SMPP

-Giao thức SMPP (Short Message Peer-to-Peer) là một giao thức mở, chuẩn công nghiệp được thiết kế để cung cấp giao diện truyền dữ liệu linh hoạt cho việc truyền dữ liệu tin nhắn ngắn giữa các Thực thể tin nhắn ngắn bên ngoài (ESME), Thực thể định tuyến (RE) và Trung tâm tin nhắn (MC). Đây là phương tiện mà các ứng dụng (gọi là ESME) có thể gửi tin nhắn SMS đến các thiết bị di động và nhận tin nhắn SMS từ các thiết bị di động.

-Hiện nay giao thức EMPP đã trở thành giao thức được chấp nhận rộng rãi trong ngành viễn thông để gửi tin nhắn SMS. Nó hoạt động như một phương tiện để gửi các chiến dịch tiếp thị, cập nhật tin tức và cập nhật kinh doanh.

Các thành phần của SMPP:

SMSC( short massage service center):

Chức năng: Là trung tâm xử lý tin nhắn ngắn, chịu trách nhiệm nhận, lưu trữ, định tuyến và gửi tin nhắn SMS đến thiết bị người dùng hoặc các hệ thống khác.

Vai trò trong SMPP: SMSC hoạt động như một máy chủ, kết nối với các ESME để xử lý yêu cầu gửi/nhận tin nhắn.

Ví dụ: Khi bạn gửi SMS, SMSC sẽ lưu tin nhắn nếu người nhận chưa sẵn sàng, sau đó chuyển tiếp khi họ online.

ESME ( external short messaging entity):

Chức năng: Là các ứng dụng hoặc hệ thống bên ngoài tương tác với SMSC để gửi hoặc nhận tin nhắn SMS.

Ví dụ: Các cổng SMS của doanh nghiệp (như gửi mã OTP), nhà cung cấp nội dung, hoặc ứng dụng nhắn tin tự động.

Vai trò trong SMPP: ESME kết nối với SMSC thông qua các phiên (bind) để thực hiện giao tiếp.

PDU (Protocol Data Unit)

Đơn vị dữ liệu giao thức, là định dạng dữ liệu được trao đổi giữa SMSC và ESME. Các loại PDU phổ biến bao gồm:

* **Submit\_SM**: Gửi tin nhắn từ ESME đến SMSC.
* **Deliver\_SM**: Chuyển tin nhắn từ SMSC đến ESME.
* **Bind**: Thiết lập kết nối giữa ESME và SMSC (có các loại như Bind\_Transmitter, Bind\_Receiver, Bind\_Transceiver).
* **Enquire\_Link**: Kiểm tra trạng thái kết nối.

SMPP được dùng để:

SMPP là thành phần chính của truyền thông SMS hiện đại và được sử dụng trong nhiều ứng dụng.

Nhắn tin doanh nghiệp sử dụng SMPP để gửi tin nhắn văn bản từ một chương trình phần mềm đến các số điện thoại cá nhân hoặc danh sách hàng loạt. Điều này bao gồm mọi thứ từ tin nhắn tiếp thị đến dịch vụ thông tin, nhắc nhở cuộc hẹn, dịch vụ chatbot và thậm chí cả yêu cầu đặt lại mật khẩu.

Các thiết bị Internet vạn vật di động (IoT) như đồng hồ đo thông minh sử dụng SMPP để truyền thông tin cập nhật về mức tiêu thụ tài nguyên và trạng thái vị trí. Khi một sự kiện như đột nhập hoặc hỏa hoạn kích hoạt hệ thống báo động thông minh, nó sẽ sử dụng SMPP để nhắn tin cho chủ sở hữu tòa nhà, có khả năng có liên kết cho phép họ truy cập nguồn cấp dữ liệu camera.

SMPP hoạt động là:

SMPP hoạt động theo mô hình máy khách-máy chủ, trong đó ESME đóng vai trò là máy khách và SMSC đóng vai trò là máy chủ .

Giao thức này tạo điều kiện thuận lợi cho giao tiếp hai chiều , cho phép gửi tin nhắn (thiết bị di động kết thúc – MT) và nhận tin nhắn (thiết bị di động bắt đầu – MO) thông qua nhiều hoạt động khác nhau. Giao thức này được thiết kế để hoạt động trên các giao thức mạng TCP/IP, đảm bảo việc phân phối tin nhắn đáng tin cậy, có thứ tự và được kiểm tra lỗi qua mạng.

Trước khi trao đổi bất kỳ tin nhắn nào, lệnh bind phải được gửi và xác nhận. Lệnh bind xác định hướng nào có thể gửi tin nhắn; bind\_transmitter chỉ cho phép máy khách gửi tin nhắn đến máy chủ, bind\_receiver có nghĩa là máy khách sẽ chỉ nhận được tin nhắn và bind\_transceiver cho phép truyền tin nhắn theo cả hai hướng. Trong lệnh bind, ESME tự xác định chính nó bằng system\_id, system\_type và password; trường address\_range được thiết kế để chứa địa chỉ ESME thường được để trống. Lệnh bind chứa tham số interface\_version để chỉ định phiên bản giao thức SMPP nào sẽ được sử dụng.

