استاندارد ملی ایران
۱۶۲۷۵
چاپ اول
اردیبهشت ۱۳۹۲

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

INSO
16275
1st. Edition
May.2013

فناوری اطلاعات - اتصال متقابل سامانه‌های باز - پروتکل امنیتی لایه‌ی شبکه

Information technology – Open systems interconnection – Network layer security protocol

ICS: 35.100.30

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی 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 وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات – اتصال متقابل سامانه‌های باز – پروتکل امنیتی لایه شبکه»

رئیس:	**سمت و/ یا نمایندگی**
فرهاد شیخ احمد، لیلا (کارشناسی‌ارشد مهندسی کامپیوتر نرم‌افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
دبیر:	
میراسکندری، سید محمدرضا (کارشناسی مهندسی کامپیوتر نرم‌افزار)	مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضاء: (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (کارشناسی مهندسی برق کنترل)	کارشناس سازمان فناوری اطلاعات ایران
جمیل پناه، ناصر (کارشناسی‌ارشد مدیریت)	کارشناس سازمان فناوری اطلاعات ایران
سعیدی، عذرا (کارشناسی‌ارشد مهندسی برق- مخابرات)	کارشناس سازمان فناوری اطلاعات ایران
سلطانی حقیقت، الهه (کارشناسی مهندسی برق مخابرات)	کارشناس سازمان فناوری اطلاعات ایران
عبداللهی ازگمی، محمد (دکترای مهندسی کامپیوتر نرم‌افزار)	استادیار دانشگاه علم و صنعت ایران
عسکرزاده، مجید (کارشناسی‌ارشد مهندسی کامپیوتر)	نماینده دانشگاه آزاد - واحد علوم و تحقیقات
فولادیان، مجید (کارشناسی‌ارشد مهندسی برق- مخابرات)	مشاور سازمان فناوری اطلاعات ایران
فیاضی، مهدی (کارشناسی مهندسی برق الکترونیک)	کارشناس مسؤول تدوین استاندارد و امنیت شبکه
قسمتی، سیمین (کارشناسی‌ارشد فناوری اطلاعات)	کارشناس سازمان فناوری اطلاعات ایران

مجاهدی، الناز (کارشناسی مهندسی کامپیوتر نرم‌افزار)	نماینده دانشگاه علم و صنعت ایران
معروف، سینا (کارشناسی مهندسی کامپیوتر سخت‌افزار)	کارشناس سازمان فناوری اطلاعات ایران
میرزایی رضایی، طیبه (کارشناسی‌ارشد فیزیک)	رییس اداره تدوین استانداردها و نظارت بر فرآیند سرویس‌ها سازمان فناوری اطلاعات

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات – اتصال متقابل سامانه‌های باز – پروتکل امنیتی لایه‌ی شبکه» که پیش‌نویس آن درکمیسیون‌های مربوط توسط سازمان فناوری اطلاعات تهیه و تدوین شده و در دویست و پنجاه و نهمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۱/۱۱/۱۵ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده‌ی ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه‌ی صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و ماخذی که برای تهیه‌ی این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 11577:1995: 1st Ed.: Information technology – Open Systems Interconnection – Network Layer security protocol

مقدمه

پروتکلی که به‌وسیله‌ی این استاندارد ملی تعریف می‌شود به‌منظور فراهم آوردن خدمات امنیتی در پشتیبانی از یک نمونه‌ی ارتباطی بین هستارهای[1] لایه‌ی پایین‌تر استفاده می‌شود. این پروتکل با در نظر گرفتن استانداردهای دیگر که به‌وسیله‌ی ساختار لایه‌ای که در توصیه‌نامه‌ی X.200 کمیته بین‌المللی تلگراف و تلفن (CCITT)[2] | ISO/IEC 7498-1 و هم‌چنین سازمان لایه‌ی شبکه که در استاندارد ISO 8648 تعریف می‌شود و به‌وسیله‌ی توصیه‌نامه‌ی X.802 |ITU-T ISO/IEC TR 13594 (مدل امنیتی لایه پایین‌تر) تعمیم داده می‌شود، مکان‌یابی شده است. این پروتکل، خدمات امنیتی را در پشتیبانی از خدمات شبکه‌ی مد اتصال[3] و مد بی‌اتصال[4] فراهم می‌آورد. به‌طور خاص، این پروتکل در لایه‌ی شبکه قرار داده می‌شود و در مرزهای بالاتر و پایین‌تر خود، واسط‌های کارکردی[5] و به‌طور صریح دارای واسط‌های خدماتی تعریف‌شده است.

برای ارزیابی انطباق یک پیاده‌سازی خاص، ضروری است که دارای بیانیه‌ای در رابطه با اینکه چه قابلیت‌ها و گزینه‌هایی برای یک پروتکل اتصال متقابل سامانه های باز (OSI)[6] مفروض پیاده‌سازی شده است، باشد. به چنین بیانیه‌ای، بیانیه انطباق پیاده‌سازی پروتکل (PICS)[7] گفته می‌شود.

1 - Entity
2 - Comité Consultatif International Téléphonique et Télégraphique
3 - Connection-mode
4 - Connectionless-mode
5 - Functional
6 - Open System Interconnection
7 - Protocol Implementation Conformance Statement (PICS)

فناوری اطلاعات – اتصال متقابل سامانه‌های باز – پروتکل امنیتی لایه‌ی شبکه

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، تعیین پروتکلی است که به‌وسیله‌ی سامانه‌های انتهایی و سامانه‌های میانی استفاده می‌شود تا خدمات امنیتی را که در استاندارد ISO 8648 و استاندارد|توصیه‌نامه‌ی CCITT X.213 | ISO/IES 8348 تعریف شده‌اند، در لایه‌ی شبکه فراهم آورد. پروتکل تعریف شده در این استاندارد ملی، پروتکل امنیتی لایه‌ی شبکه (NLSP)[1] نامیده می‌شود.

این استاندارد ملی موارد زیر را مشخص می‌کند:

۱- پشتیبانی از خدمات امنیتی زیر که در CCITT X.800 | ISP 7498-2 تعریف شده‌اند:

الف- احراز هویت هستار همتا[2]؛

ب- احراز هویت مبدأ داده[3]؛

پ- کنترل دسترسی[4]؛

ت- محرمانگی اتصال[5]؛

ث- محرمانگی بی‌اتصال[6]؛

ج- محرمانگی جریان ترافیک[7]؛

چ- یکپارچگی اتصال بدون بازیابی[8] (شامل یکپارچگی واحد داده که در آن واحدهای داده‌ی مجزا (SDUs)[9] در یک اتصال از نظر یکپارچگی محافظت شده‌اند.)؛

ح- یکپارچگی بی‌اتصال.

۲- الزامات کارکردی برای پیاده‌سازی‌هایی که ادعای انطباق با این استاندارد ملی را دارند.

رویه‌های این پروتکل با توجه به موارد زیر تعریف می‌شود:

الف- الزامات فن رمزنگاشتی[10] که می‌تواند در نمونه‌ای از این پروتکل استفاده شود؛

ب- الزاماتی بر اطلاعات حمل‌شده در همبستگی امنیتی[11] که در نمونه‌ای از ارتباط استفاده می‌شود.

1- Network Layer Security Protocol
2- Peer
3- Data Origin Authentication
4- Access Control
5- Connection Confidentiality
6- Connectionless Confidentiality
7- Traffic Flow Confidentiality
8- Connection Integrity Without Recovery
9- Single Data Unit
10- Cryptographic Technique
11- Security Association

اگرچه درجه‌ی محافظتی که برخی از سازوکارهای امنیتی می‌توانند فراهم کنند وابسته به استفاده برخی فنون خاص رمزنگاشتی است، عملکرد صحیح این پروتکل وابسته به انتخاب هر الگوریتم خاص رمزگذاری[1] یا رمزگشایی[2] نیست. این موضوع یک مسئله‌ی محلی برای سامانه‌های در حال ارتباط است.

