INSO
21517
1st.Edition
2017

Identical with
ETSI ES
282 004: 2010
V3.4.1

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۲۱۵۱۷
چاپ اول
۱۳۹۵

پروتکل‌ها و خدمات همگرای اینترنتی و مخابراتی برای شبکه‌سازی پیشرفته (TISPAN)؛ معماری کارکردی NGN؛ زیرسامانه پیوست شبکه (NASS)

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)

ICS :33.020

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri .gov.ir

به‌نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه۱۳۷۱تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔملی مرتبط با آن رشته طرح و در صورت تصویب، به‌عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استانداردملی ایرانچاپ و منتشر می‌شود. بدین ترتیب، استانداردهاییملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد(ISO)[1]،کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی(OIML)[3] است و به‌عنوان تنها رابط[4] کمیسیون کدکس غذایی(CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای‌عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت میکند. ترویج دستگاه بین المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهایملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization for Legal Metrology (OrganisationInternationale de MetrologieLegals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« پروتکل‌ها و خدمات همگرای اینترنتی و مخابراتی برای شبکه‌سازی پیشرفته (TISPAN)؛ معماری کارکردی NGN؛ زیرسامانه پیوست شبکه (NASS)»

رئیس:	**سمت و / یا محل اشتغال:**
صادقیان، حسین (کارشناسی الکترونیک)	مدیرکل استاندارد و تایید نمونه- سازمان تنظیم مقررات و ارتباطات رادیویی
دبیر:	
رضایی، رامین (کارشناسی الکترونیک)	معاون طرح و توسعه - مرکز تحقیقات صنایع انفورماتیک
اعضاء: (اسامی به ترتیب حروف الفبا)	
جمشیدی، سامان (کارشناسی الکترونیک)	کارشناس ایمنی و سازگاری الکترومغناطیسی- شرکت آزمایشگاه‌های صنایع انرژی
زندباف، عباس (کارشناسی مخابرات)	کارشناس- شرکت ارتباطات زیرساخت
سید موسوی، سیدحسن (دکتری مخابرات)	مشاور مدیرعامل- شرکت ارتباطات سیار ایران (همراه اول)
عروجی، سید مهدی (کارشناسی ارشد مدیریت فناوری اطلاعات)	سرپرست گروه تدوین استاندارد- سازمان تنظیم مقررات و ارتباطات رادیویی
غلام ابوالفضل، فرزانه (کارشناسی ارشد مخابرات)	مدیرکل فروش عمده- شرکت مخابرات ایران
محسن‌زاده، علی اکبر (کارشناسی ارشد مخابرات)	کارشناس- صنعت مخابرات ایران
نجفی، ناصر (کارشناسی ارشد الکترونیک)	مدیر پروژه‌های برون‌سازمانی- مرکز تحقیقات صنایع انفورماتیک
یگانه، حسن (کارشناسی ارشد مخابرات)	مدیر گروه ارتباطات ثابت- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

ویراستار:
تورانی، فرزام
(کارشناسی ارشد مدیریت فناوری اطلاعات)

سمت و / یا محل اشتغال:
کارشناس- شرکت خدمات انفورماتیک

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «پروتکل‌ها و خدمات همگرای اینترنتی و مخابراتی برای شبکه‌سازی پیشرفته (TISPAN)؛ معماری کارکردی NGN؛ زیرسامانه پیوست شبکه (NASS)» که پیش‌نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای منطقه‌ای به‌عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی شماره ۵ تهیه و تدوین شده، در دویست و چهل و ششمین اجلاسیه کمیته ملی استاندارد مخابرات مورخ ۹۵/۱۲/۲۵ تصویب شد. اینک این استاندارد به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد ملی برمبنای پذیرش استاندارد منطقه‌ای زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد منطقه‌ای مزبور است.

ETSI ES 282004 V3.4.1, 2010: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub- System (NASS)

مقدمه

پیش‌نویس این استاندارد در کمیسیون‌های فنی و نهایی مربوط، توسط سازمان تنظیم مقررات و ارتباطات رادیویی و مرکز تحقیقات صنایع انفورماتیک، تهیه و تدوین شده است.

پروتکل‌ها و خدمات همگرای اینترنتی و مخابراتی برای شبکه‌سازی پیشرفته (TISPAN)؛ معماری کارکردی NGN؛ زیرسامانه پیوست شبکه (NASS)

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین و توصیف معماری زیرسامانه پیوست شبکه (NASS) و نقش آن در معماری پروتکل‌ها و خدمات همگرای اینترنتی و مخابراتی برای شبکه‌سازی پیشرفته شبکه نسل آینده (TISPAN NGN)[1] است که در استاندارد ES 282 001 (زیربند 2-2) تعریف شده است.

۲ مراجع

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آنها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.
در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.
استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

۲-۱ مراجع الزامی

استانداردهای مراجع زیر برای استفاده در این استاندارد الزامی می‌باشند. برای مراجع تاریخ‌دار تنها ویرایش ذکر شده به‌کار می‌رود. برای مراجع نامشخص، آخرین ویرایش استاندارد مرجع (از جمله تمامی صحیح‌نامه‌ها و اصلاحیه‌ها) به‌کار می‌رود.

2-1 ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203)".

2-2 ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

2-3 IETF RFC 1661: "The Point-to-Point Protocol (PPP)".

2-4 ISO/IEC 7498-2: "Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

یادآوری- استاندارد ملی ایران شماره ۲-۱۶۲۷۴: سال ۱۳۹۱، سامانه‌های پردازش اطلاعات- اتصال متقابل سامانه‌های باز- مدل مرجع پایه- قسمت ۲: معماری امنیتی، با استفاده از استاندارد ISO 7498-2: 1989، تدوین شده است.

1- Telecommunications and Internet converged Services and protocols for Advanced Networking Next Generation Network

2-5 IEEE 802.1X: "IEEE Standard for Local and metropolitan area networks - Port Based Network Access Control".

2-6 ETSI TS 182 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Presence Service; Architecture and functional description [Endorsement of 3GPP TS 23.141 and OMA-AD-Presence-SIMPLE-V1-0]".

۲-۲ مراجع آگاهی‌دهنده

استانداردهای مراجع زیر برای استفاده از این استاندارد لازم نیستند اما کاربر را در حوزه موضوعی خاص یاری می‌رسانند. برای مراجع نامشخص آخرین نسخه استاندارد مرجع (از جمله تمامی تصحیح‌نامه‌ها و اصلاحیه‌ها) به‌کار می‌رود.

2-2-1 ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (3GPP TR 21.905 Release 7)".

2-2-2 ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

۳ اصطلاحات، تعاریف و کوته‌نوشت‌ها

۳-۱ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به‌کار می‌روند:

۳-۱-۱

احراز اصالت

authentication

خصوصیتی است که شناسه صحیح یک هستار یا بخش، با تضمین لازم، توسط آن ایجاد می‌شود.

یادآوری- بخش احراز اصالت شده می‌تواند یک کاربر، مشترک، محیط خانگی یا شبکه خدمت‌رسان باشد. (به گزارش فنی TR 121 905 (زیربند 1-2-2) مراجعه کنید.)

۳-۱-۲

صدور مجوز

authorization

اعطای مجوز بر مبنای شناسایی احراز اصالت است. (به استاندارد ISO/IEC 7498-2 (زیربند 4-2) مراجعه کنید.)

یادآوری- در برخی حوزه‌ها، به‌عنوان مثال خدمات تماس اضطراری، صدور مجوز ممکن است بدون احراز اصالت یا شناسایی مورد نیاز اعطا شود.

۳-۱-۳

دروازه‌راه شبکه مشتری

Customer Network Gateway

دروازه‌راه بین CPN[1] و شبکه دسترسی است.

یادآوری- دروازه‌راه شبکه مشتری مجاز است در ساده‌ترین حالت خود یک مودم پل‌دار یا مسیردهی‌شده و در پیشرفته‌ترین حالت، یک افزاره یکپارچه دسترسی (IAD)[2] باشد.

۴-۱-۳

احراز اصالت صریح

explicit authentication

احراز اصالتی که با توجه به آن، نیاز است هستار احراز اصالت شده (برای تصدیق هویت طرف مورد نظر) رویه احراز اصالت را اجرا کند.

یادآوری- به‌عنوان مثال، در امنیت IMS (مشخصات فنی TS 133 203 (زیربند 1-2))، احراز اصالت صریح با AKA[3] کاملی ارائه می‌شود که به سمت هستار کارخواه IMS (ارائه‌شده توسط IMPI[4]/IMPU[5] و ISIM[6]/USIM[7]) ارسال شده است و احراز اصالت ضمنی نیز با استفاده از نهادهای امنیتی IPsec[8] ارائه می‌شود.

۵-۱-۳

احراز اصالت ضمنی

implicit authentication

احراز اصالت مبتنی بر رابطه مورد اعتمادی است که از قبل بین دو طرف ایجاد شده است یا مبتنی بر یک یا چند خروجی رویه احراز اصالتی است که از قبل بین دو طرف ایجاد شده است.

۶-۱-۳

شناسایی خط

line identification

فرآیندی است که شناسه خط مبتنی بر پیکربندی مطمئن را ایجاد می‌کند.

1- Customer Premises Network
2- Integrated Access Device
3- Authentication and key agreement
4- IM Public identity
5- IM Private identity
6- Inter system Interface Mobility Management
7- Subscriber Identification Module UMTS
8- IP security

۳-۱-۷

کاربر NASS

NASS user

یک هستار درخواست‌کننده صدور مجوز، احراز اصالت و تخصیص آدرس IP از NASS است.

۳-۱-۸

تجهیزات کاربر

User Equipment

یک یا چند افزاره که به کاربر اجازه دسترسی به خدمات ارائه شده در شبکه‌های TISPAN NGN را می‌دهد.

یادآوری- این تجهیزات شامل افزاره‌های تحت واپایش کاربر هستند که معمولا به‌عنوان CPE، IAD، ATA[1]، RGW[2]، TE و غیره ارجاع می‌شوند اما هستارهای تحت واپایش در شبکه، مانند دروازه‌راه‌های دسترسی را شامل نمی‌شوند.

۳-۲ کوته‌نوشت‌ها

در این استاندارد کوته‌نوشت‌های زیر به‌کار می‌روند:

AAA	Authentication and Authorization and Accounting — حسابرسی و صدور مجوز و احراز اصالت
AF	Application Functions — کارکردهای کاربردی
AMF	Access Management Function — کارکرد مدیریت دسترسی
AN	Access Network — شبکه دسترسی
API	Application Programming Interface — واسط برنامه‌ریزی کاربردی
A-RACF	Access-Resource and Admission Control Function — کارکرد واپایش تصدیق و منبع دسترسی
ARF	Access Relay Function — کارکرد رله دسترسی
ASF	Application Server Functions — کارکردهای کارساز کاربردی
ATM	Asynchronous Transfer Mode — حالت انتقال غیرهمزمان
BGF	Border Gateway Function — کارکرد دروازه‌راه مرزی
CLF	Connectivity session Location and repository Function — مکان نشست اتصال و کارکرد مخزن
CNG	Customer Network Gateway — دروازه‌راه شبکه مشتری
CNGCF	CNG Configuration Function — کارکرد پیکربندی CNG
CPE	Customer Premises Equipment — تجهیزات حیطه مشتری

1- Analogue Terminal Adaptor
2- Residental Gateway

CPN	Customer Premises Network	شبکه حیطه مشتری
DHCP	Dynamic Host Configuration Protocol	پروتکل پیکربندی پویای میزبان
DNS	Domain Name Server	کارساز نام دامنه
EAP	Extensible Authentication Protocol	پروتکل احراز اصالت توسعه‌پذیر
EP	Enforcement Point	نقطه اِعمال
FQDN	Fully Qualified Domain Name	نام دامنه کاملا واجد شرایط
IBCF	Interconnection Border Control Function	کارکرد واپایش مرزی اتصال میانی
IMS	IP Multimedia SubSystem	زیرسامانه چندرسانه‌ای IP
IP	Internet Protocol	پروتکل اینترنتی
ISDN	Integrated Services Digital Network	شبکه یکپارچه خدمات رقمی (دیجیتال)
LIF	Location Information Forum	مجمع اطلاعات مکانی
NACF	Network Access Configuration Function	کارکرد پیکربندی دسترسی شبکه
NASS	Network Attachment SubSystem	زیرسامانه پیوست شبکه
PAA	PANA Authentication Agent	عامل احراز اصالت PANA
PaC	PANA Client	کارخواه PANA
PANA	Protocol for carrying Authentication for Network Access	پروتکل اجرای احراز اصالت برای دسترسی شبکه
P-CSCF	Proxy-Call Session Control Function	کارکرد واپایش نشست تماس پیشکار
PDBF	Profile Data Base Function	کارکرد دادگان نمایه
PNA	Presence Network Agent	عامل شبکه موجود
PPP	Point-to-Point Protocol	پروتکل نقطه به نقطه
PSTN	Public Switched Telephone Network	شبکه عمومی تلفن
QoS	Quality of Service	کیفیت شبکه
RACS	Resource Admission Control Subsystem	زیرسامانه واپایش تصدیق منبع
RCEF	Resource Control Emulation Function	کارکرد شبیه‌سازی واپایش منبع
TE	Terminal Equipment	تجهیزات پایانه
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks	مخابرات و خدمات همگرای اینترنتی و پروتکل‌ها برای شبکه‌های پیشرفته
UAAF	User Access Authorization Function	کارکرد صدور مجوز دسترسی کاربر
UE	User Equipment	تجهیزات کاربر
VC	Virtual Circuit	مدار مجازی
VP	Virtual Path	مسیر مجازی

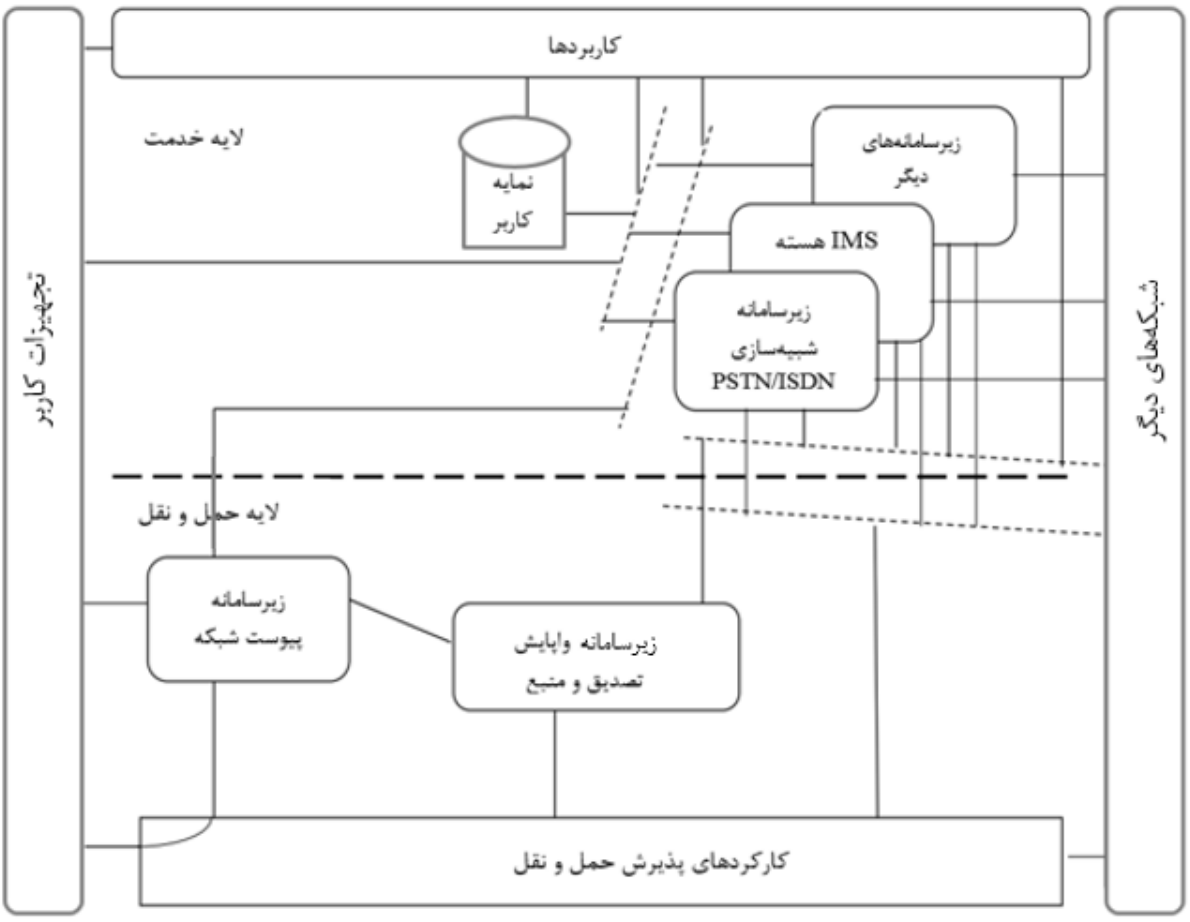
۴ توصیف کلی NASS

۴-۱ بررسی اجمالی کارکردی سطح بالا

زیرسامانه پیوست به شبکه کارکردپذیری‌های زیر را فراهم می‌کند:

- تمهیدات پویای نشانی IP و دیگر پارامترهای پیکربندی تجهیزات کاربر (به‌عنوان مثال، استفاده از DHCP).
- احراز اصالت کاربر، پیش از رویه تخصیص نشانی IP یا در خلال آن.
- احراز اصالت دسترسی به شبکه، بر پایه نمایه کاربر.
- پیکربندی شبکه دسترسی، بر پایه نمایه کاربر.
- مدیریت مکان.

مکان این زیرسامانه در معماری کلی TISPAN، در استاندارد ES 282 001 (زیربند 2-2) مشخص شده و اطلاعات آن در شکل ۴-۱ نشان داده شده است.



شکل ۴-۱ - بررسی اجمالی معماری TISPAN NGN

۴-۲ مفاهیم سطح بالای NASS

زیرسامانه NASS ثبت در سطح دسترسی و راه‌اندازی UE را برای دستیابی به خدمات TISPAN NGN فراهم می‌کند. NASS، احراز اصالت و شناسایی سطح شبکه را فراهم کرده، فضای نشانی IP شبکه دسترسی را مدیریت کرده و نشست‌های دسترسی را احراز اصالت می‌کند. همچنین NASS نقطه تماس زیرسامانه‌های کاربردها/خدمات TISPAN NGN را به UE اعلام می‌کند.

پیوست به شبکه از طریق NASS بر پایه اعتبارنامه احراز اصالت و شناسه کاربری صریح یا ضمنی ذخیره شده در NASS استوار است.

۴-۳ قابلیت تحرک، جابه‌جایی[1]

کارکردهای مدیریت قابلیت تحرک ارائه شده توسط NASS، در نشر فعلی TISPAN NGN، به قابلیت پایانه‌ای ملزم به جابه‌جایی در نقاط دسترسی و شبکه‌های دسترسی متفاوت (که ممکن است در اختیار یک فراهم‌ساز شبکه دسترسی متفاوت باشد) و یک کاربر برای استفاده از پایانه متفاوت، نقاط دسترسی و شبکه‌های دسترسی جهت بازیابی خدمات TISPAN NGN آنها محدود می‌شوند. نشر فعلی TISPAN NGN، بدون صرف‌نظرکردن از قابلیت‌های خودگردان[2] ارائه شده درون شبکه‌های دسترسی به پشتیبانی دگرسپاری و پیوستگی نشست بین شبکه‌های دسترسی نیاز ندارد.

تأثیر این الزامات جابه‌جایی در بند ۶ تعریف می‌شود.

۴-۴ ثبت سطح شبکه دسترسی

ثبت NASS شامل رویه‌های شناسایی، احراز اصالت و صدور مجوز بین UE و NASS تا دسترسی به NASS واپایش شود. دو نوع احراز اصالت برای NASS تعریف می‌شود: احراز اصالت ضمنی که به‌عنوان مثال بر پایه شناسایی خط است و احراز اصالت صریح که به‌عنوان مثال بر پایه EAP است. رابطه بین شناسه و اعتبارنامه مورد استفاده برای احراز اصالت، باید برای هر نوع راه‌حل احراز اصالت ممکن برای NASS مشخص شود.

احراز اصالت صریح بین UE و NASS الزامی است. این احراز اصالت به اجرای رویه نشانک‌دهی بین UE و NASS نیاز دارد. احراز اصالت ضمنی مجاز است توسط NASS بر پایه شناسایی خط اتصال به UE انجام شود. انتخاب نوع احراز اصالت به‌کار رفته به خط‌مشی بهره‌بردار مربوط می‌شود.

هر دو احراز اصالت صریح و ضمنی مجاز هستند که به‌طور مستقل به‌عنوان سازوکارهای احراز اصالت NASS استفاده شوند.

1- nomadism
2- autonomous

۴-۴-۱ احراز اصالت ضمنی

احراز اصالت دسترسی ضمنی، با توجه به پیکربندی شبکه دسترسی، به‌ویژه برای شبکه‌های دسترسی فراخ‌باند سیمی، تنها مجاز به احراز اصالت ضمنی از طریق شناسه منطقی یا فیزیکی روی لایه ۲، لایه حمل و نقل است. تجهیزات کاربر می‌تواند مستقیما بدون رویه احراز اصالت صریح، به شبکه دسترسی متصل باشد.

یک CNG باید بتواند مستقیما بدون رویه احراز اصالت صریح به شبکه دسترسی، دسترسی داشته باشد. نوع روش احراز اصالت ضمنی به خط‌مشی‌های بهره‌بردار وابسته است.

۴-۴-۱-۱ احراز اصالت خط

احراز اصالت خط، حالتی از احراز اصالت ضمنی است که اطمینان می‌دهد یک خط دسترسی، احراز اصالت شده و از CNG قابل دسترسی است. احراز اصالت خط باید بر پایه فعال‌سازی اتصال L2 بین CNG و شبکه دسترسی باشد.

احراز اصالت خط، اطمینان می‌دهد که خط دسترسی احراز اصالت شده و از CNG قابل دسترسی است. ID خط باید برای احراز اصالت خط استفاده شود. با توجه خط‌مشی بهره‌بردار[1] باید در خصوص احراز اصالت خط تصمیم‌گیری شود.

۴-۴-۲ احراز اصالت صریح

درصورتی‌که CNG یک مودم مسیردهنده و CPN نیز یک محدوده IP خصوصی باشد، احراز اصالت باید از CNG آغاز شود. در صورتی که CNG یک پل اتصال‌دهنده باشد، هر UE باید با NASS، همانطور که محدوده IP در CPN برای شبکه دسترسی شناخته شده، احراز اصالت شود.

در مورد هر راهکار ممکن احراز اصالت صریح، رابطه بین شناسه و اعتبارنامه مورد استفاده برای احراز اصالت، باید برای NASS شناخته شده باشد. شناسه مورد استفاده برای احراز اصالت صریح، مجاز است به سازوکار احراز اصالت به‌کار رفته و شبکه دسترسی که UE به آن متصل است، وابسته باشد. دو نمونه از این شناسه‌ها عبارتند از:

- اعتبارنامه و شناسه کاربر.
- شناسه UE.

نوع سازوکارهای احراز اصالت صریح مورد استفاده باید به پیکربندی شبکه دسترسی و خط‌مشی بهره‌بردار وابسته باشد.

۴-۴-۳ پیکربندی شبکه راه دور CNG

این رویه برای راه‌اندازی دروازه‌راه‌های CNG در حال دسترسی به زیرسامانه‌های خدمت TISPAN NGN مورد نیاز است.

1- Operator

۴-۴-۴ یافتن زیرسامانه‌های کاربردها/خدمات TISPAN NGN

NASS به عنوان قسمتی از فرآیند ثبت شبکه باید از امکان اعلان اطلاعات تماس زیرسامانه‌های کاربردها/خدمات TISPAN NGN به UE برخوردار باشد. در صورتی که زیرسامانه ISM TISPAN NGN باشد، اطلاعات تماس ارائه شده توسط NASS باید P-CSCF را شناسایی کند.

بهتر است اطلاعات تماس ارائه شده توسط NASS، به شکل نشانی IP نقطه تماس یا به شکل FQDN نقطه تماس باشد (که در آن مورد، NASS نشانی IP کارساز DNS را که می‌تواند این FQDN را به نشانی IP نقطه تماس تبدیل کند، ارائه می‌دهد.)

نقطه تماس با زیرسامانه‌های کاربردها/خدمات ISM TISPAN NGN مجاز است از نظر ایستایی به‌صورت جایگزین، در UE پیکربندی شود. به‌عنوان مثال استفاده از FQDN و توان تفکیک DNS برای بازیابی نشانی‌های IP نقاط تماس که در مورد غیرفراگرد[1] به‌کار می‌رود.

۵ معماری کارکردی

۵-۱ بررسی اجمالی

زیرسامانه پیوست شبکه (NASS) شامل هستارهای کارکردی زیر است:

- کارکرد پیکربندی دسترسی شبکه (NACF).
- مکان نشست اتصال و کارکرد مخزن (CLF).
- کارکرد صدور مجوز دسترسی کاربر (UAAF).
- کارکرد دادگان نمایه (PDBF).
- کارکرد پیکربندی CNG (CNGCF).