Trao đổi tin nhắn có thể đồng bộ, trong đó mỗi bên chờ phản hồi cho mỗi PDU được gửi hoặc không đồng bộ, trong đó nhiều yêu cầu có thể được đưa ra mà không cần chờ và được bên kia xác nhận theo thứ tự lệch; số lượng yêu cầu chưa được xác nhận được gọi là một *window* ; để có hiệu suất tốt nhất, cả hai bên giao tiếp phải được cấu hình với cùng window size.

Sau đây là một ví dụ về cách SMPP thường hoạt động trong thực tế:

Ví dụ bạn đang gửi tin nhắn văn bản từ ứng dụng của quán cà phê yêu thích để nhận được giảm giá. SMPP hoạt động trong trường hợp này là:

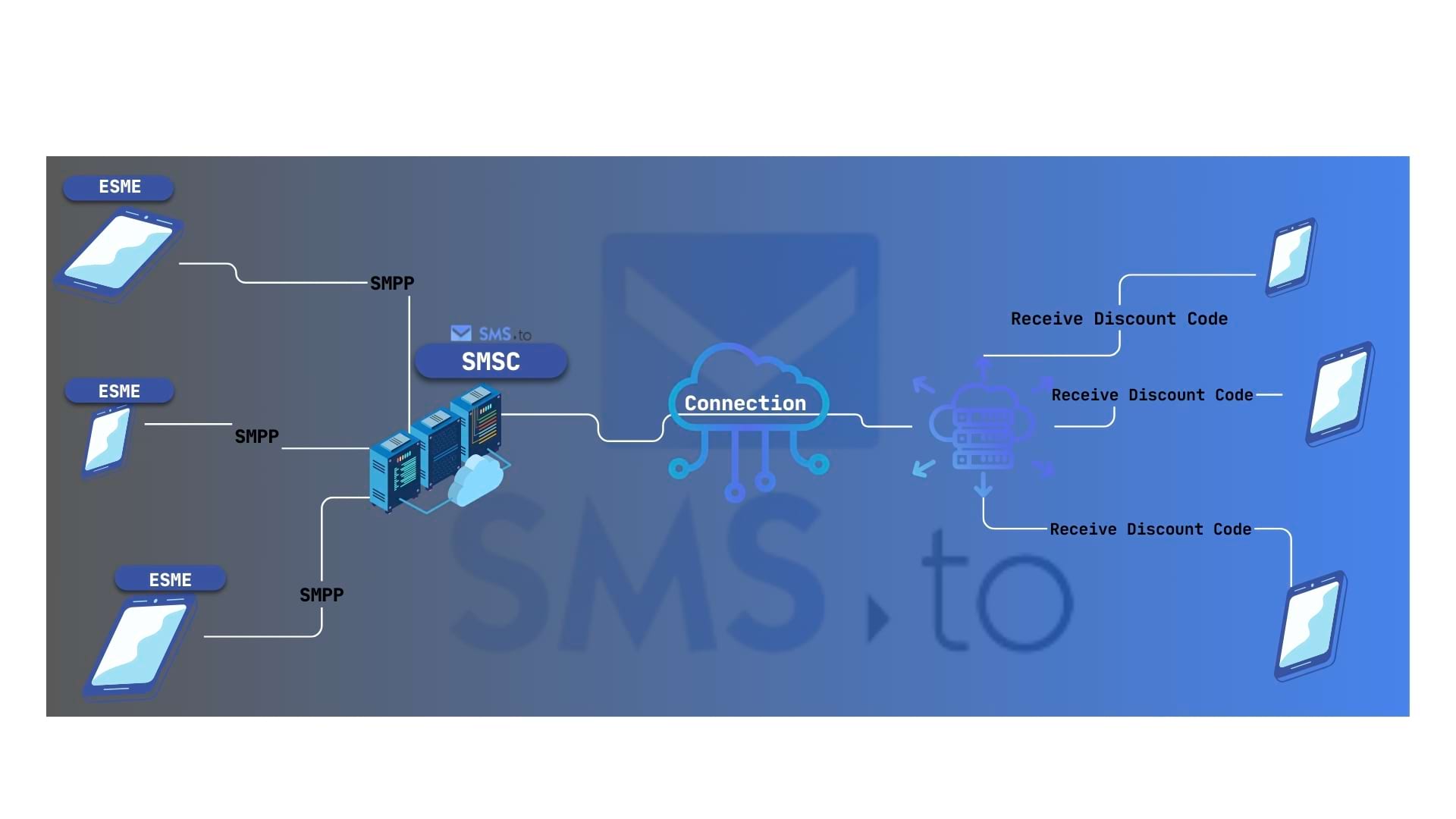
Bạn yêu cầu giảm giá : Bạn chạm vào “Gửi cho tôi mức giảm giá!” trong ứng dụng.