علاوه بر این، نه انتخاب و نه پیاده‌سازی خط‌مشی امنیتی مشخص، در حیطه‌ی کاری این استاندارد ملی نیست. انتخاب یک خط‌مشی امنیتی مشخص و درنتیجه درجه‌ی محافظتی که به‌دست خواهد آمد، به‌عنوان یک مسئله‌ی محلی در میان سامانه‌هایی که از نمونه‌ای از ارتباطات امن استفاده می‌کنند، باقی می‌ماند. این استاندارد ملی استفاده از پروتکل امنیتی یکسان را برای نمونه‌های متعدد ارتباطات امنی که شامل یک سامانه‌ی باز منفرد هستند، الزام نمی‌کند.

پیوست ت یک پیش‌برگ PICS[3] برای پروتکل امنیت لایه‌ی شبکه فراهم می‌کند که با راهنمای مرتبط به آن در استاندارد ISO/IEC 9646-2 همخوانی دارد.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزیی از این استاندارد ملی ایران محسوب می‌شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره تاریخ تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:[4]

2-1 CCITT Recommendation X.213 (1992) | ISO/IEC 8348:1993, Information technology - Open Systems Interconnection – Network Service Definition.

2-2 ITU-T Recommendation X.233 (1993) | ISO/IEC 8473:1994, Information technology - Protocol for providing the connectionless-mode network Service: Protocol specification.

2-3 ITU-T Recommendation X.802 (1994) | ISO/IEC TR 13594:--1, Information technology - Open Systems Interconnection – Lower layers security model.

2-4 ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:--1), Information technology - Open Systems Interconnection - Upper layers security model.

2-5 CCITT Recommendation X.200 (1988), Information technology - Open Systems Interconnection – Basic Reference Model: The Basic Model.
ISO/IEC 7498- 1: 1994, Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model.

---

1 - Encipherment
2 - Decipherment
3 - Protocol Implementation Conformance Statement (PICS) proforma
۴ - مراجع الزامی ردیف‌های ۲-۱ الی ۲-۴ مربوط به توصیه‌نامه‌ها|استانداردهای بین‌المللی همسان، مراجع الزامی مندرج در ردیف‌های ۲-۵ الی ۲-۱۲ مربوط به توصیه‌نامه‌ها|استانداردهای بین‌المللی معادل با محتوای فنی و مراجع الزامی ردیف‌های ۲-۱۳ و ۲-۱۸ مربوط به سایر مراجع است.

2-6 CCITT Recommendation X.209 (1988), Specification of basic encoding rules for Abstract Syntax Notation One (ASN. 1).

ISO/IEC 8825: 1990, Information technology - Open Systems Interconnection - Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1).

2-7 ITU-T Recommendation X.2 10 (1993), Information technology - Open Systems Interconnection - Conventions for the definition of OSI services.

ISO/IEC 1073 1: 1994, Information technology - Open Systems Interconnection - Basic Reference Model - Conventions for the definition of OSI Services.

2-8 CCITT Recommendation X.223 (1988), Use of X.25 to provide the OSI connection-mode network Service.

ISO/IEC 8878: 1992, Information technology - Telecommunications and information exchange between Systems - Use of X.25 to provide the OSI connection-mode network Service.

2-9 CCITT Recommendation X.290 (1992), OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications - General concepts.

ISO/IEC 9646- 1: 1994, Information technology - Open Systems Interconnection - Conformation testing methodology and framework - Part 1: General concepts.

2-10 CCITT Recommendation X.291 (1992), OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications - Abstract test Suite specification.

ISO/IEC 9646-2: 1994, Information technology - Open Systems Interconnection – Conformance testing methodology and framework - Part 2: Abstract test Suite specification.

2-11 CCITT Recommendation X.509 (1988), Information technology - Open Systems Interconnection – The Directory: Authentication framework. ISO/IEC 9594-8: 1990, Information technology - Open Systems Interconnection - The Directory - Part 8: Authentication framework.

2-12 CCITT Recommendation X.800 (1991), Security architecture for Open Systems Interconnection for CCITT applications.

ISO 7498-2: 1989, Information processing systems Interconnection – Basic Reference Model – Part 2: Security Architecture.

2-13 ISO/IEC 8208:1990, Information technology - Data communications - X.25 Packet Layer Protocol for Data Terminal Equipment.

2-14 ISO 8648: 1988, Information processing Systems - Open Systems Interconnection - Internal organization of the Network Layer.

2-15 ISO/IEC 9834- 1: 1993, Information technology - Open Systems Interconnection - Procedures for the Operation of OSZ Registration Authorities - Part 1: General procedures.

2-16 ISO/IEC 9834-3: 1990, Information technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities - Part 3: Registration of Object identifier component values for joint ISO/CCITT use.

2-17 ISO/IEC 9979: 199 1, Data cryptographic techniques - Procedures for the registration of cryptographic algorithms.

2-18 CCITT Recommendation X.25 (1993), Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for terminals operating in Packet Mode and connected to public data networks by dedicated circuits.

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به‌کار می‌رود:

۳-۱ تعاریف مدل مرجع

این استاندارد ملی از اصطلاحات زیر همان‌طورکه در CCITT X.200 | ISO/IEC 7498-1 تعریف شده‌اند، استفاده می‌کند:

الف- سامانه‌ی پایانی[1]؛

ب- هستار شبکه[2]؛

پ- لایه‌ی شبکه[3]؛

ت- پروتکل شبکه[4]؛

ث- واحد داده پروتکل شبکه[5]؛

ج- رله شبکه[6]؛

چ- خدمت شبکه[7]؛

ح- نقطه دسترسی خدمت شبکه[8]؛

خ- نشانی نقطه دسترسی خدمت شبکه[9]؛

د- واحد داده‌ی خدمت شبکه[10]؛

ذ- واحد داده پروتکل[11]؛

ر- مسیریابی[12]؛

ز- خدمت؛

ژ- واحد داده‌ی خدمت[13].

۳-۲ تعاریف معماری امنیتی

این استاندارد ملی از اصطلاحات زیر که در CCITT X.800 | ISO 7498-2 تعریف شده‌اند، استفاده می‌کند:

---

1 - End system
2 - Network entity
3 - Network Layer
4 - Network Protocol;
5 - Network Protocol Data Unit
6 - Network Relay
7 - Network Service
8 - Network Service Access Point
9 - Network Service Access Point Address
10 - Network Service Data Unit
11 - Protocol Data Unit
12 - Routing
13 - Service Data Unit

الف- کنترل دسترسی[1]؛
ب- محرمانگی[2]؛
پ- یکپارچگی اتصال بدون بازیابی[3]؛
ت- محرمانگی بی‌اتصال[4]؛
ث- یکپارچگی بی‌اتصال[5]؛
ج- احراز هویت مبدأ داده[6]؛
چ- رمزگشایی[7]؛
ح- امضای دیجیتالی[8]؛
خ- رمزگذاری[9]؛
د- احراز هویت هستار همتا[10]؛
ذ- برچسب امنیتی[11]؛
ر- خدمت امنیتی[12]؛
ز- محرمانگی جریان ترافیک[13].

۳-۳ تعاریف متعارف خدمات

این استاندارد ملی از اصطلاحات زیر همان‌طورکه در ITU-T X.210 | ISO/IEC 10731 تعریف شده‌اند، استفاده می‌کند:

الف- ارائه دهنده‌ی خدمت[14]؛
ب- کاربر خدمت[15].

۳-۴ تعاریف خدمت شبکه

این استاندارد ملی از اصطلاح زیر همان‌طورکه در CCITT X.213 | ISO 8348 تعریف شده است، استفاده می‌کند:

- نقطه‌ی پیوست زیرشبکه[16].

---

1 - Access Control
2 - Confidentiality
3 - Connection Integrity Without Recovery
4 - Connectionless Confidentiality
5 - Connectionless Integrity
6 - Data Origin Authentication
7 - Decipherment
8 - Digital Signature
9 - Encipherment
10 - Peer Entity Authentication
11 - Security Label
12 - Security Service
13 - Traffic Flow Confidentiality.
14 - Service Provider
15 - Service User
16 - Subnetwork Point of Attachment

۳-۵ سازمان داخلی تعاریف لایه‌ي شبکه

این استاندارد ملی از اصطلاحات زیر همان‌طورکه در استاندارد ISO 8648 تعریف شده‌اند، استفاده می‌کند:

الف- سامانه‌ی میانی؛

ب- سامانه‌ی رله؛

پ- زیرشبکه؛

ت- پروتکل دسترسی زیرشبکه[1]؛

ث- پروتکل همگرایی وابسته به زیرشبکه[2]؛

ج- پروتکل همگرایی مستقل از زیرشبکه[3].