NASS با هستارهای کارکردی TISPAN NGN زیر تعامل دارد:

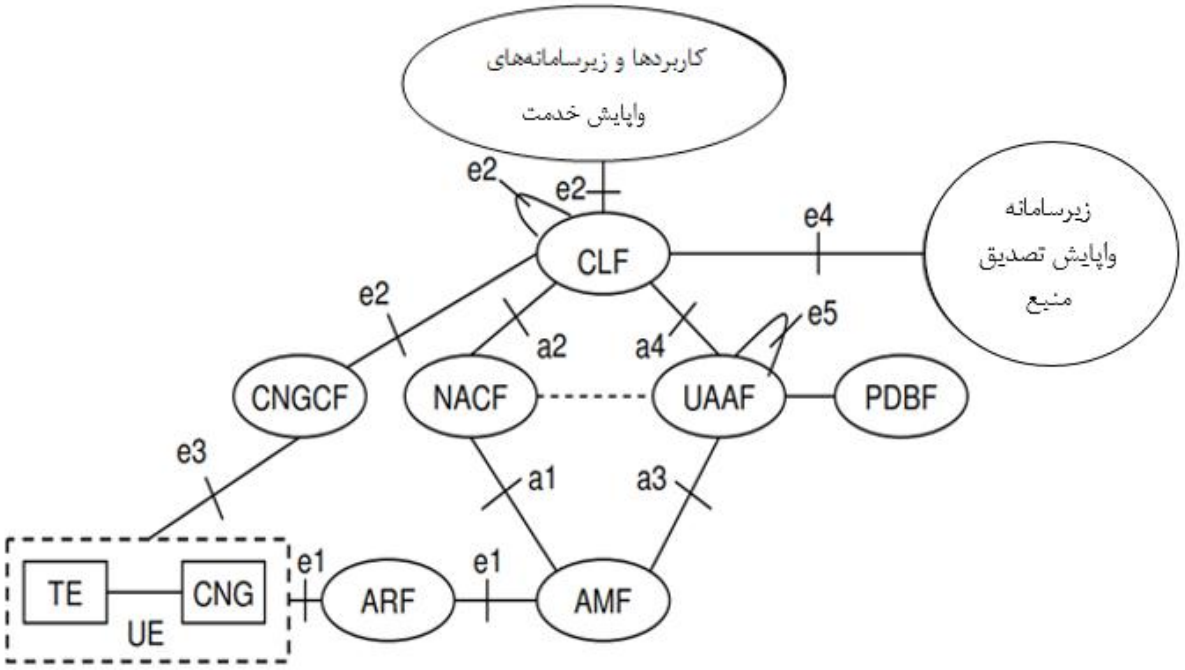
- کاربردها و زیرسامانه‌های واپایش خدمات TISPAN.
- زیرسامانه واپایش تصدیق منبع (RACS).
- کارکرد رله دسترسی (ARF) و کارکرد مدیریت دسترسی (AMF)
- تجهیزات کاربر (UE).

یک یا چند هستار کارکردی مجازند روی یک هستار فیزیکی منفرد نگاشت شوند. چنانچه یک هستار کارکردی توسط دو هستار فیزیکی پیاده‌سازی شود، واسط بین هستارهای فیزیکی خارج از هدف و دامنه کاربرد استاندارد محسوب می‌شوند.

1- Non-roaming

هستارهای کارکردی در زیرسامانه پیوست شبکه (NASS) مجاز هستند روی دو دامنه سازمانی توزیع شوند. برای تأثیر فراگرد توزیع NASS به بند ۶ مراجعه کنید.

شکل ۵-۱ بررسی اجمالی روابط بین این هستارهای کارکردی و دیگر زیرسامانه‌های معماری NGN را ارائه می‌دهد. واسطهای مربوط به سامانه‌های هزینه‌یابی نشان داده نمی‌شوند. پیوست **الف** پیکربندی‌های فیزیکی بالقوه و آگاهی‌دهنده‌ای را ارائه می‌دهد که معماری کارکردی NASS در آن‌ها قابل کاربرد است.



شکل ۵-۱- معماری زیرسامانه پیوست شبکه

۵-۲ هستارهای کارکردی

۵-۲-۱ کارکرد پیکربندی دسترسی شبکه

کارکرد پیکربندی دسترسی شبکه، مسئول تخصیص نشانی IP به UE است. این کارکرد همچنین پارامترهای دیگر پیکربندی شبکه مانند نشانی کارساز(های) DNS، نشانی پیشکارهای نشانک‌دهی برای پروتکل‌های خاص (مانند نشانی P-CSCF در هنگام دسترسی به IMS) را توزیع می‌کند.

بهتر است NACF بتواند شناسانه شبکه دسترسی را برای UE فراهم کند. این اطلاعات به‌طور انحصاری شبکه دسترسی را شناسایی می‌کنند که UE به آن ملحق شده است. UE مجاز است این اطلاعات را به صورت اشاره‌شده به کاربردها، ارسال کند تا CLF مکان‌یابی شود.

یادآوری ۱- حمل و نقل شناسانه دسترسی به توسعه پروتکل‌های موجود وابسته است. (به‌عنوان مثال گزینه جدید DHCP با استفاده از گزینه DHCP ۱۲۰) چنانچه NASS از ابزارهای حمل و نقل این پارامتر به UE برخوردار نباشد، این کارکرد پشتیبانی نخواهد شد.

یادآوری ۲- کارسازهای DHCP یا کارسازهای RADIUS پیاده‌سازی‌های نوعی NACF هستند.

۵-۲-۲ خالی

۵-۲-۳ مکان نشست اتصال و کارکرد مخزن

مکان نشست اتصال و کارکرد مخزن وابستگی بین نشانی IP تخصیص‌یافته به UE و اطلاعات مکان شبکه مربوط است که توسط NACF فراهم شده است، به‌عبارتی مشخصه‌های تجهیزات حمل و نقل دسترسی، شناسانه خط (ID دسترسی منطقی)، شناسه لبه IP و غیره را ثبت می‌کند. CLF ارتباط بین اطلاعات مکانی شبکه که از NACF دریافت شده است و اطلاعات جغرافیایی مکان را ثبت می‌کند. CLF همچنین می‌تواند شناسه کاربر NASS را ذخیره کند که نشانی IP (اطلاعات دریافتی از UAAF) همراه نمایه QoS شبکه مرتبط و اولویت‌های مربوط به حریم خصوصی اطلاعات مکانی به آن تخصیص یافته است. در صورتی که CLF نمایه/شناسه کاربر NASS را ذخیره نکند، باید بتواند این اطلاعات را از UAAF بازیابی کند. برای جزئیات مدل اطلاعاتی CLF و مدل حالت، به زیربندهای ۵-۲-۳-۱ و ۵-۲-۳-۲ مراجعه کنید.

CLF به پرسمان‌های مکانی از کاربردها و زیرسامانه‌های واپایش خدمت پاسخ می‌دهد. مجاز است اطلاعات واقعی تحویل داده شده توسط CLF، بسته به توافقات درخواست‌کننده و اولویت‌های کاربر NASS در زمینه حریم خصوصی مکان آن، شکل‌های مختلفی داشته باشند. (به‌عنوان مثال، مکان شبکه، مختصات جغرافیایی، نشانی پستی و غیره) هر نوع اطلاعات خصوصی که می‌تواند سطح دقت اطلاعات مکانی قابل ارائه را نشان دهد نیز با اطلاعات مکانی واقعی ارسال می‌شود.

یادآوری ۱- اشارات و تأثیرات توسعه مجوز نمایش خصوصی در دست مطالعه (FFS)[1] هستند که باید روی نقطه مرجع e2[2] (مطابق شکل ۵-۱)، به کارکرد واپایش خدمات کاربردی کارکردها در لایه کاربردی و از دسترسی ارسال شوند. (شبکه‌های PBX)

یادآوری ۲- تصمیم‌گیری در زمینه مجوز تغییر در نسخه‌های اولیه این استاندارد به‌عنوان تغییر بنیادی، در دست مطالعه است.

یادآوری ۳- بازیابی اطلاعات جغرافیایی از مشخصه‌های مکانی شبکه کاربر NASS مربوط توسط CLF، خارج از هدف و دامنه کاربرد این استاندارد است.

یادآوری ۴- اطلاعات جغرافیایی، مجاز است با توجه به نوع دسترسی و کاربرد، حالت‌های متفاوتی داشته باشد. تعریف این قالب نیز باید با OCG EMTEL که درباره نیاز به LIF در محیط‌های خاص، مطابق الزامات قانون‌گذار تصمیم می‌گیرد، پیوند داشته باشد. این میدان داده برای استفاده به‌عنوان نگهدارنده مکان این اطلاعات منظور می‌شود.

CLF، برای برقراری ارتباط بین نشانی IP تخصیص‌یافته توسط NACF به کاربر و خط ID، با NACF است.

CLF همچنین اطلاعات نمایه شبکه دسترسی کاربر NASS را ثبت می‌کند تا اطلاعات نمایه برای RACS در احراز اصالت UE قابل دسترس باشد.

CLF قادر است اطلاعات دریافتی از NACF و UAAF بر پایه ID دسترسی منطقی را هم‌بسته کند.

1- For Future Study

۲- e1، e2، ..... و a1، a2، a3، ..... واسط‌های بین هستارها هستند.

۵-۲-۳-۱ مدل اطلاعاتی

مکان CLF نشان‌دهنده شماری از رکوردهای معرف نشست‌های فعال است. این رکوردها شامل اطلاعات دریافت شده از NACF و UAAF، اطلاعات موجود در فهرست AFهای مشترک برای رویدادهای خاص و داده‌های افزونه پیکربندی شده از نظر ایستایی هستند. جدول زیر نشان می‌دهد کدام عناصر اطلاعاتی برای هر یک از این نشست‌ها ذخیره می‌شوند.

یادآوری- در صورتی که PPP مورد استفاده قرار گیرد، مجاز است ID دسترسی فیزیکی از UAAF برای CLF ارائه شود.

جدول ۵-۱- توصیف نشست دسترسی

اطلاعات دریافتی از NACF	
نشانی منحصر به فرد جهانی	
– نشانی IP واگذارشده	نشانی IP کاربر پیوست NASS
– دامنه نشانی	دامنه نشانی‌دهی که در آن نشانی IP معنی‌دار است.
ID دسترسی فیزیکی (اختیاری)	شناسه دسترسی فیزیکی است که کاربر NASS به آن متصل است.
ID دسترسی منطقی	شناسه دسترسی منطقی استفاده شده توسط کاربر پیوست NASS است. در مورد xDSL، ID دسترسی منطقی مجاز است به‌طور آشکاری حاوی شناسه درگاه، حامل ترافیک VP و/یا حامل ترافیک VC باشد.
نوع پایانه	نوع تجهیزات کاربر که نشانی IP به آن تخصیص یافته است.
اطلاعات دریافتی از UAAF/PDBF	
ID کاربر NASS	شناسه کاربر NASS پیوست
ID دسترسی منطقی	شناسه دسترسی منطقی که توسط کاربر NASS پیوست استفاده شده است.
ID نشانی فیزیکی (اختیاری)	شناسه دسترسی فیزیکی که کاربر NASS به آن متصل می‌شود.
نشانی CNGCF (اختیاری) (به یادآوری ۶ مراجعه کنید.)	نشانی هستار CNGCF است که بازیابی داده‌های پیکربندی از آن توسط تجهیزات کاربر مجاز است.
شناسه P-CSCF (اختیاری) (به یادآوری ۷ مراجعه کنید.)	شناسه P-CSCF برای دسترسی خدمات IMS است.
نشانگر خصوصی	آیا اطلاعات مکانی می‌تواند به خدمات و کاربردها فرستاده شود.
اطلاعات نمایه QoS (به یادآوری‌های ۲ و ۳ مراجعه کنید.)	
– طبقه خدمت حمل و نقل	طبقه خدمت حمل و نقل به اشتراک گذاشته شده توسط کاربر پیوست NASS. طبقه خدمت حمل و نقل به یک رفتار پیش‌رو در سطح حمل و نقل مربوط می‌شود.
– نوع رسانه	نوع (انواع) رسانه که نمایه QoS در آن به کار می‌رود.
– پهنای باند اشتراکی UL	بیشینه مقدار پهنای باند اشتراک‌یافته توسط کاربر پیوست NASS در جهت پیوند فراسو
– پهنای باند اشتراکی DL	بیشینه مقدار پهنای باند اشتراک‌یافته توسط کاربر پیوست NASS در جهت پیوند فروسو
– بیشینه اولویت	بیشینه اولویت مجاز برای هر نوع درنظر گرفتن درخواست.
– نام درخواست‌کننده	درخواست‌کننده(های) مجاز توسط نمایه QoS را شناسایی می‌کند.
تنظیمات آغازین دروازه (اختیاری)	
– فهرست مقاصد مجاز به‌همراه	در مورد داده‌های تک‌پخشی، فهرست نشانی‌های IP مقصد پیش‌فرض و/یا درگاه‌ها و/یا

اطلاعات دریافتی از NACF	
جریان‌های چندپخشی	گستره‌های درگاهی و/یا پیشوندهایی است که ترافیک برای آنها قابل ارسال است. در مورد چندپخشی، فهرست نشانی‌های گروه چندپخشی IP و/یا فهرست (نشانی IP منبع، نشانی گروه چندپخشی IP) جفت‌هایی است که ترافیک توسط کاربر NASS پیوست از آن قابل دریافت است. گستره‌های نشانی درون این فهرست پشتیبانی می‌شوند. (به یادآوری ۴ مراجعه کنید.)
– فهرست مقاصد ردشده به همراه جریان‌های چندپخشی	در مورد داده‌های تک‌پخشی، فهرست نشانی‌های IP مقصد پیش‌فرض، درگاه‌ها، پیشوندها و گستره‌های درگاهی است که ترافیک برای آنها رد می‌شود. در مورد چندپخشی، فهرست نشانی‌های گروه چندپخشی IP و/یا فهرست (نشانی IP منبع، نشانی گروه چندپخشی IP) جفت‌هایی است که برای آنها ترافیک به سمت کاربر NASS پیوست باید رد شود. گستره‌های نشانی درون این فهرست پشتیبانی می‌شوند. (به یادآوری ۴ مراجعه کنید.)
– پهنای باند پیش فرضی UL	بیشینه مقدار پهنای باند است که می‌تواند بدون صدور مجوز صریح در جهت پیوند فراسو استفاده شود.
– پهنای باند پیش فرضی DL	بیشینه مقدار پهنای باند است که می‌تواند بدون صدور مجوز صریح در جهت پیوند فروسو استفاده شود.
اطلاعات ایستای مشتق‌شده از ID دسترسی فیزیکی	
اطلاعات مکانی	
ID کاربر پیش فرض NASS	
اطلاعات ایستای مشتق‌شده از ID دسترسی منطقی	
نقطه تماس RACS	نشانی عنصر RACS که بهتر است نمایه کاربر NASS اجرا شود.
نوع شبکه دسترسی	نوع شبکه دسترسی است که اتصال IP روی آن برای کاربر NASS فراهم می‌شود.
اطلاعات مدیریت رویداد	
اطلاعات مدیریت رویداد (به یادآوری ۵ مراجعه کنید.)	
– نوع رویداد	نوع رویداد مورد پایش
– شناسه‌های AF	فهرست AF که باید از وقایع این رویداد تهیه شود.

یادآوری ۱- نمایشی است که نشان می‌دهد آیا کاربردها می‌توانند با توجه به سطح امنیت آنها اطلاعات مکانی را ارزیابی کنند.

یادآوری ۲- نمایه دسترسی مجاز است شامل نمایه چندگانه QoS باشد.

یادآوری ۳- پهنای باند واقعی قابل دسترسی توسط NASS شناخته نمی‌شود. این اطلاعات می‌توانند توسط RACS برپایه ID دسترسی منطقی مشتق شوند.

یادآوری ۴- چنانچه یک مقصد تک‌پخشی و/یا جریان چندپخشی در هیچ یک از دو لیست عرضه نشود، مقاصد تنظیمات دروازه برای آن نشانی‌ها تحت واپایش RACS قرار می‌گیرد.

یادآوری ۵- مواردی بیش از نوع رویداد و شناسه‌های AF مربوطه مجاز به ذخیره هستند.

یادآوری ۶- چنانچه نشانی CNGCF روی CLF پیکربندی شود و نشانی CNGCF از UAAF/PDBF دریافت شود، انتخاب نشانی مناسب به خط‌مشی بهره‌بردار وابسته است.

یادآوری ۷- چنانچه شناسه P-CSCF روی CLF پیکربندی شود و شناسه P-CSCF از UAAF/PDBF دریافت شود، انتخاب آنها به خط‌مشی بهره‌بردار وابسته است.

رکوردهای متعدد مجازند حاوی ID دسترسی فیزیکی و/یا ID دسترسی منطقی و/یا ID کاربر NASS باشند، چرا که کاربر NASS مجاز است با استفاده از دسترسی فیزیکی یکسان یا متفاوت بیش از یک، نشست IP روی همان دسترسی منطقی یا دسترسی منطقی متفاوت (به‌عنوان مثال، ATM VC) ایجاد کند. CLF به

ایجاد هیچ نوع پیوندی بین چنین رکوردهایی نیاز ندارد، گرچه ممکن است این کار را برای هدف بهینه‌سازی ظرفیت ذخیره‌سازی خود انجام دهد.

۵-۲-۳-۲ مدل حالت

رفتار CLF در هنگام مدیریت سوابق دسترسی، می‌تواند توسط مدل حالت توصیف شده در این بند نشان داده شود. این مدل حالت، برای محدود کردن پیاده‌سازی‌های یک CLF موردنظر نیست. پیاده‌سازی‌ها تا زمانی مجازند از مدلی متفاوت استفاده کنند که همان رفتار خارجی را نمایش دهند.

این مدل حالت، یک ماشین حالت نشست (SSM)[1] است که می‌تواند هریک از پنج حالت زیر را داشته باشد:

- **Null**: این حالت عدم وجود رکورد دسترسی را نشان می‌دهد.
- **Wait_For_Bind_Indication_and_Profile**: این حالت زمانی ثبت می‌شود که رکورد دسترسی در نتیجه دریافت درخواستی برای اشتراک یک رویداد خلق شود، (به‌عنوان مثال رویداد ورود به شبکه) در حالی‌که هیچ رکورد نشستی برای شناسانه کاربر NASS مربوط یا نشانی منحصر به فرد جهانی وجود ندارد. یک رکورد جزئی ایجاد می‌شود و CLF منتظر رویداد Bind_Indication می‌ماند.
- **Wait_For_Bind_Indication**: این حالت زمانی ثبت می‌شود که یک رکورد دسترسی در نتیجه دریافت اطلاعات نمایه کاربر NASS ایجاد شود، در حالی که هیچ رکورد نشستی برای شناسه کاربر NASS مربوط یا نشانی منحصر به فرد جهانی وجود ندارد. یک رکورد جزئی ایجاد می‌شود و CLF منتظر رویداد Bind_Indication می‌ماند.
- **Wait_For_Profile_Information**: این حالت، رکورد نشست جزئی را در جایی نشان می‌دهد که اطلاعات نمایه کاربر NASS درحال از دست رفتن است.
- **Active_Session**: این حالت، رکورد نشست را در جایی نشان می‌دهد که توصیف کامل نشست‌های دسترسی موجود باشد.

CLF جریان‌های اطلاعاتی را در نقاط مرجع e2، e4، a2 و a4 دریافت و ارسال می‌کند. جریان‌های اطلاعاتی ورودی برپایه شناسهٔ کاربر NASS یا نشانی منحصر به فرد جهانی به سمت SSM هدایت می‌شوند.

یک نمونه SSM زمانی ایجاد می‌شود که «Bind_Indication یا Event_Subscription_Indication نشان‌دهنده یک شناسه کاربر NASS ناشناخته» یا «نشانی منحصر به فرد جهانی» روی دهد.

رویدادهای زیر توسط ماشین حالت نشست CLF مدیریت شده و موجب نقل و انتقال بین حالت‌ها می‌شوند:

1- Session State Machine

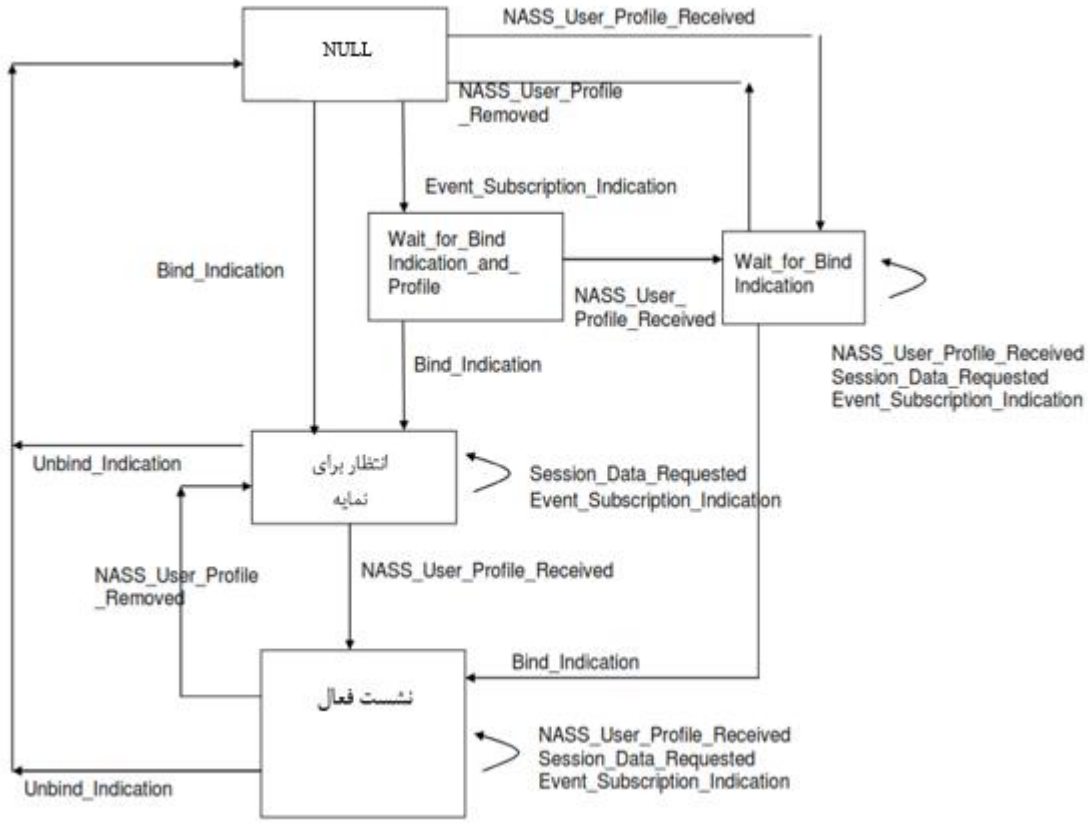
- *Event_Subscription_Indication*: این رویداد زمانی رخ می‌دهد که یک جریان اطلاعاتی درخواست ثبت رویداد (به زیربند ۵-۵-۱ مراجعه کنید) از AF دریافت شود.

یادآوری- زمانی که رویداد CLF واقعی روی می‌دهد، جریان اطلاعات درخواست اعلام رویداد به AF بازگردانده می‌شود. این امر هیچ انتقال حالت را در پی ندارد.

- *Bind_Indication*: این رویداد زمانی رخ می‌دهد که جریان اطلاعات نشان پیوند در نقطه مرجع a2 دریافت شود. (به زیربند ۵-۳-۲ مراجعه کنید.)
- *Unbind_Indication*: این رویداد زمانی رخ می‌دهد که جریان اطلاعات نشان عدم پیوند در نقطه مرجع a2 دریافت شده یا زمانی که جواب وصول منفی، در پاسخ به یک پرسمان اطلاعات پیوند دریافت شود. (به زیربند ۵-۳-۲ مراجعه کنید.)
- *NASS_User_Profile_Received*: این رویداد درصورت دریافت غیرهمزمان یک جریان اطلاعاتی پیش‌رانش[1] نمایه دسترسی در نقطه مرجع a4 یا در نتیجه ارسال یک جریان اطلاعات، پس‌رانش[2] نمایه دسترسی یا زمانی که داده پیکربندی درونی یک نمایه کاربر NASS پیش‌فرض را نشان دهد، روی می‌دهد.
- *NASS_User_Profile_Removed*: این رویداد زمانی رخ می‌دهد که جریان اطلاعات نمایه دسترسی برداشت شده در نقطه مرجع a4 دریافت می‌شود.
- *Session_Data_Requested*: این رویداد زمانی رخ می‌دهد که یک جریان اطلاعات پس‌رانش نمایه دسترسی در نقطه مرجع e4 یا یک جریان اطلاعات درخواست پرسمان اطلاعات در نقطه مرجع e2 دریافت شود. این امر باعث می‌شود پاسخ پرسمان اطلاعات یا یک جریان اطلاعات پیش‌رانش نمایه دسترسی به روی نقطه مرجع e2 یا e4 ارسال شود.

شکل ۵-۱-الف بررسی اجمالی گذارهای حالت مبتنی بر رویدادهای فوق را ارائه می‌دهد.

1- Push
2- Pull



شکل ۵-۱ الف- مدل حالت CLF برای مدیریت رکوردهای دسترسی

۵-۲-۴ کارکرد صدور مجوز و احراز اصالت کاربر

کارکرد صدور مجوز و احراز اصالت کاربر، احراز اصالت کاربر NASS را همراه با بررسی صدور مجوز، برای دسترسی شبکه، بر پایه نمایه‌های کاربر NASS انجام می‌دهد. برای هر کاربر NASS، UAAF داده‌های احراز اصالت و اطلاعات صدور مجوز دسترسی را از اطلاعات نمایه شبکه کاربر NASS مشمول در PDBF بازیابی می‌کند. همچنین UAAF مجاز است گردآوری داده‌های حسابرسی را برای هر کاربر NASS احراز اصالت شده توسط NASS اجرا کند.

کارکرد صدور مجوز و احراز اصالت کاربر همچنین می‌تواند به‌عنوان یک پیشکار عمل کند. در آن‌صورت پیشکار می‌تواند با UAAF که به‌عنوان کارساز حاوی داده‌های احراز اصالت کاربر PDBF NASS عمل می‌کند، ارتباط برقرار کرده و آن را مکان‌یابی کند. پیشکار UAAF می‌تواند درخواست‌های احراز اصالت و دسترسی را همراه با پیام‌های حسابرسی دریافت‌شده از AMF به سمت UAAF که به‌عنوان کارساز عمل می‌کند، هدایت کند. پاسخ‌های بازگشتی از UAFF عمل‌کننده به‌عنوان یک کارساز، از طریق پیشکار UAFF به AMF باز خواهدگشت.

