frame format, allowing eight bits per sample, reduced to seven every sixth sample or frame when one bit was "robbed" for signaling the state of the channel. The standard does not allow an all zero sample which would produce a long string of binary zeros and cause the repeaters to lose bit sync. However, when carrying data (Switched 56) there could be long strings of zeroes, so one bit per sample is set to "1" (jam bit 7) leaving 7 bits x 8,000 frames per second for data.

A more detailed understanding of how the rate of 1.544 Mbit/s was derived is as follows. (This explanation glosses over T1 voice communications, and deals mainly with the numbers involved.) Given that the telephone system nominal voiceband (including guardband) is 4,000 Hz, the required digital sampling rate is 8,000 Hz (see Nyquist rate). Since each T1 frame contains 1 byte of voice data for each of the 24 channels, that system needs then 8,000 frames per second to maintain those 24 simultaneous voice channels. Because each frame of a T1 is 193 bits in length (24 channels X 8 bits per channel + 1 framing bit = 193 bits), 8,000 frames per second is multiplied by 193 bits to yield a transfer rate of 1.544 Mbit/s (8,000 X 193 = 1,544,000).

Initially, T1 used **Alternate Mark Inversion** (AMI) to reduce frequency bandwidth and eliminate the DC component of the signal. Later **B8ZS** became common practice. For AMI, each mark pulse had the opposite polarity of the previous one and each space was at a level of zero, resulting in a three level signal which however only carried binary data. Similar British 23 channel systems at 1.536 Mbaud in the 1970s were equipped with ternary signal repeaters, in anticipation of using a 3B2T or 4B3T code to increase the number of voice channels in future, but in the 1980s the systems were merely replaced with European standard ones. American T-carriers could only work in AMI or B8ZS mode.

The AMI or B8ZS signal allowed a simple error rate measurement. The D bank in the central office could detect a bit with the wrong polarity, or "bipolarity violation" and sound an alarm. Later systems could count the number of violations and reframes and otherwise measure signal quality and allow a more sophisticated alarm indication signal system.

SDP

The term **Service Delivery Platform** (SDP) usually refers to a set of components that provide a services delivery architecture (such as service creation, session control & protocols) for a type of service. There is no standard definition of SDP in the industry although the TM Forum (TMF) is working on defining specifications in this area. Different players will define its components and its breadth and depth in a slightly different way.

As SDPs evolve, they will often require integration of telecom and IT capabilities and the creation of services beyond technology and network boundaries. SDPs available today are optimized for the delivery of a service in a given technological or network domain (examples of such SDPs include web, IMS, IPTV, Mobile TV, etc.). They will typically provide a service control environment, a service creation environment, a service orchestration and execution environment, and abstractions for media control, presence/location, integration, and other low-level communications capabilities. SDPs are applied to both consumer and business applications.

The business objective of implementing the SDP is to enable rapid development and deployment of new converged multimedia services, from basic POTS phone services to complex audio/video conferencing for multiplayer games (MPGs).

The emergence of Application Stores, to create applications for devices such as Apple's iPhone, has put the focus on the SDP as a means for Communication Service Providers (CSPs) to compete and generate revenue from data.[1] Using the SDP to expose their network assets to both the internal and external development communities, including web 2.0 developers, CSPs can manage the lifecycles of thousands of innovative applications and the vast pool of developers.[2] Solutions that provide developer-friendly software and a means to govern the vast numbers of developers and applications will be critical for CSPs looking to gain a foothold in the App Store market.[3]

Telecommunications companies like Telcordia Technologies, Nokia Siemens Networks, Nortel, Avaya, Ericsson and Alcatel-Lucent have provided communications integration interfaces and infrastructure since the early to mid 1990s. The cost-saving success of IP-based VoIP systems as replacements for proprietary PBX systems and desktop phones has prompted a revolutionary shift in industry focus from proprietary systems to open, standard technologies.

The change in network architecture towards IP and change to open environments has promoted innovative software focused telecommunication companies like Teligent Telecom and HP - Communication & Media Solutions as vendors in this segment.[4] This strong focus on open environments has also given systems integrators such as Tieto, Accenture, IBM, TCS, HP, Alcatel-Lucent, Tech Mahindra infosys, Wipro and CGI the opportunity to offer turnkey pre-packaged, integration services and there are also, technology silo-ed focused, turn-key SDP

solutions. In addition, new consortia of telecommunications software product companies are also emerging. By offering pre-integrated software products, consortia offer an alternative means for operators to create SDPs based on key product elements - such as convergent billing and content/partner relationship management.

