Átvitelvezérlés és vezérelt átvitel az NGN-ben

KANÁSZ-NAGY LAJOS

Magyar Telekom PKI Távközlésfejlesztési Igazgatóság
kanasz.nagy.lajos@t-com.hu

Kulcsszavak: NGN átvitel, átvitelvezérlés, NASS, RACS, hozzáférés-vezérlés, QoS-vezérlés

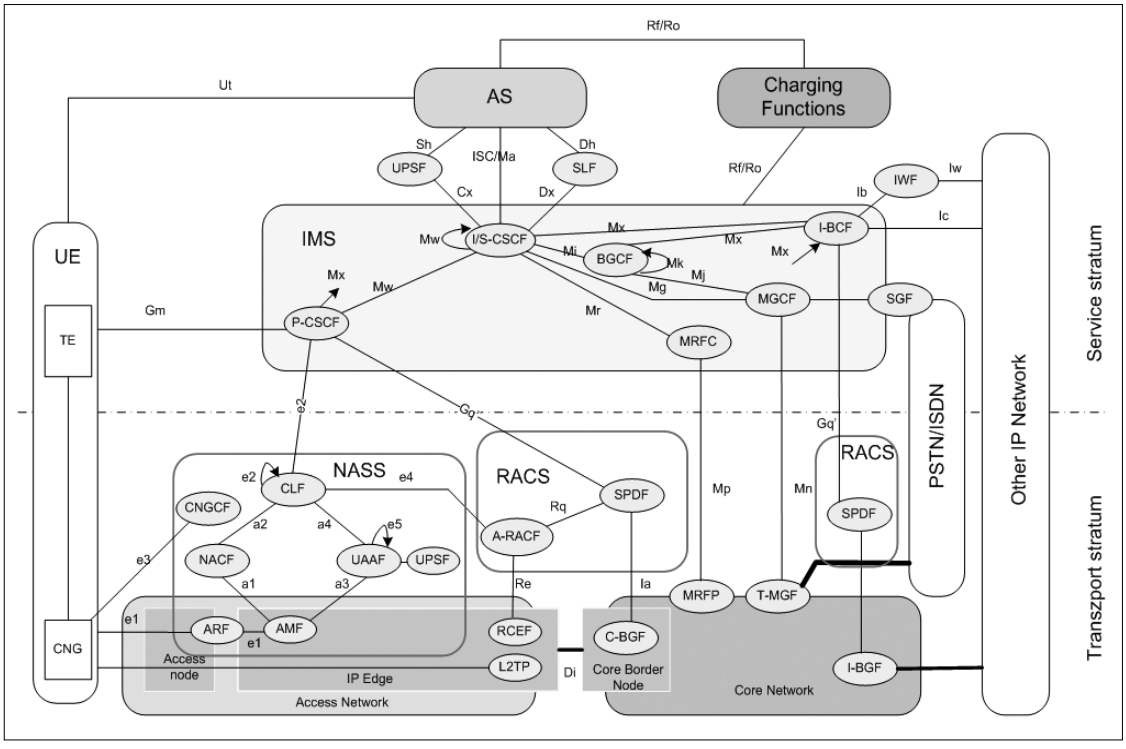
A teljes kiépítésű IMS alapú NGN multimédia szolgáltatásokat képes nyújtani szolgáltatói garanciákkal, különböző nagy adatátviteli sebességű elérési technológiákon. A változatos szolgáltatások tetszőleges kombinációja megköveteli a hálózat átviteli képességeinek dinamikus vezérlését. Ennek megvalósításához hatékony átvitelvezérlésre és vezérelt átviteli hálózatra van szükség. A cikk betekintést nyújt az NGN transzport vezérlő architektúrába és a megvalósítás egyes elveibe a témában megjelent szabványok tükrében.

1. Bevezető

Az NGN (Next Generation Network) több éve témája a szakmai sajtónak. Kezdetben a beszédátvitel IP hálózaton történő megvalósítása volt a fejlesztések célja. A távközlési szolgáltatók számára azonban az Internet, a mobil és a kábeltévé piac szorításában egy új, multimédiát, mobilitást, valósidejű alkalmazásokat is kiszolgáló, rugalmas szolgáltatás- és alkalmazásfejlesztést támogató rendszer vált szükségessé a kiépült nagy adatátviteli sebességű elérési hálózatokon. Az áttörést a 3GPP által szabványosított, az UMTS platformra fejlesztett IMS alrendszer jelentette. Az IMS vált az NGN általános célú szolgáltatásvezérlő alrendszerévé, mivel a fejlesztők célkitűzései megegyeztek TISPAN NGN fejlesztési céljaival, lehetővé téve a fix-mobil konvergenciát.

Az IMS alapú NGN több viszonylat (session) egyidejű felépítését nyújtja, melyek átviteli minőségét, biztonságát a transzportvezérlés biztosítja. Az NGN szolgáltatás és transzport vezérlő alrendszereivel, dinamikus erőforrás felhasználásával lehetővé teszi valamennyi ma ismert technológiafüggő szolgáltatás nyújtását (pl. 3Play), de azok kombinációit is egy-egy alkalmazáson belül. A variációs lehetőségek számát nehéz megbecsülni.

Az NGN-ben a *service stratum* (alkalmazási réteg, szolgáltatásvezérlés és a hozzájuk rendelhető felhasználói és üzemeltetési síkok) és a *transport stratum* (transzportvezérlés vagy más néven átvitelvezérlés, és a hozzárendelhető felhasználói és üzemeltetési síkok) elkülönülnek egymástól, külön fejlődési lehetőséget biztosítva a két stratum-nak.



1. ábra
TISPAN NGN architektúra
ES 282 007,
ES 282 003,
ES 282 004
felhasználásával

Rövidítések

AF	Application Function
AKA	Authentication and Key Agreement
A-RACF	Access-Resource and Admission Control Function
ASP	Application Service Provider
BGF	Border Gateway Function
BGS	Border Gateway Services
C-BGF	Core Border Gateway Function
CCI	Charging Correlation Information
CLF	Connectivity session Location and repository Function
CPE	Customer Premises Equipment (i.e. (routed) modem, residential gateway, integrated access device)
CSCF	Call Session Control Function
DiffServ	Differentiated Services
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Service Code Point
EAP	Extensible Authentication Protocol
FR	Frame Relay
I-BCF	Interconnection Border Control Function
I-BGF	Interconnection Board Gateway Function
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
L2TF	Layer 2 Termination Function
LSP	Label Switched Path
MPLS	Multi Protocol Label Switching
NA(P)T	Network Address and optional Port Translation
NASS	Network Attachment Sub-system
NAT	Network Address Translation
P-CSCF	Proxy-CSCF
PDF	Policy Decision Function
PPP	Point to Point Protocol
RACS	Resource and Admission Control Subsystem
RCEF	Resource Control Enforcement Function
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SBP	Service Based Policy control
SDP	Session Description Protocol
SIM	Subscriber Identification Module
SIP	Session Initiation Protocol
SPDF	Service-based Policy Decision Function
TCP	Transmission Control Protocol
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
UDP	User Datagram Protocol
UE	User Equipment
UNI	User-to-Network Interface
USIM	UMTS Subscriber Identification Module

Az NGN kibontakozásához, az NGN-hez fűzött elképzelések megvalósításához elengedhetetlen annak a transzportnak a megvalósítása, mely képes értelmezni és végrehajtani az alkalmazásokhoz szükséges, a szolgáltatásvezérlés által igényelt minőségű átvitelt. Ehhez szükséges az egy végponthoz kapcsolható párhuzamos kapcsolatok dinamikus QoS vezérlése. A TISPAN architektúrában *(1. ábra)* ezt a funkciót az RACS valósítja meg.