۳-۶ تعاریف پروتکل شبکه بی‌اتصال

این استاندارد ملی از اصطلاحات زیر همان‌طورکه در ISO/IEC 8473-1 | ITU-T X.233 تعریف شده‌اند، استفاده می‌کند:

الف- واحد داده‌ای پروتکل (PDU) اولیه[4]؛

ب- موضوع محلی[5]؛

پ- هم‌گذاری مجدد[6]؛

ت- قطعه[7].

۳-۷ تعاریف مدل امنیتی لایه‌ي بالاتر

این استاندارد ملی از اصطلاحات زیر همان‌طورکه در ISO/IEC 10745 | ITU-T X.803 تعریف شده‌اند، استفاده می‌کند:

الف- خط‌مشی تعامل امن[8]؛

ب- رابطه‌ی امنیتی[9].

۳-۸ تعاریف آزمون انطباق[10]

این استاندارد ملی از اصطلاحات زیر همان‌طورکه در ISO/IEC 9646-1 | CCITT X.290 تعریف شده‌اند، استفاده می‌کند:

الف- پیش‌برگ PICS؛

ب- بیانیه‌ی انطباق پیاده‌سازی پروتکل؛

پ- مرورکلی انطباق ایستا[1].

1- Subnetwork Access Protocol;
2 - Subnetwork Dependent Convergence Protocol
3 - Subnetwork Independent Convergence Protocol
4 - Initial Protocol Data Unit (PDU)
5 - Local Matter
6 - Reassembly
7 - Segment
8 - Secure Interaction Policy
9 - Security Relationship
10 - Conformance Testing

۳-۹ سایر تعاریف

در این استاندارد ملی، تعاریف زیر به‌کار می‌رود:

۳-۹-۱

شناسه‌ي همبستگي امنیتی (SA-ID)[۲] بي‌حرکت[۳]

یک **SA-ID** که به دلیل الزامات جلوگیری از استفاده‌ي مجدد، برای نسبت‌دهی به همبستگي امنیتی در دسترس نیست.

۳-۹-۲

کلید دوتایی

یک زوج از مقادیر کلید مرتبط (کلید عمومی) یا یکسان (کلید محرمانه) برای استفاده بین دو طرف خاص.

۳-۹-۳

اطلاعات کنترل امنیتی

به‌منظور برقراری یا حفظ یک همبستگی امنیتی، اطلاعات کنترل پروتکل (PCI)[۴] به‌وسیله‌ی یک پروتکل امنیتی مبادله می‌شود.

۳-۹-۴

صفات-SA[۵]

مجموعه‌ای از اطلاعات مورد نیاز برای کنترل امنیت ارتباطات بین یک هستار و همتا(های) راه دور[۶] آن.

۳-۹-۵

همبستگي امنیتی

یک رابطه‌ي امنیتی بین هستارهای لایه پایین‌تر ارتباطی که برایشان صفات-**SA** متناظر وجود دارد.

۳-۹-۶

یکپارچگی واحد داده

شکلی از یکپارچگی اتصال که در آن یکپارچگی واحد داده منفرد (SDU)[۷] اختصاصی محافظت می‌شود، اما خطاها در دنباله‌ی SDUها تشخیص داده نمی‌شوند.

---

1 - Static Conformance Overview.
2 - Security Association Identifier
3 - Frozen
4 - Protocol Control Information
5 - Security Association Attributes
6 - Remote
7 - Single Data Unit

۳-۹-۷

درون باند[1]

توسط سازوکارهای پروتکلی با استفاده از همبستگی امنیتی واحد پروتکل داده (SA PDU)[2] که در این استاندارد ملی تعریف شده است، انجام می‌گیرد.

۳-۹-۸

برون باند[3]

با روشی به غیر از استفاده از **SA PDU** انجام می‌شود.

۳-۹-۹

قواعد امنیتی

اطلاعات محلی که با توجه به خدمات امنیتی انتخاب شده، سازوکارهای امنیتی را برای استفاده مشخص می‌کنند که شامل تمام پارامترهای مورد نیاز برای کارکرد سازوکارها هستند.

یادآوری– این اطلاعات می‌توانند یک قسمت از قواعد برهم‌کنش[4] امنیتی را شکل دهند که در CCITT X.803 | ISO/IEC 10745 تعریف شده‌اند.

۳-۹-۱۰

برچسب[5]

به «برچسب امنیتی» مراجعه شود. (استاندارد|توصیه‌نامه‌ی X.800 CCITT | 2-7498 ISO).

۴ کوته‌نوشت‌ها

۴-۱ واحدهای داده

واحد داده‌ی پروتکل شبکه	Network Protocol Data Unit	NPDU
واحد داده‌ی خدمت شبکه	Network Service Data Unit	NSDU
واحد داده‌ی پروتکل	Protocol Data Unit	PDU
واحد داده‌ی خدمت	Service Data Unit	SDU

۴-۲ فیلدهای واحد داده‌ي پروتکل

نشان‌گر طول	Length Indicator	LI

۴-۳ پارامترها

کیفیت خدمت	Quality Of Service	QOS

1 - In-Band
2 - Security Association Protocol Data Unit
3 - Out-Of-Band
4 - Interaction
5 - Label

۴-۴ موارد متفرقه

ASSR	Agreed Set of Security Rules	مجموعه قواعد امنیتی مورد توافق
CL	Connectionless Mode	مد بی‌اتصال
CLNP	Connectionless Mode Network Protocol	پروتکل شبکه‌ی مد بی‌اتصال
CLNS	Connectionless Mode Network Service	خدمت شبکه‌ی مد بی‌اتصال
CO	Connection Mode	مد اتصال
CSC-PDU	Connection Security Control PDU	کنترل امنیت اتصال PDU
DU	Data Unit	واحد داده
EKE	Exponential Key Exchange	مبادله نمایی کلید
ES	End System	سامانه‌ی پایانی
ICV	Integrity Check Value	مقدار وارسی یکپارچگی
IS	Intermediate System	سامانه‌ی میانی
ISN	Integrity Sequence Number	عدد دنباله‌ی یکپارچگی
KEK	Key Enciphering Key	کلید رمزگذاری اصلی
NLSP	Network Layer Security Protocol	پروتکل امنیتی لایه‌ی شبکه
NLSP CO	NLSP for Connection Mode	NLSP برای مد اتصال
NLSP CL	NLSP for Connectionless Mode	NLSP برای مد بی‌اتصال
NLSPE	NLSP Entity	هستار NLSP
NS	Network Service	خدمت شبکه
NSAP	Network Service Access Point	نقطه دسترسی به خدمات شبکه
PCI	Protocol Control Information	اطلاعات کنترل پروتکل
PDU	Protocol Data Unit	واحد داده‌ی پروتکل
SA	Security Association	همبستگی امنیتی
SA-ID	Security Association Identifier	شناسه‌ی همبستگی امنیتی
SA-P	Security Association Protocol	پروتکل همبستگی امنیتی
SA-PDU	Security Association PDU	PDU همبستگی امنیتی

SCI	Security Control Information	اطلاعات کنترل امنیت
SDT PDU	Secure Data Transfer PDU	PDU انتقال داده‌ی امن
SN	Subnetwork	زیرشبکه
SNAcP	Subnetwork Access Protocol	پروتکل دسترسی زیرشبکه
SNICP	Subnetwork Independent Convergence Protocol	پروتکل همگرایی مستقل از زیرشبکه
SNPA	Subnetwork Point of Attachment	نقطه‌ی اتصال زیرشبکه
UN	Underlying Network	شبکه‌ی اصلی

۵ مرور کلی پروتکل

۵-۱ مقدمه

دو حالت پایه عملیاتی از پروتکل NLSP وجود دارد که عبارتند از:

الف- مد بی‌اتصال برای NLSP (NLSP-CL)[1]- جهت استفاده در ارائه یک خدمت شبکه مد بی‌اتصال امن.

ب- مد اتصال برای NLSP (NLSP-CO)[2]- جهت استفاده در ارائه یک خدمت شبکه مد اتصال[3] امن.