As SDPs evolve beyond technology silos, several blended applications will be possible:

- Users can see incoming phone calls (Wireline or Wireless), IM buddies (PC) or the locations of friends (GPS Enabled Device) on their television screen
- Users can order VoD (Video On Demand) services from their mobile phones or watch streaming video that they have ordered as a video package for both home and mobile phone
- An airline customer receives a text message from an automated system regarding a flight cancellation, then opts to use a voice self-service interface to reschedule

History

The late 1990s saw a period of unprecedented change in enterprise applications as the grip of client-server architectures gradually relaxed and allowed the entrance of n-tiered architectures. This represented the advent of the application server, a flexible compromise between the absolutes of the dumb terminal and the logic-heavy client PC. Although entrants into the application server ring were many and varied, they shared common advantages: database vendor abstraction, open standard (mostly object-oriented) programming models, high availability and scalability characteristics, and presentation frameworks, among others. These transformations were triggered by business forces including the rampaging tidal wave that was the Internet boom, but none of it would have been possible without the proliferation of standards such as the TCP/IP protocol, the Java programming language, and the Java EE web application server architecture. It is against this backdrop of transformation that telecom's era of rapid change was set in motion.

Up until the first few years of 2000, the markets for commercial and business telecommunication technologies were still saturated with proprietary hardware and software. Open standards started to become popular as IP technologies were introduced and with the rapid expansion of Voice-over-IP (VoIP) for transmission of voice data over packet networks and the Session Initiation Protocol (SIP) for standardized media control, especially regarding enterprise voice communication.

In this new standards-supported environment, convergence of the voice and data worlds has become less a moniker for disastrous telecom/IT integration attempts and more a true avenue for the production of new and better consumer and business services. The last few years have seen the introduction or proliferation of various SIP programming libraries (reSIProcate, Aricent, MjSip and its derived port by HSC) and products based on the relatively new SIP standard, and the IP Multimedia Subsystem standard defined by the 3GPP has gained a huge following. The Service Delivery Platform, whose power comes in large part from the quality and acceptance of

these supporting standards, is rapidly gaining acceptance as a widely applicable architectural pattern.

In industry today there are multiple definitions of Service Delivery Platform (SDP) being used with no established consensus as to a common meaning. Because of this, and the need for service providers to understand how to better manage SDPs, the TM Forum (TMF) has started standardizing the concept of Service Delivery Framework (SDF) and SDF management. The SDF definition provides the terminology and concepts needed to reference the various components involved, such as applications and enablers, network and service exposure, and orchestration.

What is needed to deliver a blend of personalized services from multiple SDPs to end users is a means to inter-work those SDPs through common service enablers and network resources. Underpinning these service aspects though has been a fundamental concept that the user's attributes and the services they receive require a common repository and a common data model, such as those provided by a LDAP/X.500 directory or HSS database. Early SDP implementations of this nature started in the mid / late 1990's for ISP converged services. Larger and more complex SDPs have been implemented over the last 5 years in MSO type environments and for mobile operators.

SDPs: Their Context and Next Generation Systems

SDPs are commonly considered for the telco type environments as a core system which interconnects the customer's access and network infrastructure with the OSS systems and BSS systems. SDPs in this context are usually associated to a particular service regime such as mobile telephones or for converged services.

SDPs are also considered in the context of very large transformation, convergence and integration programs which require a considerable budget. The difficulty in such projects is that there may be hundreds of thousands of design and implementation decisions to be made - once the architecture is agreed. Naturally this issue alone dictates the need for software development and operational engineering skills. Probably the best way of reducing these design and integration issues is to simulate the SDP on a small scale system before the major project actually starts. This allows the solution architecture to be verified that it meets the operational, service delivery and business requirements.

In the new world of converged service delivery, SDPs should also be considered not just as a core function within an operator but as a number of interconnected, distributed service nodes (e.g.) for redundancy reasons and for different service profiles to different business and market sectors. Many operators provide commercial scale/grade products such as bundled voice, web hosting, VPNs, mail, conference and messaging facilities to government and corporate clients. The evolution of such bundled services could be from fragmented management systems to a "Virtual Private Service Environment" where the operator runs a dedicated SDP for each of its customers who require their services on demand and under their control.