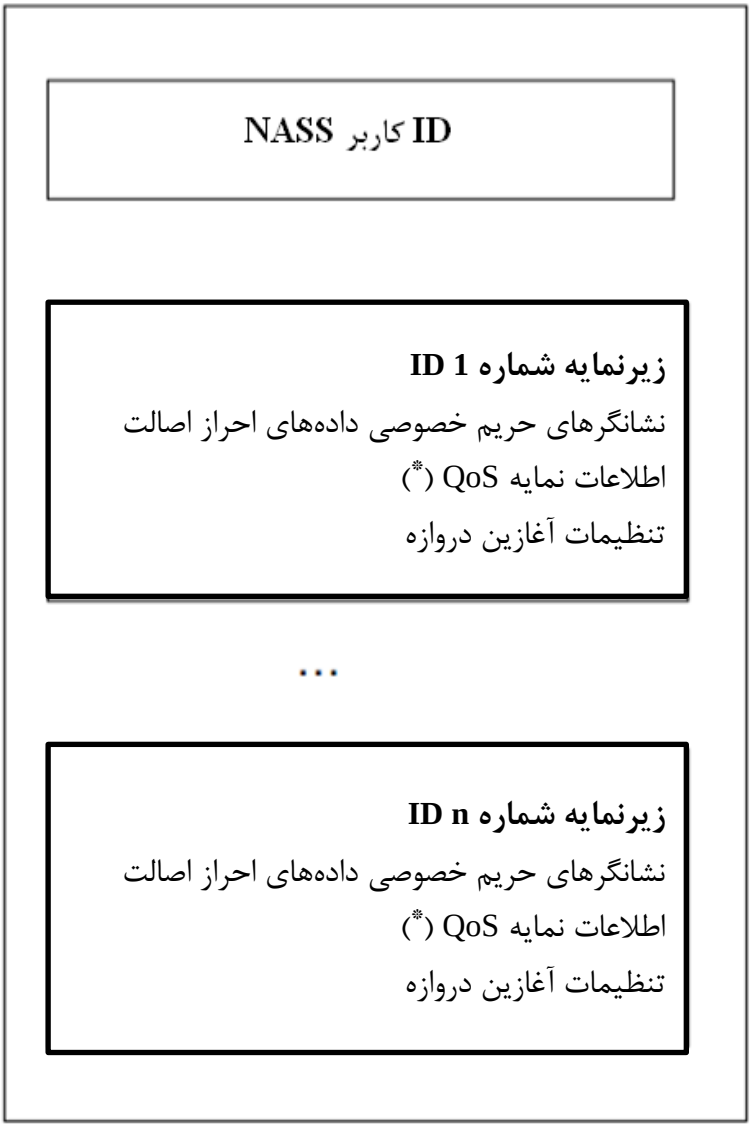
در صورتی‌که PPP به‌کار رود، AMF به PPP پایان داده و آن را به نشانک‌دهی روی واسط a3 ترجمه می‌کند. فرض بر این است که UAAF بتواند از طریق یک واسط درونی با NACF در تماس باشد تا یک نشانی IP را به‌دست آورد. (UAFF و NACF در کارکردهای درونی مورد PPP قرار دارند.) نقطه مرجع a1

نشانک‌دهی DHCP را حمل نمی‌کند، به جای آن واسط a3 برای ارائه اطلاعات پیکربندی IP به AMF استفاده می‌شود.

یادآوری- پشتیبانی از جابه‌جایی، شامل تمایز بین کاربر درخواست‌کننده دسترسی به شبکه و کاربر دارای دسترسی فیزیکی است که از طریق آن درخواست صادر می‌شود. تأثیر این تمایز روی UAAF به مطالعه بیشتر نیاز دارد.

۵-۲-۵ کارکرد دادگان نمایه

کارکرد دادگان نمایه، هستار کارکردی است که شامل داده احراز اصالت کاربر NASS (شناسه کاربر NASS، فهرست روش‌های احراز اصالت پشتیبانی شده، مواد کلیدی و غیره) و اطلاعات مربوط به پیکربندی مورد نیاز دسترسی شبکه است. این داده «نمایه شبکه کاربر NASS» نامیده می‌شود. نمایه شبکه کاربر NASS مجاز است به زیرنمایه‌هایی تقسیم شود (به شکل ۵-۲ مراجعه کنید) که هر یک از آنها به یک یا چند ID دسترسی منطقی مرتبط می‌شود. پشتیبانی از ID دسترسی منطقی اختیاری است.



(*) هر زیرنمایه مجاز است شامل بیش از یک مجموعه اطلاعات نمایه QoS باشد.

شکل ۵-۲- رکورد کاربر NASS در PDBF

کارکرد PDBF به پرسمان‌های UAAF روی نمایه کامل یا روی یک زیرنمایه خاص پاسخ می‌دهد. در مورد دوم، اشتقاق یک Id زیرنمایه از ID دسترسی منطقی، وظیفه UAAF (یا UAAF-پیشکار) است.
در این نشر، واسط بین UAAF و PDBF مشخص نمی‌شود، به‌عبارتی UAAF و PDBF یا هم مکان هستند یا توسط یک واسط استاندارد نشده به هم متصل می‌شوند.
PDBF می‌تواند با UPSF هم‌مکان باشد. (در استاندارد ES 282 001 (زیربند 2-2) توصیف می‌شود.)

۵-۲-۶ کارکرد پیکربندی CNG

کارکرد پیکربندی CNG، در طی راه‌اندازی و به‌روزرسانی CNG مورد استفاده قرار می‌گیرد. CNGCF اطلاعات پیکربندی افزونه CNG (به‌عنوان مثال، پیکربندی یک حفاظ در CNG به‌طور درونی، نشانه‌گذاری

QoS بستک‌های IP) را با توجه به اطلاعات پیکربندی ارائه شده توسط NACF فراهم می‌کند. این داده با داده‌های پیکربندی شبکه، ارائه شده توسط NACF تفاوت دارد.

همچنین CNGCF مجاز است هشدارهای CNG در زمینه قابلیت دسترسی تجهیزات پایانه را مدیریت کند. در واقع CNGCF مجاز است اطلاعات پیکربندی را به صورت غیرمستقیم از طریق CNG یا مستقیما برای تجهیزات TE فراهم کند. همچنین مجاز است آزمون‌های نگهداری و نتایج فرآیند ارسال شده توسط CNG یا تجهیزات TE را راه‌اندازی کند.

همچنین CNGCF مجاز است با CLF ارتباط داشته باشد تا اطلاعات مربوط به CNG و دسترسی متصل به آن را بازیابی کند. در چنین مواردی، CNGCF از رویه‌های توصیف شده در زیربند ۵-۵-۱ استفاده می‌کند. اطلاعات بازیابی‌شده از CLF (به‌عنوان مثال، شناسانه خط و/یا شناسانه کاربر NASS) مجازند به‌عنوان ورودی برای انتخاب داده‌های پیکربندی مورد استفاده قرار گیرند تا به CNG تحویل داده شوند.

۵-۲-۷ خالی

۵-۳ نقاط مرجع درونی

۵-۳-۱ خالی

۵-۳-۲ نقطه مرجع NACF – CLF

این نقطه مرجع به NACF امکان می‌دهد پیوند بین نشانی IP شناسه کاربر NASS تخصیص‌یافته و اطلاعات مکانی مربوط (ID لبه IP، ID خط) را در CLF ثبت کند.
جریان‌های اطلاعاتی زیر، روی واسط CLF به NACF مورد استفاده قرار می‌گیرند:

- نشانه پیوند.
- تأیید پیوند.
- نشانه عدم پیوند.
- پرسمان اطلاعات پیوند.
- تأیید پرسمان اطلاعات پیوند.

۵-۳-۲-۱ نشانه پیوند

جریان اطلاعات نشانه پیوند شامل اطلاعات مندرج در جدول ۵-۲ است:

جدول ۵-۲- نشانه پیوند (CLF - NACF)

نشانی منحصر به فرد جهانی	
– نشانی IP واگذارشده	نشانی IP تخصیص یافته به کاربر NASS.
– دامنه نشانی‌دهی	دامنه نشانی‌دهی است که در آن نشانی IP معنی‌دار است.
ID دسترسی فیزیکی (اختیاری)	شناسه دسترسی فیزیکی که کاربر NASS به آن متصل می‌شود.
ID دسترسی منطقی	شناسه دسترسی منطقی مورد استفاده کاربر NASS پیوست (به یادآوری ۱ مراجعه کنید.)
نوع پایانه (اختیاری)	نوع تجهیزات کاربر (به یادآوری ۲ مراجعه کنید.)
یادآوری ۱- چنانچه NACF به‌عنوان یک کارساز DHCP اجرا شود، این پارامتر روی گزینه ۸۲ [1]، زیر گزینه‌های ۱ و ۲ DHCP نگاشت می‌شود. **یادآوری ۲**- چنانچه NACF به‌عنوان یک کارساز DHCP اجرا شود، این پارامتر روی گزینه ۷۷ DHCP نگاشت می‌شود.	
۱- به شکل ۷-۳ الف مراجعه شود.	

۵-۳-۲-۲ تأیید پیوند

جریان اطلاعات تأیید پیوند، اطلاعاتی را انتقال می‌دهد که ممکن است به کاربر NASS بازگردانده شود. اطلاعات بازگشت شده توسط CLF در پاسخ به یک نمایش پیوند از UAAF دریافت می‌شود یا توسط PDBF از طریق UAAF بازیابی می‌شود. این جریان اطلاعات شامل عناصر مندرج در جدول ۵-۳ است.

جدول ۵-۳- تأیید پیوند (NACF - CLF)

نشانی CNGCF (اختیاری)	نشانی هستار CNGCF که بازیابی داده‌های پیکربندی از آن توسط تجهیزات کاربر مجاز است.
اطلاعات جغرافیایی مکان (اختیاری)	اطلاعات جغرافیایی مکان
شناسه P-CSCF (اختیاری)	شناسه P-CSCF برای دسترسی خدمات IMS

۵-۳-۲-۳ نشانه عدم پیوند

جریان اطلاعات عدم پیوند با خاتمه پیوند بین نشانی IP و شناسه کاربر NASS یا در هنگام آزادسازی اتصال اصلی PPP یا منبع لایه ۲، توسط NACF، ارسال می‌شود.

جدول ۵-۴- نشانه پیوند (CLF - NACF)

نشانی منحصر به فرد جهانی	
– نشانیIP واگذارشده	نشانی IP تخصیص‌یافته به کاربر NASS
– دامنه نشانی‌دهی	دامنه نشانی‌دهی که نشانی IP در آن معنی‌دار است.

۵-۳-۲-۴ پرسمان اطلاعات پیوند

جریان اطلاعاتی پرسمان اطلاعات پیوند برای درخواست اطلاعات پیوند (به‌عنوان مثال زمینه رویه‌های بهبود) از NACF، توسط CLF مورد استفاده قرار می‌گیرد.

جدول ۵-۴ الف- پرسمان اطلاعات پیوند (NACF - CLF)

نشانی منحصر به فرد جهانی	
– نشانی IP واگذارشده	نشانی IP تخصیص‌یافته به کاربر NASS
– دامنه نشانی‌دهی	دامنه نشانی‌دهی که نشانی IP در آن معنی‌دار است.

۵-۳-۲-۵ تأیید پرسمان اطلاعات پیوند

جریان اطلاعاتی تأیید پرسمان اطلاعات پیوند توسط NACF مورد استفاده قرار می‌گیرد تا CLF را از نتیجه درخواست اطلاعات پیوند آگاه کند. زمانی که پرسمان اطلاعاتی موفقیت‌آمیز باشد، جریان اطلاعات تأیید، حاوی اطلاعات مندرج در جدول ۵-۴ب است.

جدول ۵-۴ب- تأیید پرسمان اطلاعات پیوند (CLF - NACF)

ID دسترسی فیزیکی (اختیاری)	شناسه دسترسی فیزیکی که کاربر NASS به آن متصل می‌شود.
ID دسترسی منطقی	شناسه دسترسی منطقی مورد استفاده کاربر NASS پیوست است. (به یادآوری ۱ مراجعه کنید.)
نوع پایانه (اختیاری)	نوع تجهیزات کاربر (به یادآوری ۲ مراجعه کنید.)
یادآوری ۱- چنانچه NACF به‌عنوان یک کارساز DHCP اجرا شود، این پارامتر روی گزینه ۸۲، زیرگزینه‌های ۱ و ۲ DHCP نگاشت می‌شود. **یادآوری ۲**- چنانچه NACF به‌عنوان یک کارساز DHCP اجرا شود، این پارامتر روی گزینه ۷۷ DHCP نگاشت می‌شود.	

۵-۳-۳ خالی

۵-۳-۴ نقطه مرجع UAAF - CLF (a4)

این نقطه مرجع به CLF اجازه می‌دهد ارتباط بین شناسه کاربر NASS و اولویت‌های کاربر NASS را در زمینه حریم خصوصی اطلاعات مکانی ارائه‌شده توسط UAAF ثبت کند. نقطه مرجع a4 همچنین برای ثبت اطلاعات نمایه شبکه کاربر NASS (نمایه QoS) استفاده می‌شود. CLF مجاز است نمایه شبکه کاربر NASS را از UAAF بازیابی کند.

رابطه UAAF–CLF مجاز است در حالت پس‌رانش یا پیش‌رانش عمل کند. حالت پیش‌رانش زمانی استفاده می‌شود که UAAF در پردازش درخواست‌های دسترسی شبکه لحاظ شود تا دسترسی به شبکه مجاز شناخته شده یا رد شود. (به‌عنوان مثال، زمانی که احراز اصالت صریح مورد استفاده قرار می‌گیرد.) حالت پس‌رانش زمانی استفاده می‌شود که احراز اصالت ضمنی مورد استفاده قرار گیرد یا در پشتیبانی از رویه‌های بازیابی CLF استفاده شود.

جریان‌های اطلاعاتی زیر روی واسط CLF به UAAF استفاده می‌شوند:

- پیش‌رانش نمایه دسترسی.
- پس‌رانش نمایه دسترسی.
- نمایه دسترسی برداشت.

۵-۳-۴-۱ پیش‌رانش نمایه دسترسی

جریان اطلاعات پیش‌رانش نمایه دسترسی برای پیش‌راندن اطلاعات نمایه دسترسی از UAAF به CLF با احراز اصالت موفقیت‌آمیز کاربر NASS استفاده می‌شود. UAAF مجاز است تصمیم بگیرد برخی نمایه‌ها را به صورت id نمایه در همان پیش‌رانش نمایه دسترسی ارسال کند (به دلیل آنکه اطلاعات واقعی نمایه در CLF قابل دسترس فرض می‌شود) و برخی نمایه‌های دیگر را به صورت توصیفات نمایه کامل ارسال کند. این اطلاعات توسط UAAF از PDBF بازیابی می‌شود. این اطلاعات شامل عناصر مندرج در جدول ۵-۵ هستند.

یادآوری- در صورت کاربرد PPP، UAAF مجاز است ID دسترسی فیزیکی را برای CLF فراهم کند.

جدول ۵-۵- پیش‌رانش نمایه دسترسی

پیش‌رانش نمایه دسترسی (UAAF - CLF)	
ID کاربر NASS	شناسه کاربر NASS درخواست‌کننده اتصال IP
نشانی منحصر به فرد جهانی (به یادآوری ۳ مراجعه کنید.)	
– نشانی IP واگذارشده	نشانی IP کاربر NASS پیوست
– دامنه نشانی	دامنه نشانی‌دهی که نشانی IP در آن معنی‌دار است.
ID دسترسی منطقی	شناسه دسترسی منطقی مورد استفاده کاربر NASS پیوست
ID دسترسی فیزیکی (اختیاری)	شناسه دسترسی فیزیکی که کاربر NASS به آن متصل می‌شود.
نشانی CNGCF (اختیاری)	نشانی هستار CNGCF که بازیابی داده‌های پیکربندی توسط تجهیزات کاربر مجاز است.
شناسه P-CSCF (اختیاری)	شناسه P-CSCF برای دسترسی به خدمات IMS
نشانگر حریم خصوصی	آیا امکان ارسال بیرونی اطلاعات مکانی به خدمات و کاربردها وجود دارد یا خیر
اطلاعات نمایه QoS (به یادآوری ۱ مراجعه کنید.) (اختیاری)	
– ID نمایه QoS (به یادآوری ۵ مراجعه کنید.)	شناسه مجموعه‌ای از اطلاعات نمایه QoS
– توصیف نمایه QoS (به یادآوری ۵ مراجعه کنید.)	
– طبقه خدمت انتقال	طبقه خدمت انتقال به اشتراک گذاشته شده توسط کاربر NASS پیوست شده. طبقه خدمت انتقال با رفتار پیش‌رو در سطح انتقال در ارتباط است.
– نوع رسانه	نوع (انواع) رسانه‌هایی که نمایه QoS در آنها به‌کار می‌رود.
– پهنای باند به اشتراک گذاشته شده UL	بیشینه مقدار پهنای باند به اشتراک گذاشته شده توسط کاربر NASS پیوست در جهت پیوند فراسو.
– پهنای باند به اشتراک گذاشته شده DL	بیشینه مقدار پهنای باند به اشتراک گذاشته شده توسط کاربر NASS

پیش‌رانش نمایه دسترسی (UAAF - CLF)	
	پیوست در جهت پیوند فروسو.
– بیشینه اولویت	بیشینه اولویت مجاز برای هر درخواست ذخیره‌سازی.
– نام درخواست‌کننده	درخواست‌کننده(های) مجوزدار از طرف نمایه QoS را مشخص می‌کند.
تنظیم آغازین دروازه (به یادآوری ۲ مراجعه کنید.) (اختیاری)	
– ID تنظیم آغازین دروازه (به یادآوری ۶ مراجعه کنید.)	شناسه مجموعه‌ای از تنظیمات آغازین دروازه است
– توصیف تنظیم آغازین دروازه (به یادآوری ۶ مراجعه کنید.)	
– فهرست مقصدهای مجاز و جریان‌های چندپخشی	در مورد داده‌های تک‌پخشی، فهرست نشانی‌های IP با مقصد پیش‌فرض و/یا درگاه‌ها و/یا گستره‌های درگاه و/یا پیشوندهایی است که ترافیک به سمت آنها قابل ارسال است. در مورد چندپخشی، فهرست نشانی‌های گروه چندپخشی-IP و/یا فهرست (نشانی منبع IP، نشانی‌های گروه چندپخشی-IP) جفت‌هایی است که ترافیک توسط کاربر پیوست NASS از آنها قابل دریافت است. گستره‌های نشانی درون فهرست پشتیبانی می‌شوند. (به یادآوری ۴ مراجعه کنید.)
– فهرست مقصدهای ردشده و جریان‌های چندپخشی	در مورد تک‌پخشی، فهرست نشانی‌های IP با مقصد پیش‌فرض، درگاه‌ها، پیشوندها و گستره‌های درگاهی است که ترافیک به سمت آنها رد می‌شود. در مورد چندپخشی، فهرست نشانی‌های گروه چندپخشی-IP و/یا فهرست (نشانی منبع IP، نشانی‌های گروه چندپخشی-IP) جفت‌هایی است که برای آنها ترافیک به سمت کاربر پیوست NASS باید رد شود. گستره‌های نشانی درون فهرست پشتیبانی می‌شوند. (به یادآوری ۴ مراجعه کنید.)
– پهنای باند پیش فرضی UL	بیشینه مقدار پهنای باندی است که می‌تواند بدون صدور مجوز صریح در جهت پیوند فراسو مورد استفاده قرار گیرد.
– پهنای باند پیش فرضی DL	بیشینه مقدار پهنای باندی است که می‌تواند بدون صدور مجوز صریح در جهت پیوند فروسو مورد استفاده قرار گیرد.

یادآوری ۱- نمایه دسترسی مجاز است حاوی نمایه‌های QoS چندگانه باشد.

یادآوری ۲- پیش از آنکه درخواست‌های ذخیره‌سازی منبع از کاربردها/خدمات دریافت شوند، این اطلاعات توسط RACS برای پیکربندی کارکردپذیری RCEF استفاده می‌شود.

یادآوری ۳- در صورت کاربرد PPP، UAAF باید نشانی منحصر به فرد جهانی را برای CLF فراهم کند. در صورت کاربرد DHCP این پارامتر اختیاری است.

یادآوری ۴- چنانچه یک مقصد تک‌پخشی و/یا جریان چندپخشی در هیچ یک از دو فهرست وجود نداشته باشد، تصمیمات مربوط به تنظیمات دروازه برای آن نشانی‌ها تحت واپایش RACS قرار می‌گیرد.

یادآوری ۵- یکی از دو ID نمایه QoS یا توصیف نمایه QoS مجازند منظور شوند ولی هر دوی آنها به طور همزمان مجاز نیستند.

یادآوری ۶- توصیف تنظیمات آغازین دروازه یا ID تنظیمات آغازین دروازه مجازند لحاظ شوند اما هر دو آنها به طور همزمان مجاز نیستند.

۵-۳-۴-۲ پس‌رانش نمایه دسترسی

جریان اطلاعات پس‌رانش نمایه دسترسی توسط CLF استفاده می‌شود تا اطلاعات نمایه دسترسی از UAAF را درخواست کند. این جریان اطلاعاتی زمانی استفاده می‌شود که CLF-UAAF در حالت پس‌رانش یا در زمینه رویه‌های بازیابی CLF عمل کند. این اطلاعات شامل عناصر مندرج در جدول ۵-۶ هستند.

جدول ۵-۶- پس‌رانش نمایه دسترسی (UAAF - CLF)

نشانی منحصر به فرد جهانی (به یادآوری ۱ مراجعه کنید.)	
– نقطه انتهایی نشانی IP	نشانی IP کاربر NASS پیوست.
– دامنه نشانی	دامنه نشانی‌دهی که در آن نشانی IP معنی‌دار است.
ID دسترسی منطقی (اختیاری)	شناسه دسترسی منطقی مورد استفاده کاربر NASS پیوست
ID کاربر NASS (به یادآوری ۲ مراجعه کنید.)	شناسه کاربر NASS پیوست
یادآوری ۱- چنانچه جریان اطلاعاتی برای پشتیبانی از رویه‌های بازیابی مورد استفاده قرار گیرد و واسط در حالت پیش‌رانش عمل کند، نشانی منحصر به فرد جهانی باید لحاظ شود. **یادآوری ۲**- چنانچه واسط در حالت پس‌رانش عمل کند، ID کاربر NASS باید لحاظ شود.	

پاسخ به جریان اطلاعات پس‌رانش نمایه دسترسی، یک جریان اطلاعات پیش‌رانش نمایه دسترسی است.

۵-۳-۴-۳ نمایه دسترسی برداشت

جریان اطلاعات نمایه دسترسی برداشت توسط UAAF مورد استفاده قرار می‌گیرد تا از CLF خواسته شود اطلاعاتی که درباره یک کاربر NASS نگهداری کرده است را حذف کند. این رویداد در نتیجه فعالیت‌های مدیریت شبکه رخ می‌دهد.

جدول ۵-۷- نمایه دسترسی برداشت (CLF - UAAF)

نشانی منحصر به فرد جهانی (به یادآوری مراجعه کنید.)	
– نقطه انتهایی نشانی IP	نشانی IP کاربر NASS پیوست.
– دامنه نشانی	دامنه نشانی‌دهی که در آن نشانیIP معنی‌دار است.
ID نشانی منطقی (اختیاری)	شناسه دسترسی منطقی مورد استفاده توسط کاربر NASS پیوست.
ID کاربر NASS (به یادآوری مراجعه کنید)	شناسه کاربر NASS پیوست.
یادآوری- یکی از دو مورد نشانی منحصر به فرد جهانی یا Id کاربر NASS باید لحاظ شوند.	

۵-۳-۵ نقطه مرجع NACF – UAAF

این نقطه مرجع در این استاندارد مشخص نمی‌شود.

۵-۳-۶ نقطه مرجع UAAF – UAAF (e5)

این نقطه مرجع برای استفاده بین یک پیشکار-UAAF و یک کارساز-UAAF در نظر گرفته شده است که مجاز است در دامنه‌های اجرایی متفاوتی قرار داشته باشد. این نقطه مرجع به پیشکار-UAAF امکان می‌دهد از کارساز -UAAF، صدور مجوز و احراز اصالت مبتنی بر نمایه‌های کاربر NASS را درخواست کند. این نقطه همچنین به پیشکار-UAAF اجازه می‌دهد داده‌های حسابرسی را برای نشست خاص کاربر NASS به سمت کارساز-UAAF یا درخواست‌های دریافتی از یک CLF را هدایت می‌کند.

پیشکار-UAAF درخواست‌های صدور مجوز و دسترسی را همراه با پیام‌های حسابرسی دریافت شده روی واسط a3 از AMF به سمت کارساز-UAAF روی واسط e5 هدایت می‌کند. در عوض، پاسخ‌های دریافتی از کارساز-UAAF روی واسط e5 به سمت AMF روی واسط a3 رانش خواهد شد.

پیشکار-UAAF درخواست‌های دریافتی روی واسط a4 از CLF را به سمت کارساز -UAAF روی واسط e5 هدایت می‌کند. درعوض پاسخ‌های بازگشتی از کارساز-UAAF روی واسط e5 به سمت CLF روی واسط a4 رانش خواهد شد.

رابطه مطمئن دوطرفه به چیدمان بین پیشکار-UAAF و کارساز-UAAF نیاز خواهد داشت تا این تبادل را تسهیل کند.