هر دو حالت NLSP به‌عنوان یک زیر-لایه از لایه‌ی شبکه عمل می‌کنند. خدمات فراهم شده برای هستار بالا، خدمت NLSP و خدماتی که قرار است برای NLSP فراهم شود، خدمات شبکه اصلی (UN)[4] نامیده می‌شوند. نخستینه‌ها[5] و پارامترها به‌صورت پیشوند با NLSP یا UN می‌آیند تا به وضوح، خدمتی را که به آن ارجاع می‌شود تمیز دهند. خدمت UN و NLSP «واسطهای ادراکی[6]» هستند، به بیان دیگر، به‌گونه‌ای توصیف شده‌اند که گویا یک خدمت لایه‌ای هستند اما بسته به مکان قرار گرفتن زیرلایه NLSP به صورت بالقوه می‌توانند به‌طور کامل در داخل لایه‌ی شبکه قرار گیرند. (مطابق با پیوست ث)

هر دو حالت NLSP می‌توانند در سامانه‌های پایانی و سامانه‌های میانی پیاده‌سازی شوند. هر دو حالت به نشانی منبع و مقصد NLSP و دیگر پارامترهای NLSP CONNECT اجازه می‌دهند که به‌صورت اختیاری محافظت شوند. حالت بااتصال برای NLSP می‌تواند در هر جایی داخل لایه‌ی شبکه عمل کند. مد بی‌اتصال برای NLSP می‌تواند در هر جایی داخل لایه‌ی شبکه در بالای پروتکل همگرایی وابسته به زیرشبکه عمل کند. (به استاندارد ISO 8648 رجوع شود.)

این پروتکل به‌نحوی طراحی شده است که بتواند برای برآورده کردن محدوده‌ای از الزامات در محیط‌هایی که دغدغه‌ی اصلی آن‌ها امنیت بالا است تا محیط‌هایی که دغدغه اصلی آن‌ها کارایی بهینه است، مناسب باشد.

---

1 - NLSP for Connectionless Mode
2 - NLSP for Connection Mode
3 - Connection Oriented
4 - Underlying Network
5 - Primitives
6 - Notional Interfaces

به‌طور مشخص، یک گزینه‌ی «بدون سرآیند[1]» در NLSP-CO ارائه شده است، که به‌وسیله‌ی آن اثر کمینه روی کارایی ارتباطات به‌دست آید، هر چند ممکن است امنیت کاهش یابد.
پروتکل NLSP، از مفهوم همبستگی امنیتی (SA) که ممکن است خارج از یک UNITDATA بی‌اتصال یا اتصال مشخص وجود داشته باشد، استفاده می‌کند. یک مجموعه از صفات تعریف کننده‌ی پارامترهای امنیت (برای مثال: الگوریتم‌ها، کلیدها و غیره) برای SA تعریف شده است.
پروتکل، حالت یکسانی از خدمت (CO یا CL) را در قلمروهای بالاتر و پایین‌تر خود فراهم می‌کند.
این پروتکل از محدوده وسیعی از سازوکارهای امنیتی مشخص پشتیبانی می‌کند. (هم استاندارد شده و هم استاندارد نشده) کاربران و پیاده‌سازها باید سازوکارهای امنیتی را برای استفاده با این پروتکل انتخاب کنند که برای اعمال خدمات امنیتی آن‌ها و سطح محافظت مورد نیاز، مناسب باشند. بندهای ۹ تا ۱۲ و پیوست پ، پشتیبانی از یک مجموعه سازوکارهای مشخص برای تمام خدمات امنیتی مورد نیاز NLSP را تعریف می‌کنند.
محافظت امنیتی که NLSP برای فراهم‌سازی آن تلاش می‌کند، از الزامات خدمات امنیتی که به‌وسیله‌ی مدیریت حوزه‌ی امنیتی برقرار شده، ناشی می‌شود.

یادآوری- استفاده از پارامتر QOS محافظت خدمات امنیتی NLSP، یک مسأله محلی و خارج از حیطه‌ی این استاندارد ملی است.

۲-۵ مرور کلی خدمات فراهم‌شده

پروتکل NLSP، خدمات امنیتی را که در توصیه‌نامه‌ی CCITT X.800 | ISO 7498-2 تعریف شده‌اند (برای این‌که مناسب لایه‌ی شبکه شوند) فراهم می‌کند؛ هم‌چنین خدمات لایه‌ی شبکه OSI (به‌گونه‌ای که در توصیه‌نامه‌ی CCITT X.213 | ISO/IEC 8348 تعریف شده‌اند) را نیز ارائه می‌کند.
در صورتی که خدمات امنیتی زیر انتخاب شده باشند، NLSP-CL از آن‌ها پشتیبانی می‌کند:
الف- احراز هویت مبدأ داده.
ب- کنترل دسترسی.
پ- محرمانگی بی‌اتصال - این محافظت به‌صورت اختیاری شامل تمام پارامترهای خدمت NLSP می‌شود که وابسته به خدمات امنیتی انتخابی است.
ت- محرمانگی جریان ترافیک.
ث- یکپارچگی بی‌اتصال - این محافظت به‌صورت اختیاری شامل تمام پارامترهای خدمت NLSP می‌شود که وابسته به خدمات امنیتی انتخابی است.
NLSP-CO، در صورتی که خدمات امنیتی زیر انتخاب شده باشند، از آن‌ها پشتیبانی می‌کند:
الف- احراز هویت هستار همتا.
ب- کنترل دسترسی.

1 - No-header

پ- محرمانگی اتصال - این محافظت به‌صورت اختیاری شامل تمام پارامترهای اتصال NLSP می‌شود که وابسته به خدمات امنیتی انتخابی است.
ت- محرمانگی جریان ترافیک.
ث- یکپارچگی اتصال بدون بازیابی- این محافظت به‌صورت اختیاری شامل تمام پارامترهای اتصال NLSP است که وابسته به خدمات امنیتی انتخابی است. هم‌چنین این محافظت به‌صورت اختیاری شامل یکپارچگی یک دنباله از SDUها است.

۵-۳ مرور کلی خدمات مفروض

خدمات مفروض زیر NLSP به‌عنوان خدمات اصلی شبکه (UN)[1] مورد اشاره قرار می‌گیرند. خدمات اصلی که به‌وسیله‌ی NLSP-CL فرض می‌شوند، از نخستینه‌های مشابه با آن‌هایی که در خدمات شبکه بی‌اتصال (توصیه‌نامه‌ی CCITT X.213 | ISO/IEC 8348) تعریف شده‌اند، استفاده می‌کنند.
برای NLSP-CO، واسط-UN در دو قسمت مدل‌سازی می‌شود:
الف- خدمتی که از نخستینه‌های یکسان با توصیه‌نامه‌ی CCITT X.213 | ISO/IEC 8348 به‌علاوه پارامتری که پارامتر احراز هویت UN نامیده می‌شود، استفاده می‌کند.
ب- نگاشت این خدمات به خدمات شبکه استاندارد یا به‌طور مستقیم به توصیه‌نامه‌ی CCITT X.25 | ISO/IEC 8208.
به نشانی شبکه‌ای که در نخستینه NLSP آورده می‌شود به اصطلاح NLSP-address گفته می‌شود.
این پارامتر خدماتی، هستار کاربر NLSP که می‌تواند یک هستار انتقال باشد یا نباشد (بسته به این‌که آیا دیگر پروتکل‌های لایه‌ی شبکه بالای NLSP استفاده شده‌اند و آیا محیط پروتکل امنیت لایه‌ی شبکه (NLSPE) در یک ES یا یک IS قرار گرفته است.) را شناسایی می‌کند.
نشانی شبکه‌ای که به شبکه‌ی اصلی داده می‌شود، نشانی UN نامیده می‌شود. پارامتر UN معادل با نشانی SNPA است. (اگر و تنها اگر هیچ پروتکلی بین NLSP-entity و هستار دسترسی زیرشبکه عمل نکند.)

۵-۴ همبستگی‌های امنیتی و قواعد امنیتی

۵-۴-۱ همبستگی‌های امنیتی

عملیات NLSP به‌وسیله‌ی مجموعه‌ای از اطلاعات مدیریت امنیت کنترل می‌شود (به‌عنوان مثال اطلاعات انتخاب خدمات امنیتی، شناسه‌ی الگوریتم امنیتی، کلیدهای رمزنگاشتی) که صفات همبستگی امنیتی (صفات SA) نامیده می‌شوند. مجموعه‌ای از صفات همبستگی امنیتی که برای حاکم کردن خدمات امنیتی پیش‌بینی شده بین هستارهای ارتباطی مورد نیاز هستند، به اصطلاح همبستگی امنیتی نامیده می‌شود.
توضیحات بیشتر در مورد همبستگی‌های امنیتی در توصیه‌نامه‌ی ITU-T X.802 | ISO/IEC TR 13594 (مدل امنیتی لایه‌های پایین‌تر) آورده شده است.