SDPs can also be used to manage independent wireless enabled precincts such as shopping malls, airports, retirement villages, outcare centres. In this case a "lightweight" easy to deploy platform could be used. See wwite: Next Generation Governance and Service Delivery Platform.

Elements of an SDP

Service Creation Environment

Often a telecom software developer's primary access point, the Service Creation Environment (SCE, also Application Creation Environme or Integrated Development Environment) is used by the developer to create software, scripts, and resources representing the services to be exposed. These can range in complexity from basic Eclipse plug-ins (as with Ubiquity's UDS, or Ubiquity Development Studio) to completely abstracted, metadata-driven telecom application modeling applications (like Avaya's discontinued CRM Central product).

The purpose of the SCE is to facilitate the rapid creation of new communication services. Ignoring factors like marketing for the moment, the easier it is for developers to create services for a given platform, the greater will be the number of available services, and thus the acceptance of the platform by the broader telecom market. Therefore, a telecom infrastructure provider can gain significant advantage with an SDP that provides for rapid service creation.

The leveraging of converged Java EE and SIP service creation environments has accelerated the adoption of specific Service Delivery Platform solutions. Java-based applications developers, traditionally focused on IT applications, are now rapidly developing real-time communications applications using Java EE and network connecting protocols like SIP and Parlay X web services. Software vendors are combining these technologies (e.g., Oracle Jdeveloper and Oracle Communication and Mobility Server with basic Eclipse plug-in) to reach out to a broader developer base.

Execution Environment

Media Control

Presence/Location

One aspects of an SDP is that it must be centered on the new "point of presence". This is the point of user access to their converged services where their preferences and entitlements are evaluated in real time. Preference and entitlement processing ensures that the user's services in their device/location contexts are delivered correctly. As entitlements are related to the product and service management regimes of the operator, the core architecture of an SDP should define managed products, services, users, preference and entitlement processes.

The implementation of standards remains a critical factor in Presence applications. The implementation of standards such as SIP and SIMPLE (Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions) is becoming more prevalent. SIMPLE Presence

provides a standard portable and secure interface to manipulate presence information between a SIMPLE client (watcher) and a presence server (presence agent). See JSR 164 for SIMPLE Presence. Providers of SIMPLE Presence servers include Oracle and Italtel.

Integration

The use of standards for exposure for interfaces across SDPs and within the SDP should minimize the need for integration in three main areas: (1) southbound to underlying network core components (2) between support application such as CRM, billing, and service activation (3) third party applications and services. The implementation of SOA in a complete end-to-end solution strive to minimize integration needs via standards-based interfaces and web services.

Software vendors who provide end-to-end solution for the IT SDP, Business Support Systems, Operating Support Systems, and SOA middleware suites include HP, wwite, IBM, Oracle and Sun microsystems. Network equipment vendors also provide SDPs such as IMS, IPTV, Mobile TV, etc. and offer the evolution of these SDPs.

If you have any questions on any of our terminology listed below (or any that are not), do not hesitate to contact us and we will answer any query you may have.

ACD - Automatic Call Distributor

The mechanism by which telephone calls are distributed to 'agents', typically within a call centre environment. A software application that runs on a PBX to provide call centre functionality.

ADSL - Asynchronous Digital Subscriber Line

Allows data transmission along standard telephone wires. ADSL has a higher data download speed than it has upload, ranging from 256k/s to 24mb/s.

ASR - Automated Speech Recognition

The ASR function allows the caller to speak simple commands into the auto attendant system (iAB) to progress the call, e.g. "YES" or "NO", "one", "two", "three" etc.

BSC - Base Station Controller

A device (or software) that controls the BTSs within a GSM network. Within Private Mobile Networks one BSC can control and manage the signalling and voice channels for 100 BTSs.

BTS - Base Tranceiver Station

A GSM antenna - this is responsible for transmitting and receiving the specific GSM frequency for a particular network. This could be in the form of a picocell for Private Mobile Networks but would also apply, on a much larger scale with a large GSM mast, to Vodafone, Orange etc.