بنابراین این واسط از تبادل پیام AAA بین پیشکار-UAAF و کارساز-UAAF پشتیبانی می‌کند. RADIUS[1] و Diameter[2] دو گزینه احتمالی برای پروتکل‌های حامل روی این واسط هستند. نمایه‌ها و الزامات مناسب برای این پروتکل‌ها بخشی از مرحله ۳ کار برای این واسط هستند.

۵-۳-۶-۱ اطلاعات مبادله‌شده روی e5

عناصر اطلاعاتی مندرج در جدول ۵-۸ روی نقطه مرجع e5 مبادله می‌شوند:

جدول ۵-۸- عناصر اطلاعاتی که روی نقطه مرجع e5 مبادله می‌شوند

عنصر اطلاعاتی	توصیف
ID کاربر NASS	شناسه کاربر NASS درخواست‌کننده اتصال IP
نشانگر حریم خصوصی	آیا امکان ارسال بیرونی اطلاعات مکانی به خدمات و کاربردها وجود دارد یا خیر
نشانی منحصر به فرد جهانی	
– نشانی IP واگذارشده	نشانی IP کاربر NASS پیوست
– دامنه نشانی	دامنه نشانی‌دهی که در آن نشانی IP معنی‌دار است.
اطلاعات نمایه QoS (به یادآوری ۱ مراجعه کنید.)	
– طبقه خدمت حمل و نقل	طبقه خدمت حمل و نقل به اشتراک گذاشته شده توسط کاربر

۱- شعاع

۲- قطر

عنصر اطلاعاتی	توصیف
	NASS پیوست. طبقه خدمت حمل و نقل به رفتار هدایت‌کننده در سطح حمل و نقل مرتبط است.
– نوع رسانه	نوع (انواع) رسانه‌هایی که نمایه QoS برای آنها به کار می‌رود.
– پهنای باند به اشتراک گذاشته شده UL	بیشینه مقدار پهنای باند به اشتراک گذاشته شده توسط کاربر NASS پیوست در جهت پیوند فراسو.
– پهنای باند به اشتراک گذاشته شده DL	بیشینه مقدار پهنای باند به اشتراک گذاشته شده توسط کاربر NASS پیوست در جهت پیوند فروسو.
– بیشینه اولویت	بیشینه اولویت مجاز برای هر نوع درخواست ذخیره‌سازی .
– نام درخواست‌کننده	درخواست‌کننده(هایی) را شناسایی می‌کند که توسط نمایه QoS مجاز شده است(اند).
تنظیمات آغازین دروازه (به یادآوری ۲ مراجعه کنید.) (اختیاری)	
– فهرست مقصدهای مجاز همراه با جریان‌های چندپخشی	در مورد تک‌پخشی، فهرست نشانی‌های IP با مقصد پیش‌فرض و/یا درگاه‌ها و/یا گستره‌های درگاه‌ها و/یا پیشوندهایی است که ترافیک به سمت آنها قابل ارسال است. در مورد چندپخشی، فهرست نشانی‌های گروه چندپخشی-IP و/یا فهرست (نشانی منبع IP، نشانی گروه چندپخشی-IP) جفت‌هایی است که ترافیک از آنها توسط کاربر پیوست NASS قابل دریافت است. گستره‌های نشانی درون فهرست پشتیبانی می‌شوند. (به یادآوری ۳ مراجعه کنید.)
– فهرست مقصد ردشده همراه با جریان‌های چندپخشی	در مورد تک‌پخشی، فهرست نشانی‌های IP با مقصد پیش‌فرض، درگاه‌ها، پیشوندها و گستره‌های درگاهی است که ترافیک به سمت آنها رد می‌شود. در مورد چندپخشی، فهرست نشانی‌های گروه چندپخشی-IP و/یا فهرست (نشانی منبع IP، نشانی‌های گروه چندپخشی-IP) جفت‌هایی است که برای آنها ترافیک به سمت کاربر پیوست NASS باید رد شود. گستره‌های نشانی درون فهرست پشتیبانی می‌شوند. (به یادآوری ۳ مراجعه کنید.)
– پهنای باند پیش‌فرض UL	بیشینه مقدار پهنای باندی است که می‌تواند بدون صدور مجوز صریح در جهت پیوند فراسو مورد استفاده قرار گیرد.
– پهنای باند پیش‌فرض DL	بیشینه مقدار پهنای باندی است که می‌تواند بدون صدور مجوز صریح در جهت پیوند فروسو مورد استفاده قرار گیرد.

یادآوری ۱- نمایه دسترسی مجاز است شامل نمایه‌های چندگانه QoS باشد.

یادآوری ۲- پیش از دریافت درخواست‌های ذخیره‌سازی منبع از کاربردها/خدمات، این اطلاعات توسط RACS برای پیکربندی کارکردپذیری RCEF مورد استفاده قرار می‌گیرد.

یادآوری ۳- چنانچه یک جریان چندپخشی و/یا مقصد تک‌پخشی در هیچ یک از دو فهرست وجود نداشته باشد، تصمیمات مربوط به تنظیم دروازه‌راه برای آن نشانی‌ها تحت واپایش RACS قرار می‌گیرند.

۵-۴ واسط با زیرسامانه واپایش تصدیق و منبع (RACS)

۵-۴-۱ واسط بین CLF و RACF (e4)

این نقطه مرجع برای ارتباط بین نشانی منحصر به فرد جهانی و/یا ID کاربر NASS از یک طرف و شناسانه دسترسی (فیزیکی یا منطقی) از سوی دیگر، از CLF به RACS مورد استفاده قرار گیرد. این نقطه به RACS اجازه می‌دهد تا مقدار منابع شبکه موجود را تعیین کند. همچنین نقطه مرجع e4 مجاز است برای گذر دادن اطلاعات نمایه QoS و تنظیمات آغازین دروازه‌راه از CLF به RACS مورد استفاده قرار گیرد. این امر به RACS اجازه می‌دهد در هنگام پردازش درخواست‌های تخصیص منبع، آنها را در نظر بگیرد. اطلاعات مبادله شده روی نقطه مرجع e4 عبارتند از:

- پیوند بین ID دسترسی منطقی (ID خط)، نشانی IP واگذارشده و ID لبه IP، اطلاعات نمایه شبکه کاربر NASS برای ملاحظه آنها در هنگام پردازش درخواست‌های تخصیص منبع.

جریان‌های اطلاعاتی زیر، روی واسط CLF به A-RACF استفاده می‌شوند:

- پیش‌رانش نمایه دسترسی.
- پس‌رانش نمایه دسترسی.
- نشانه آزادسازی اتصال IP.

۵-۴-۱-۱ پیش‌رانش نمایه دسترسی

جریان اطلاعاتی پیش‌رانش نمایه دسترسی برای پیش‌راندن اطلاعات نمایه دسترسی از CLF به A-RACF استفاده می‌شود. بهتر است اطلاعات از داده‌های پیکربندی یا از نمایه کاربر NASS (به عبارتی در PDBF) به سمت CLF که نشانی هستار A-RACF را می‌داند، هدایت شود. این جریان اطلاعاتی زمانی رخ می‌دهد که واپایش تصدیق منبع برای یک کاربر NASS الزامی باشد. این جریان می‌تواند در موارد زیر روی دهد:

- زمانی که یک نشانی IP به‌عنوان قسمتی از فرآیند پیوست اولیه شبکه به یک کاربر NASS تخصیص داده شده است؛
- پس از تکمیل موفقیت‌آمیز مرحله صدور مجوز و احراز اصالت رویه پیوست شبکه NASS (به منظور گشایش دروازه برای ادامه با مرحله دوم (پیکربندی IP) رویه پیوست شبکه)؛
- در صورتی که اصلاحی روی نمایه انجام شود که از قبل به سمت RACS هدایت شده است.

مکان CLF مجاز است تصمیم بگیرد برخی نمایه‌ها را به شکل یک id نمایه در همان پیش‌رانش نمایه دسترسی (به دلیل اینکه اطلاعات واقعی نمایه در A-RACF قابل دسترس فرض می‌شوند) و برخی دیگر را به شکل توصیف‌های نمایه کامل ارسال کند. پیش‌رانش نمایه دسترسی شامل مؤلفه‌های مندرج در جدول ۵-۹ می‌شود:

جدول ۵-۹- پیش‌رانش نمایه دسترسی (A-RACF - CLF)

پیش‌رانش نمایه دسترسی (A-RACF - CLF)	
ID کاربر NASS	شناسه کاربر NASS درخواست‌کننده اتصال IP
ID دسترسی فیزیکی (اختیاری)	شناسه دسترسی فیزیکی است که کاربر NASS به آن متصل می‌شود. (به یادآوری ۱ مراجعه کنید.)
ID دسترسی منطقی	شناسه دسترسی منطقی است که کاربر NASS به آن متصل می‌شود. (به یادآوری‌های ۲ و ۳ مراجعه کنید.)
نوع شبکه دسترسی	نوع شبکه دسترسی است که اتصال IP روی آن برای کاربر NASS ارائه می‌شود.
نشانی IP منحصر به فرد جهانی	
– نشانی IP واگذارشده	نشانی IP کاربر NASS پیوست
– دامنه نشانی	دامنه نشانی‌دهی که در آن نشانی IP معنی‌دار است.
اطلاعات نمایه QoS (به یادآوری ۴ مراجعه کنید.) (اختیاری)	
– ID نمایه QoS (به یادآوری ۷ مراجعه کنید.)	شناسانه مجموعه‌ای از اطلاعات نمایه QoS است.
– توصیف نمایه QoS (به یادآوری ۷ مراجعه کنید.)	
– طبقه خدمت حمل و نقل	طبقه خدمت حمل و نقل به اشتراک گذاشته شده توسط کاربر NASS. طبقه خدمت حمل و نقل به رفتار پیش‌رونده در سطح حمل و نقل مربوط می‌شود.
– نوع رسانه	نوع (انواع) رسانه‌هایی که نمایه QoS برای آنها به کار می‌رود.
– پهنای باند به اشتراک گذاشته شده UL	بیشینه مقدار پهنای باند به اشتراک گذاشته شده توسط کاربر NASS پیوست در جهت پیوند فراسو.
– پهنای باند به اشتراک گذاشته شده DL	بیشینه مقدار پهنای باند به اشتراک گذاشته شده توسط کاربر NASS پیوست در جهت پیوند فروسو.
– بیشینه اولویت	بیشینه اولویت مجاز برای هر نوع درخواست ذخیره‌سازی.
– نام درخواست‌کننده	درخواست‌کننده‌ای(هایی) را شناسایی می‌کند که توسط نمایه QoS مجاز شده است (اند).
تنظیمات آغازین دروازه‌راه (به یادآوری ۵ مراجعه کنید.) (اختیاری)	
– ID تنظیمات آغازین دروازه‌راه (به یادآوری ۸ مراجعه کنید.)	شناسانه مجموعه‌ای از تنظیمات آغازین دروازه‌راه است.
– توصیف تنظیمات آغازین دروازه‌راه (به یادآوری ۸ مراجعه کنید.)	
– فهرست مقصدهای مجاز به همراه جریان‌های چندپخشی	در مورد تک‌پخشی، فهرست نشانی‌های IP با مقصد پیش‌فرض و/یا درگاه‌ها و/یا گستره‌ها درگاهی و/یا پیشوندهایی است که ترافیک به سمت آنها قابل ارسال است. در مورد چندپخشی، فهرست نشانی‌های گروه چندپخشی-IP و/یا فهرست (نشانی منبع IP، نشانی گروه چندپخشی-IP) جفت‌هایی است که ترافیک توسط کاربر پیوست NASS از آنها قابل دریافت است. گستره‌های نشانی درون فهرست پشتیبانی می‌شوند. (به یادآوری ۶ مراجعه کنید.)

پیش‌رانش نمایه دسترسی (A-RACF - CLF)	
– فهرست مقصدهای ردشده[1] به همراه جریان‌های چندپخشی	در مورد تک‌پخشی، فهرست نشانی‌های IP با مقصد پیش‌فرض، درگاه‌ها، پیشوندها و گستره‌های درگاهی است که ترافیک به سمت آنها رد می‌شود. در مورد چندپخشی، فهرست نشانی‌های گروه چندپخشی-IP و/یا فهرست (نشانی منبع IP، نشانی‌های گروه چندپخشی-IP) جفت‌هایی است که برای آنها ترافیک به سمت کاربر پیوست NASS باید رد شود. گستره‌های نشانی درون فهرست پشتیبانی می‌شوند. (به یادآوری ۶ مراجعه کنید.)
– پهنای باند پیش‌فرض UL	بیشینه مقدار پهنای باندی است که می‌تواند بدون صدور مجوز صریح در جهت پیوند فراسو مورد استفاده قرار گیرد.
– پهنای باند پیش‌فرض DL	بیشینه مقدار پهنای باندی است که می‌تواند بدون صدور مجوز صریح در جهت پیوند فروسو مورد استفاده قرار گیرد.
یادآوری ۱- در مورد xDSL، ID دسترسی فیزیکی معرف سیم مسی است. **یادآوری ۲**- بهتر است ID دسترسی منطقی RACS را قادر سازد اطلاعات زیر را استنباط کند: شناسایی و ظرفیت پهنای باند منابع لایه ۲ که ترافیک کاربر NASS روی آن حمل می‌شود. نشانی گره(های) فیزیکی پیاده‌کننده BGF و RCEF . **یادآوری ۳**- در مورد xDSL، ID دسترسی منطقی مجاز است آشکارا شامل شناسه درگاه، حامل ترافیک VP و/یا حامل ترافیک VC باشد. **یادآوری ۴**- نمایه دسترسی مجاز است شامل نمایه چندگانه QoS باشد. **یادآوری ۵**- پیش از دریافت درخواست‌های ذخیره‌سازی منبع، از کاربردها/خدمات، اطلاعات توسط RACS برای پیکربندی کارکردپذیری RCEF مورد استفاده قرار می‌گیرد. **یادآوری ۶**- چنانچه یک مقصد تک‌پخشی و/یا جریان چندپخشی در یکی از دو فهرست ظاهر نشود، تصمیمات تنظیم دروازه برای آن نشانی‌ها تحت واپایش RACS قرار می‌گیرد. **یادآوری ۷**- یکی از دو ID نمایه QoS یا توصیف نمایه QoS مجازند لحاظ شوند ولی هر دوی آنها به طور همزمان، مجاز نیستند. **یادآوری ۸**- یکی از دو مورد توصیف تنظیمات آغازین دروازه یا ID تنظیمات آغازین دروازه مجازند لحاظ شوند اما هر دو آنها به طور همزمان، مجاز نیستند.	
1 -Denied	

۵-۴-۱-۲ پس‌رانش نمایه دسترسی

جریان پس‌رانش اطلاعات نمایه دسترسی توسط RACS برای درخواست اطلاعات نمایه دسترسی از CLF (به‌عنوان مثال، در زمینه رویه‌های بازیابی) مورد استفاده قرار می‌گیرد. این اطلاعات شامل عناصر مندرج در جدول ۵-۱۰ است:

جدول ۵-۱۰- پس‌رانش نمایه دسترسی (A-RACF - CLF)

نقطه انتهایی نشانی IP	نشانی IP کاربر NASS پیوست
دامنه نشانی	دامنه نشانی‌دهی که درآن نشانی IP معنی‌دار است.
ID کاربر NASS (اختیاری)	شناسه کاربر NASS پیوست

پاسخ به جریان اطلاعات پس‌رانش نمایه دسترسی، یک جریان اطلاعاتی پیش‌رانش نمایه دسترسی است.

۵-۴-۱-۳ نشانه آزادسازی اتصال IP

جریان اطلاعاتی نشانه آزادسازی اتصال IP توسط NASS که برای گزارش از دست رفتن اتصال IP استفاده می‌شود. این امر RACS را قادر می‌سازد نمایه دسترسی را از دادگان درونی بردارد. این رویداد در صورت

رهاسازی نشانی IP تخصیص‌یافته (به‌عنوان مثال پایان زمان‌سنج استیجاری DHCP) یا در نتیجه آزادسازی منابع اصلی لایه ۲ رخ می‌دهد.

جدول ۵-۱۱ - نشانه آزادسازی اتصال (A-RACF - CLF)

نقطه انتهایی نشانی IP	نشانی IP کاربر NASS پیوست
دامنه نشانی	دامنه نشانی‌دهی که در آن نشانی IP معنی‌دار است.
ID کاربر NASS (اختیاری)	شناسه کاربر NASS پیوست

۵-۵ واسط‌های بین NASS و سطح کاربرد و زیرسامانه‌های واپایش خدمت

۵-۵-۱ واسط بین کارکردهای کاربردی و CLF (e2)

این نقطه مرجع، امکانی را برای AF فراهم می‌کند تا اطلاعات مربوط به مشخصه‌های نشست اتصال IP را که برای دسترسی این نوع کاربردها (به‌عنوان مثال اطلاعات مکانی شبکه) به‌کار می‌روند، از CLF بازیابی کند. همچنین مجاز است این اطلاعات توسط یک CNGCF برای بازیابی اطلاعات از CLF مورد استفاده قرار گیرد.

در متن این استاندارد، کارکرد کاربردی یک اصطلاح کلی برای نمایش هر جزء از معماری لایه خدماتی ارائه‌دهنده -یا فراهم‌کننده دسترسی به- کاربردهایی است که به اطلاعاتی درباره مشخصه‌های نشست اتصال IP نیاز دارد که جهت دسترسی به این نوع کاربردها مورد استفاده قرار گرفته‌اند. نمونه‌هایی از این نوع کارکردهای کاربردی P-CSCF و IBCF در IMS (استاندارد ES 282 007 (زیربند 2-2-2)) هستند، رده‌های خاص کارکردهای کارساز کاربردی (ASF) (استاندارد ES 282 001 (زیربند 2-2)) یا یک PNA در مشخصات فنی TS 182 008 (زیربند 2-6) تعریف شده است.

شکل اطلاعات مکانی که توسط CLF ارائه می‌شود، به درخواست‌کننده وابسته است.

جریان‌های اطلاعاتی زیر روی واسط CLF به AF مورد استفاده قرار می‌گیرند:

- درخواست پرسمان اطلاعات.
- پاسخ پرسمان اطلاعات.
- درخواست ثبت رویداد.
- پاسخ ثبت رویداد.
- درخواست رویداد اعلام.
- پاسخ رویداد اعلام.

۵-۵-۱-۱ درخواست پرسمان اطلاعات

جریان اطلاعاتی درخواست پرسمان اطلاعات شامل اطلاعات مندرج در جدول ۵-۱۲ است:

جدول ۵-۱۲ - درخواست پرسمان اطلاعات (AF - CLF)

نشانی IP منحصر به فرد جهانی (به یادآوری ۱ مراجعه کنید)	
– نشانی IP تخصیص‌یافته	نشانی IP کاربر NASS
– دامنه نشانی	دامنه نشانی‌دهی که در آن نشانی IP معنی‌دار است. (به یادآوری ۲ مراجعه کنید.)
ID کاربر NASS (به یادآوری ۱ مراجعه کنید)	شناسه کاربر NASS پیوست.
شناسه AF	شناسه کارکرد کاربردی درخواست‌کننده
یادآوری ۱- یکی از دو مورد نشانی IP منحصر به فرد جهانی یا ID کاربر NASS باید لحاظ شوند. **یادآوری ۲**- دامنه نشانی‌دهی توسط AF یا با استفاده از داده‌های پیکربندی (که در این مورد تمام کاربرهای NASS توسط AF به همان دامنه نشانی‌دهی تعلق دارند) یا از واسط منطقی یا فیزیکی شناخته می‌شود که درخواست خدمات راه‌اندازی کننده پرسمان مکان روی آن دریافت شده است.	

۵-۵-۱-۲ پاسخ پرسمان اطلاعات

جریان‌های اطلاعاتی پاسخ پرسمان اطلاعات، شامل اطلاعات مندرج در جدول شماره ۵-۱۳ هستند:

جدول ۵-۱۳- پاسخ پرسمان اطلاعات (AF - CLF)

ID کاربر NASS (اختیاری)	شناسه کاربر NASS پیوست (به یادآوری ۱ مراجعه کنید.)
اطلاعات مکان (اختیاری) (به یادآوری ۲ مراجعه کنید.)	اطلاعات مکانی (یا یک نشانگر به این‌گونه اطلاعات) به شکلی که برای کاربرد درخواست کننده مناسب باشد.
نقطه تماس RACS (اختیاری)	نشانی IP یا FQDN هستار RACS در جایی که درخواست منبع باید ارسال شود (به عبارتی نشانی SPDF).
نوع پایانه (اختیاری)	نوع تجهیزات کاربر.
نوع شبکه دسترسی (اختیاری)	نوع شبکه دسترسی که اتصال IP روی آن برای کاربر NASS ارائه می‌شود.
ID دسترسی فیزیکی (اختیاری)	شناسه دسترسی فیزیکی که کاربر NASS به آن متصل می‌شود. (به یادآوری ۲ مراجعه کنید)
ID دسترسی منطقی (اختیاری)	شناسه دسترسی منطقی که کاربر NASS به آن متصل می‌شود. (به یادآوری ۲ مراجعه کنید)
یادآوری ۱- این شناسه مجاز است در هنگام تعامل با RACS توسط AF استفاده شود. **یادآوری ۲**- افشای این اطلاعات به کاربرد درخواست‌کننده و محدودیت‌های حریم خصوصی کاربر NASS وابسته است. محدودیت‌های حریم خصوصی در نشانگر حریم خصوصی ذخیره شده در CLF تعریف می‌شود.	

۵-۵-۱-۳ درخواست ثبت رویداد

جریان اطلاعاتی درخواست ثبت رویداد شامل اطلاعات مندرج در جدول ۵-۱۴ است:

جدول ۵-۱۴- درخواست ثبت رویداد (AF - CLF)

دوره زمانی اشتراک	دوره‌ای است که اشتراک یک رویداد خاص برای آن فعال خواهد بود.
ID کاربر NASS (اختیاری)، (به یادآوری ۱ مراجعه کنید.)	شناسه کاربر NASS پیوست (در مورد رویدادهای خاص کاربر NASS، مانند مثال رویداد ثبت ورود-کاربر-NASS).
رویداد	نوع-رویداد (به‌عنوان مثال، رویداد ثبت ورود کاربر NASS) و قالب برای توصیف اعلام/رله رویداد
نشانی IP منحصر به فرد جهانی (اختیاری)، (به یادآوری ۱ مراجعه کنید)	نشانی منحصر به فرد جهانی که با UNI مرتبط با کاربر NASS پیوست‌شده به شبکه، متناظر است.
– نشانی IP تخصیص‌یافته	نشانی IP کاربر NASS [Ipv4 یا Ipv6]
– دامنه نشانی	دامنه نشانی‌دهی که در آن نشانی IP معنی‌دار است. (به یادآوری ۲ مراجعه کنید.)
شناسه AF (اختیاری)	شناسه کارکرد کاربردی درخواست‌کننده.
یادآوری ۱- دست کم یکی از دو شناسانه (ID کاربر NASS یا نشانی IP منحصر به فرد جهانی) باید تامین شود. **یادآوری ۲**- دامنه نشانی‌دهی توسط AF یا با استفاده از داده‌های پیکربندی (که در این مورد تمام کاربرهای NASS کارسازی شده توسط AF به همان دامنه نشانی‌دهی تعلق دارند) یا از واسط منطقی یا فیزیکی شناخته می‌شود که درخواست خدمات مرتبط روی آن دریافت شده بود.	

چنانچه AF یک P-CSCF باشد، این جریان اطلاعاتی کاربرد ندارد.

۵-۵-۱-۴ پاسخ ثبت رویداد

جریان اطلاعاتی پاسخ ثبت رویداد شامل اطلاعات زیر است.

جدول ۵-۱۵- پاسخ ثبت رویداد (AF - CLF)

اقدام به‌روزرسانی	اقدام/ اطلاعات اجرایی برای یک رویداد: به‌عنوان مثال فعال‌شده (ثبت رویدادی که به طور موفقیت‌آمیز دریافت شده است و اعلام رویداد برای «رویداد» فعال شده.)
ID کاربر NASS (به یادآوری مراجعه کنید.)	شناسه کاربر NASS پیوست (در مورد رویدادهای مخصوص کاربر مانند رویداد ثبت ورود-کاربر NASS.)
رویداد	نوع-رویداد (به عنوان مثال، رویداد ثبت ورود کاربر NASS.)
نشانی منحصر به فرد جهانی (به یادآوری مراجعه کنید.)	نشانی منحصر به فرد جهانی که با UNI مرتبط با کاربر NASS پیوست‌شده به شبکه متناظر است.
– نشانی IP تخصیص یافته	نشانی IP کاربر NASS پیوست
– دامنه نشانی	دامنه نشانی‌دهی که در آن نشانی IP معنی‌دار است.
یادآوری- دست کم یکی از دو شناسه (ID کاربر NASS یا نشانی IP منحصر به فرد جهانی) باید تأمین شود.	

چنانچه AF یک P-CSCF باشد، این جریان اطلاعاتی کاربرد ندارد.

۵-۵-۱-۵ درخواست رویداد اعلام

جریان اطلاعاتی درخواست رویداد اعلام شامل اطلاعات مندرج در جدول ۵-۱۶ است:

جدول ۵-۱۶- درخواست رویداد اعلام (AF -> CLF)

نشانی منحصر به فرد جهانی	
– نشانی IP واگذارشده	نشانی IP کاربر NASS پیوست است.
– دامنه نشانی	
ID کاربر NASS	شناسه کاربر NASS پیوست است.
رویداد	رویداد (به‌عنوان مثال رویداد ثبت ورود کاربر NASS)

چنانچه AF یک P-CSCF باشد، این جریان اطلاعاتی کاربرد ندارد.