1 - Underlying Network (UN)

صفات SA مورد نیاز برای هر دوی NLSP-CL و NLSP-CO در زیربند ۶-۲ تعریف می‌شوند. صفات SA مورد نیاز برای NLSP-CL در زیربند ۷-۴ تعریف شده است. صفات مورد نیـاز برای NLSP-CO در زیربند ۸-۴ تعریف شده است. دیگر صفات مختص سازوکار در زیربندهای ۱۰-۲، ۱۱-۲ و ۱۲-۲ تعریف شده‌اند.

به‌منظور محافظت از یک نمونه ارتباطی (یک SDU بی‌اتصال یا یک اتصال)، از یک SA مناسب موجود استفاده می‌شود، یا در صورتی که SA مناسبی وجود نداشته باشد، نیاز است که یک SA بین طرف‌های ارتباطی برقرار شود.

همبستگی امنیتی می‌تواند برون باند یا با استفاده از SA-P درون باند NLSP برقرار شود. SA-P پروتکل امنیتی لایه‌ی شبکه، اطلاعات کنترل امنیتی (SCI) را از طریق استفاده از SA PDUها و/یا SDT PDUها با محتـوای نـوع داده‌ی SA-P مبادله می‌کنـد. اگر قـرار باشـد SCI به‌صـورت رمز نشـده حمل شود باید از SA-PDUها استفاده شود. اگر قرار باشد SCI محافظت‌شده باشد، باید از SA-PDU یا SDT PDU استفاده کرد. از این SCI برای کامل کردن صفات SA بر پایه‌ی صفات از قبل ایجاد شده‌ی SA و قواعد امنیتی استفاده می‌شود.

هم‌چنین NLSP-CO از مبادله اطلاعات برای به‌روزرسانی صفات SA «پویا» (به‌عنوان مثال، کلیدهای دایر، به پیوست چ مراجعه شود) در طی برقراری اتصال و داخل یک اتصال پشتیبانی می‌کند. یک به‌روزرسانی در داخل صفات SA پویا نباید خدمات امنیتی فراهم شده را تغییر دهد.

استفاده از یک SA-P درون باند به همراه NLSP-CL در زیربند ۷-۵ تعریف شده است. استفاده از SAP درون باند به همراه NLSP-CO در زیربند ۸-۵ (درطی برقراری اتصال) و در زیربند ۸-۱۱-۱ (در طی انتقال داده) تعریف می‌شود. یک پروتکل برای پی‌بردن به SA-P درون باند در پیوست پ این استاندارد تعریف شده است. مثالی از یک سازوکار جهت ایجاد کلیدی برای استفاده با این پروتکل در پیوست ح آورده شده است.

۵-۴-۲ قواعد امنیتی

تنظیم تعدادی از صفات SA توسط خط‌مشی امنیتی محدود می‌شود. این قسمت از خط‌مشی امنیتی با اصطلاح مجموعه‌ای از قواعد امنیتی برای هستار پروتکل بیان می‌شود. مجموعه‌ی قواعد امنیتی برای یک هستار پروتکل می‌تواند صفات SA، مانند طول فیلد، الگوریتم‌های رمزگذاری و غیره را برای این‌که یک مقدار منفرد باشند یا مجموعه‌ای از مقادیر باشند (برای محدود شدن بیشتر با روش‌های دیگر، برای مثال، مدیریت سامانه‌های OSI یا استفاده از مبادله‌ی SA-P)، محدود کند.

جایی که سطوح محافظت جایگزین پیشنهاد می‌شوند، مجموعه قواعد امنیتی، محدودیت‌های جایگزین را تعریف می‌کند تا کیفیت‌های متفاوتی از محافظت مورد نیاز را برآورده سازد.

وقتی که از مجموعه قواعد امنیتی در بین NLSPEها استفاده می‌شود، نیاز است که یک شناسه‌ی یکتا برای آن برقرار و به‌عنوان مجموعه قواعد امنیتی مورد توافق (ASSR) شناخته شود. شناسه‌ی ASSR می‌تواند به‌عنوان قسمتی از برقراری همبستگی امنیتی مبادله شود.

توضیحات بیشتر در مورد قواعد امنیتی در ISO/IEC TR 13594 (مدل امنیتی لایه‌های پایین‌تر) آورده شده است.

۵-۵ مرورکلی پروتکل- کارکردهاي محافظت

۵-۵-۱ گستره‌ي محافظت

هر دوی NLSP-CO و NLSP-CL، سه حالت مختلف عملیاتی دارند که از سه درجه‌ی محافظت پایه پشتیبانی می‌کنند:

الف- *محافظت از تمامی پارامترهای خدماتی NLSP*

در این حالت، تمامی پارامترهای خدمت NLSP، شامل نشانی‌ها و تمامی داده‌های کاربر، به‌غیر از آن‌هایی که با فراهم‌آورنده‌ی خدمت مذاکره شده‌اند (QOS، انتخاب تأیید دریافت[1]، انتخاب داده پیشتاز[2])، محافظت می‌شوند.

این حالت به‌وسیله‌ی صفت Param_Prot که در SA برابر با TRUE است انتخاب می‌شود.

ب- *محافظت از NLSP-Userdata*

در این حالت، داده‌ی کاربر محافظت می‌شود اما دیگر پارامترهای خدمت NLSP محافظت نمی‌شوند.

این حالت به‌وسیله‌ی صفت Param_Prot که در SA برابر با FALSE است، انتخاب می‌شود.

زیرحالت‌های بیشتری برای محافظت از NLSP-Userdata در حالت NLSP-CO وجود دارد:

- همه داده‌های کاربر NLSP محافظت می‌شوند. (که شامل NLSP-Userdata در نخستینه‌های خدماتی NLSP-CONNECT، NLSP-DATA و NLSP-DISCONNECT است.)

- NLSP-Userdata در NLSP DATA محافظت می‌شوند.

زیرحالت‌های NLSP به‌وسیله‌ی صفت SA، Protect-Connect-Params انتخاب می‌شوند. (به زیربند ۸-۳ مراجعه شود.) اگر Protect-Connect-Params مقدار TRUE داشته باشد، تمام داده‌های کاربر محافظت‌شده هستند، در غیر این صورت تنها NLSP-Userdata در NLSP-DATA محافظت‌شده است. اگر Param-Prot برابر TRUE باشد، Protect-Connect-Params باید به‌طور حتم مقدار TRUE داشته باشد. (یعنی تمام داده‌های کاربر NLSP محافظت‌شده است.)

پ- *بدون محافظت*

در این حالت، تمامی پارامترهای خدماتی به‌طور مستقیم بر روی پارامترهای خدمت UN معادل رونوشت می‌شوند. تمام رویه‌های NLSP، کنار گذاشته[3] می‌شوند.

این حالت به‌صورت محلی بر پایه‌ی نشانی‌های همتای در حال ارتباط و نیازهای خدمات امنیتی محلی انتخاب می‌شود.

۵-۵-۲ کیفیت محافظت

تحقق QOS امنیت (محافظت) در لایه‌های پایین‌تر OSI توسط پیاده‌سازی‌هایی صورت می‌گیرد که خدمات امنیتی را برای به‌کارگیری از طریق خط‌مشی امنیتی کنترل‌شده‌ی محلی انتخاب می‌کنند. هر نشان

1 - Receipt Confirmation Selection
2 - Expedited Data Selection
3 - Bypassed

درون باند از خدمات امنیتی انتخاب شده در یک پروتکل همبستگی امنیتی حمل می‌شود (به‌صورت ضمنی با استفاده از یک برچسب امنیتی یا به‌صورت صریح توسط دیگر روش‌ها) که مستقل از یک نمونه ارتباطی است. درنتیجه، هرگونه تغییرات مربوط به انتخاب خدمات امنیتی، مستقل از انتقال پارامتر QOS در سراسر قلمروهای واسط خدمات است.