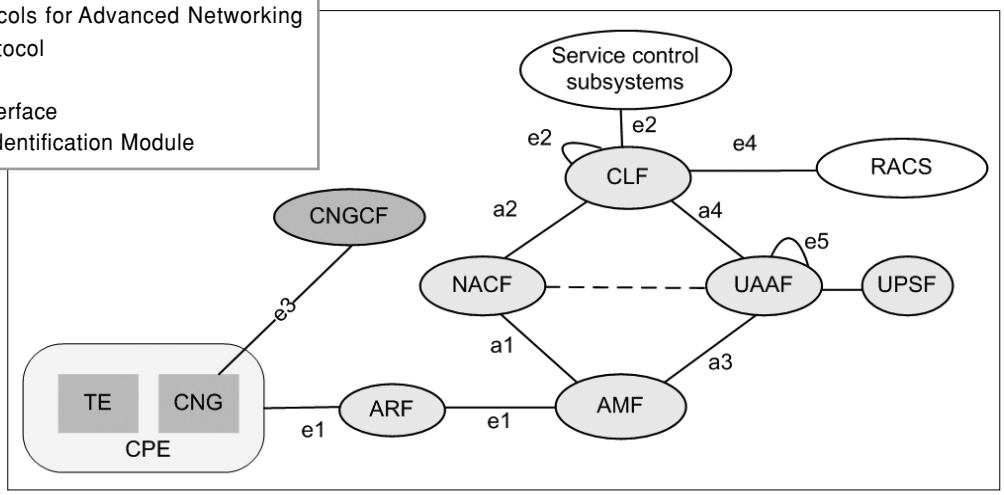
Az NGN multimédia képessége együtt jár azzal, hogy az NGN platform különböző felhasználói (user) igényeket elégít ki, ezért a felhasználókat profiljaik alapján meg kell különböztetni. A felhasználói profilok mind a transzport-, mind pedig a service stratum-ban eltérőek lehetnek, ennek megfelelően mindkét stratum-ban a felhasználókat, előfizetőket autentikálni, erőforrásokhoz való hozzáférésüket szabályozni szükséges. Az NGN transzport hozzáférés-vezérlését az NASS valósítja meg.

A cikk a transzport (átvitel)-vezérlés és a vezérelt transzport (átvitel) egyes megvalósítási elveibe kíván betekintést nyújtani a szabványosítás eddigi eredményei alapján.

2. Hozzáférés-vezérlés (NASS)

A hálózati erőforrások hozzáférésének ellenőrzése jelentős szerepet játszik az NGN-ben, hiszen az elérhető transzport képességek széles skálájához fér hozzá az a felhasználó, aki sikeresen regisztrált. Igen fontos, hogy ezt a többszörös képességekkel rendelkező transzport esetén hatékonyan tegyük.

Az NASS architektúrát több elérési technológia, a mobilitás, az említett multimédia képességek figyelembevételével fejlesztették *(2. ábra)*. A funkcióiba beletartozik az eszköz és a felhasználó autentikációja, a végberendezés transzporthálózati felhasználói profiljának kijelölése, a hálózati jogosultságainak megadása, konfigurálása. A NASS a végberendezés helyére, az access tulajdonságaira vonatkozó aktuális adatokat és (a felhasználó hálózati jogosultságait tartalmazó) profil adatokat ad át a szolgáltatásvezérlés (e2 interfész) és az RACS (e4 interfész) számára.



2. ábra
TISPAN NASS architektúra

A CLF adatok NACF és UAAF által történő feltöltésével az UE és a felhasználó transzporthálózati regisztrációja megtörténik. Az NGN működése és biztonsága szempontjából alapvető követelmény, hogy az NASS regisztráció után a felhasználónak csak szolgáltatásvezérlővel, esetleg alkalmazásszerverekkel való kommunikációra legyen jogosultsága.

Hívásfelépítésre, távközlési szolgáltatások igénybevételére csak a szolgáltatás szintű regisztráció után szerezhet jogosultságot. A szolgáltatás minőségéért és biztonságáért csak ezen az úton vállalhat garanciákat az NGN-szolgáltató.

2.1 Az NASS felépítése és működése

Access Relay Function (ARF)

Az ARF e1 interfészt valósít meg az UE felé. Helyi hálózati szintű információkat fűz be UE és az NASS kommunikációjába. Az UE rajta keresztül kap hálózati konfigurációs paramétereket. Részletes működését lásd később.

Access Management Function (AMF)

Az AMF menedzseli az UE autentikációs és hálózati konfigurációs folyamatait. Az AMF fordítja le az UE által kibocsátott kéréseket, melyek lehetnek IP-cím allokációs kérések az NACF felé, vagy autentikációs kérések az UAAF felé. Az UAAF azonosítása, majd engedélyezése alapján az AMF hálózati hozzáférést engedélyez az UE számára. A részletes működés később kerül tárgyalásra.

User Access Authorization Function (UAAF)

Az UAAF hajtja végre a felhasználó authentikációját, jogosultságának ellenőrzését. Az azonosítást a hálózati hozzáférést leíró felhasználói profilok alapján hajtja végre, melyeket a PDBF-ből (Profile Data Base Function) hív le. Az UAAF a PDBF rekordokból számlázási alapadatokat is megad a CLF számára (például magas havidíj esetén a forgalmidíj-számlázás súlyozása alacsonyabb lehet, mint alacsony havidíj esetén).

Az UAAF több authentikációs eljárást is támogat. Transzport szintű megvalósításából következően azon hordozó protokollok jöhetnek számításba, melyek L2 szinten működnek. Az a3 referenciaponton megengedhető a RADIUS [14] protokoll, az a4 ponton Diameter [15] implementálása szükséges.

Megjegyzés: az UAAF és PDBF lehetőséget ad a tanúsítványalapú azonosításra és feljogosításra [2,4].

Az authentikációs protokollok (EAP) képesek az egyed-tanúsítvány alapú azonosításának „lebonyolítására”. Minden egyed tanúsítványhoz hozzáfűzhető több attribútum-tanúsítvány [17], melyek érvényessége eltérő időkhöz kötött és elsősorban az entitáshoz rendelhető jogosultságokat írják le. Az attribútum-tanúsítványokat az egyed-tanúsítvány alapján a szolgáltatást nyújtó szervezet bocsáthatja ki. A PDBF attribútum-tanúsítványokban is tartalmazhatja azokat az információkat, melyek a felhasználó és végberendezése hálózati csatlakozását leírják. A megoldás kidolgozása a gyártókon múlik. Az [6] szabvány tárgyalja az attribútum-tanúsítvány és az egyed-tanúsítvány kapcsolatát.

Roaming esetén az UAAF proxy-ként működik.

Profile Database Function (PDBF)

A PDBF funkcionális egység tartalmazza a felhasználó authentikációs adatait (UID, a támogatott authentikációs eljárások listáját, kulcselemeket stb.) és információkat a hálózati elérés konfigurációjára, valamint díjazására vonatkozóan. Ezen információkat a felhasználó és a transzportszolgáltató közötti szerződés határozza meg. Mindezt felhasználói hálózati profilnak (User Network Profile) nevezi a szabvány.

Megjegyzés: A PDBF-UAAF interfész egyelőre nem szabványosított.

Network Access Configuration Function (NACF)

Az NACF felelős az IP címek UE-hez rendeléséért, lefoglalásáért, továbbá hálózati paramétereket is megad az UE részére, például a DNS szerverek IP címét, a jelzés proxy címét stb. Az NACF egyedi access hálózati azonosítóval látja el az UE-t.

Az NACF implementációja lehet DHCP vagy RADIUS szerver alapú, azzal a kiegészítéssel, hogy a szerver a felhasználó hálózati konfigurációs adatait Diameter protokollon legyen képes továbbítani a CLF felé. Mindazonáltal a távközlési berendezés szállítók dolgoznak az NASS feladataira optimalizált implementációkon. Az a1 referenciaponton megengedhető a RADIUS protokoll, a2 ponton azonban Diameter implementálása szükséges.

Connectivity Session Location and Repository Function (CLF)

A CLF rögzíti az UE-hez rendelt IP cím és a vonatkozó helyi hálózati információk kapcsolatát, például az elérési hálózati eszközök azonosítóit, IP port azonosítót stb., valamint a helyi hálózati információk (Line ID) és a földrajzi információk kapcsolatát (NACF-től kapott adatok).