۵-۵-۱-۶ پاسخ رویداد اعلام

جریان اطلاعاتی پاسخ رویداد اعلام شامل اطلاعات مندرج در جدول ۵-۱۷ است:

جدول ۵-۱۷- پاسخ رویداد اعلام (CLF -> AF)

نشانی منحصر به فرد جهانی	نشانی منحصر به فرد جهانی که با UNI مرتبط با کاربر NASS پیوست به شبکه متناظر است.
– نشانی IP تخصیص‌یافته	نشانی IP کاربر NASS پیوست است.
– دامنه نشانی	دامنه نشانی‌دهی که در آن نشانی IP معنی‌دار است.
ID کاربر NASS	شناسه کاربر NASS پیوست است.
رویداد	نوع-رویداد
نتیجه	کد نتیجه (به‌عنوان مثال، موفقیت، شکست دائمی و غیره)

چنانچه AF یک P-CSCF باشد، این جریان اطلاعاتی کاربرد ندارد.

۵-۶ نقاط مرجع بین NASS و تجهیزات کاربر

۵-۶-۱ احراز اصالت و تخصیص نشانی IP (e1)

هیچ نقطه مرجع مستقیمی بین NASS و تجهیزات کاربر برای پشتیبانی از احراز اصالت و تخصیص نشانی IP وجود ندارد. ارتباط بین NASS و تجهیزات کاربر از طریق ARF و AMF روی می‌دهد.

واسط e1 مجاز است در طرف UE روی یک CNG یا یک TE پایان‌دهی شود؛ مورد دوم زمانی به‌کار می‌رود که TE اتصال مستقیمی با NASS داشته باشد.

این نقطه مرجع، UE را قادر می‌سازد درخواست‌ها برای تخصیص نشانی IP و دیگر پارامترهای ممکن پیکربندی شبکه را به‌منظور دسترسی به شبکه راه‌اندازی کند. این درخواست‌ها توسط AMF از طریق ARF دریافت می‌شوند.

درخواست‌ها برای تخصیص نشانی IP و پارامترهای پیکربندی شبکه یا به شکل درخواست DHCP یا درخواست PPP هستند.

در مورد DHCP افزایش توسعه، این طور فرض می‌شود که لبه IP در صفحه حمل و نقل شامل یک کارکرد رله دسترسی (ARF) است که به‌عنوان رله DHCP، بین کارخواه DHCP در تجهیزات کاربر و کارساز DHCP در زیرسامانه پیوست شبکه کار می‌کند.

پیش از ارسال درخواست به زیرسامانه پیوست شبکه، کارکرد رله مجاز است اطلاعات مکانی شبکه را به اطلاعات دریافت شده از کاربر NASS بیافزاید. نقطه مرجع، تجهیزات کاربر را قادر می‌سازد اعتبارنامه‌های کاربر NASS (کلمه عبور، نشان، گواهی و غیره) را به زیرسامانه پیوست شبکه (NASS) ارائه دهد تا احراز اصالت دسترسی شبکه اجرا شود. این نقطه مرجع همچنین مجاز است NASS را قادر سازد پارامتر احراز اصالت را برای UE فراهم کند تا در هنگام نیاز به رویه احراز اصالت دو جانبه، احراز اصالت شبکه انجام شود. بر پایه نتیجه احرازاصالت، AMF دسترسی شبکه به تجهیزات کاربر را مجاز دانسته یا رد می‌کند.

یادآوری- در هنگام استفاده از DHCP برای تخصیص نشانی IP و پیکربندی تجهیزات کاربر روی واسط (e1)، IEEE 802.IX و PANA پروتکل‌های انتخاب شده برای احراز اصالت هستند (e1).

۵-۶-۲ واسط بین CNGCF و CNG (e3)

این نقطه مرجع به CNGCF امکان می‌دهد تا CNG آزمون‌های نگهداری راه‌انداز، پایش عملکرد و هشدارهای دریافت را پیکربندی کند. واسط e3 در حین راه‌اندازی و به‌روزرسانی CNG مورد استفاده قرار می‌گیرد تا اطلاعات افزونه پیکربندی شبکه برای CNG فراهم شود زمانی که این اطلاعات، برای ایجاد امکان دسترسی CNG به کاربردها/خدمات TISPAN، روی واسط (e1) قابل دسترس نیستند.

همچنین CNGCF مجاز است افزاره‌های TE متصل به یک CNG را به‌طور غیرمستقیم از طریق CNG یا مستقیما در تجهیزات TE، برای پیکربندی، نگهداری، پایش عملکرد و اهداف هشدار، مدیریت کند.

نقطه مرجع e3 باید از رویه‌های زیر پشتیبانی کند:

- احراز اصالت/شناسایی CNG به CNGCF (به‌عنوان مثال برای ارسال اطلاعات مناسب پیکربندی (به‌روزرسانی میان‌افزار)) از CNGCF.
- احراز اصالت CNGCF به CNG قبل از اینکه یک CNG به‌عنوان مثال پیکربندی راه دور را بپذیرد.
- آزمون‌های نگهداری راه‌انداز از CNGCF و گزارش نتایج آزمون از CNG.
- پیکربندی CNG.
- اعلان CNGCF درباره قابلیت دسترسی TE.
- ارائه پیکربندی و به‌روزرسانی برای افزاره‌های TE.
- آزمون‌های نگهداری راه‌انداز از CNGCF و گزارش نتایج آزمون از تجهیزات TE.

یادآوری- TR-069 (مجمع DSL)، HTTP، FTP و TFTP پروتکل‌های نامزد برای این واسط هستند.

۵-۶-۳ نقاط مرجع با AMF

این نقطه مرجع (a1) به AMF اجازه می‌دهد از NACF درخواست کند یک نشانی IP را به تجهیزات کاربر و همچنین دیگر پارامترهای پیکربندی شبکه تخصیص دهد.

این نقطه مرجع (a3) به AMF اجازه می‌دهد از UAAF برای احراز اصالت کاربر NASS و بررسی اشتراک شبکه درخواست کند.

۶ نگاشت روی نقش‌های شبکه

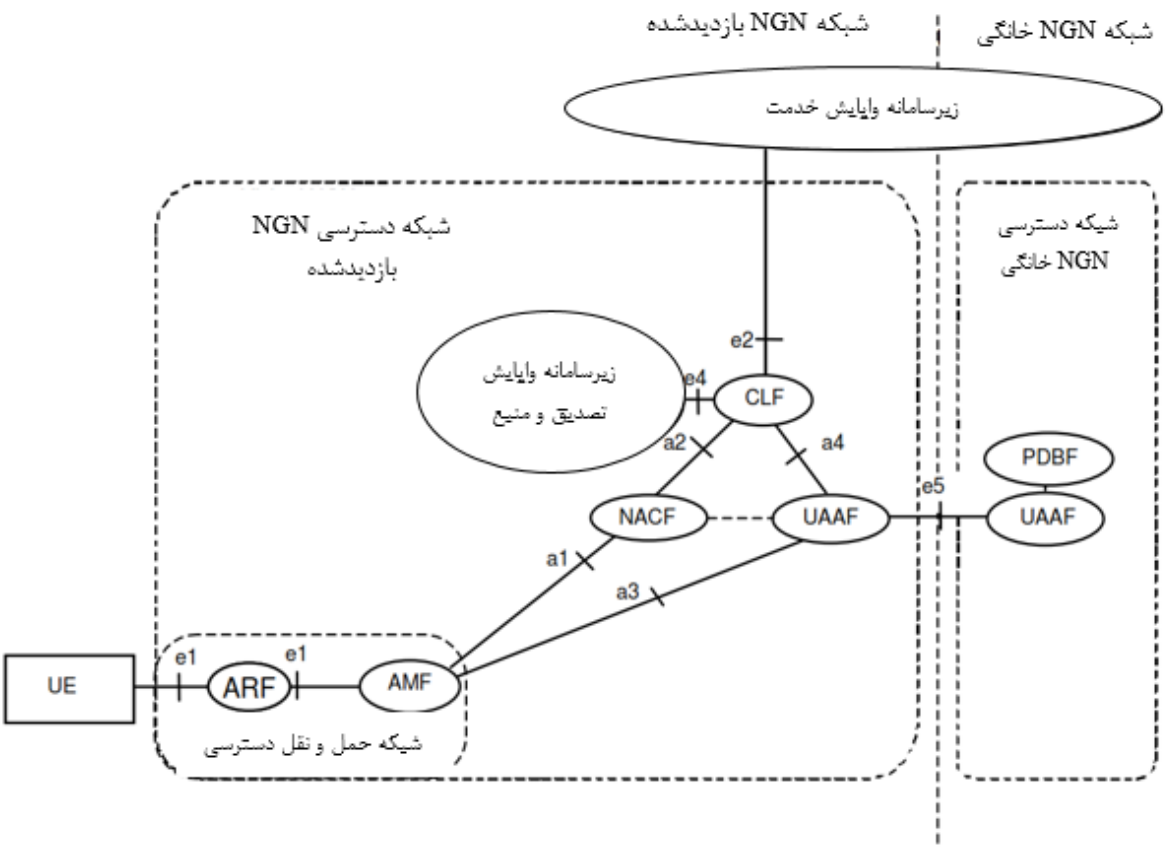
معماریNASS هیچ نقش تجاری را فرض نمی‌کند با این وجود برای رعایت الزامات جابه‌جایی و فراگرد، معماری NASS می‌تواند روی نقش‌های متعدد شبکه کارکردی حاضر در محیط دسترسی فراخباند ثابت، به صورت ارائه شده در شکل ۶-۱ نگاشت شود.

شکل ۶-۱- نقش‌های شبکه کارکردی در TISPAN NGN

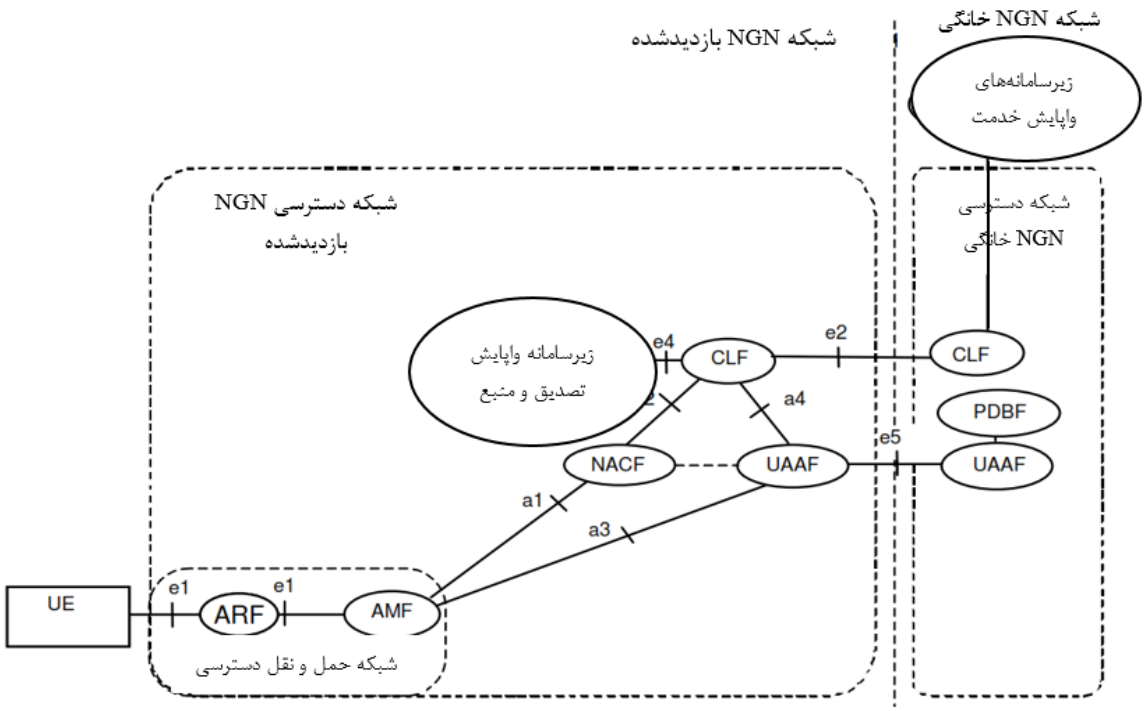
شکل‌های ۶-۲ و ۶-۳ نگاشت NASS را ارائه می‌دهد. نمونه‌هایی از شبکه دسترسی در این شکل شبکه دسترسی xDSL یا یک نقطه دسترسی WLAN است.

شکل ۶-۲ فرانامه ۱ را نشان می‌دهد که در آن زیرسامانه واپایش خدمت (تا حدی) توسط شبکه NGN بازدید شده ارائه می‌شود. شکل ۶-۳ فرانامه ۲ را شفاف می‌سازد که در آن شبکه NGN خانگی زیرسامانه واپایش خدمت را ارائه می‌دهد.

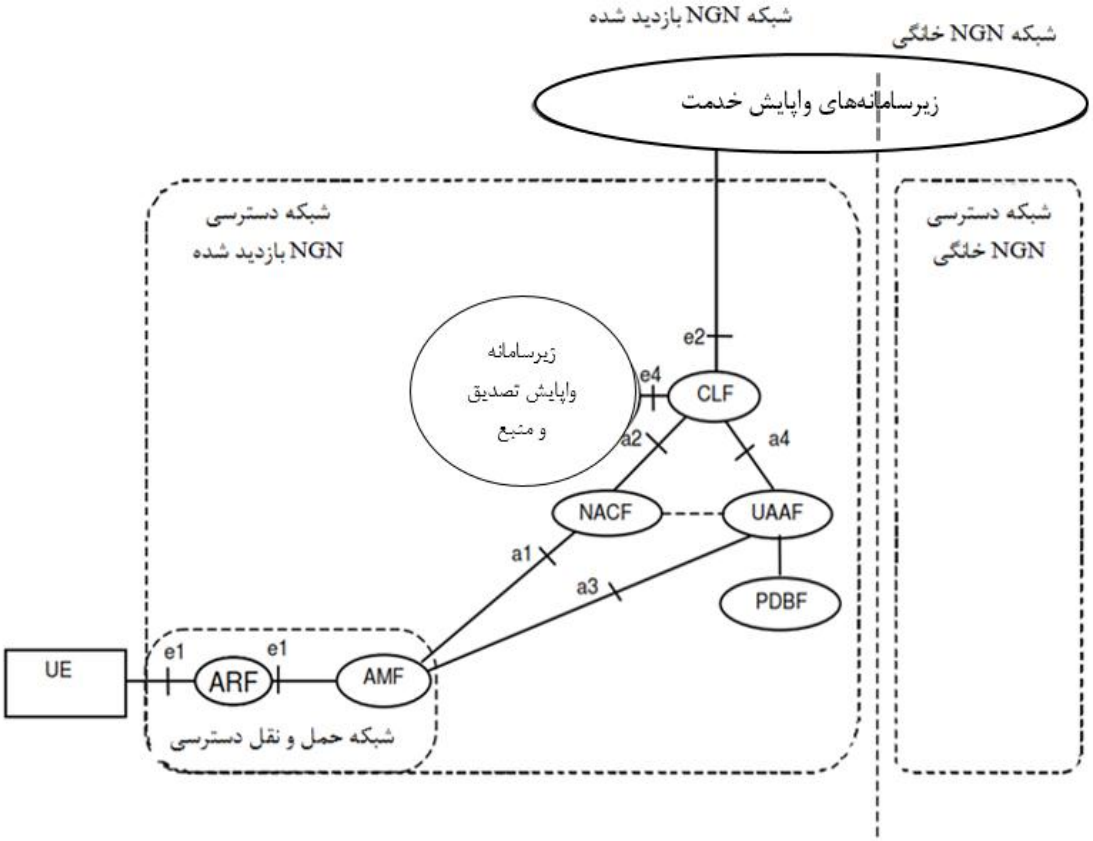
شکل‌های ۶-۴ و ۶-۵ هر دو فرانامه‌های ۳ و ۴ را نشان می‌دهند که در آنها یک TE بازدیدکننده، احراز اصالت دسترسی را انجام نمی‌دهد. در شکل ۶-۴، TE بازدیدکننده قادر است از طریق توافق فراگرد در سطح زیرسامانه‌های واپایش خدمت به خدمات خانگی آن دسترسی یابد. با این وجود این تعریف در حوزه هدف و دامنه کاربرد این استاندارد نیست و در استاندارد ES 282 001 (زیربند 2-2) مشخص می‌شود. شکل ۶-۵ فرانامه‌ای را ارائه می‌دهد که در آن زیرسامانه‌های خدماتی دسترسی شبکه خانگی در شبکه بازدیدشده از طریق یک پیشکار-CLF در شبکه خانگی برای اطلاعات مکانی به CLF دسترسی می‌یابند. واسط e2 در اینجا به‌عنوان یک واسط CLF به CLF استفاده می‌شود.



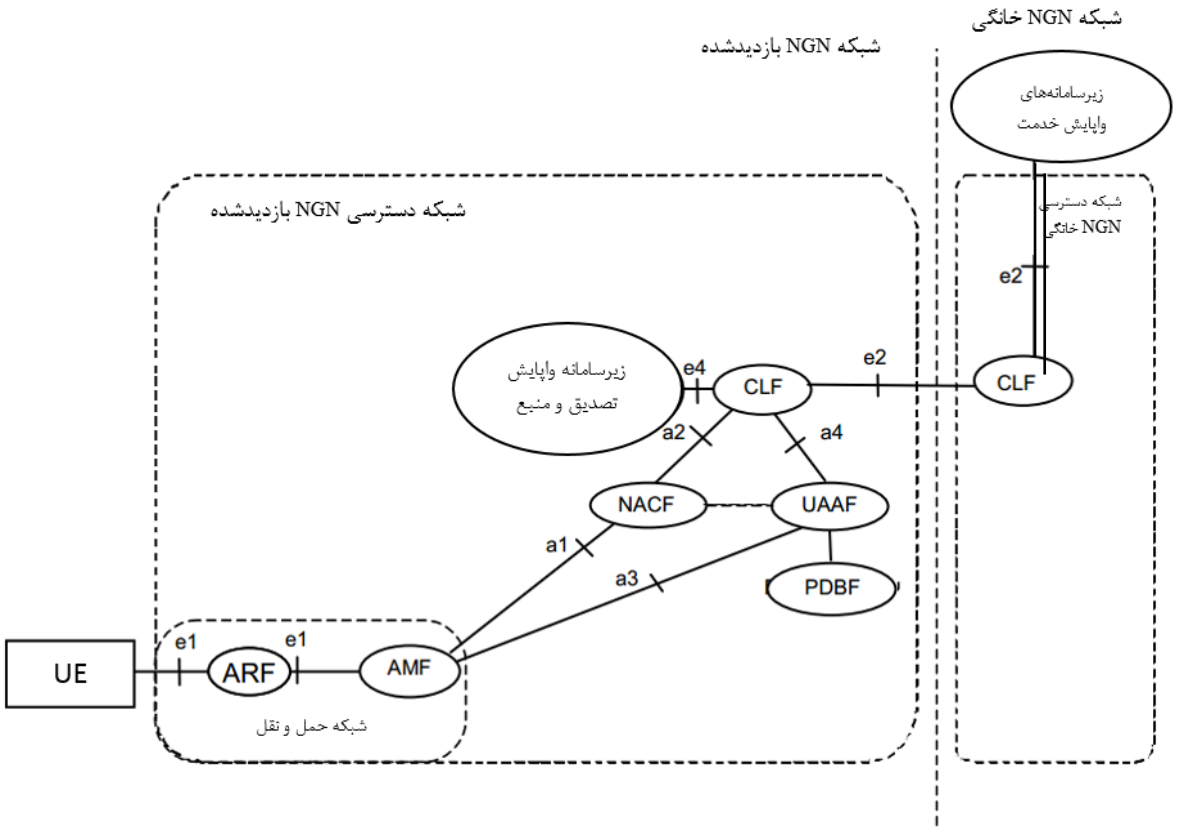
شکل ۶-۲- NASS نگاشت‌شده روی نقش‌های شبکه کارکردی- فرانامه ۱



شکل ۶-۳- NASS نگاشت‌شده روی نقش‌های شبکه کارکردی- فرانامه ۲ (خدمات NGN از شبکه خانگی)



شکل ۶-۴ - NASS نگاشت‌شده روی نقش‌های شبکه کارکردی- فرانامه ۳



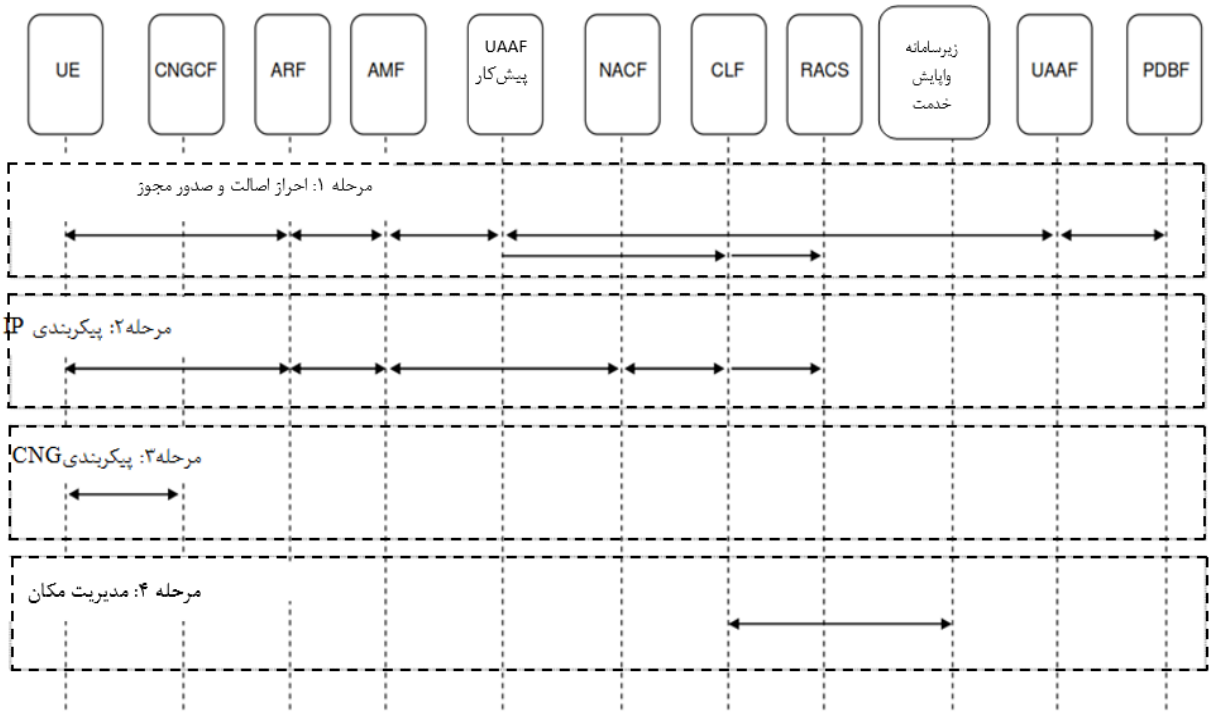
شکل ۶-۵ – زیرسامانه NASS نگاشت‌شده روی نقش‌های شبکه کارکردی- فرانامه ۴

۷ جریان‌های اطلاعات

رویه‌های توصیف‌شده در این استاندارد، برای ارائه توصیف سطح بالا برای کارهای بیشتر مرحله ۳ و نه به صورت جامع و کامل مورد نظر هستند.

۷-۱ جریان‌های اطلاعات سطح بالا

این زیربند جریان‌های اطلاعاتی سطح بالایی را ارائه می‌دهد که فرآیند پیوست شبکه و توزیع اطلاعات نمایه شبکه کاربر NASS دسترسی را درون NASS و به سمت RACS تعریف می‌کند.



شکل ۷-۱- جریان اطلاعاتی سطح بالا

زیرسامانه NASS به رویه-مراحل متعددی در فرآیند پیوست شبکه متکی است. شکل ۷-۱ جریان اطلاعاتی سطح بالا و رویه‌های متفاوت NASS را نشان می‌دهد. بسته به پروتکل‌ها (به‌عنوان مثال، PPP، DHCP و غیره) و فرانامه‌های گسترش مورد استفاده، این رویه-مراحل می‌توانند در مرتبه متفاوتی نسبت به مرتبه‌های نشان داده شده در شکل ۷-۱ به‌کار روند، گرچه به دلایل امنیتی لازم است همواره ابتدا رویه-مرحله احراز اصالت به‌طور موفقیت‌آمیز کامل شود. رویه‌های متفاوت پروتکل مجازند برای رویه-مراحل متفاوت رویه پیوست ترکیب شوند (به‌عنوان مثال، ترکیب رویه‌های DHCP و PPP، ترکیب DHCP و PANA و غیره):

رویه-مرحله ۱- احراز اصالت و صدور مجوز: در اولین رویه-مرحله فرآیند پیوست شبکه، UE احراز اصالت شده و مجاز شناخته خواهد شد. فرآیند احراز اصالت به سازوکارها و شناسه‌هایی متکی است که در بندهای ۴ و ۵ قبلی توصیف شده‌اند. این بدان معنی است که باید احراز اصالت خط و/یا احراز اصالت دسترسی مورد استفاده قرار گیرد. شناسه‌های کاربردی عبارتند از: شناسه کاربر NASS و اعتبارنامه تهیه شده توسط کاربر NASS. رویه-مرحله ۱ همچنین شامل صدور مجوز دسترسی به شبکه بر پایه نمایه کاربر NASS است. یک نمایه پیکربندی خاص کاربر NASS، که به‌عنوان مثال با QoS در ارتباط است، مجاز است از شبکه خانگی NGN به شبکه بازدیدشده NGN بارگیری شود. (از کارساز-UAAF به حالت پیشکار UAAF) زمانی که احراز اصالت موفقیت‌آمیز بوده و UE مجاز به استفاده از منابع شبکه دسترسی باشد، پیکربندی شبکه دسترسی بر پایه نمایه کاربر NASS اجرا می‌شود. این امر همچنین به‌طور ضمنی بیان می‌کند که اطلاعات نمایه شبکه کاربر NASS احراز اصالت شده، باید از طریق نقطه مرجع a4 به سمت CLF

هدایت شود. اطلاعات نمایه باید دست کم شامل شناسه خط (خط ID)، شناسه کاربر NASS و نمایه QoS شبکه کاربر NASS باشد که ممکن است نمایه QoS بارگیری‌شده از شبکه خانگی NGN یا نمایه پیش فرض بوده و شناسه لبه IP (ID لبه-IP) باشد. چنانچه روش احراز اصالت انتخاب شده و/یا نمایه کاربر NASS به تقویت خط‌مشی‌های دسترسی، بلافاصله پس از احراز اصالت (و قبل از تخصیص نشانی-IP) نیاز داشته باشد، مجاز است CLF نمایه کاربر NASS را از طریق نقطه مرجع e4[1] به RACS پیش راند.