یادآوری- ممکن است که در آنجا نیاز به نشان دادن خدمات امنیتی به لایه‌های بالاتر وجود داشته باشد. گرچه، هیچ نیاز فوری برای تعریف الزامات QOS محافظت مشخصی که تا کنون برقرار شده‌اند، وجود ندارد.

۵-۵-۳ کارکردهاي محافظت داده

۵-۵-۳-۱ SDT مبتنی بر PDU

هم NLSP-CO و هم NLSP-CL می‌توانند از طریق استفاده از یک انتقال داده امن PDU (SDT PDU)، از پارامترهای خدمت NLSP محافظت کنند. هم‌چنین NLSP-CO یک روش جایگزین برای محافظت از داده‌ی کاربر NLSP دارد که با TRUE شدن صفت SA بدون سرآیند[1] (به زیربند ۸-۳ مراجعه شود) انتخاب می‌شود.

استفاده از رویه‌های مبتنی بر SDT PDU از طریق موارد زیر از پارامترهای خدمت NLSP محافظت می‌کند:

الف- کدبندی پارامترهای خدمت NLSP به‌عنوان یک رشته‌ی هشت‌تایی قبل از کپسوله‌سازی[2]؛

ب- اگر برچسب‌گذاری امنیتی صریح[3] انتخاب شده باشد (برچسب صفت SA برابر TRUE است)، یک برچسب امنیتی را در Octet-String-Before-Encapsulation قرار می‌دهد؛

پ- اعمال یک کارکرد کپسوله‌سازی (و واکپسوله‌سازی[4]) که از سازوکارهای زیر پشتیبانی می‌کند:

- محرمانگی جریان ترافیک؛
- یکپارچگی و احراز هویت مبدأ داده؛
- محرمانگی.

که برای خدمات امنیتی انتخاب‌شده، مناسب هستند. این کارکرد یک رشته هشت‌تایی محافظت‌شده را فراهم می‌آورد.

زیربندهای ۶-۴-۱-۱ و ۶-۴-۲-۱ رویه‌های عمومی و مستقل از سازوکار را، جهت استفاده از SDT PDU در محافظت داده، تعریف می‌کنند. بند ۱۱ پشتیبانی یک کلاس از سازوکار برای کپسوله‌سازی مبتنی بر SDT PDU را تعریف می‌کند. دیگر رویه‌های کپسوله‌سازی (که به‌صورت خصوصی تعریف می‌شوند) نیز می‌توانند با SDT PDU استفاده شوند.

---

1 - No Header
2 - Encapsulation
3 - Explicit
4 - Decapsulation

۵-۵-۳-۲ بدون سرآیند (تنها NLSP-CO)

حالت NLSP-CO بدون سرآیند با استفاده از یک کارکرد کپسوله‌سازی که طول داده‌ی محافظت‌شده را تغییر نمی‌دهد، از NLSP-Userdata محافظت می‌کند. NLSP هیچ‌گونه اطلاعات کنترل پروتکلی را به داده‌ی محافظت‌شده اضافه نمی‌کند. خدمات امنیتی پشتیبانی‌شده، به سازوکارهای استفاده‌شده بستگی خواهند داشت، اما کارکرد کپسوله‌سازی باید حداقل محرمانگی را فراهم آورد. حالت بدون سرآیند می‌تواند تنها برای محافظت از یک پارامتر خدمت منفرد (NLSP-Userdata) استفاده شود و بنابراین تنها زمانی می‌تواند استفاده شود که Param_Prot برابر FALSE باشد. زیربندهای ۶-۴-۱-۲ و ۶-۴-۲-۲ رویه‌های عمومی و مستقل سازوکار را برای استفاده از حالت بدون سرآیند جهت محافظت از داده تعریف می‌کنند. بند ۱۲ پشتیبانی از یک کلاس از سازوکار برای کپسوله‌سازی بدون سرآیند را تعریف می‌کند. دیگر رویه‌های کپسوله‌سازی (که به‌صورت خصوصی تعریف می‌شوند) نیز می‌توانند با حالت بدون سرآیند استفاده شوند.

۵-۵-۴ کنترل امنیت اتصال (فقط NLSP-CO)

زمانی که یک اتصال برقرار می‌شود، PDUهای کنترل امنیتی اتصال مبادله می‌شوند تا حالت برقراری اتصال NLSP، نشانه‌گذاری شود. (توسط نگاشت SA-P درون باند یا نخستینه‌های NLSP CONNECT به نخستینه‌های UN-CONNECT یا UN-DATA) علاوه‌براین، CSC-PDU می‌تواند از احراز هویت هستار همتا پشتیبانی کند و مقادیر را برای صفات SA پویا مانند کلیدها و اعداد دنباله یکپارچگی برقرار کند. این امر امکان استفاده‌ی مجدد از یک SA که از قبل برقرار شده است را می‌دهد. (بدون این‌که سربار SA-P را تحمیل کند.) همچنین می‌تواند در هر زمان طی مدت حیات یک اتصال استفاده شود تا دوباره احراز هویت SA را اثبات (اثبات دانش به اشتراک گذاشته شده‌ی) یا صفات پویا را به‌روزرسانی کند.

CSC-PDU، فقط در مد اتصال NLSP استفاده می‌شود. در بند ۸ رویه‌های عمومی و مستقل از سازوکار برای استفاده از CSC-PDU تعریف شده است. بند ۱۰، پشتیبانی از یک کلاس سازوکار را برای احراز هویت و مدیریت کلید تعریف می‌کند. دیگر رویه‌هایی که به‌صورت خصوصی برای پشتیبانی از دیگر کلاس‌های سازوکار تعریف شده‌اند، می‌توانند با CSC-PDU استفاده شوند.

یادآوری- هنگامی که از سازوکارهای جایگزین برای احراز هویت استفاده می‌شود، اگر از سازوکار ISN که در بند ۱۱ تعریف شده است، استفاده شود، سازوکار جایگزین باید یک مقدار اولیه برای ISN ایجاد کند.

۵-۵-۵ PDUهای استفاده شده به‌وسیله‌ي NLSP

PDUهای زیر به‌وسیله‌ی NLSP استفاده می‌شوند:

الف- PDU انتقال داده‌ی امن– برای محافظت از پارامترهای نخستینه‌ی خدمت NLSP و سایر داده‌ها از طریق کپسوله‌سازی که طرح آن در زیربند ۵-۵-۳-۱ بیان شده است. ساختار این PDU در زیربند ۱۳-۳ تعریف شده است.

ب- PDU کنترل امنیت اتصالات– برای کنترل حالت برقراری اتصال NLSP-CO و فراهم کردن اختیاری احراز هویت هستار همتا، همچنین تغییر صفات SA پویا که طرح آن در زیربند ۵-۵-۴ آمده است. ساختار این PDU در زیربند ۱۳-۵ تعریف شده است.

یادآوری– CSC-PDU فقط به NLSP-CO قابل اعمال است.

پ- SA PDU – یک PDU که امکان مبادله‌ی درون باند اطلاعات کنترل امنیتی را به‌منظور مدیریت SA (که طرح آن در زیربند ۵-۴-۱ مشخص شده است) فراهم می‌کند. ساختار این PDU در زیربند ۱۳-۴ تعریف شده است.

علاوه‌براین، با NLSP-CO، داده می‌تواند به‌صورت اختیاری، بدون اضافه کردن هرگونه اطلاعات کنترل پروتکل اضافی (یعنی بدون استفاده از STD PDU) محافظت شود. (که طرح آن به جای استفاده از SDT PDU در زیربند ۵-۵-۳-۲ بیان شده است.)

۵-۶ مرور کلی پروتکل NLSP-CL

۵-۶-۱ بندهای تعریف‌کننده NLSP-CL

رویه‌های NLSP-CL در بندهای ۶ و ۷ و همراه با رویه‌های مختص سازوکار اختیاری برای کپسوله‌سازی در بند ۱۱ تعریف شده‌اند. این رویه‌ها از SDT PDU که در زیربند ۱۳-۳ تعریف شده‌است، و به‌صورت اختیاری از SA PDU که در زیربند ۱۳-۴ تعریف شده است، استفاده می‌کنند.