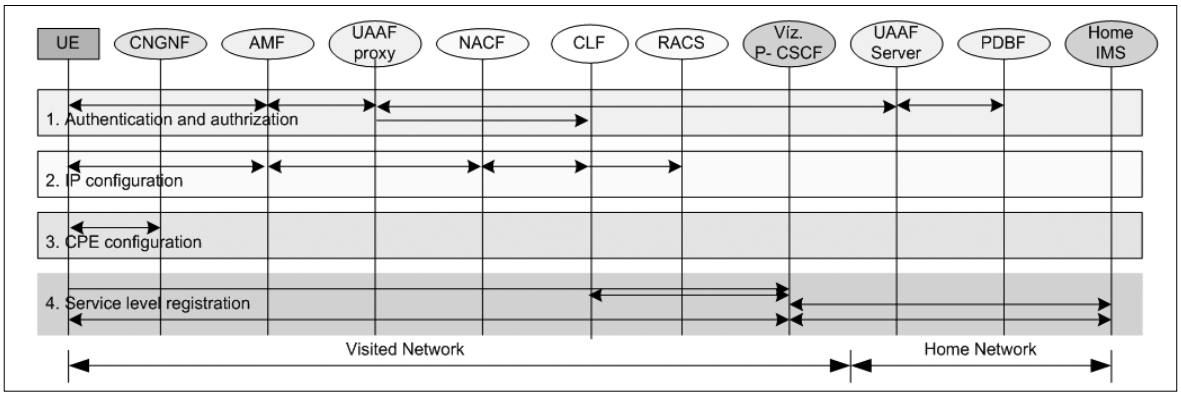
A CLF tárolja a jogosult felhasználó/UE azonosító adatait is, valamint hálózati QoS profilját és a felhasználó rögzített igényeit a helymeghatározó információkra vonatkozón (UAAF-től kapja). A CLF az NACF-től és az UAAF-től kapott információkat egy logikai elérési hálózati azonosító (Logical Access ID) alapján tudja összekapcsolni.

CNG Configuration Function (CNGCF)

A CNGCF-t a CNG inicializálását, illetve frissítését végzi. A CNGCF olyan konfigurációs információt nyújt a CNG-nek, mint például a CNG-n belüli tűzfal konfiguráció, vagy az IP csomagok QoS jelölésével kapcsolatos információk stb. Ezek az adatok különböznek az NACF által nyújtott hálózati konfigurációs adatoktól.

Az NASS működése

Az NASS működését a *3. ábrán* követhetjük végig.



3. ábra NASS és IMS regisztráció fő lépései

Az első fázis az autentikáció, az ütemdiagram a roaming esetén lejátszódó folyamatot ábrázolja. Miután a látogatott hálózatba bejelentkező eszköz autentikálta magát a honos hálózatban, a honos hálózat UAAF-je megküldi a látogatott hálózattal szerződésben egyeztetett, és a felhasználóra vonatkozó profil adatokat. A látogatott hálózat UAAF-je ezután bejegyzi a felhasználót a helyi CLF-be, majd nyugtát küld az AMF-nek és azon keresztül az UE-nek a hálózati konfigurációs fázis indítására. A hálózati konfigurációs fázis az UE és az NACF között zajlik az ARF és AMF közreműködésével. A CNG konfigurációjára, illetve szolgáltatás szintű regisztrációra csak az első két fázis után kerülhet sor.

2.2. Az NASS vezérlés végrehajtó elemei transzport eszközökben

Látható, hogy az ARF és az AMF része az NASS logikai rendszerének, megvalósítás szempontjából a transzporthálózat csomóponti elemeiben szerepelnek.

Az ismertetett NASS elemek hálózati eszközökben megjelenő elemei különböző elérési technológiákban más és más megvalósításban szerepelnek. Az NASS hálózati eszközökben megvalósítandó funkcionális elemeinek működését Ethernet-protokoll esetére vizsgáljuk.

Az e1 interfész szerepének áttekintése

Az TISPAN NASS architektúrája látogatott és honos hálózatra általánosan a *4. ábra* szerinti. A látogatott hálózat NASS kapcsolata a honos hálózattal az e5-ös interfészen lehetséges.

Az UE a hozzáférési hálózathoz e1 interfészen kapcsolódik. UE e1-en keresztül kérhet hitelesítést és jogosultságot a hozzáféréshez, valamint hálózati konfigurációt, azaz ezen keresztül kaphat IP címet és a hálózati kiszolgálók IP címeit (DNS, P-CSCF stb.). Az UE szemszögéből nézve az IP edge rendelkezik egy ARF funkcionalitással, ami az UAAF-el és az NACF-fel tart kapcsolatot az AMF-en keresztül. Valójában UE kéréseket (ARF-en keresztül) az AMF fogadja és ülteti át Diameter, vagy RADIUS protokoll elemekre.

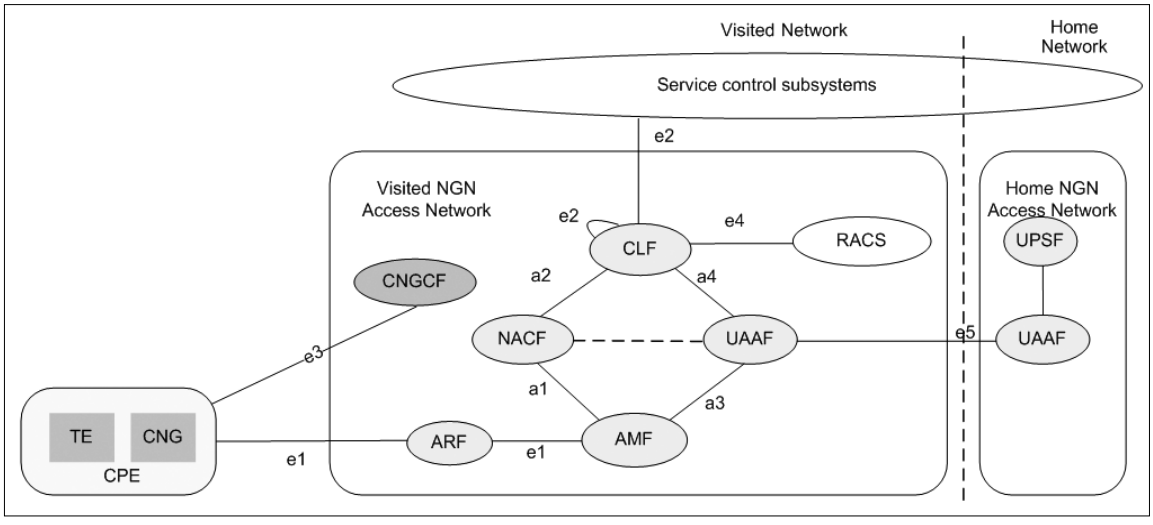
A TISPAN NGN architektúrában az ARF a helyi hurok információ megadásáért felelős. Nem módosítva az UE kérést, a helyi hurok információt beleszerkeszti a PPP vagy a DHCP protokollba. Az e1 interfészen történik az UE és a hálózat kölcsönös autentikációja. Sikeres autentikáció esetén az AMF engedélyezi, ellenkező esetben letiltja az UE hálózati elérését.

A következő fejezetek a 3. ábra szerinti folyamatokat tárgyalják Ethernet-hálózatokra.

2.2.1. Autentikációs fázis Ethernet elérési hálózatokban

Alapműködés

Az Ethernet-hálózatokban az autentikációs adatcserét lebonyolító protokollt az IEEE 802.1x szabvány írja le. Ez a protokoll az EAPoL (Extensible Authentication Protocol over LAN), ami az EAP üzenetek lebonyolítását végzi a hozzáférési hálózatban.



4. ábra NASS roaming eset

A 802.1x 3 olyan funkcionalitásokat definiál, amelyek az autentikációs és autorizációs eljárásokat végzik. Ezek a következők:

- **Supplicant:** ezt a funkciót abban az eszközben kell megvalósítani, ami a csatlakozni kíván a hálózathoz access-csomóponti eszközön keresztül. A Supplicant autentikáció esetén username/password, certificate, token stb. típusú „igazolvánnyal" (credentials) azonosítja magát a hálózatban.
- Az **Authenticator** funkciót az access node valósítja meg az access-vezérlés felügyeletével: engedélyezi, vagy visszautasítja a hálózati hozzáférést. Az elnevezés elgondolkoztató, mivel a funkció inkább a jogosultságkezeléshez áll közelebb, az autentikációs protokollokat sem ez a funkció végződteti, azokra transzparens. A használó felől viszont csak ez a funkcionalitás látható.
- Az **Authentication Server** pedig hitelesítéssel és a jogosultság engedélyezésével kapcsolatos döntéseket hozza meg. Az autentikációs szerver magában foglalja az eléréséhez szükséges proxy funkciókat is.

A TISPAN NGN architektúra elemeivel való kapcsolatot az *5. ábra* szemlélteti. Ahogy az ábrán látható, az UE és az ARF/AMF (Authenticator) közötti az EAP üzeneteket az EAPoL, míg az AMF és az UAAF közöttit RADIUS, vagy Diameter protokoll szállítja. Itt az Authenticator „csomagolja át" az UE-től EAPoL-on érkező EAP üzeneteket az UAAF-hez küldendő RADIUS vagy Diameter alapú EAP üzenetekké. A kapcsolatban több proxy is részt vehet.