یادآوری ۱- رویه- مرحله ۱ مجاز است به‌عنوان قسمتی از رویه تخصیص نشانی IP رخ دهد. (رویه-مرحله ۲)

رویه-مرحله ۲- پیکربندی IP: پیکربندی IP شامل «تخصیص نشانی IP» (رویه-مرحله a2) و «اطلاعات نشانی‌دهی نقطه دسترسی خدمات» (رویه-مرحله 2b) است:

رویه-مرحله ۲-الف: تخصیص نشانی IP: امکان ایجاد پویای نشانی IP و فراهم کردن اطلاعات پیکربندی IP برای UE. در حین رویه-مرحله ۲-الف، NACF اطلاعات پیکربندی IP را تخصیص می‌دهد. NACF شناسه خط (ID خط) را از طریق نشانک‌دهی از e1 دریافت می‌کند و نگاشت بین اطلاعات پیکربندی IP تخصیص‌یافته و ID خط را ایجاد می‌کند. این اطلاعات نگاشتی از طریق نقطه مرجع a2 به سمت CLF هدایت می‌شود که آن را با شناسه کاربر NASS و نمایه شبکه کاربر NASS مرتبط می‌سازد و این اطلاعات را از طریق نقطه مرجع e4 به سمت RACS پیش می‌راند. RACS کارکردپذیری آن را در امتداد اطلاعات نمایه شبکه کاربر NASS که از CLF دریافت کرده، پیکربندی می‌کند.

رویه-مرحله ۲-ب: اطلاعات نشانی‌دهی نقطه تماس زیرسامانه‌های خدماتی: در رویه - مرحله ۲-ب، UE اطلاعات نشانی‌دهی IP را برای دسترسی به زیرسامانه‌های کاربرد/خدمات TISPAN NGN کسب می‌کند. (به‌عنوان مثال، نشانی IP در P-CSCF)

رویه-مرحله ۳- پیکربندی UE: CNGCF مجاز است پارامترهای UE را پیکربندی کند.

رویه-مرحله ۴- مدیریت مکان: زیرسامانه‌های خدمات TISPAN NGN اطلاعات مکانی را از طریق نقطه مرجع e2 از CLF بازیابی می‌کند در صورتی که زیرسامانه‌های خدماتی TISPAN NGN به اطلاعات مکان دسترسی در دامنه‌ای متفاوت نیاز داشته باشند، نشانک‌دهی برای بازیابی اطلاعات مکانی باید از طریق یک پیشکار CLF جای گرفته در همان شبکه‌ای به جلو هدایت شود که زیرسامانه خدمات TISPAN NGN بازیابی‌کننده اطلاعات در آن قرار دارد. پارامتر اصلی برای بازیابی اطلاعات مکانی، باید شناسه کاربر NASS و/یا نشانی IP تخصیص‌یافته به کاربر NASS توسط NASS باشد.

۱- منظور از e1 و e2 و ... واسط های بین هستارها است.

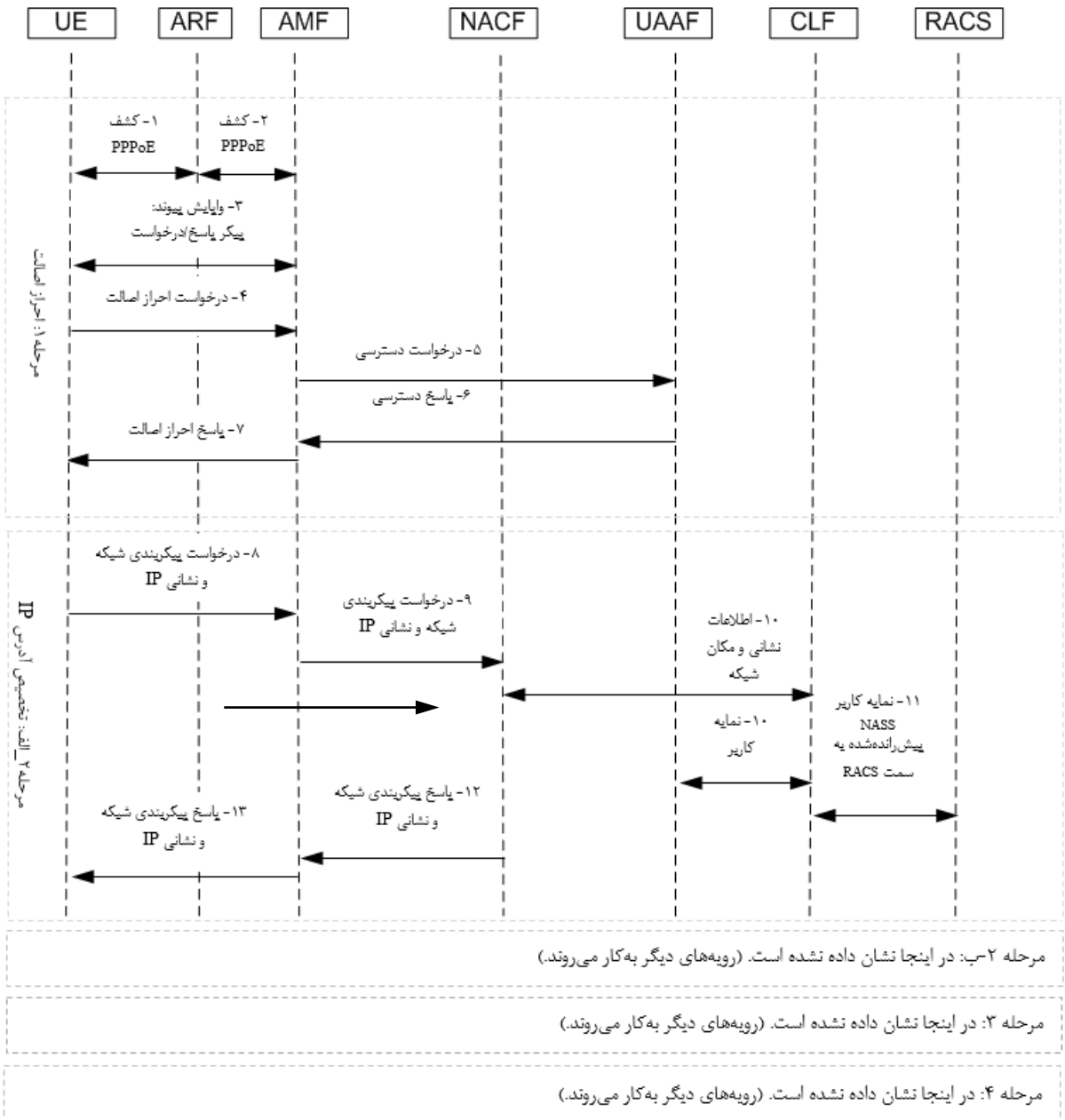
یادآوری ۲- هر رویه- مرحله مجاز است یک یا چند بار درخواست شود. به‌عنوان مثال، توالی رویه- مرحله ۱ که به دنبال آن رویه- مرحله ۲ قرار دارد، مجاز است دوبار درخواست شود: اولین درخواست همراه با احراز اصالت ضمنی که در زیربند ۴-۱-۱ با تخصیص نشانی موقتی IP دنبال می‌شود تا کارسازهای احراز اصالت تماس را فعال سازد؛ دومین درخواست همراه احراز اصالت صریح با تخصیص نشانی IP هدف کلی دنبال می‌شود.

یادآوری ۳- مراحل متفاوت احراز اصالت مجازند با کاربرهای متفاوت NASS مطابقت داشته باشند (به‌عنوان مثال، نشانی IP تخصیص‌یافته در حین اولین درخواست رویه-مرحله ۲ نشانی تخصیص‌یافته به کاربر NASS پیش فرضی در نظر گرفته می‌شود که با Id خط مرتبط است در حالی‌که نشانی IP تخصیص‌یافته در حین دومین درخواست رویه-مرحله ۲ به‌عنوان نشانی تخصیص‌یافته به کاربر NASS احراز اصالت شده در حین دومین درخواست رویه-مرحله ۱ در نظر گرفته می‌شود) یا همان کاربر NASS که در این صورت هر مجموعه داده احراز اصالت با زیرنمایه‌های متفاوت این کاربر NASS در PDBF در ارتباط است.

۲-۷ رویه‌های مرتبط با PPP

این زیربند، نمونه جریان‌های اطلاعاتی از NASS را در صورت کاربرد PPP (زیربند 3-2) ارائه می‌دهد. این مثال‌ها برای پوشش کارکردپذیری کامل NASS موردنظر نیستند.

یادآوری ۱- این زیربند تنها برای نمونه در نظر گرفته شده است و رویه‌های مرحله ۳ را از پیش توصیف نمی‌کند.



شکل ۷-۲- احراز اصالت و تخصیص نشانی IP با استفاده از PPP/PPPoE

این مثال روی رویه-مراحل ۱ و ۲-الف فرآیند پیوست شبکه (به‌عبارتی احراز اصالت و تخصیص نشانی IP) تمرکز دارد. رویه-مراحل ۲-ب، ۳ و ۴ در اینجا در نظر گرفته نمی‌شوند.

مراحل ۱ و ۲- UE رویه‌های کشف PPPoE را برای شناسایی AMF مناسب اجرا کرده و در صورتی‌که مورد نیاز PPP باشد، یک رابطه همتا-به-همتا را با AMF ایجاد می‌کند. ARF کارکرد عامل میانی PPPoE را پیاده‌سازی کرده و اطلاعات شناسایی خط دسترسی را به داخل پیام‌های PPPoE ثبت می‌کند.

۳- پارامترهای پیوند داده از جمله تبادل رویه احراز اصالت مورد استفاده، بین UE و AMF، مبادله می‌شوند.

۴- UE احراز اصالت را آغاز کرده و یک جریان اطلاعاتی متناظر را به AMF ارسال می‌کند. این مثال فرض می‌کند که شناسه کاربر NASS و اطلاعات کلمه عبور، درون جریان اطلاعاتی تهیه می‌شوند.

۵- کارکرد AMF درخواست PPP را به «درخواست دسترسی به UAAF» که کاربر NASS مرتبط با UE را احراز اصالت کرده، ترجمه می‌کند.
۶- کارکرد UAAF با یک پذیرش دسترسی (با فرض موفقیت احراز اصالت) به AMF پاسخ می‌دهد.
۷- کارکرد AMF به UE درباره موفقیت‌آمیز بودن احراز اصالت تکمیل شده آگاهی می‌دهد.
یادآوری ۲- مراحل ۱ تا ۷ می‌توانند با فاز «کشف PPPoE» PPPoE و فاز «پروتکل واپایش پیوند (LCP)» PPP مرتبط باشند. رویه-مرحله «احراز اصالت»، فرآیند پیوست شبکه دسترسی را به‌عنوان قسمتی از فاز LCP از PPP به‌طور کامل اجرا می‌کند. جریان اطلاعاتی مراحل ۸ تا ۱۳ رویه-مرحله «تخصیص نشانی IP» را در خلال این جریان تماس، به‌طور نمونه مرتبط با فاز «پروتکل‌های واپایش شبکه (NCPها)» از PPP اجرا می‌کنند که باید پروتکل‌های متفاوت لایه-شبکه را پیکربندی کند.

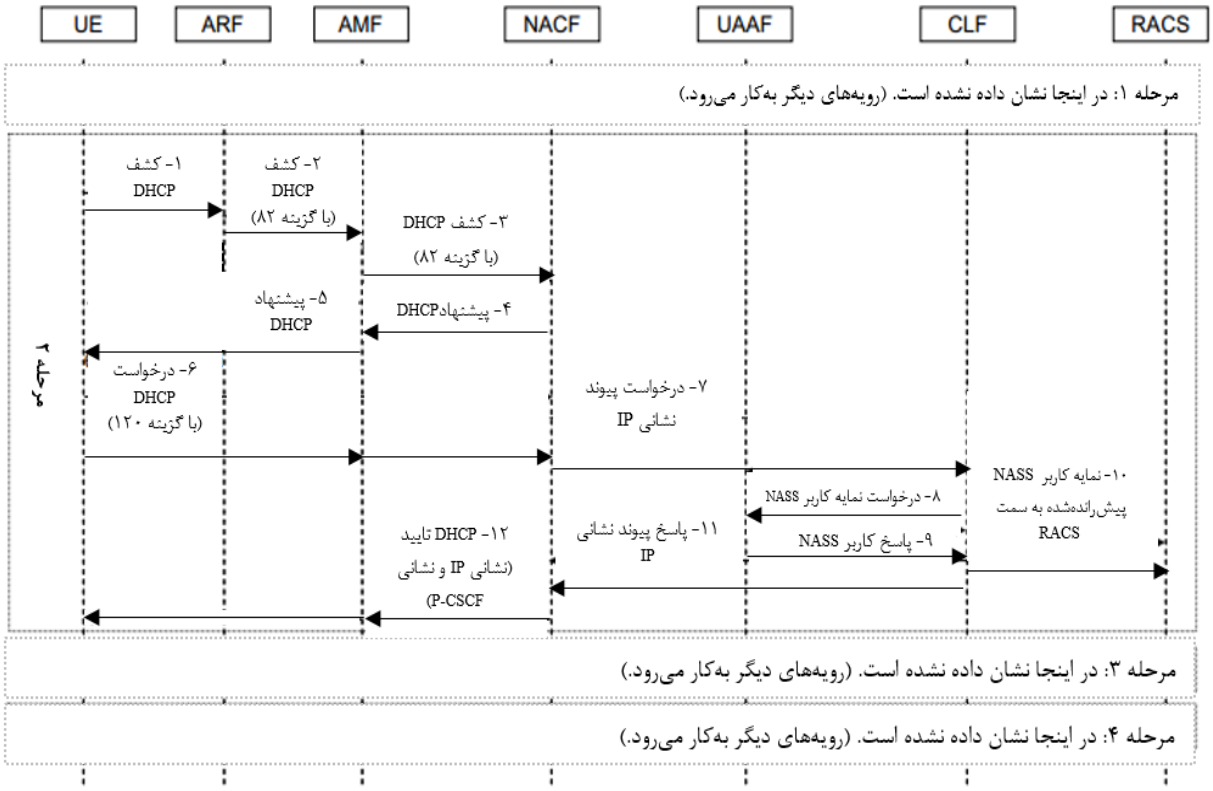
مراحل ۸ و ۹- UE درخواستی را به NACF ارسال می‌کند تا اطلاعات نشانی‌دهی IP را کسب کند.
۱۰- کارکرد NACF و UAAF اطلاعات نشانی IP و نمایه کاربر NASS را به سمت CLF پیش می‌رانند.
۱۱- CLF نمایه کاربر NASS را در امتداد نشانی‌دهی IP مرتبط و اطلاعات مکانی را از طریق نقطه مرجع e4 به سمت RACS پیش می‌راند.
مراحل ۱۲ و ۱۳- NACF نشانی‌دهی IP و اطلاعات پیکربندی شبکه را در اختیار UE قرار می‌دهد.

۷-۳ رویه‌های مرتبط با DHCP

این زیربند، نمونه جریان‌های اطلاعاتی از NASS را در صورت استفاده از DHCP ارائه می‌دهد. این مثال‌ها برای پوشش کارکردپذیری کامل NASS منظور نشده‌اند.
یادآوری- این زیربند تنها برای نمونه در نظر گرفته شده است و رویه‌های مرحله ۳ را از پیش توصیف نمی‌کند.

۷-۳-۱ پیکربندی IP با استفاده از DHCP

این مثال روی رویه-مرحله ۲ فرآیند پیوست شبکه (به‌عبارتی پیکربندی IP) تمرکز دارد. رویه-مراحل ۱، ۳ و ۴ در اینجا در نظر گرفته نمی‌شوند.
مرحله۱- در اینجا نشان داده نشده است. (رویه‌های دیگر به‌کار می‌رود.)



شکل ۷-۳- پیکربندی IP با استفاده از DHCP

۱- تجهیزات UE رویه تخصیص نشانی IP را با ارسال یک پیام کشف DHCP آغاز می‌کند.

۲- کارکرد ARE پیام را دریافت کرده، اطلاعات افزونه را به کشف DHCP (به‌عنوان مثال، شناسایی خط) اضافه کرده و پیام را به سمت AMF هدایت می‌کند. اطلاعات اضافه شده توسط ARF می‌تواند برای اهداف متعددی چون احراز اصالت ضمنی، احراز اصالت NASS–دسته‌بندی‌شده یا خدمات بر مبنای مکان به کار رود.

۳- کارکرد AMF، کشف DHCP را دریافت کرده و آن را با NACF که به‌عنوان کارساز DHCP کار می‌کند، رله می‌کند.

مراحل ۴ و ۵- NACF با یک پیشنهاد DHCP، به UE پاسخ می‌دهد.

۶- UE برای درخواست نشانی IP و نشانی زیرسامانه کاربردها/خدمات TISPAN NGN (به‌عنوان مثال، P-CSCF)، از طریق گزینه DHCP ۱۲۰، یک درخواست DHCP را ارسال می‌کند. این درخواست توسط AMF به NACF رله می‌شود.

۷- کارکرد NACF به CLF اعلام می‌کند که یک نشانی IP به UE تخصیص‌یافته است.

مراحل ۸ و ۹- CLF نمایه کاربر NASS را از UAAF بازیابی می‌کند و آن را با نشانی IP دریافت شده مرتبط می‌سازد.

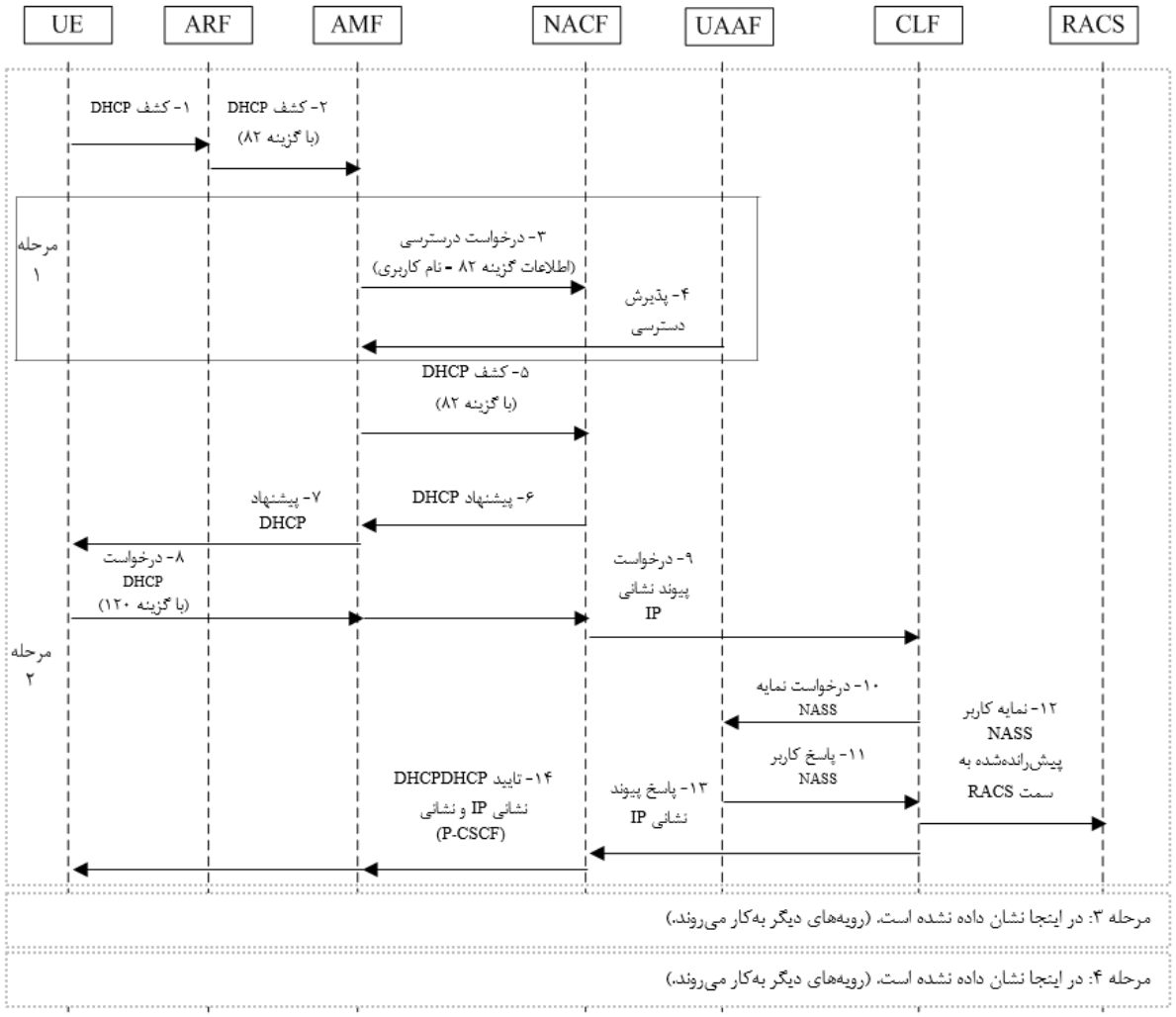
۱۰- مکان CLF نمایه کاربر NASS را در امتداد نشانی‌دهی IP مربوط و اطلاعات مکانی، از طریق نقطه مرجع e4 به سمت RACS پیش می‌راند.

۱۱- مکان CLF انقیاد موفقیت‌آمیز نشانی IP با نمایه کاربر NASS را برای NACF تأیید می‌کند. همچنین این پیام مجاز است حاوی اطلاعات نشانی نقطه تماس زیرسامانه‌های کاربردها/خدمات TISPAN NGN باشد.

۱۲- NACF نشانیIP تخصیص‌یافته و همچنین نشانی IP یا FQDN نقطه تماس زیرسامانه‌های کاربردها/خدمات TISPAN NGN را (به‌عنوان مثال P-CSCF) که توسط AMF به UE رله می‌شود، ارائه می‌دهد.

۷-۳-۲ احراز اصالت ضمنی و پیکربندی IP با استفاده از DHCP

این مثال روی رویه-مراحل ۱ و ۲ فرآیند پیوست شبکه (به‌عبارتی پیکربندی IP و احراز اصالت ضمنی) تمرکز دارد. رویه-مراحل ۳ و ۴ در اینجا در نظر گرفته نمی‌شوند.



شکل ۷-۳ الف- احراز اصالت ضمنی و پیکربندی IP با استفاده از DHCP

۱- تجهیزات UE، تخصیص نشانی IP و رویه احراز اصالت ضمنی را با ارسال یک پیام کشف DHCP آغاز می‌کند.

۲-کارکرد ARE پیام را دریافت کرده، اطلاعات افزونه (به‌عنوان مثال، شناسایی خط) را به کشف DHCP اضافه کرده و پیام را به سمت AMF هدایت می‌کند. یادآوری می‌شود که اطلاعات اضافه شده توسط ARF لزوما تنها برای احرازاصالت ضمنی به‌کار نمی‌رود بلکه می‌تواند برای اهداف دیگری چون خدمات بر مبنای مکان، احراز اصالت NASS–دسته‌بندی شده و غیره نیز استفاده شود.

۳- کارکرد AMF، کشف DHCP را دریافت کرده و درخواست دسترسی را به UAAF ارسال می‌کند تا کاربر NASS مرتبط با UE که کشف DHCP را ارسال کرده است، احراز اصالت شود. ارتباط نمایه کاربر NASS و UE توسط اطلاعات شناسایی خط تسهیل می‌شود.

۴- کارکرد UAAF درصورتی با یک پذیرش دسترسی پاسخ می‌دهد که نمایه کاربر NASS بتواند به‌طور موفقیت‌آمیزی با اطلاعات شناسایی خط تامین شده، مرتبط شود.

یادآوری- جریان اطلاعاتی مراحل ۳ و ۴ رویه-مرحله «احراز اصالت ضمنی» فرآیند پیوست شبکه دسترسی را درون این جریان تماس اجرا می‌کند.

۵- کارکرد AMF کشف DHCP را به NACF که به‌عنوان یک کارساز DHCP عمل می‌کند، ارسال می‌کند.
یادآوری- چنانچه NACF و UAAF در یک مکان قرار گیرند، رویه-مرحله ۱ پس از مرحله ۵ مجاز است آغاز شود.

مراحل ۶ و ۷- NACF با یک پیشنهاد DHCP، به UE پاسخ می‌دهد.
۸- تجهیزات UE درخواست DHCP را برای درخواست نشانی IP و درخواست نشانی زیرسامانه کاربردها/خدمات TISPAN NGN (به‌عنوان مثال، P-CSCF) از طریق گزینه ۱۲۰ DHCP، ارسال می‌کند. این درخواست توسط AMF به NACF رله می‌شود.
۹- کارکرد NACF به CLF اعلام می‌کند که یک نشانی IP به UE تخصیص یافته است.
یادآوری ۲- مرحله ۹ مجاز است درست پس از مرحله ۶ انجام شود.