Call Management

A general term used to describe the process of determining the manner in which telephone calls are handled and their ultimate destination. Usually used with respect to incoming calls, i.e. calls received by an organisation.

CLI – Calling Line Identity

CLI is a telephone service that transmits a caller's number to the called party's telephone. Where available, CLI can also provide a name associated with the calling telephone number.

CPE - Customer Premise Equipment

Usually refers to a telephony system (PBX) that physically exists at the customer's premises. The alternative is a hosted service.

CRM - Customer Relationship Management

A business philosophy that involves anticipating, understanding and responding to customer needs whilst maximising profits.

DDI - Direct Dial Inbound

A service whereby a call made to a DDI number can be routed directly to an internal extension without intervention by a switchboard operator.

DECT - Digital Enhanced Cordless Telecommunications

DECT (Digital Enhanced Cordless Telecommunications) is a digital wireless telephone technology, DECT uses time division multiple access (TDMA) to transmit radio signals to phones. Whereas GSM is optimized for mobile travel over large areas, DECT is designed especially for a smaller area with a large number of users, such as in cities and corporate complexes. A user can have a telephone equipped for both GSM and DECT (this is known as a dual-mode phone) and they can operate seamlessly.

IP-PBX

A telephone switching system that uses a signalling system based on the Internet Protocol as opposed to traditional PBXs that are based on a Time Division Multiplex (TDM) protocol.

Stored Program Control exchange (SPC)

Stored Program Control exchange (SPC) is the technical name used for telephone exchanges controlled by a computer program stored in the memory of the system. Early exchanges such as Strowger, panel, rotary, and crossbar switches were electromechanical and had no software control. SPC was introduced on a small scale in so called electronic switching systems in the 1960s (the 101ESS PBX was a minor Bell System example) and on a large scale in the 1970s

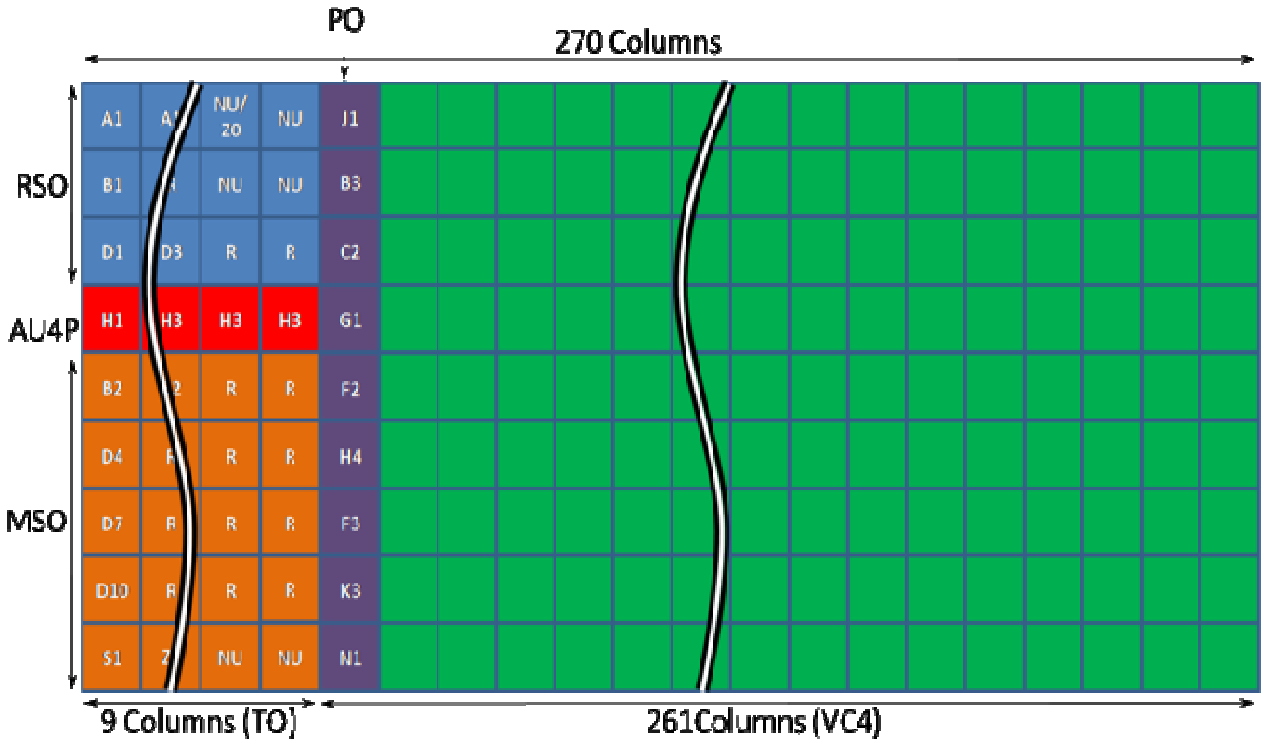
(1ESS switch from Bell System, AXE telephone exchange from Ericsson). SPC allowed more sophisticated calling features. As SPC exchanges evolved, reliability and versatility increased. In the 1980s SPC completely took over the industry, making the term redundant except for historical interest.

