ИЗПОЛЗВАНЕ НА IP ПРЕНОСНА СРЕДА ЗА CSS7 СИГНАЛИЗАЦИЯ.

проф. Маргарита Петкова, Дана Жечева – НБУ

mpetkova@nbu.bg

CSS7 SIGNALLING OVER IP TRANSPORT MEDIA

prof. Margarita Petkova, Dana Jecheva – NBU

mpetkova@nbu.bg

Key words: *SIGTRAN, IP – TDM networks, NGN signalling*

The presentation considers convergence between IP and TDM networks especially new protocols and standards for provision their inter working. The attention is paid to the family of protocols SIGTRAN and Cisco protocols Backhaul protocol and Reliable UDP.

It is specifies the necessity for implementation of such solution as well as its advantages and disadvantages. The approaches for solution of the problems in the transition from TDM to NGN networks and technologies are considered too.

The basic elements of SIGTRAN architecture are defined: MGC–Media Gateway Controller, SG–Signaling Gateway ,MG–Media Gateway, IP SCP, IP telephone and other types of IP terminals.

Functionality of SIGTRAN is described further – flow control, identification, error recognition and error correction.

Security problems are considered too – authentication, integrity, confidentiality, availability.

The transport of MTP over IP networks and the respective protocols used are explained at the end.

Ключови думи: *SIGTRAN, IP – TDM мрежи, NGN сигнализации*

Докладът разглежда конвергенцията на IP и TDM мрежите и новите протоколи и стандарти, възникнали за да се осигури съвместната им работа. По-конкретно се разглеждат фамилията от протоколи SIGTRAN и дефинираните от Cisco протоколи Backhaul protocol и Reliable UDP.

Систематизират се необходимостта от прилагане на такова решение, както и предимствата и недостатъците до които води то, след което се разглеждат начините за решаване на възникналите проблеми при прехода към новата технология.

Дефинират се основните елементи на SIGTRAN архитектурата: MGC–Media Gateway Controller, SG–Signaling Gateway, MG–Media Gateway, IP SCP, IP телефон и/или друг вид терминал.

Понататък е описана функционалнотсса на този протокол – контрол на потока, идентификация, разпознаване и корекция на грешките.

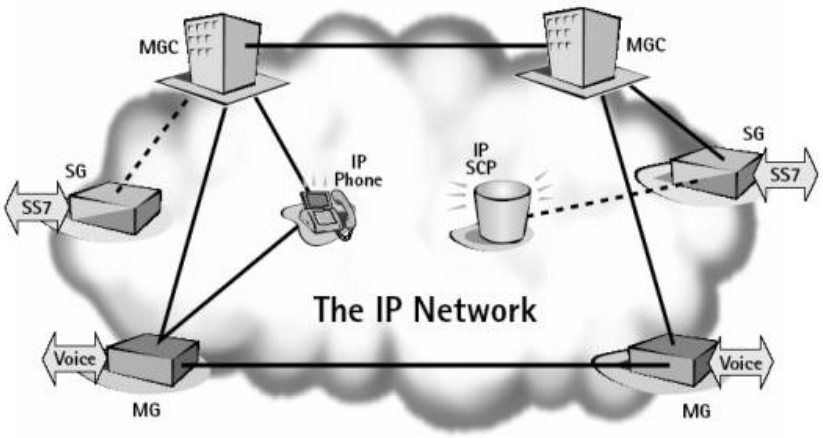
Разгледани са също проблемите на сигурността – автентификация, интнегритет, конфиденциалност, достъпност.

1. SIGTRAN – Понятие и основни елементи

SIGTRAN е име на работна група на IETF, дефинирала спецификациите на семейство от протоколи, най-значим от които е Stream Control Transmission Protocol (SCTP), използван за пренос на PSTN сигнализацията SS7 през IP мрежите (фиг.1).

Основните елементи на SIGTRAN архитектурата са:

- Контролерът на медийните шлюзове MGC (Media Gateway Controller), отговорен за контрола на посредничеството между сигналния шлюз SG и медийния шлюз MG и контролиращ двупосочно достъпа между IP частта и PSTN
- Сигналният шлюз SG (Signaling Gateway), отговорен за връзката по посока към SS7 мрежата и за предаването на сигнални съобщения към IP частта.
- Медийният шлюз MG (Media Gateway), отговорен за пакетирането на гласовия трафик и предаването му през IP мрежата към местоназначението.
- IP ориентираният мъзел за управление на интелигентни услуги IP SCP (IP-enabled Service Control Point), съществуващ в IP мрежата, но адресируем от SS7 мрежата.
- IP телефони и/или друг вид терминали.



Фигура 1

SIGTRAN протоколите специфицират начините за конвертиране и надеждното транспортиране на SS7 сигналните съобщения през IP мрежите. Архитектурата дефинира два основни компонента:

- **транспортен протокол**, който отговаря за преноса на SS7 слоя и
- **адаптивен модул**, който емулира долните слоеве на протокола.