زیربندهای زیر مرور کلی بر عملیات NLSP-CL دارند؛ بندهای مشخصی که در بالا آورده شدند عملیات NLSP-CL را تعریف می‌کنند.

۵-۶-۲ کارکردهاي NLSP-CL

پروتکل امنیتی لایه‌ی شبکه از توانایی انتقال داده‌ی بی‌اتصال محافظت‌شده یا محافظت‌نشده بین کاربران NLSP همتا (در صورتی که قواعد کنترل دسترسی در ASSR این اجازه را داده باشند) پشتیبانی می‌کند. هستار NLSP به‌صورت محلی (با استفاده از خدمات امنیتی انتخاب شده، نشانی NLSP مقصد و دیگر اطلاعات مدیریت) مشخص می‌کند که آیا محافظت مورد نیاز است یا خیر. انتقال داده‌ی محافظت‌شده می‌تواند همراه با محافظت از تمامی پارامترهای خدمت NSP یا فقط NLSP-Userdata باشد که به‌وسیله‌ی ویژگی Param_Prot SA تعیین شده است.

در هنگام دریافت یک درخواست NLSP-UNITDATA:

- هستار NLSP، SA را وارسی می‌کند و مشخص می‌کند که آیا ارتباط محافظت‌نشده با نشانی مقصد مجاز است و اگر چنین است، چه محافظتی مورد نیاز است.

- اگر هیچ محافظتی مورد نیاز نباشد، هستار NLSP تمام نخستینه‌ها و پارامترهای NLSP را بدون تغییر به نخستینه‌ها و پارامترهای UN متناظر رونوشت می‌کند.

- اگر محافظت نیاز باشد، هستار NLSP، پارامترهای خدمت را کپسوله‌سازی می‌کند، یک SDT PDU را تشکیل می‌دهد و آن را به‌عنوان UN-Userdata از یک درخواست UN-UNITDATA به همراه نشانی منبع UN، نشانی مقصد UN و پارامترهای UN QOS انتقال می‌دهد. این امر می‌تواند تنها از داده‌ی کاربر NLSP یا از تمام پارامترهای خدمت NLSP محافظت کند.

در زمان دریافت یک نشان UN-UNITDATA، هستار NLSP:

- از نشانی منبع UN و اطلاعات محلی استفاده کرده تا تعیین کند که آیا ارتباط با نشانی مقصد مجاز است و اگر چنین است، چه محافظتی مورد نیاز است.

- اگر محافظت مورد نیاز نباشد، پارامترهای خدمت UN، بدون تغییر به پارامترهای NLSP رونوشت می‌شوند.

- اگر محافظت مورد نیاز باشد، هستار NLSP، SDT PDU را وارسی می‌کند و NLSP-Userdata، به‌صورت اختیاری سایر پارامترهای خدمت NLSP را با استفاده از کارکرد واکپسوله‌سازی، استخراج می‌کند. داده‌ی کاربر، نشانی مبدأ، نشانی مقصد و پارامترهای QOS در اظهار NLSP-UNITDATA به NLSP-user ارسال می‌شوند.

یادآوری– در زمان انتقال، NLSP می‌تواند بعد از (قبل از دریافت) کارکرد پروتکل توصیه‌نامه‌ی ITU-T X.233 | ISO/IEC 8473-1 (که از CLNP PDUها محافظت می‌کند)، عمل کند. هم‌چنین، در زمان انتقال، NLSP می‌تواند قبل از (بعد از دریافت) کارکرد[1] پروتکل CLNP با NLSP PDUهایی که در فیلدهای داده CLNP PDU حمل می‌شوند، عمل کند. برای بحث بیشتر در رابطه با استفاده از NLSP و CLNP، به پیوست ث مراجعه کنید.

به‌دلیل اینکه برخی از پارامترهای CLNP می‌توانند رابطه‌ی امنیتی داشته باشند، انتخاب چنین پارامترهایی، بعد از NLSP در زمان انتقال، باید در خط‌مشی امنیتی محلی مد نظر قرار گیرند. برخی از پارامترهای اختیاری که باید مورد نظر قرار گیرند، عبارتند از: ثبت مسیر، مسیریابی مبدأ جزیی و کامل و شمارش پرش. هر یک از این پارامترها می‌توانند اطلاعاتی در رابطه با شبکه بدهد که نباید در دسترس مشاهده‌گر[2] شبکه قرار گیرد.

برای تعیین اینکه آیا یک NLSP-CL PDU در داخل CLNP PDU حمل شده است، در زمان دریافت، دریافت‌کننده باید انتخاب‌کننده‌ی نشانی مقصد را وارسی کند که تماماً صفر باشد یا اینکه شناسه‌ی پروتکل NLSP را در داخل فیلد داده‌ی CLNP PDU (که در زیربند ۱۳-۳ تعریف شده است) وارسی کند. هر دوی

1 - Functionality
2 - Observer

این وارسی‌ها می‌تواند برای نشان دادن اینکه این PDU برای پردازش توسط لایه‌ی شبکه است (نه برای ارسال آن به لایه‌ی انتقال) استفاده شود.

۵-۷ مرور کلی پروتکل NLSP-CO

۵-۷-۱ بندهای تعریف‌کننده NLSP-CO

رویه‌ها برای NLSP-CO مبتنی بر No-Header در بندهای ۶ و ۸ تعریف شده‌اند و همراه با رویه‌های مختص سازوکار اختیاری برای کپسوله‌سازی در بند ۱۲ و برای کنترل امنیت اتصال در بند ۱۰ آمده‌اند. این رویه‌ها از CSC-PDU (که در زیربند ۱۳-۵ تعریف شده است) و به‌صورت اختیاری از SA PDU (که در زیربند ۱۳-۴ تعریف شده است)، استفاده می‌کنند.

رویه‌های NLSP مبتنی بر استفاده از SDT PDU در بندهای ۶ و ۸ تعریف شده‌اند؛ و همراه با رویه‌های مختص سازوکار اختیاری برای کپسوله‌سازی در بند ۱۱ و برای کنترل امنیت اتصال در بند ۱۰ آمده است=اند. این رویه‌ها از CSC-PDU که در زیربند ۱۳-۳ و CSC-PDU که در زیربند ۱۳-۵، و به‌صورت اختیاری از SA PDU که در زیربند ۱۳-۴ تعریف شده‌اند، استفاده می‌کنند.

زیربندهای زیر، تنها مرور کلی بر عملیات NLSP-CO را ارائه می‌کنند؛ بندهای مشخص که در بالا معرفی شده‌اند، عملیات NLSP-CO را تعریف می‌کند.

۵-۷-۲ اتصالات محافظت‌نشده‌ی NLSP-CO

اگر ارتباطات محافظت‌نشده بین نشانی‌های فراخوانی‌شده و فراخواننده مجاز باشد، تمام پارامترهای خدمت NLSP/UN به‌طور مستقیم به/از واسط خدمت NLSP از/به رابط خدمت UN رونوشت می‌شوند.

۵-۷-۳ NLSP-CONNECT

در زمان دریافت یک درخواست NLSP-CONNECT، NLSPE وارسی می‌کند که آیا در حال حاضر SA با مشخصات مورد نیاز وجود دارد؛ اگر چنین بود، می‌تواند برای محافظت از اتصال استفاده شود. در غیر این‌صورت، SA جدید به‌عنوان قسمتی از کارکردهای NLSP-CONNECT به‌صورت درون باند یا در یک مهلت زمانی مفروض به‌صورت برون باند برقرار می‌شود. اگر هیچ یک از این دو نتواند انجام شود، یک NLSP-DISCONNECT برگردانده می‌شود.

دو حالت پایه از برقراری یک اتصال NLSP پشتیبانی می‌شود. در یکی، پارامترهای NLSP CONNECT در نخستینه‌های خدمت UN-CONNECT حمل می‌شوند. در دیگری، پارامترهای NLSP CONNECT، پس از کپسوله‌شدن در یک SDT PDU و بعد از اینکه اتصال UN برقرار شد، در UN-DATA حمل می‌شوند.

دو حالت برقراری اتصال NLSP اشکال گوناگونی دارند، یکی برای استفاده با مبادلات درون باند SA-P (با استفاده از SA PDU و/یا SDT PDU به‌همراه نوع داده‌ی محتوای SA-P) که در UN-DATA حمل می‌شود، دیگری برای استفاده با یک SA که برون باند برقرار شده است.