STM-1

The **STM-1** (**Synchronous Transport Module level-1**) is the SDH ITU-T fiber optic network transmission standard. It has a bit rate of 155.52 Mbit/s. The other levels are STM-4, STM-16 and STM-64. Beyond this we have wavelength-division multiplexing (WDM) commonly used in submarine cabling

Frame structure

The STM-1 frame is the basic transmission format for SDH. A STM-1 frame has a byte-oriented structure with 9 rows and 270 columns of bytes, for a total of 2,430 bytes (9 rows * 270 columns = 2430 bytes). Each byte corresponds to a 64kbit/s channel.[3]



TO: Transport Overhead (**RSO** + **AU4P** + **MSO**)

- **MSO**: Multiplex Section Overhead
- **RSO**: Regeneration Section Overhead
- **AU4P**: AU-4 Pointers

VC4: Virtual Container-4 payload (**PO** + **VC-4 Data**)

- **PO**: Path Overhead

[edit] Frame characteristics

The STM-1 base frame is structured with the following characteristics:

- **Length**: 270 column x 9 row = 2430 bytes
- **Duration** (Frame repetition time): 125 µs i.e. 8000 frames/s
- **Rate** (Frame capacity): 2430 x 8 x 8000 = 155.520 Mbit/s
- **Payload** = 2349bytes x 8bits x 8000frames/sec = 150.336 Mbit/s

BHCA

In telecommunications, **busy hour call attempts** (**BHCA**) is a teletraffic engineering measurement used to evaluate and plan capacity for telephone networks. BHCA is the number of telephone calls attempted at the busiest hour of the day (peak hour), and the higher the BHCA, the higher the stress on the network processors. BHCA is not to be confused with busy hour call completion (BHCC) which measures the throughput capacity of the network. If a bottleneck in the network exists with a capacity lower than the estimated BHCA, then congestion will occur resulting in many failed calls and customer dissatisfaction.

BHCA is usually used when planning telephone switching capacities and frequently goes side by side with the Erlang unit capacity calculation. As an example, a telephone exchange with a capacity of one million BHCA is estimated to handle 250,000 subscribers. The overall calculation is more complex however, and involves accounting for available circuits, desired blocking rates, and Erlang capacity allocated to each subscriber.

H.245

H.245 is a control channel protocol used with[in] e.g. H.323 and H.324 communication sessions, and involves the line transmission of non-telephone signals. It also offers the possibility to be tunneled within H.225.0 call signaling messages. This eases firewall traversing.

H.245 is capable of conveying information needed for multimedia communication, such as encryption, flow control, jitter management, preference requests, as well as the opening and closing of logical channels used to carry media streams. It also defines separate *send* and *receive* capabilities and the means to send these details to other devices that support H.323.

Handshake issues

One major drawback within the initial version of H.323 was the lengthy, four-way H.245 protocol handshake required during the opening up the logical channels of a telephony session.

Later versions of H.323 introduced the *Fast Connect* procedure, using the fastStart element of an H.225.0 message. Fast Connect brought the negotiation down to a two-way handshake. Another recommendation, H.460.6, Extended Fast Connect Feature, exists that defines a one-way handshake.

MCU

A **Multipoint Control Unit** (MCU) is a device commonly used to bridge videoconferencing connections.

The Multipoint Control Unit is an endpoint on the LAN that provides the capability for 3 or more terminals and gateways to participate in a multipoint conference. The MCU consists of a mandatory Multipoint Controller (MC) and optional Multipoint Processors (MPs).