Например, ако основен протокол на трето ниво е MTP (Message Transport Protocol), SIGTRAN протоколите предоставят еквивалентна функционалност на MTP второ ниво. Ако основен протокол е ISUP или SCCP, SIGTRAN протоколите предоставят същата функционалност на MTP нива 2 и 3.

2. Функционалност на SIGTRAN протоколите

SIGTRAN протоколите предоставят функционалност, необходима за поддържането на сигнализацията по общ канал SS7 през IP мрежите [1].

Тази функционалност включва:

- контрол на потока;
- последователен пренос на сигнални съобщения в единичния контролен поток;
- идентификация на пораждащата и терминиращата сигнала точки;
- идентификация на гласовите трасета;
- откриване и коригиране на грешки;
- възстановяване при прекъсване на междинните компоненти по трасето;
- контрол за избягване на претоварването на мрежата;
- контрол на състоянието на съседните възли (достъпен, недостъпен, неработещ и т.н.);
- поддръжка на механизми за сигурност и защита на цялостта на сигнализиращата информация;
- разширения, които да подпомагат сигурността и евентуални бъдещи изисквания.

Изисквания, налагани от нискочестотните SS7 мрежи, като например необходимостта от сегментиране и реасемблиране на съобщения, по-големи от 272 байта, не са приложими в IP мрежите и затова не се поддържат от SIGTRAN протоколите.

Производителността при преноса на SS7 съобщения през IP мрежите е от критична важност. Ето защо на база на ITU SS7/C7 стандартите и потребителските очаквания са наложени строги изисквания към този параметър. Например, докато ITU стандартът специфицира, че изграждането на връзката от край до край не

може да превишава 20 до 30 секунди след началното изпращане на началното адресно съобщение за ISUP (IAM), то потребителите изискват доста по-кратки времена за отговор и по-бързи комуникации. Поради тази причина VoIP мрежите трябва да бъдат проектирани така, че да задоволяват напълно потребителските нужди и очаквания, както и ITU стандартите за производителност.

3. Сигурност при пренос на сигнализацията

Освен за производителност към преноса на SS7 сигнални съобщения през IP мрежите, изисквания има и към сигурността при пренасянето на информацията [3].

Ако сигналните съобщения се транспортират през частен Интернет, трябва да бъдат приложени необходимите мерки за сигурност, изисквани от мрежовия оператор. За сигнализиращи съобщения, пренасяни през обществената част на Интернет, използването на методи за защита е препоръчително, но не и задължително.

Съществуват няколко механизми за защита, използвани в IP мрежите. За пренос на сигнализираща информация през Интернет работната група SIGTRAN препоръчва използването на IP механизъм за сигурност (IPSEC).

IPSEC предоставя следните услуги за сигурност:

- ***Автентификация*** (authentication) - гарантира, че информацията е изпратена от/към точно определен доверен потребител.
- ***Интегритет*** (integrity): гарантира, че информацията не е била модифицирана или частично загубена докато пътува между потребителите.
- ***Конфиденциалност*** (Confidentiality): транспортираната информация е криптирана, за да се избегне неоторизиран достъп до нея.
- ***Достъпност*** (availability): осигурява работоспособността на крайните потребители дори при атаки към тях от неоторизирани потребители.

SIGTRAN не дефинира нови механизми за сигурност, тъй като съществуващите вече методи за защита на инаформацията се смятат за достатъчно надеждни и сигурни при пренос на SS7 сигнални съобщения през IP мрежите

4. Транспортиране на MTP през IP мрежите

За транспортиране на MTP съобщения през SS7/IP мрежите ITU специфицира следните изисквания [4]:

- MTP ниво 3 peer-to-peer процедурите изискват време за отговор от 0,5 до 1,2 секунди;

- не повече от 1 на 10 млрд. съобщения да бъде транспортирано грешно (не на време, не в правилната последователност), загубено по време на преноса или да съдържа грешка;
- максимален downtime 10 минути на година, или по-малко, което означава 99,9998% наличност на сигнално трасе;
- дължината на съобщението е 272 байта при нискочестотните SS7 и 4091 байта при високочестотните, широколентови SS7.

За да се постигне необходимата функционалност и производителност при пренасянето на SS7 сигнализация през IP мрежата, работната група SIGTRAN препоръчва три нови протокола - M2UA, M2PA, и M3UA (фиг. 1) [2].

4.1. Протокол M2UA

Дефинираният от SIGTRAN протокол M2UA за транспортиране на MTP3 сигнални съобщения през IP мрежите използва Протокола за упрвление пренасяния поток SCTP (Stream Control Transmission Protocol). Протоколът M2UA предоставя на потребителите същите услуги каквито предоставя в SS7 ниво MTP2 към MTP3.

M2UA се използва между сигналния шлюз и контролера на медийните шлюзове в IP мрежите. Сигналният шлюз SG получава от Възела за управление на интелигентните услуги SCP в PSTN частта SS7 съобщения през нива MTP1 и MTP2, след което транспортира съобщенията на ниво MTP3 и нагоре към Медийния контролер MGC или към друга IP крайна точка, използвайки протокола M2UA.