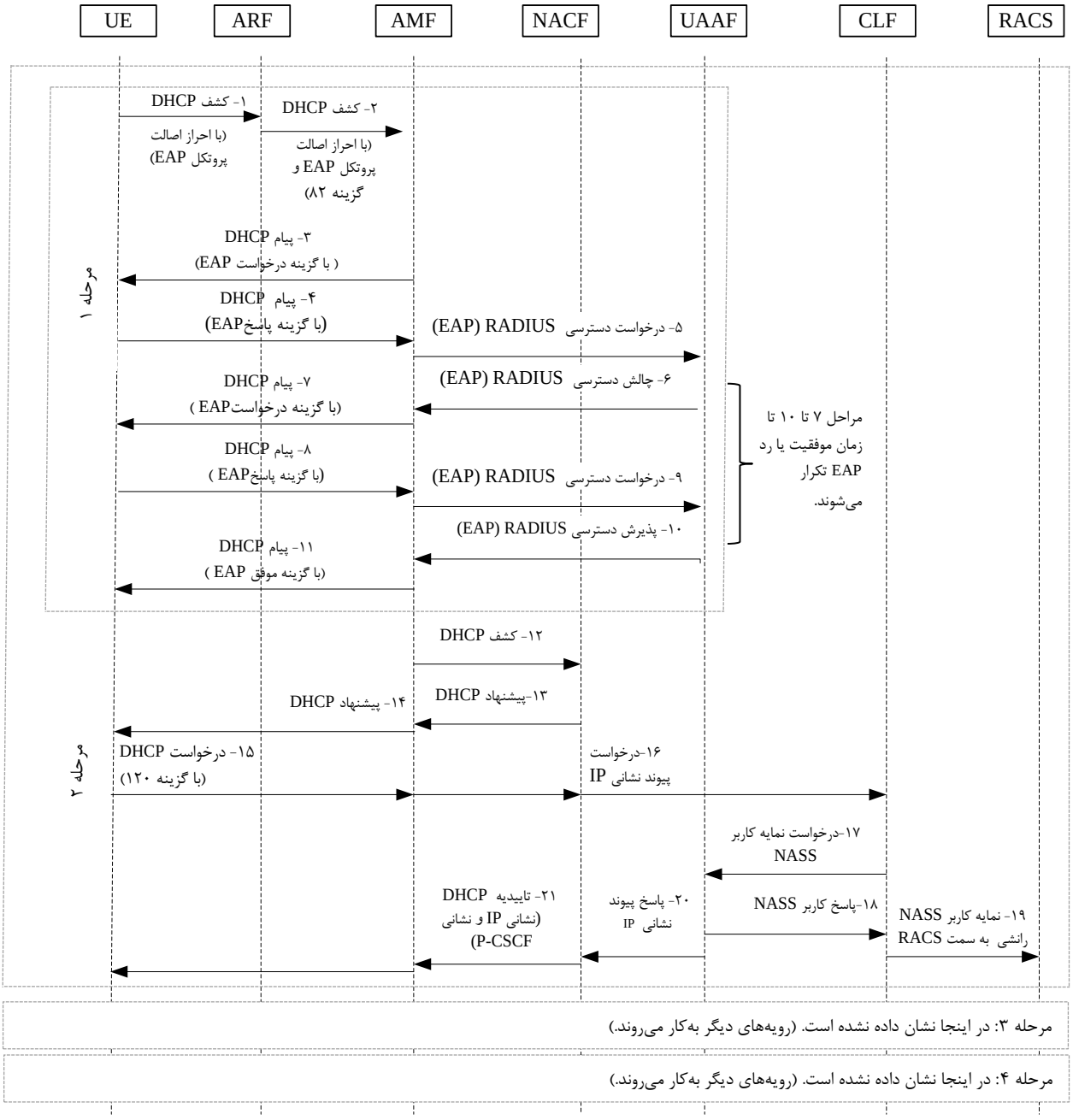
مراحل ۱۰ و ۱۱- CLF نمایه کاربر NASS را از UAAF بازیابی می‌کند و آن را با نشانی IP دریافت شده، مرتبط می‌سازد.
۱۲- مکان CLF نمایه کاربر NASS را به‌همراه نشانی‌دهی IP مربوط و اطلاعات مکانی، از طریق نقطه مرجع e4 به سمت RACS پیش می‌راند.
۱۳- CLF انقیاد موفقیت‌آمیز نشانی IP با نمایه کاربر NASS را برای NACF تأیید می‌کند. ممکن است این پیام حاوی اطلاعات نشانی نقطه تماس زیرسامانه‌های کاربردها/خدمات TISPAN NGN باشد.
۱۴- کارکرد NACF نشانی IP تخصیص‌یافته و همچنین نشانی IP یا FQDN نقطه تماس زیرسامانه‌های کاربردها/خدمات TISPAN NGN (به‌عنوان مثال، P-CSCF) را ارائه می‌دهد که توسط AMF به UE رله می‌شود.

۷-۳-۳ احراز اصالت صریح و پیکربندی IP با استفاده از DHCP

این مثال روی رویه-مراحل ۱ و ۲ فرآیند پیوست شبکه (به‌عبارتی پیکربندی IP و احراز اصالت) تمرکز دارد. رویه - مراحل ۳ و ۴ در اینجا در نظر گرفته نمی‌شوند.

یادآوری ۱- دیگر پروتکل‌های حمل و نقل می‌توانند برای اجرای احراز اصالت صریح (به‌عنوان مثال، PANA (به زیربند ۷-۵ مراجعه کنید) یا 802.1X (به زیربند ۷-۴ مراجعه کنید)) مورد استفاده قرار گیرند که در این‌صورت DHCP تنها برای رویه-مرحله ۲ به‌کار می‌رود.

یادآوری ۲- جریان اطلاعاتی ارائه شده در اینجا، تنها ماهیت نمونه‌ای دارد. این جریان هیچ یک از رویه‌های مرحله ۳ را که با ویژگی‌های IETF مرتبط نیستند توصیف نمی‌کند.



شکل ۷-۳ ب- احراز اصالت صریح و پیکربندی IP با استفاده از DHCP

۱- تجهیزات UE تخصیص نشانی IP و رویه احراز اصالت ضمنی را از طریق ارسال پیام کشف DHCP همراه گزینه پروتکل احراز اصالت EAP آغاز می‌کند.

۲- کارکرد ARF پیام را دریافت کرده، اطلاعات افزونه (به‌عنوان مثال، شناسایی خط برای خدمات مبتنی بر مکان) را به کشف DHCP اضافه کرده و پیام را به سمت AMF هدایت می‌کند.

۳- کارکرد AMF با پیام DHCP EAP به UE پاسخ می‌دهد.

۴- تجهیزات UE با پیام DHCP EAP به AMF پاسخ می‌دهد.

۵- کارکرد AMF درخواست دسترسی را به UAAF ارسال می‌کند.

۶- UAAF به AMF پاسخ می‌دهد.

۷- کارکرد AMF پیام DHCP EAP را به UE ارسال می‌کند.
۸- تجهیزات UE با پیام DHCP EAP به AMF پاسخ می‌دهد.
۹- کارکرد AMF درخواست دسترسی را به UAAF ارسال می‌کند.
۱۰- کارکرد UAAF به AMF پاسخ می‌دهد.
یادآوری- مراحل ۷ تا ۱۰ تا زمان موفقیت یا شکست EAP تکرار خواهند شد. این نمودار تبادل موفقیت‌آمیز EAP را فرض می‌کند.

۱۱- کارکرد AMF پیام DHCP را با موفقیت EAP به UE ارسال می‌کند.

۱۲- کارکرد AMF کشف DHCP را به NACF که به‌عنوان یک کارساز DHCP عمل می‌کند، ارسال می‌کند.

مراحل ۱۳ و ۱۴- NACF با یک پیشنهاد DHCP، به UE پاسخ می‌دهد.

۱۵- تجهیزات UE درخواست DHCP را برای درخواست نشانی IP و درخواست نشانی زیرسامانه کاربردها/خدمات TISPAN NGN (به‌عنوان مثال، P-CSCF)، از طریق گزینه ۱۲۰ DHCP، ارسال می‌کند. این درخواست توسط AMF به NACF رله می‌شود.

۱۶- NACF به CLF اعلام می‌کند که یک نشانی IP به UE تخصیص یافته است.

مراحل ۱۷ و ۱۸- CLF نمایه کاربر NASS را از UAAF بازیابی کرده و آن را با نشانی IP دریافتی، مرتبط می‌سازد.

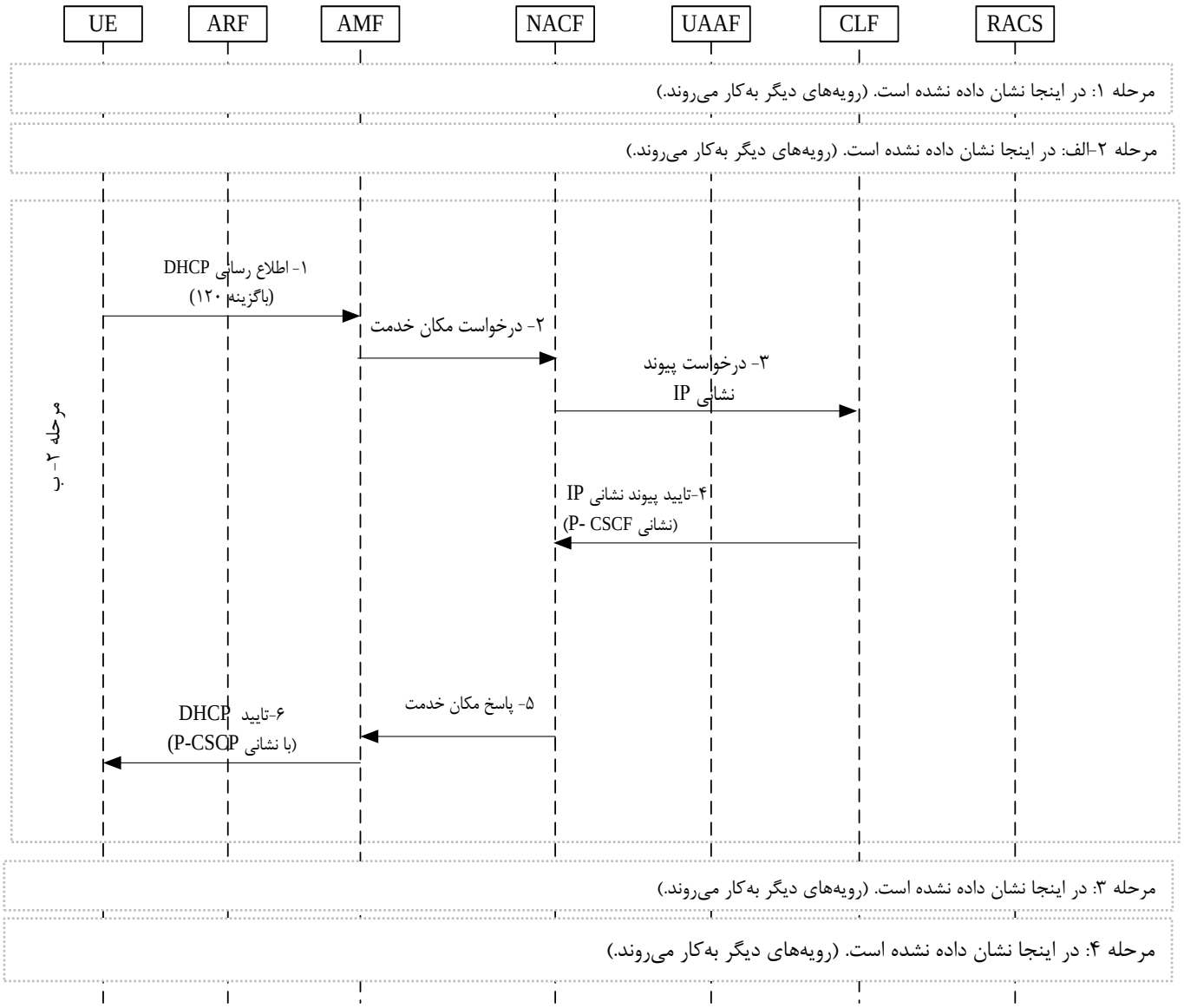
۱۹- مکان CLF نمایه کاربر NASS را همراه با نشانی‌دهی IP مربوط و اطلاعات مکانی از طریق نقطه مرجع e4 به سمت RACS پیش می‌راند.

۲۰- مکان CLF انقیاد موفقیت‌آمیز نشانی IP با نمایه کاربر NASS را برای NACF تأیید می‌کند. این پیام همچنین مجاز است حاوی اطلاعات نشانی نقطه تماس زیرسامانه‌های کاربردها/خدمات TISPAN NGN باشد.

۲۱- کارکرد NACF نشانی IP تخصیص‌یافته و همچنین نشانی IP یا FQDN نقطه تماس زیرسامانه‌های کاربردها/خدمات TISPAN NGN (به‌عنوان مثال، P-CSCF) را که توسط AMF به UE رله می‌شود، ارائه می‌دهد.

۷-۳-۴ پیکربندی نقطه تماس زیرسامانه‌های خدماتی با استفاده از DHCP

این مثال روی رویه-مرحله ۲-ب فرآیند پیوست شبکه (به‌عبارتی اطلاعات نشانی‌دهی نقطه تماس زیرسامانه‌های خدماتی) تمرکز دارد. رویه-مراحل ۱، ۲-الف، ۳ و ۴ در اینجا در نظر گرفته نمی‌شوند.



شکل ۷-۳ پ - پیکربندی نقطه تماس زیرسامانه‌های خدماتی با استفاده از DHCP

مراحل ۱ و ۲- UE اعلان DHCP را برای درخواست پارامترهای شبکه از جمله نشانی IP نقطه تماس (به‌عنوان مثال، P-CSCF) زیرسامانه کاربردها/خدمات TISPAN NGN ارسال می‌کند. این درخواست توسط AMF به NACF رله می‌شود.

۳- NACF نشانی IP نقطه تماس (به‌عنوان مثال، P-CSCF) زیرسامانه کاربردها/خدمات TISPAN NGN را با استفاده از جریان اطلاعاتی انقیاد از CLF درخواست می‌کند.

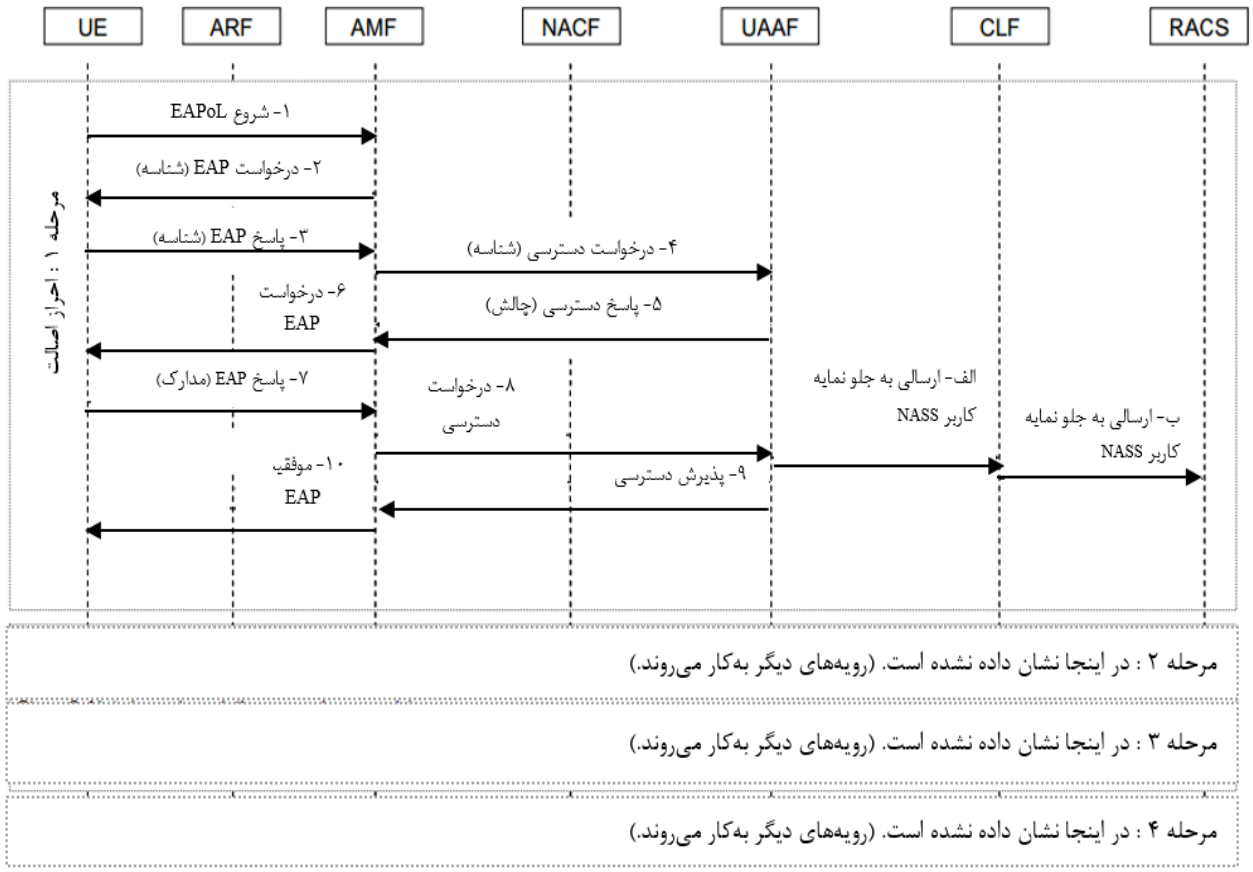
۴- مکان CLF با جریان اطلاعاتی تأیید انقیاد که حاوی نشانی IP نقطه تماس (به‌عنوان مثال P-CSCF) زیرسامانه کاربردها/خدمات TISPAN NGN است، به NACF پاسخ می‌دهد.

مراحل ۵ و ۶- NACF نشانی IP نقطه تماس (به‌عنوان مثال، P-CSCF) زیرسامانه‌های کاربردها/خدمات TISPAN NGN را در اختیار AMF قرار می‌دهد که سپس توسط AMF به UE رله می‌شود.

۷-۴ رویه‌های مبتنی بر دسترسی اترنت IEEE 802

این زیربند نمونه جریان‌های اطلاعاتی از NASS را در صورتی ارائه می‌دهد که از رویه‌های اترنت IEEE 802 استفاده شود. این مثال‌ها برای پوشش کارکردپذیری کامل NASS منظور نشده‌اند.

یادآوری- این زیربند تنها به‌عنوان نمونه در نظر گرفته می‌شود و رویه‌های مرحله ۳ را از پیش توصیف نمی‌کند.



شکل ۷-۴الف- احراز اصالت با استفاده از رویه‌های اترنت IEEE 802

این مثال روی رویه-مرحله ۱ فرآیند پیوست شبکه (به عبارتی احراز اصالت) تمرکز دارد. رویه-مراحل ۲، ۳ و ۴ در اینجا در نظر گرفته نمی‌شوند. جریان اطلاعاتی نمونه که در شکل ۷-۴ الف نشان داده شده است، استفاده از EAP-MD5 را در نظر می‌گیرد. رمز به اشتراک گذاشته شده مرتبط با کاربر NASS که هدف آن احراز اصالت است برای UE و UAAF قابل دسترس فرض می‌شود.

۱- UE مکالمات احراز اصالت را آغاز می‌کند.

مراحل ۲ و ۳- AMF شناسه کاربر NASS را بازیابی می‌کند.

۴- AMF اطلاعات شناسه را برای UAAF فراهم می‌کند.

مراحل ۵ و ۶- UAAF چالش تصادفی را به UE ارسال می‌کند.

مراحل ۷ و ۸- UE با درهم‌سازی چالش که با استفاده از رمز به اشتراک گذاشته شده ایجاد شده، پاسخ می‌دهد.

۹- کارکرد UAAF درهم‌سازی را صحت‌سنجی کرده و احراز اصالت را می‌پذیرد (یا رد می‌کند). این مثال احراز اصالت را موفق فرض می‌کند بنابراین UAAF با پذیرش دسترسی به AMF پاسخ می‌دهد.

۱۰- کارکرد AMF تکمیل موفقیت‌آمیز رویه احراز اصالت را به UE اعلام می‌کند.

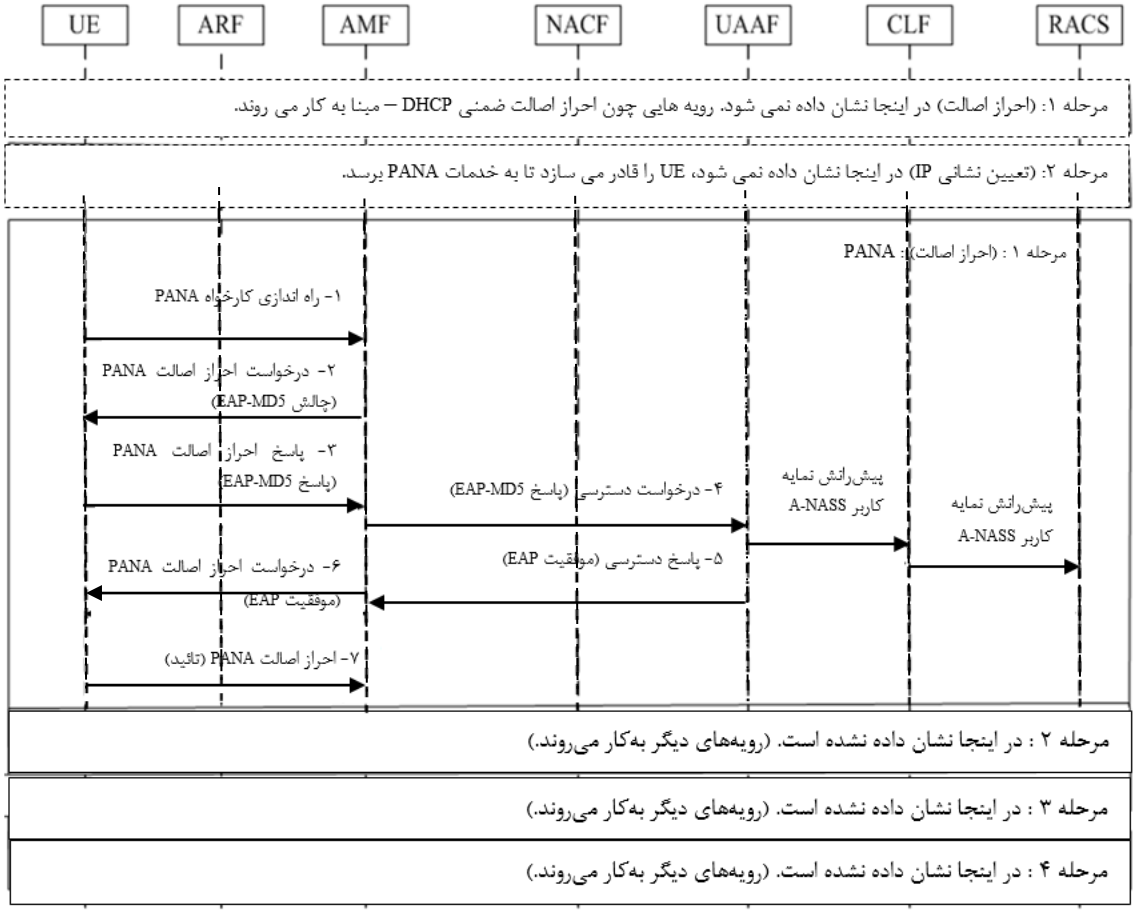
الف- کارکرد UAAF قسمت‌های مناسب نمایه کاربر NASS را به سمت CLF پیش می‌راند. مرحله الف می‌تواند درست پس از مرحله ۸ اجرا شود. (با فرض یک درخواست دسترسی موفقیت‌آمیز)

ب- مکان CLF قسمت مناسب نمایه کاربر NASS را به RACS پیش می‌راند. این امر RACS را قادر می‌سازد تا خط‌مشی‌های دسترسی (مانند بستن/بازکردن دروازه‌ها) را درست پس از احراز اصالت، در صورت نیاز، اجرا کند.

۷-۵ رویه‌های مرتبط مبتنی بر PANA

این زیربند نمونه جریان‌های اطلاعاتی از NASS را در صورتی ارائه می‌دهد که PANA برای احرازاصالت شبکه دسترسی، مورد استفاده قرار گیرد. این مثال‌ها برای پوشش کارکردپذیری کامل NASS منظور نمی‌شود.

یادآوری ۱- این زیربند تنها به‌عنوان نمونه در نظر گرفته می‌شود و رویه‌های (پروتکل) مرحله ۳ را از پیش توصیف نمی‌کند.



شکل ۷-۴ب- احراز اصالت با استفاده از رویه‌های مبتنی بر PANA

این مثال روی رویه-مرحله ۱ فرآیند پیوست شبکه (به‌عبارتی احراز اصالت) تمرکز دارد. رویه-مراحل ۲، ۳ و ۴ بعدی در اینجا در نظر گرفته نمی‌شوند.

یادآوری ۲- ویژگی‌های PANA به کارخواه‌های PANA برای دسترسی به یک نشانی IP، پیش از اجرای احراز اصالت مبنی بر PANA نیاز دارند. دستیابی به این نشانی از طریق پیکربندی ایستا یا فراخوانی رویه‌های مرحله ۲ مجاز است که در این صورت رویه‌ها می‌توانند با توجه به پیکربندی شبکه و خط‌مشی بهره‌بردار نشانی پیوند-محلی، نشانی نامشخص یا نشانی IP پیوند-غیرمحلی باشند. زمانی که UE یک نشانی پیوند-محلی را دریافت می‌کند یا به یک نشانی نامشخص تخصیص داده می‌شود، نشانه آن است که یک فراخوانی دومی رویه-مرحله ۲ پس از احراز اصالت موفقیت‌آمیز مورد نیاز است تا یک نشانی IP هدف کلی به UE اختصاص یابد.