RADIUS vagy Diameter

Mindkét protokoll hálózati elemek közötti biztonsági protokoll. A RADIUS-t Internet AAA szerverek elérésére fejlesztették ki, kliens-szerver kapcsolatot tesz lehetővé. Az AAA szerver-t RADIUS szerverként is nevezik.

Az NGN számára azonban korlátot jelent, hogy nincs visszaigazolás az üzenetekről és nem tud peer-to-peer üzemmódban működni. Ezért az NGN vezérlő rendszerében a hálózati eszközök közötti biztonsági kommunikációra a Diameter-t specifikálták kiküszöbölendő az említett hibákat.

Az NGN-ben csak azokon a helyeken engedhető meg a RADIUS alkalmazása, ahol a kliens-szerver típusú működés van. A RADIUS kapcsolatoknak ugyanakkor meg kell felelnie a távközlési hálózatokra előírt magas rendelkezésreállási igényeknek, ezért a RADIUS-t hordozó hálózatot jóval magasabb megbízhatóságúra kell méretezni, mint a Diameter alkalmazása esetén.

Az EAP-ról röviden

Az Extesible Authentication Protocol [10] jelentősége abban áll az NGN transzport szintű autentikációban, hogy a hordozó technológiától független, általános keretrendszert tud nyújtani az UE és az UAAF közötti autentikációs eljárásokban.

Rugalmassága lehetővé teszi, hogy több, magasabb rétegekben megvalósított hitelesítési eljárást is képes megvalósítani L2 szinten. Üzenetei könnyen átültethetők RADIUS vagy Diameter protokollra az AMF és UAAF/NACF között. Így ugyanazon eljárások alkalmazhatók transzport- és szolgáltatásvezérlés szintjén. Az EAP támogatja a kölcsönös autentikációt és a kulcscsere algoritmusokat.

Megvalósított EAP eljárások: EAP-SIM, EAP-PEAP/EAP-MSCHAPv2, EAP-TTLS/MS-CHAPv2, EAP-AKA, EAP-TLS. A lista nem korlátozó jellegű.

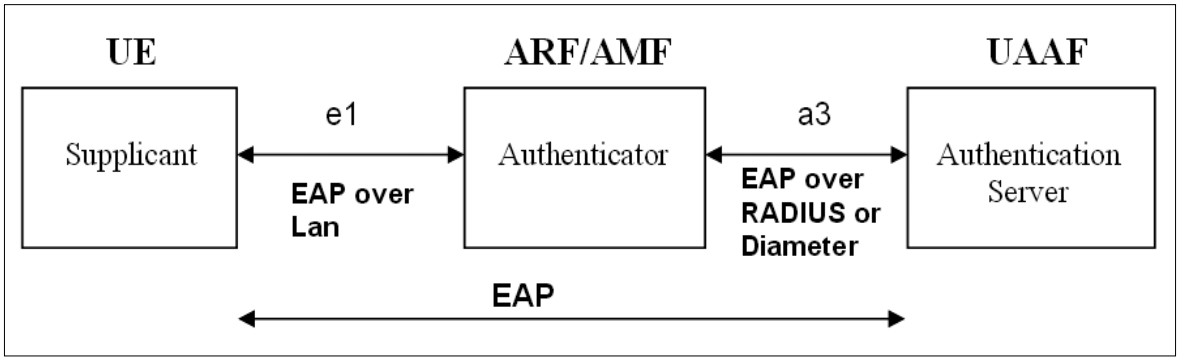
A *6. ábrán* a 802.1x alapú autentikáció folyamata látható.

Ha az UE-ben a 802 réteget valósították meg, akkor az UE egy EAPoL Start keret elküldésével indítja a folyamatot. Az Authenticator (ARF/AMF) veszi a keretet, majd válaszképpen egy azonosító iránti kérést küld az UE felé (EAP-Request). Ha a Supplicant (UE) támogatja az EAP autentikációs mechanizmust, akkor egy EAP-Response válaszban elküldi azonosító adatait.

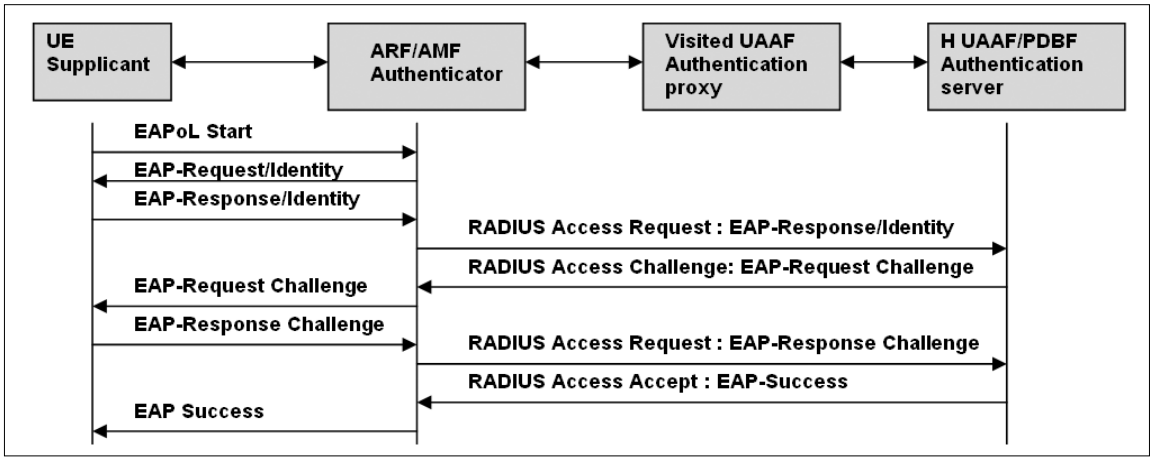
Megjegyzés: az azonosítónak általában két része van: username és realm.

A kettőt általában egy Network Access Identifierben (NAI) adják meg: username@realm. A második részét a honos hálózati autentikációs szerver azonosítására használja a látogatott hálózat. Ez persze feltételezi azt, hogy a látogatott hálózatnak van szerződése, kapcsolata a honos hálózattal. Ha ilyen nincs, akkor a látogatott hálózat nem ismeri a honos hálózatot és autentikációs hibát jelez az UE felé. Ebben az esetben az UE-nek, vagy egy másik NAI-vel kell próbálkoznia (más domain névvel), vagy ki kell építenie egy új NAI-t a látogatott hálózattal.

Ha ezek a próbálkozások is kudarcot vallanak, akkor az UE hálózati hozzáférését letiltja a vezérlés, vagy limitált hozzáférést engedélyez (Green garden) számára.



5. ábra 802.1X funkcionális egységek



6. ábra 802.1x alapú autentikáció RADIUS protokoll felett

Az Authenticator kicsomagolja az UE-től érkező EAP üzenetet, majd becsomagolja azt az UAAF felé menő RADIUS, vagy Diameter üzenetbe. Az EAP és a 802.1x egy keretrendszert ad az UE és az UAAF közötti autentikációhoz, ami architektúrájában és működésében is megfelel az NASS-nek. Az EAP autentikáció pozitív eredményéről EAP-Success, negatív eredményéről EAP-Failure üzenetet küld az Autentikációs szerver.

802.1x esetén az ARF és az AMF mindig egybeépített funkcionalitások. (TS 183 019). Az AMF az Authenticator funkciót valósítja meg, amit egy L2 hop-on belül kell megvalósítani a Supplicant (UE-ben található) funkcióval.

Annak érdekében, hogy a valós felhasználói adatok ne kerülhessenek más birtokába, mint a honos hálózatéba (4. ábra), a kezdeti azonosító cserében az UE használhat általános (default) user nevet, mint például „anonymus”, vagy „user”. PEAP és TTLS esetén tunnel alakul ki az UE és a honos UAAF között, így más számára láthatatlanná válnak a felhasználói adatok.

Tanúsítvány alapú kölcsönös autentikáció adja a legbiztonságosabb hitelesítési eljárást. A látogatott hálózatnak ebben a fázisban nincs szüksége a használó azonosítására, csak a honos hálózat nevére. Mindazonáltal a sikeres autentikáció után a látogatott hálózatnak meg kell kapnia a honos hálózattól a díjazási és számlázási azonosítókat, adatokat. Ezeket a honos hálózat generálja a látogatott hálózattal való elszámolás céljából. Az azonosítót tehát csak a honos UAAF-el kell közölni.