Liên hệ ứng dụng SMSC : Ứng dụng của quán cà phê, hoạt động như một ESME, sử dụng SMPP để gửi yêu cầu của bạn đến SMSC của mạng di động.

SMSC gửi tin nhắn SMS của bạn : SMSC nhận được yêu cầu và gửi tin nhắn văn bản có mã giảm giá đến điện thoại của bạn.

Bạn nhận được tin nhắn SMS giảm giá : Điện thoại của bạn nhận được tin nhắn với mã giảm giá cho ly cà phê!

(HÌNH ẢNH MINH HỌA)



Có những nguy cơ bất thường là:

-Các vấn đề và lỗi kết nối : Trong quá trình truyền tin nhắn từ nhà mạng này sang nhà mạng khác, có thể có những sự cố có thể gây trở ngại cho quá trình này. Những sự cố này xuất hiện dưới dạng lỗi như số lượng từ SMS vượt quá hoặc người nhận không hợp lệ.

Ngoài ra, giao thức SMPP không phù hợp với kết nối công cộng. Sử dụng mạng công cộng để gửi tin nhắn SMS bằng giao thức SMPP sẽ ngăn chặn mức độ bảo mật và kiểm soát thường được yêu cầu đối với các ứng dụng nhắn tin cấp doanh nghiệp hoặc cấp độ quan trọng.

Để tránh lỗi SMPP, hãy đảm bảo bạn nhập đúng ID cho người nhận và không vượt quá giới hạn số lượng từ. Ngoài ra, bạn nên sử dụng kết nối riêng tư chuyên dụng khi thiết lập giao thức SMS SMPP để đảm bảo kết nối ổn định.

-Chọn nhà cung cấp SMPP phù hợp : Một trong những vấn đề thường gặp mà doanh nghiệp gặp phải khi sử dụng SMPP là chọn nhà cung cấp SMS SMPP tốt.

Quá trình này rất quan trọng vì nhà cung cấp của bạn sẽ quyết định mức độ hiệu quả của quá trình truyền tải tin nhắn.

Vì vậy, khi chọn nhà cung cấp dịch vụ SMS SMPP số lượng lớn, bạn nên cân nhắc phiên bản họ sử dụng và ngân sách của bạn. Bạn cũng nên cân nhắc số lượng tin nhắn bạn có thể gửi bằng phần mềm SMPP số lượng lớn mỗi giây.

-Mối lo ngại tiềm ẩn về bảo mật : Mặc dù giao thức SMPP không được trang bị cấu trúc bảo mật , bạn vẫn có thể thiết lập các biện pháp để đảm bảo tin nhắn của mình được an toàn.

Ví dụ, bạn có thể tích hợp SMPP với Transport Layer Security (TLS), một kênh mã hóa đảm bảo tính riêng tư và toàn vẹn của tin nhắn.

TLS bao gồm một cơ chế xác thực máy chủ, giúp các máy khách SMPP xác minh danh tính của máy chủ mà chúng đang kết nối. Điều này ngăn chặn các cuộc tấn công trung gian, trong đó kẻ tấn công mạo danh máy chủ SMPP để chặn hoặc thao túng tin nhắn. Xác thực máy chủ dựa trên các chứng chỉ kỹ thuật số do các cơ quan cấp chứng chỉ (CA) đáng tin cậy cấp.

-Vấn đề về hiệu suất:

**Quá tải hệ thống**: Nếu ESME gửi quá nhiều tin nhắn cùng lúc mà không tuân theo giới hạn "window size" của SMPP, SMSC có thể từ chối hoặc trì hoãn xử lý.

**Độ trễ cao**: Khi mạng chậm hoặc SMSC xử lý không kịp, tin nhắn có thể bị giao chậm, ảnh hưởng đến trải nghiệm người dùng.

-Lỗi xử lý tin nhắn: Nếu SMSC hoặc ESME không quản lý tốt Message\_ID, tin nhắn có thể gửi hoặc nhận nhiều lần.; Trong trường hợp SMSC bị lỗi hoặc magj không ổn định, tin nhắn có thể bị rơi mà ko có thông báo; Với tin nhắn dài nếu không cấu hình đúng nội dung có thể bị cắt xén hoặc hiển thị sai.

-Rủi ro pháp lý và tuân thủ: Nếu ESME gửi SMS spam hoặc nội dung vi phạm pháp luật hệ thống có thể bị phạt ; Một số quốc gia yêu cầu lưu trữ tin nhắn để kiểm tra. Nếu không tuân thủ, có thể gặp rủi ro.