جریان اطلاعاتی نمونه که در شکل ۷-۴ ب نشان داده شده است، استفاده از EAP-MD5 روی PANA را در نظر می‌گیرد. یک رمز به اشتراک گذاشته شده مرتبط با کاربر NASS که هدف آن احراز اصالت است برای UE و UAAF قابل دسترس فرض شده است.

۱- تجهیزات UE مکالمات احراز اصالت را آغاز می‌کند.

۲- کارکرد AMF شناسه کاربر NASS را بازیابی کرده و چالش تصادفی را به UE ارسال می‌کند.

۳- تجهیزات UE با درهم‌سازی چالشی که با استفاده از رمز به اشتراک گذاشته شده ایجاد شده، پاسخ می‌دهد.

۴- کارکرد AMF شناسه کاربر NASS، چالش تصادفی و پاسخ UE مربوطه را برای UAAF فراهم می‌کند.

۵- کارکرد UAAF درهم‌سازی را صحت‌سنجی کرده و احراز اصالت را می‌پذیرد (یا رد می‌کند). این مثال یک احراز اصالت موفقیت‌آمیز را فرض می‌کند، بنابراین، UAAF با یک پاسخ دسترسی که نشان‌دهنده UE احراز اصالت شده است، پاسخ می‌دهد.

۶- کارکرد AMF تکمیل موفقیت‌آمیز رویه احراز اصالت را به UE اعلام می‌کند.

۷- تجهیزات UE احراز اصالت موفقیت‌آمیز را تایید می‌کند.

الف- کارکرد UAAF قسمت‌های مناسب نمایه کاربر NASS را به سمت CLF پیش می‌راند. با فرض احراز اصالت موفق، مرحله الف می‌تواند درست به موازات مرحله ۵ یا پس از آن اجرا شود.

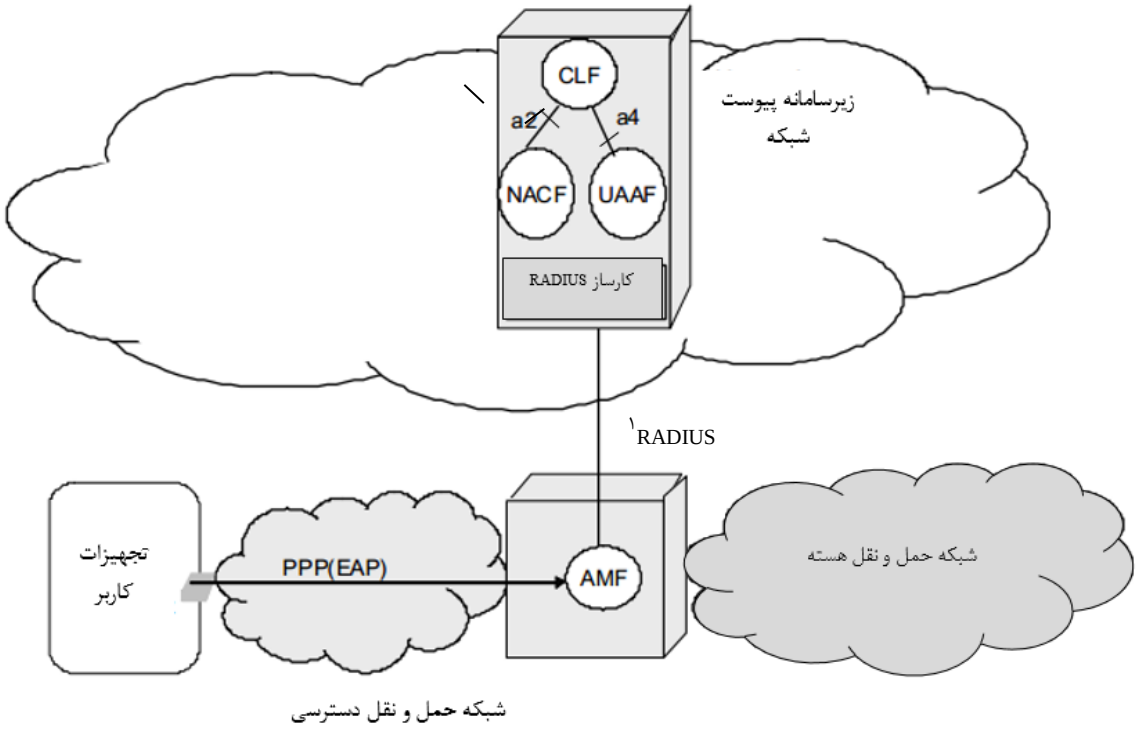
ب- مکان CLF، قسمت مناسب نمایه کاربر NASS را به RACS پیش می‌راند. این امر به RACS اجازه می‌دهد در صورت نیاز، خط‌مشی‌های دسترسی (مانند بستن/بازکردن دروازه‌ها) را درست پس از احراز اصالت، اجرا کند. همچنین مرحله ب مجاز است تا رویه-مرحله بعدی به تعویق افتد، همانطور که مجاز است CLF برای تخصیص نشانی IP (رویه-مرحله ۲) پیش از پیش‌راندن اطلاعات به RACS، منتظر بماند.

پیوست الف

(آگاهی‌دهنده)

پیکربندی‌های فیزیکی

الف-۱ مورد PPP

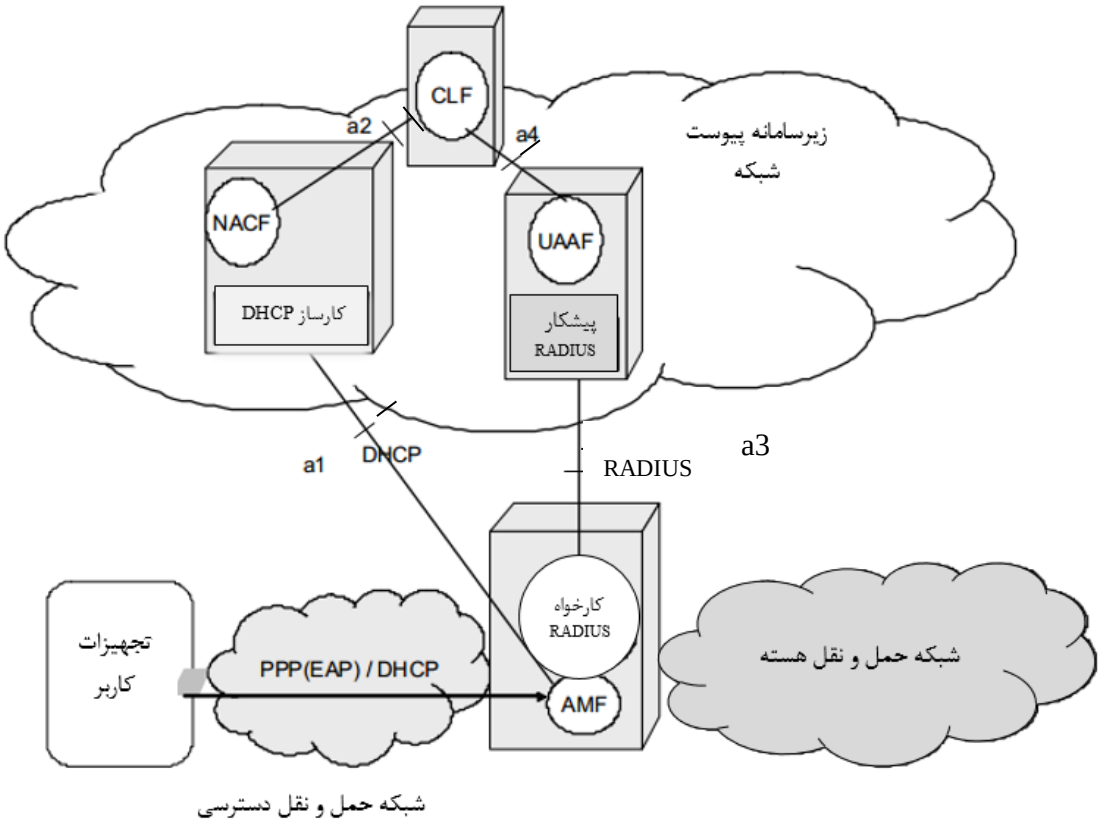


[1] Remote Authentication Dial-In-User Service

شکل الف-۱- پیکربندی مبتنی بر PPP

یادآوری- به‌خاطر سادگی، اتصال واسطها به RACS نشان داده نشده است.

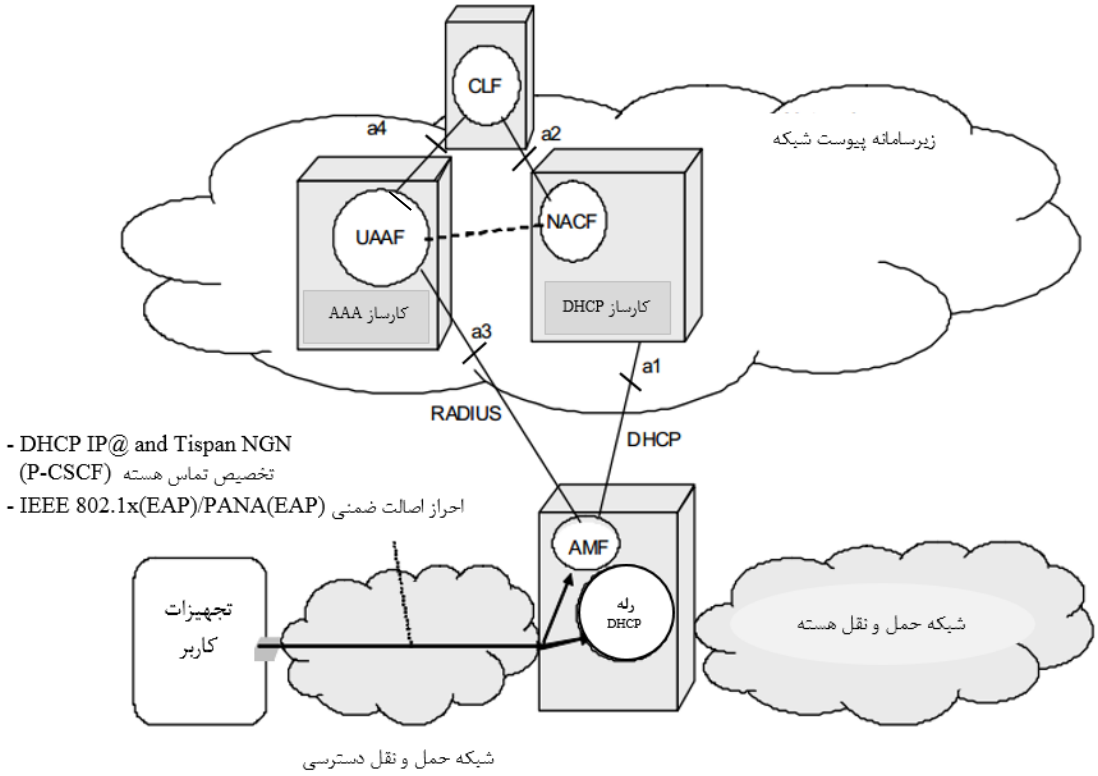
الف-۲ PPP با پیکربندی DHCP



شکل الف-۲ - پیکربندی مبتنی بر PPP همراه با پیکربندی IP مبتنی بر DHCP

(تخصیص نقطه تماس زیرسامانه‌های کاربردها/خدمات TISPAN به CNG)

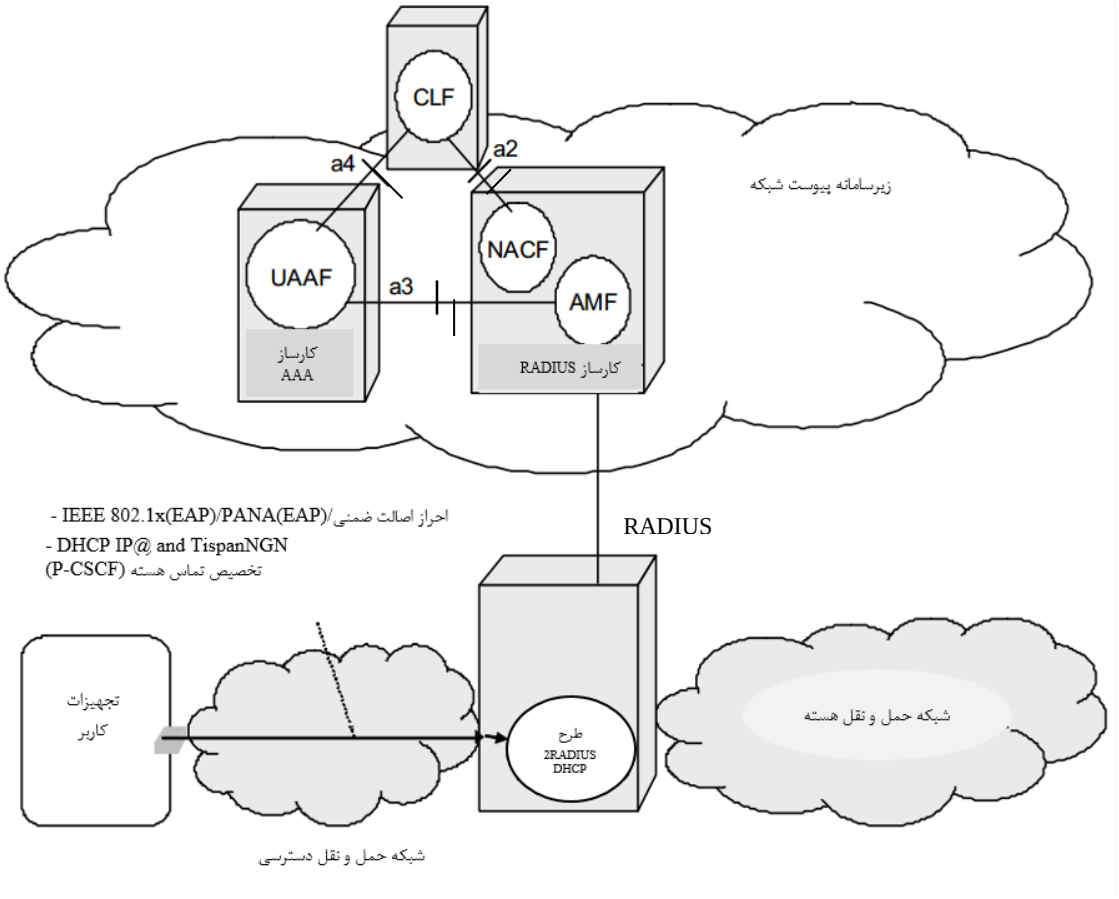
الف-۳ DHCP (گزینه ۱)



شکل الف-۳- پیکربندی مبتنی بر DHCP (گزینه ۱)

یادآوری- به خاطر سادگی، اتصال واسطها به RACS نشان داده نشده‌اند.

الف-۴ DHCP (گزینه ۲)



شکل الف-۴- پیکربندی مبتنی بر DHCP (گزینه ۲)

یادآوری- به‌خاطر سادگی، اتصال واسطها به RACS نشان داده نشده است.

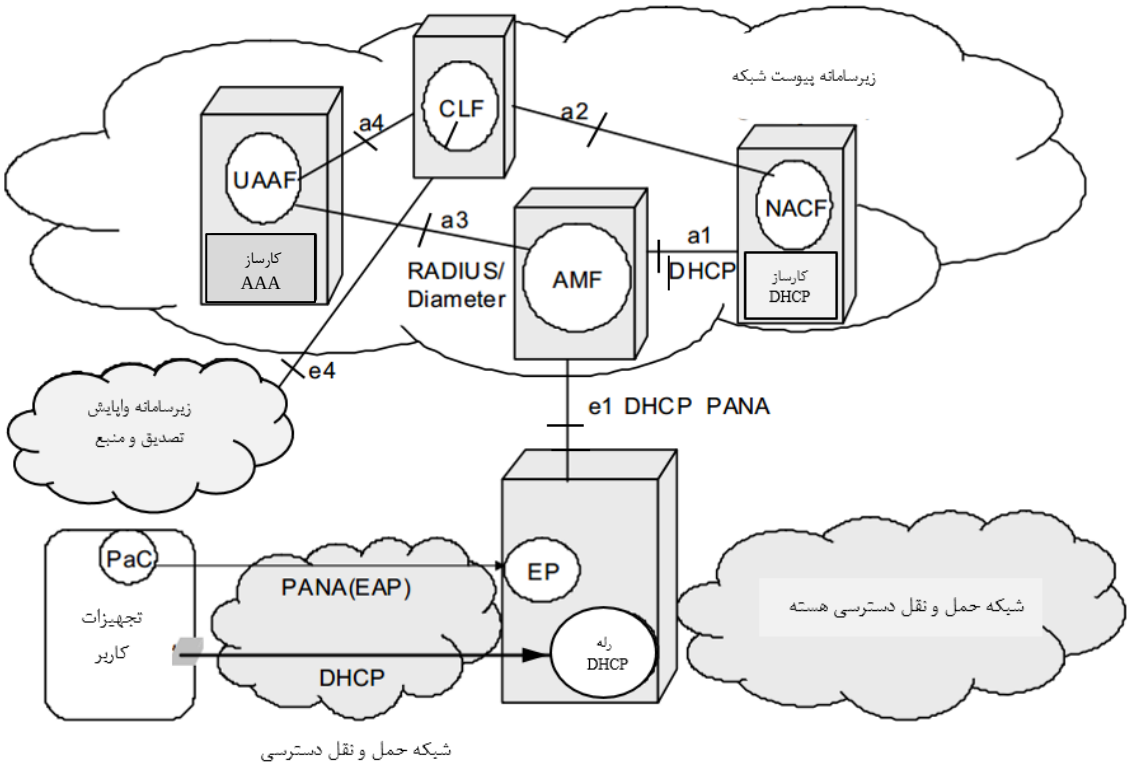
الف-۵ پیکربندی مبتنی بر PANA

احراز اصالت کاربر NASS مجاز است، با یک پیاده‌سازی مبتنی بر DHCP، در لایه IP با استفاده از PANA (پروتکل برای اجرای احراز اصالت دسترسی شبکه) تعریف شده درون IETF ارائه شود. این پروتکل IP، EAP را بین PaC مستقر در تجهیزات کاربر و PAA در سطح حمل و نقل، حمل می‌کند. این نشانک‌دهی PANA از نقطه تقویت (EP) که دسترسی کاربرهای NASS غیرمجاز به شبکه را واپایش می‌کند، عبور می‌کند.

عامل PAA به منظور صحت‌سنجی اعتبارنامه‌ها و حقوق PaC به یک کارساز احراز اصالت مراجعه می‌کند. چنانچه کارساز احراز اصالت روی همان تجهیزات فیزیکی که PAA قرار دارد جای گرفته باشد، یک API برای این تعامل کافی است. زمانی که آنها از هم جدا باشند، استفاده از فنون RADIUS یا Diameter برای این هدف مجاز است.

زمانی که کاربر NASS برای دسترسی به شبکه به‌طور موفقیت‌آمیزی احراز اصالت شده و مجاز شناخته شده باشد، PAA اطلاعات پیکربندی را به EP ارسال می‌کند تا خط‌مشی‌های تقویت برای هر بسته (به‌عبارتی پالایه‌ها) را که روی ترافیک ورودی و خروجی تجهیزات کاربر به‌کار رفته است، اصلاح کند.

شکل الف-۵ پیاده‌سازی مبتنی بر PANA را برای پیکربندی فیزیکی NASS توصیف می‌کند:



شکل الف-۵- پیکربندی مبتنی بر PANA

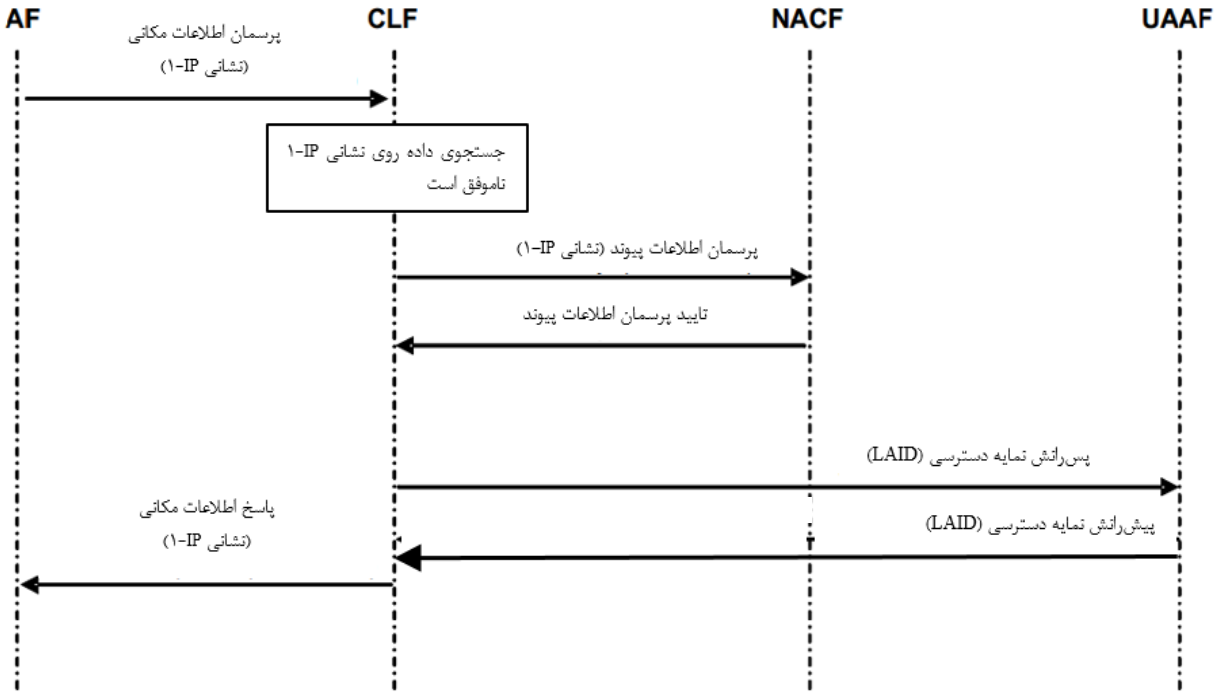
پیوست ب

(آگاهی‌دهنده)

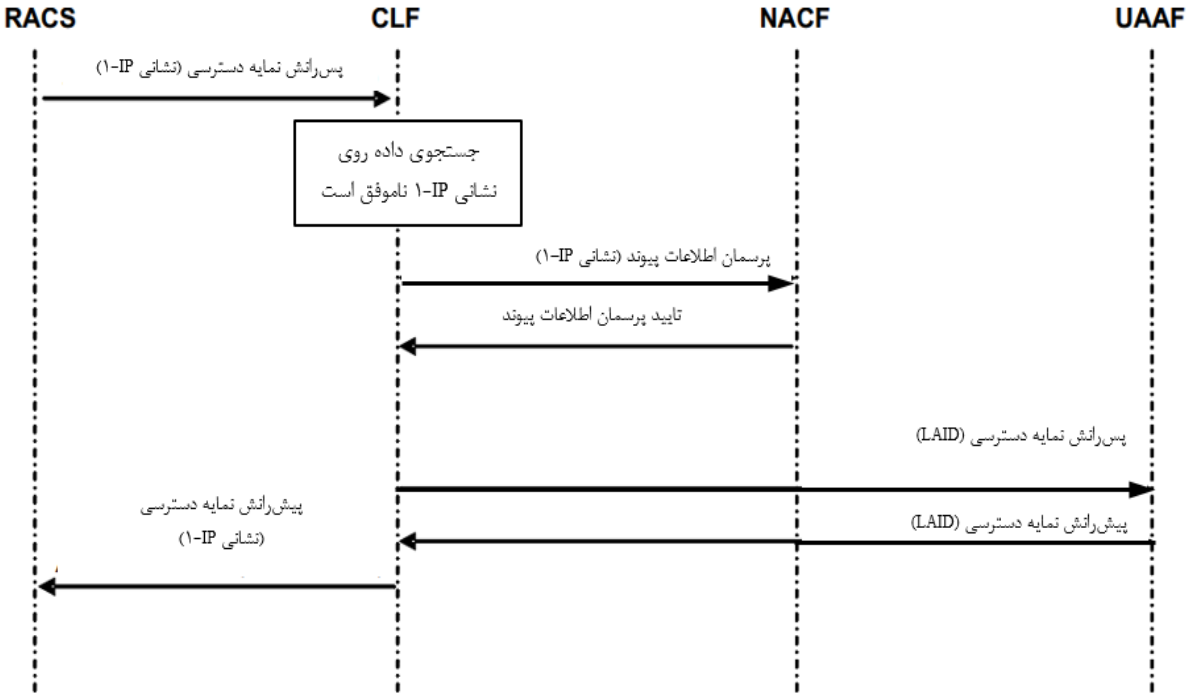
رویه‌های بازیابی برای عناصر کارکردی درون NASS

ب-۱ جریان تبادل اطلاعات مفهومی برای بازیابی وضعیت CLF

جزئیات جریان واقعی تبادل اطلاعاتی برای بازیابی کامل وضعیت CLF جزء هدف و دامنه کاربرد این استاندارد نیست. در زیر دو نمونه برای رویه‌های بازیابی CLF ارائه شده است، در حالتی که CLF برای اطلاعاتی مورد پرسمان قرار گیرد که در حال حاضر درون دادگان CLF قابل دسترس نباشد.



شکل ب-۱- بازیابی وضعیت CLF : پرسمان اطلاعات از AF



شکل ب-۲- بازیابی وضعیت CLF: پرسمان اطلاعات از RACS

کتابنامه

[1] ETSI TR 180 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Release definition".

[2] IETF RFC 4058: "Protocol for Carrying Authentication for Network Access (PANA) Requirements".

[3] IETF RFC 2131: "Dynamic Host Configuration Protocol"