802.1x az xDSL/FTTx elérési hálózatban

Hogyan működik az előbbiekben leírt eljárás xDSL/FTTx esetén?

Az xDSL/FTTx access legalább egy access node-ot (DSLAM, MSAN, OLT a GPON rendszerben) tartalmaz, ami az UE számára hozzáférést biztosít az aggregációs hálózat erőforrásaihoz.

Az UE 802.1x Supplicant szerepkörben működik, az access node-ban, vagy azzal összekapcsolva valósul meg az Authenticator funkció, míg az Authentication server az UAAF. Ha az UE tartalmazza a CNG-t és a vonatkozó előfizetői hálózati eszközöket, akkor az 802.1x szerinti Supplicant funkciót a CNG-ben kell megvalósítani annak érdekében, hogy eleget tegyünk a 802.1x azon követelményének, hogy a Supplicant és az Authenticator távolsága nem lehet több egy L2 hop-nál.

Megjegyzés: A fenti korlát azt is jelenti, hogy azok a felhasználók, akik terminál szinten azonosíthatók és a CNG-hez kapcsolódnak, nem autentikálhatók a NASS-el. Ez a probléma a NASS és CNG specifikáció továbbgondolását igényli.

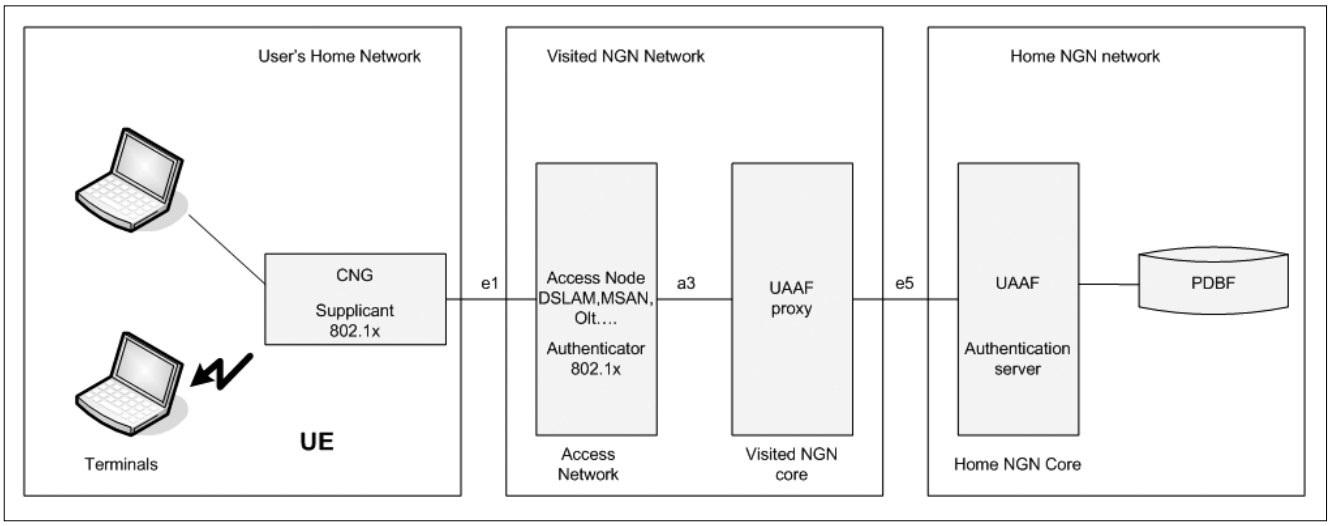
802.1X a WLAN elérési hálózatban

A WLAN elérési hálózatban is legalább egy Access Point van, ami rádiókapcsolatot biztosít a WLAN UE-k számára. A hozzáférési hálózat, vagy a core (mag-)hálózat tartalmaz egy vezérlőt (AC, Access Controller), ami képes menedzselni az AP-kat.

WLAN esetén a mobil UE valósítja meg a 802.1x szerinti Supplicant funkciót, az AP az Authenticator és az Authenticaton Server-t pedig az UAAF.

WLAN hozzáférés esetén az autentikációs folyamat a következő:

1. UE 802.11 AP-t keres és connection request-et generál. Az AP, mint Authenticator válaszul elkéri az UE azonosító adatait.
2. Az AP autentikáció kérésben továbbítja az UE adatait a helyi UAAF felé. Ezt az Access Controller-en (AC) keresztül teszi. Az AP és az AC együtt valósítják meg az ARF és AMF funkciókat.
3. Ha az UAAF proxy tudja autentikálni az UE-t, akkor azt helyben megteszi. Ha nem, akkor az UE nevében található domain név alapján továbbítja azt a honos hálózatnak.
4. A honos hálózati UAAF autentikál az UE-vel, például EAP protokollon, a honos PDBF adatai alapján. Az UAAF az autentikáció eredményét és egy viszonylati kulcsot küld vissza a látogatott UAAF-nek és az AP-nak, mivel azok eddig ki voltak zárva az egyeztetés folyamatából. Ahhoz, hogy az AP-n keresztül UE biztonságosan csatlakozhasson a hálózathoz, AP-nak ismernie kell a viszonylati kulcsot.
5. Az AP konfigurálja a viszonylati kulcsot az adatkapcsolati rétegben és jelzi, hogy UE sikeresen autentikált. Eddig a pillanatig az AP-nak miden UE csatlakozási, címszerzési kísérletét blokkolnia kell.



7. ábra NGN transzportszintű hozzáférés 802.1x alapú vezetékes hozzáférési modellje

2.2.2. Hálózati konfigurációs fázis

Mint korábban látható volt, az NASS architektúrában az NACF felelős a hálózati konfigurációért. A sikeres autentikációs fázis után az AMF-en keresztül lebonyolított DHCP kérésre az NACF IP címet ad vissza az UE-nek, amennyiben megkapta az UE vonali és/vagy áramköri információit.

Az ARF szerepe DHCP esetén

Az ARF-nek RFC 2131-nek megfelelő DHCP v4 Relay Agent-et kell megvalósítania, ami pedig megvalósítja a DHCP Relay Agent Information kiterjesztést (Option 82).

Amikor az ARF az első üzenetet veszi egy adott MAC címről, akkor azt össze kell tudnia kapcsolni azokkal az előfizetői transzport erőforrásokkal (felhasználói áramkör, vonal azonosító stb.), ahonnan az üzenet érkezett. Az NACF által ezen előfizetői erőforrásokhoz rendelt IP címet az ARF-nek össze kell kapcsolnia a MAC címmel, és a kapcsolatot belül tárolnia kell. Ezzel megállíthatja minden olyan csomag továbbítását az NGN felé, ahol az IP cím és a MAC cím nincs összekapcsolva (antispoofing), például WLAN elérés esetén.

Az AMF működése DHCP kérés esetén

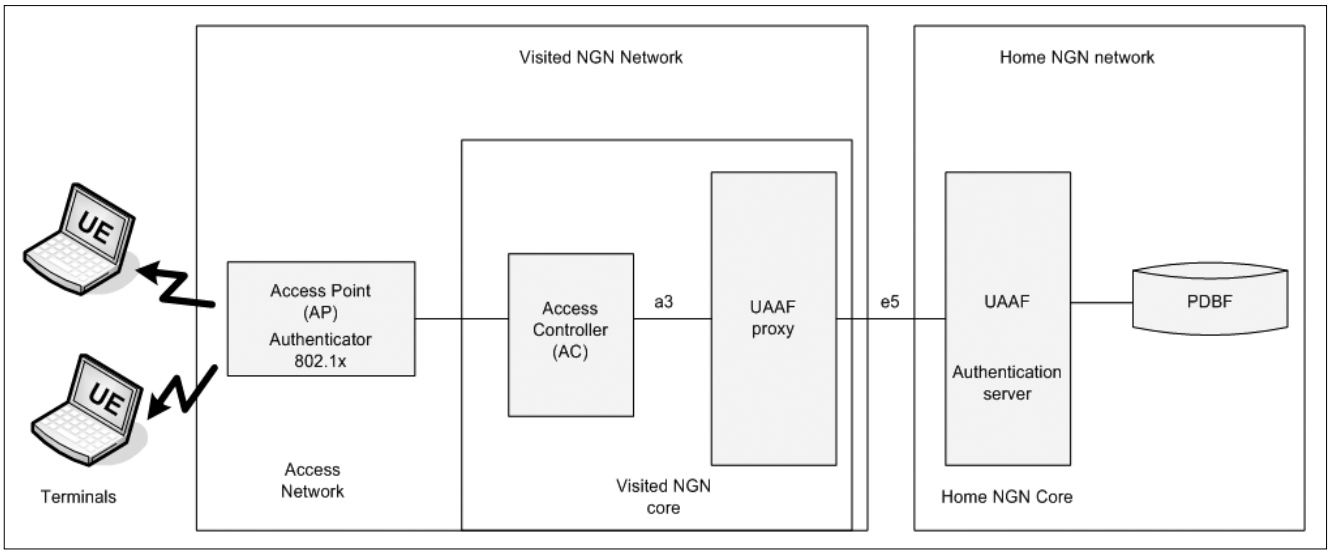
Az AMF-nek DHCP kérés esetén csak ismétlő funkciója van az UE és az NACF között és viszont. Az ismétlő funkcióba beletartozik, hogy a kérést RADIUS, vagy Diameter protokollra helyezi és továbbítja az NACF felé. Az AMF szerepe PPP esetén jelentősebb: végződteti a protokollt, menedzseli az autentikációs és a hálózati konfigurációs fázist. A PPP tárgyalására terjedelmi okokból itt nem térünk ki.