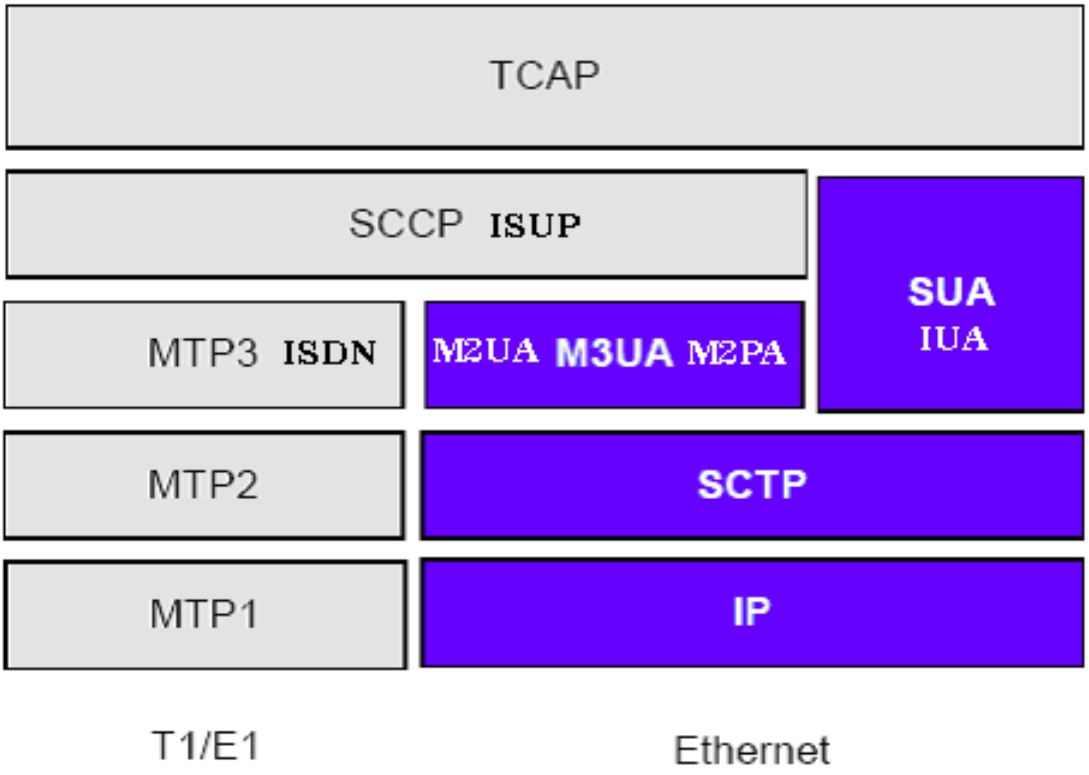
4.2. Протокол M2PA

Протоколът M2PA, аналогично на M2UA, транспортира SS7 MTP2 сигнални съобщения през IP, използвайки SCTP. Разликата е, че M2PA поддържа пълно уравление на съобщенията между които и да е два SS7 възела, комуникиращи през IP мрежа.

4.3. Протокол M3UA

Протоколът M3UA е дефиниран от SIGTRAN за транспорт на MTP3 сигнални съобщения през IP мрежите. Протоколи като TCAP и RANAP, подсигуряващи въвеждането на съвременни приложения за мобилни и интелигентни мрежи в сигнализацията по общ канал, могат да бъдат пренасяни от SCCP на SS7, използвайки M3UA или SIGTRAN протокола, наречен SUA.

Протоколът M3UA се използва между сигналния шлюз и контролера SGM или към базите от данни за IP телефония. Той разширява достъпа на сигналния шлюз до услугите на ниво MTP3 и до отдалечените IP крайни точки. Ако IP крайна точка е свързана към повече от един сигнален шлюз, M3UA слоят в IP крайната точка определя статуса на конфигурираните за SS7 дестинациите и маршрутизира съобщенията според наличността на ресурси и натовареността на трасетата към тези дестинации през всеки сигнален шлюз.



Фигура 2

ЗАКЛЮЧЕНИЕ

Бързият преход, с който се преобразуват основните транспортни мрежи за работа в IP среда, наложен от икономически съображения в изключително конкурентния телекомуникационен пазар и очертаващия се продължителен период на съществуване на цифрови TDM мрежи (фиксирани и мобилни), предрагащи основните услуги за масовия потребител (телефония и нискоскоростни данни) налагат бързото усъвършенстване и ускорено прилагане на серията от SIGTRAN протоколи.

REFERENCES

[1] "SS& over IP Signalling Transport & SCTP", Web Pro Forum Tutorial, www.iec.org

[2] "SS7/IPInterworking Tutorial – Signalling", 2006

[3] Jim Darroch, "Introduction to SIGTRAN£, , *www.analogzone.com*

[4] Jonathan Lennox, Henning Schulzrinne, Feature Interaction in Internet Telephony, Colombia University