Ethernet hozzáférési hálózat és aggregáció esetén az ARF-nek a DSLAM-ban kell megvalósulnia, hiszen ott állnak rendelkezésre vonali és áramköri információk, míg az AMF a BRAS szintjén is implementálható.

IPv6 alapú elérési hálózatok

IPv6-alapú hozzáférési hálózatban az UE-nek, az ARF/AMF-nek és az NACF-nek RFC 3315 szerint (sor-

8. ábra NGN hozzáférés 802.1x alapú WLAN access-modellje



rendben) DHCPv6 klienst, DHCPv6 ismétlőt és DHCPv6 szervert kell megvalósítania. Az RFC 3315 valamennyi kiterjesztését támogatnia kell (TS 183 019 v2.2.0).

3. QoS vezérlés az NGN transzporthálózatban – RACS

Az NGN architektúrában a Resource and Admission Control Subsystem (ETSI nevén RACS, ES 282 003; ITU nevén RACF, Y.2111) egy döntési szerepben működő alrendszer a QoS-t megvalósító transzportfunkciók és a szolgáltatásvezérlő alrendszerek között. Az RACS által végzett eljárás alapú döntési funkció (Policy Decision Function) transzport előfizetésen (NASS-től kapott használói profil), szolgáltatás szintű megállapodásokon, hálózati eljárási szabályokon, szolgáltatás-prioritásokon [Y.2171], transzporterőforrás-státuszon és a használattal kapcsolatos információkon alapszik.

A szolgáltató számára az RACS képességek teszik lehetővé, hogy beléptetésvezérlést (admission controll) és megfelelő hordozószolgálati eljárásokat tudjon nyújtani multimédiás alkalmazások számára, ellentétben az Internettel, ahol ez csak automatikus szabályozással (TCP), best effort minőségben van megoldva és az alkalmazásoknak nincs hatásuk a transzportra.

Az RACF egy absztrakt megközelítését adja a transzporthálózati infrastruktúrának az AF felé és leveszi a szolgáltatók válláról a transzport részletes ismeretének terhét (hálózati topológia, hálózati elemek közti kapcsolat, erőforrás-használat és QoS mechanizmusok, illetve technológiák stb.) Az RACS együttműködik az AF-el és a transzportfunkciókkal számos alkalmazás érdekében (SIP alapú hívásfelépítés, videoátvitel), melyek igénylik a transzporterőforrás vezérlését, úgymint QoS vezérlés, NAT/firewall vezérlés és NAT címadaptáció (NAT traversal).

Az RACS az AF kérése alapján policy alapú transzporterőforrás-vezérlést valósít meg, transzporterőforrás rendelkezésreállást határoz meg, beléptetéssel kapcsolatos döntéseket hoz és a helyi döntési szabályok végrehajtásához vezérlést ad a transzporterőforrásoknak. A hálózati képességek megvalósítása érdekében az RACS együttműködik a transzport egyes funkcionális egységeivel és vezérli azokat. Ilyen a sávszélességlefoglalás és -hozzárendelés, csomagszűrés, forgalom osztályba sorolása, színezése, szabályozása (policing), prioritás kezelés, NAPT és firewall vezérlés.

Az RACS képes együttműködni más NGN szolgáltatók alkalmazás- és szolgáltatásvezérlőivel.

3.1. Felépítés és működés

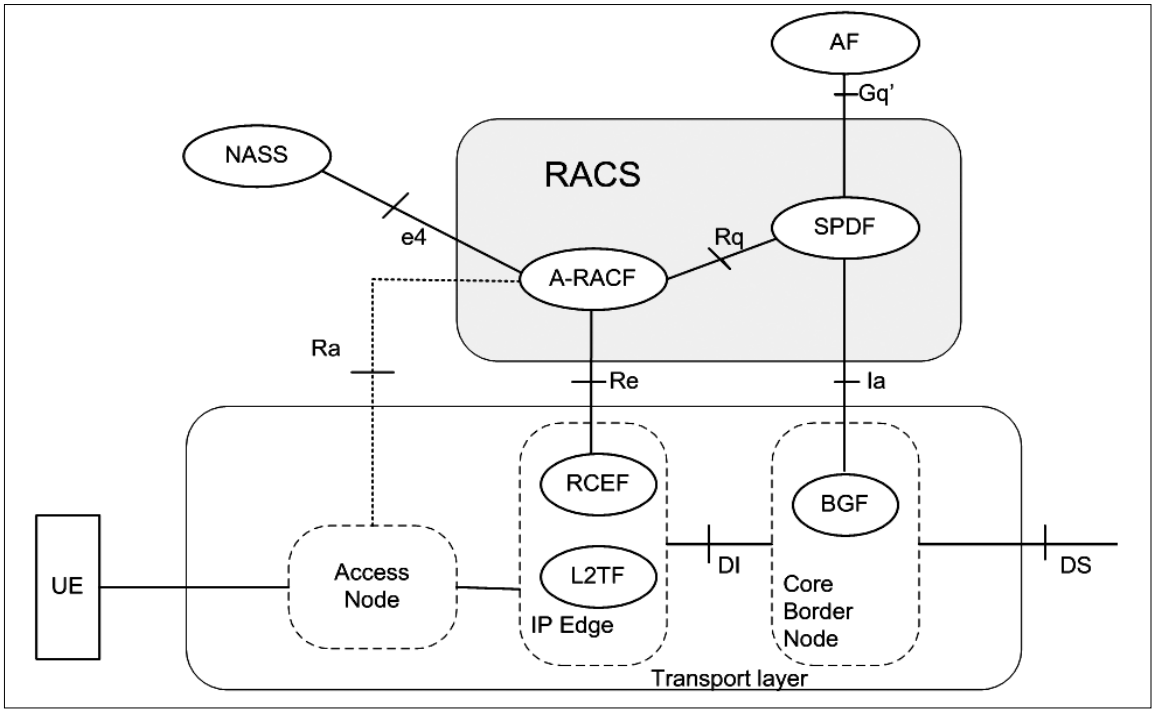
Az RACS két fő eleme az xRACF (Recource Admission Control Function) és az SPDF (Session Decision Function), melyek az Rq [10] interfészen állnak egymással kapcsolatban. Az RACF két verzióját specifikálták, az Access (A-RACF) és a Core (C_RACF) változatot.

Az RACS a Gq' interfészen kap erőforrásvezérléssel kapcsolatos információt az alkalmazásoktól, szolgáltatásvezérlő alrendszerektől, IMS esetén a P-CSCF-től, vagy az I-BGCF-től.

Az RACS e4 Diameter alapú interfészen kap felhasználói profil adatokat az NASS-től.

Megjegyzés: Az RACS architektúra TISPAN változata látható a *9. ábrán*. A szabványosítási testület egyértelműen az A-RACF felügyeletére bízza az NASS adatokat azzal a meggondolással, hogy annak ellenőriznie kell a használói profilban megadott QoS igények kielégítésének lehetőségét.

Az ITU más filozófiát vall az NASS csatlakoztatásával kapcsolatban, ők az SPDF-nek (PD-FE) megfelelő funkcionalitáshoz kapcsolják az NASS-t e4 inter-



9. ábra
TISPAN RACS architektúra (ES 282 003)

fészen. A két entitás az Rq (ES 283 026) referenciaponton cserél információt, így bármelyik megkaphatja a profil adatokat, ha szükséges.

Az RACS a transzporteszközökbe épített RCEF és BGF funkciókon keresztül fejti ki hatását a transzportra. A vezérlés szempontjából ezen funkcionalitások interfészei (Re, Ia) meghatározók. Működésüket lásd később.

SPDF

Az SPDF (Service-based Policy Decision Function) döntési pontot képez az AF és a transzport, azon belül a BGF (Border Gateway Function) között. A BGF-et az Ia referenciaponton vezérli, ami a maghálózat határán működik.

Az SPDF az adott domain-ben az utolsó döntési pont, ahol a helyi hálózati viszonyokhoz illeszkedő eljárási szabályoknak megfelelő döntést lehet hozni, engedélyezni vagy tiltani a média folyamot. Képes együttműködni szomszédos adminisztratív domain-ekben működő SPDF-fel erőforrás-foglalás céljából. Az SPDF a helyi operátor által meghatározott szolgáltatási policynak megfelelően hoz döntéseket. Az AF-től, vagy más együttműködő SPDF-től kapott kéréshez köthető szolgáltatásközpontú policy például a következő információs elemeken és azok kombinációján alapulhat: kérelmező entitás neve (Requestor Name), szolgáltatási osztály (Service Class), szolgáltatás prioritása (Service Priority), foglalási osztály (Reservation Class) stb., melyeket egy „transport control request message" -ben kap.

Az SPDF rejti el a hálózati topológiát az AF és az együttműködő SPDF elől. Funkciójából következően egy általános hálózati képet és használati módot mutat az AF (P-CSCF, I-BGF, más domain-ben működő SPDF) felé, függetlenül az alatta működő transzporthálózattól.

Vezérli a közeli és a távoli NA(P)T-t (NAPTC), továbbá nyitja és lezárja az átjárási pontot a maghálózat felé (GC, Gate Control).

Leképezi az AF-től vagy más SPDF-től érkező szolgáltatási QoS követelményeket és prioritásokat a hálózati QoS paramétereknek (pl. az ITU Y1541szerintieknek) és prioritásoknak. Ez a funkciója közös az A-RACF hasonló funkciójával.

Dönt a csomag és az IP folyam prioritásainak megváltoztatásáról, valamint a bitfolyam adatátviteli sebességének határairól. Az SPDF ezen funkciója az L3/L2 forgalomi policy egyik paraméterét adja az A-RACF számára.

Az SPDF az Rq referenciaponton Diameter alapú interfészen kommunikál az A-RACF-al. Ezen keresztül (Initial Reservation for a session) egy adott session részére erőforrást foglal az A-RACF segítségével. A session paramétereit képes módosítani (Session Modification) és lezárni (Session Termination).

A-RACF

– Az RACF tárolja az előfizetői profilt, miután a felhasználót autentikálta és regisztrálta a NASS, és adatai megjelentek a CLF-ben. Ez a funkció a TISPAN architektúrában jelenik meg, és mint azt az előzőekben jeleztük az ITU architektúrában az SPDF (PD-FE) fogadja a felhasználóiprofil-adatokat.
– Erőforráskérés esetén azonosítja az igénylő folyamat erőforrásigényét, ellenőrzi, hogy a felhasználói profilban megadott access elvárások illeszkednek-e a helyi access képességéhez. Ha igen, akkor jóváhagyja az erőforráskérést.
– Azonosítja és engedélyezi a felhasználó folyamat igényét, ellenőrzi a felhasználói profilban rögzített erőforrásigény illeszkedését az access képességeihez. Ellenőrzi a QoS rendelkezésreállást.
– Az SPDF kérése alapján erőforráslefoglalást hajt végre, L3/L2 forgalmi policy-t határoz meg és állít be.
– Az NGN QoS paramétereket illeszti a technológiafüggő hálózati QoS paraméterekhez.
– Technológiafüggő és erőforrás-rendelkezésreálláson alapuló döntéseket hoz adott folyamat engedélyezéséről vagy tiltásáról.
– QoS jelzésrendszeren kapott erőforrásigény esetén dönt a prioritások átrendezéséről az erőforrások foglaltsága függvényében.
– Képes az adatfolyam-prioritások kezelésére az SPDF-től kapott erőforráskérés alapján
– Megfelelteti az AF-től vagy SPDF-től érkező szolgáltatási QoS követelményeket és prioritásokat a hálózati QoS paramétereknek (pl. az ITU Y1541szerintieknek) és prioritásoknak.
– Dönt a csomag és az IP folyam prioritásainak megváltoztatásáról, valamint a bitfolyam adatátviteli sebességének határairól.
– Képes kiválasztani az aktuális médiafolyam számára – figyelembe véve a helyi hálózati eljárási szabályokat – a kért átviteli osztályt, a minőségi követelményeket és a hálózati erőforrás státuszát, valamint jelezni a kiválasztott útvonalat az RCEF-nek.
– Az A-RACF képes forgalommméréssel összefüggő elszámolási információkat adni „Request/Modify/Release/Abort" parancsok esetén.

3.2. CPE-k QoS osztályai

Az ITU és az ETSI QoS vezérlés szempontjából osztályozza a CPE-ket. Az ITU Y.2111 szerint három típus lehetséges:

• **Type 1:** A CPE nem rendelkezik QoS jelzésképességgel sem a service-, sem a transport-stratum felé. A CPE képes együttműködni a service-stratummal, de nem tud QoS- igénnyel fellépni. Ebben az esetben az NGN szolgáltatáshoz a hálózat rendeli hozzá a hálózati QoS-t és minden alkalommal eljár a CPE érdekében (Proxy).

• **Type 2:** A CPE képes QoS egyeztetésre a service-stratummal (pl. SIP telefon SDP-vel RFC 4566), de nincs QoS jelzésképessége a transzport felé. Ebben az esetben a szolgáltatásvezérlés a kapcsolati

egyeztetés során a jelzésekből (SDP-Session Description Protocol) kinyeri QoS igényt, és azt végrehajtatja a transzporthálózattal.

• **Type3:** A CPE QoS egyeztetési képességekkel bír a transzporthálózattal (pl. UMTS telefon) és közvetlenül kér QoS kiszolgálást. Az RACS-nek ebben az esetben is képesnek kell lennie az access forgalmi viszonyainak megfelelő döntés meghozatalára.

Ennek megfelelően két erőforrásvezérlési módot különböztetünk meg

– *Push mód:* ebben az esetben az RACS adja meg a jogosultságot, döntését a helyi eljárási szabályok alapján önállóan hozza meg és utasítja a transzportot annak végrehajtására.
– *Pull mód:* ebben az esetben a CPE transzport szintű QoS jelzésképességgel rendelkezik és kér kiszolgálást. A RACS adja meg a jogosultságot, de figyelembe veszi a helyi eljárási szabályokat, a használat mértékét, ennek megfelelően módosíthatja a kérést, majd vezérli a transzportot a módosított kérés végrehajtására.

3.3. A vezérelt transzport elemei

Az NGN jelenlegi hálózati protokollja az IP. A kapcsolódó folyamatoknak az átvitellel kapcsolatos QoS-t IP-n kell érzékelnie (QoE, Quality of Experience). A QoS megvalósítása az alsóbb rétegekben is megtörténhet (L2 QoS mechanizmusok), vagy a két rétegben működő mechanizmusok összehangolásával (L2/L3 QoS mechanizmusok). Az NGN szempontjából elérendő cél a dinamikus QoS, melyre a transzport eszközökben az BGF és RCEF lesz hatással.

BGF

A BGF (Border Gateway Function) csomagkapcsolt hálózatok közötti átjáró (gateway) a felhasználói sík média forgalmának kezelésére. A BGF policy végrehajtási és NAT funkciókat lát el az SPDF vezérlése mellett a hálózat valamennyi szegmensében: hozzáférési, aggregációs és maghálózati szinten.

A BGF a micro-flow (egy adott alkalmazás sessionhöz tartozó önálló csomag folyam) szinten működik. A BGF policy végrehajtó funkciója tulajdonképpen az átmenet vezérlése: blokkolja az „önjáró” és átengedi a jogosult adatfolyamokat.

Az iránytól független micro-flow paramétereit az SPDF határozza meg az úgynevezett szabványos adat-ötössel: forrás IP cím, cél IP cím, forrás port, cél port, protokoll. Azokat az adatfolyamokat (micro-flow), melyeknek paraméter ötösét nem ismeri az SPDF, azt nem engedi át a BGF.

Ha már engedélyezte az adatfolyamot, az SPDF utasíthatja a BGF-et, hogy forgalomszabályozást alkalmazzon (pl. traffic conditioning filter), ami korlátozza az áteresztő képességet az SPDF által meghatározott szinten. Például új session-t indít a szolgáltatásvezérlés, és a beszédátvitel folyamatossága érdekében kisebb átviteli sebesség mellett, erősebb beszédtömörítő eljárást kell alkalmazni, hogy az új szolgáltatás számára elegendő sávszélességet biztosítsunk.

A BGF-nek a következő szolgáltatások végrehajtását kell vezérelnie: NAT, helyi cím illesztés (NAT traversal), csomagprioritások aktualizálása (QoS marking), átviteli sebesség szabályozása, forgalommérés, erőforrásallokáció „micro-flow” szinten, a kimenő és bemenő forgalom kapuzása (gate control) az SPDF-től kapott információk alapján.

RCEF

Az RCEF (Resource Enforcement Function) az elérési hálózat felépítésétől függően az IP Edge vagy Access csomópontokban helyezkedik el. Az RCEF a transzport-processzhez tartozó logikai egység, amin keresztül az RACS érvényesíteni tudja a helyi forgalmi szabályokat és ezzel az erőforrás optimális használatát.

Az RCEF szabványosítása még a kezdeteknél tart, gyártói megközelítésekről csak műhelytitok szinten hallhatunk információkat.

Az RCEF hajtja végre a transzport erőforrásokra vonatkozó eljárási szabályokat technológiafüggő aggregációs szinten (VLAN, VPN and MPLS). Funkcióit pusztán transzportkapcsolati információk alapján (pl. VLAN/VPN ID, and LSP Label) is működtetheti. Az RCEF képességekhez sorolják az LSP-vel kapcsolatos sávszélesség-módosítást, vagy az ATM forgalmi paramétereinek beállítását, mint például a cellasebesség, vagy a burst-méret.

Ha „QoS push” módban működik az RCEF, akkor az RACF által előzőleg beállított policy-t hajtja végre az adott adatfolyamra. „QoS pull” módban ugyancsak a policy-t hajtja végre abban az értelemben, hogy a transzport eszközöktől veszi az átviteli igényt (QoS signalling), erőforrást kér az RACF-től, majd az RACF-től kapott átviteli policy alapján kezeli az erőforrást.

Az Acces node-ban, vagy az IP edge node-ban helyezkedik el.

Az RCEF-be beállított forgalmi szabályok L2 és/vagy L3 szintű QoS eljárásokban végződnek. Ilyen eljárások lehetnek:

– Egyszerű L2 QoS mechanizmus, például VP/VC alapú ATM hálózatokban, DLCI alapú FR hálózatokban, vagy VLAN tag az Ethernet hálózatokban.
– Közbenső L2/L3 QoS mechanizmus, pl. MPLS.
– Egyszerű L3 QoS, például DiffServ.
– L2 feletti L3 QoS mechnizmus, például DiffServ over ATM, vagy DiffServ over FR.
– Közbenső L2/L3-ra épülő L3 QoS mechanizmus, például DiffServ és MPLS integrációja.

Az RCEF-nek alapvetően a következő szolgáltatások végrehajtását kell helyileg vezérelnie: csomagprioritások aktualizálása (QoS marking) az access-erőforrások használatának figyelembevételével, átviteli sebesség szabályozása, erőforrás-allokáció, a forgalom kapuzása (gate control) az A-RACF-tól kapott információk alapján.

3.4. Az NGN vezérlés hatása az IP eszközökben alkalmazott QoS mechanizmusokra

Internet elérés esetén nincs lehetőség az átviteli minőség és a session-ba való belépés szabályozására, ezért a szolgáltatások minőségére nem lehet garanciát vállalni, ami valós idejű szolgáltatások esetén kritikus.

Az NGN transzport- és szolgáltatásvezérlése több oldalról is kézben tartják az NGN átvitelt. Az előbbiekből láthattuk, hogy a transzportvezérlés a hálózati csatlakozás előtt többek között felhasználó hitelesítést, profilbeállítást, az erőforrások lefoglalását, a felhasználói profil access képességekkel való összevetését végzi el, majd a session indítását a rendelkezésre álló erőforrások és helyi policy függvényében engedélyezi. Szükséges mindez ezért, mert a multimédia folyamok egymás konkurenseként működnek az access-ben.

Csomagkapcsolt hálózatokban az átvitel minőségét az adott session-re vonatkoztatott hálózati áteresztő képesség (throughput), csomagkésleltetés (packet delay), késleltetés-ingadozás (jitter) és az eldobási arány határozza meg. A multimédia igényeket kielégítő NGN átviteli hálózatnak és vezérlésének ezen paraméternégyes alkalmazásonkénti fenntartását kell felvállalnia minden adatfolyamra végponttól végpontig. Az egyes médiák által igényelt átviteli minőséget több szabvány tárgyalja [pl. ITU Y.1541].

Az NGN transzport vezérelt QoS eljárásai L2 mechanizmusokra (VP, VC, VLAN stb.) és a professzionális IP QoS menedzsmentnél megismert L3 mechanizmusokra épülnek. Ezek a „classification”, a „DiffServ”, a „congestion management”, a „queue management”, „link efficiency”, „traffic shaping” és „traffic policing”, melyek tárgyalása túllépné a cikk kereteit.

4. Összefoglalás

Az NGN többcélú, minőségi átvitelt garantáló, IP alapú távközlési szolgáltatói hálózat, amely dinamikus alkalmazásfejlesztési, szolgáltatás megvalósítási lehetőségeket kínál.

Ahhoz, hogy az NGN több egyidejű, dinamikusan felmerülő, különböző minőségű (VoIP, videotelefon, IPTV, videokonferencia, white board, SMS stb. szolgáltatásokhoz tartozó QoS) átviteli követelménynek képes legyen eleget tenni, fejlett *átvitelvezérléssel* és azt végrehajtani képes *vezérelt átviteli hálózattal* kell rendelkeznie.

A cikk összefoglalta az NGN átvitelvezérlés főbb elemeit, azok szerepét az NGN erőforrásokhoz való hozzáférésben, a hozzáférés forgalmának helyi policy szerinti kontrolljában.

Irodalom

[1] ETSI ES 282 001 v1.1.1
NGN Functional Architecture Release 1 (08/2005)

[2] ETSI ES 282 004 v1.1.1
Network Attachment Sub-System (NASS) (06/2006)

[3] ETSI ES 282 003 v1.1.1
Resource and Admission Control Sub-system (RACS); Functional Architecture (06/2006)

[4] ETSI ES 282 007 v1.1.1
IP Multimedia Subsystem (IMS); Functional architecture

[5] IEEE Std 802.1x-2001
Port-Based Network Access Control

[6] ITU X.509 The Directory:
Public-key and attribute certificate frameworks (8/2005)

[7] ETSI TS 183 019 v.1.1.1
Network Attachment;
Network Access xDSL and WLAN Access Networks; Interface Protocol Definitions (12/2005)

[8] ETSI TS 183 019 v.2.2.0
User-Network Interface Protocol Definitions (07/2007)

[9] IETF RFC 3748
Extensible Authentication Protocol (EAP)

[10] ETSI ES 283 026 v.1.1.1
Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification.

[11] ITU Y.2171
Admission control priority levels in NGN (9/2006)

[12] ITU Y.2111
Resource and admission control functions in NGN (09/2006)

[13] ITU-T Y.1541
Network performance objectives for IP-based services (05/2002)

[14] IETF RFC 3579
RADIUS (Remote Authentication Dial in User Service) Support For Extensible Authentication Protocol (EAP)

[15] IETF RFC 4072
Diameter Extensible Authentication Protocol (EAP) Application.

[16] IETF RFC 4187
Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA).

[17] Kanász-Nagy Lajos:
„Biztonság a távközlésben”
PKI közlemények 48. kötet,
Matáv Rt., Budapest, 2004, pp.141–153.

[18] Kanász-Nagy Lajos:
Nyilvános kulcsú rendszerek a jövő távközlési hálózatában (konferencia kiadvány),
PKI Tudományos Napok 2005.
Magyar Telekom Rt., Budapest, 2005.