PDU کنترل امنیت اتصال (CSC) برای اعلام حالت برقراری اتصال استفاده می‌شود و اگر SA-P درون باند در حال حمل شدن نباشد، از مبادله‌ی CSC-PDUها نیز استفاده می‌شود تا:

الف- صفات امنیتی مختص سازوکار را برای استفاده در محافظت اتصال (برای مثال، کلیدها، اعداد دنباله‌ی یکپارچگی) برقرار سازد؛
ب- احراز هویت هستار همتا را انجام دهد.
بند ۱۰ پشتیبانی اختیاری برای سازوکارهای -چالش-پاسخ مبتنی بر احراز هویت و مدیریت کلید را تعریف می‌کند.
در حالتی که NLSP-CONNECT در UN-CONNECT با SA-P درون باند حمل شود، یک اتصال UN برقرار می‌شود تا قبل از انجام تبادل UN-CONNECT که پارامترهای NLSP-CONNET را حمل می‌کند، SA-P را حمل و رها سازد. CSC-PDUها در دومین تبادل UN-CONNECT استفاده می‌شوند تا هستار-های NLSP همتا را دوباره احراز هویت کنند.
برقراری SA از طریق تبادل SA PDUها یا SDT PDUهایی که اطلاعات مورد نیاز برای تنظیم صفات SA مورد نیاز را حمل می‌کنند، به‌دست می‌آید. پیوست پ یک پروتکل SA را برای این منظور تعریف می‌کند.
اگر پارامترهای NLSP-CONNECT نیاز به محافظت داشته باشند، قبل از انتقال در کپسول گذاشته می‌شوند.

۵-۷-۴ NLSP-DATA

در زمان دریافت یک درخواست NLSP-DATA:
الف- اگر محافظت مبتنی بر SDT PDU انتخاب‌شده باشد، هستار NLSP، پارامترهای خدمت مناسب را در کپسول می‌گذارد، یک SDT PDU تشکیل و آن را به‌عنوان داده‌ی کاربر UN از یک درخواست UN-DATA انتقال می‌دهد.
ب- اگر محافظت مبتنی بر No_Header انتخاب شده باشد، NLSP-Userdata رمزگذاری و به‌عنوان UN-Userdata از یک درخواست UN-DATA انتقال داده می‌شود.
در زمان دریافت از یک نشان UN-DATA:
الف- اگر SDT PDU مبتنی بر محافظت انتخاب‌شده باشد، هستار NLSP، PDU را وارسی می‌کند و NLSP Userdata و احتمالاً یک درخواست تأیید NLSP را با استفاده از کارکرد واکپسوله‌سازی استخراج می‌کند.
ب- اگر محافظت مبتنی بر No_Header انتخاب‌شده باشد، NLSP-Userdata برای به‌دست آوردن NLSP داده‌ی کاربر رمزگشایی می‌شود.
پ- پارامترهای خدمت NLSP در نشان NLSP-DATA به کاربر NLSP فرستاده می‌شود.

۵-۷-۵ NLSP-EXPEDITED-DATA

این داده‌ها نیز به شیوه‌ای مشابه با درخواست NLSP-DATA پردازش می‌شوند.

یادآوری– در زمان استفاده از SDT PDU، کارکرد کپسوله‌سازی می‌تواند اندازه‌ی داده را بسط دهد. در نتیجه، اندازه‌ی محدود فیلد داده‌ی کاربر ممکن است نیاز داشته باشد که که داده پیشتاز محافظت‌شده در هنگام عبور از شبکه اصلی بیشتر قطعه‌بندی و هم‌گذاری شود.

۵-۷-۶ NLSP-RESET

NLSP-RESET به‌طور مستقیم توسط NLSP به شبکه‌ی اصلی فرستاده می‌شود. اتصال امن دوباره احراز هویت می‌شود و صفات مختص سازوکار با استفاده از CSC-PDUهای حمل شده در UN-DATA دوباره برقرار می‌شوند.

یادآوری– به دلیل اینکه داده ممکن است از دست برود، امکان دارد مقداردهی اولیه برخی از سازوکارهای امنیتی ضروری باشد. به‌ویژه، سازوکارهای دنباله‌گذاری یکپارچگی باید بتوانند از حملات بازپخش[1]، حتی پس از از دست دادن داده، جلوگیری کنند.

۵-۷-۷ NLSP_DATA_ACKNOWLEDGE

اگر قرار باشد که تمام پارامترهای خدمت NLSP محافظت شوند (یعنی Param_Prot برابر TRUE است)، عمل کپسوله‌سازی انجام شده، در یک SDT PDU قرار داده می‌شود و به‌وسیله‌ی NLSP به زیرلایه UN ارسال می‌شود. در غیر این‌صورت، این نخستینه‌ی خدمت به‌طور مستقیم به UN-DATA-ACKNOWLEDGE نگاشت می‌شود.

۵-۷-۸ NLSP_DISCONNECT

در هنگام دریافت یک درخواست NLSP-DISCONNECT، اگر محافظت از پارامترهای خدمت به‌وسیله‌ی حالت انتخاب‌شده‌ی محافظت (به زیربند ۵-۵-۱ مراجعه شود) مورد نیاز باشد، هستار NLSP یک PDU انتقال داده‌ی امن (که شامل درخواست NLSP-DISCONNECT، NLSP-Userdata و سایر پارامترهای اختیاری دیگر است) را ایجاد می‌کند. این PDU یا در داخل UN-DATA قبل از آزادسازی ارتباط UN حمل می‌شود، یا چنانچه امکان‌پذیر باشد، SDT PDU می‌تواند در یک پارامتر UN-Userdata از یک UN-DISCONNECT حمل شود.

اگر محافظت از پارامترهای درخواست NLSP-DISCONNECT مورد نیاز نباشد، این پارامترها در یک درخواست UN-DISCONNECT فرستاده می‌شوند.

۵-۷-۹ کارکردهاي ديگر

همچنین NLSP از کارکردهای زیر که در اتمام مهلت زمانی یا رویدادهای خارجی دیگر راه‌اندازی می‌شوند، پشتیبانی می‌کند:

الف- تبادل CSC-PDU برای تغییر صفات SA پویا مانند کلیدها.

ب- تبادل آزمون امنیتی برای وارسی اینکه جنبه‌های رمزنگاشتی SA به‌درستی تنظیم شده باشند.

پ- انتقال SDT PDUها که تنها شامل یک فیلد لت‌گذاری ترافیک[2] برای محرمانگی جریان ترافیک می‌شود.

1 - Replay
2 - Traffic padding

۶ کارکردهاي پروتکلی مشترک NLSP-CL و NLSP-CO

۶-۱ معرفی

این بند کارکردهای پروتکلی را توصیف می‌کند که بین مد اتصال و بی‌اتصال NLSP مشترک هستند. این‌ها به‌گونه‌ای که در بندهای ۷ و ۸ بیان می‌شوند، استفاده می‌شوند.

۶-۲ صفات SA مشترک

صفات SA زیر، مد اتصال و مد بی‌اتصال NLSP را کنترل می‌کنند. توصیف آن‌ها شامل یادمان‌هایی[1] می‌شود که برای ارجاع به این صفات در استاندارد حاضر استفاده شده‌اند.

یادآوری– جایی که یک صفت SA «به‌وسیله‌ی ASSR محدود می‌شود»، این محدودیت می‌تواند یک مقدار منفرد یا یک مجموعه از مقادیر را تعریف کند. جایی که ASSR محدوده‌ای از مقادیر را تعریف می‌کند، مقدار صفت می‌تواند به‌وسیله‌ی مدیریت سامانه‌های OSI، یک مبادله‌ی SA-P یا توسط روش‌هایی که خارج از حیطه‌ی این استاندارد است، تعریف شود.

الف- شناسایی SA:

My_SA-ID: عدد صحیح در محدوده‌ی
۰ تا ۱- (حداکثرطول**۲۵۶)
شناسه‌ی محلی SA. مقدار این صفت، باید در زمان برقراری SA تنظیم شود.

Your_SA-ID: عدد صحیح در محدوده‌ی
۰ تا ۱- (حداکثرطول**۲۵۶)
شناسه‌ی راه دور SA. مقدار این صفت باید در زمان برقراری SA تنظیم شود. حداکثر طول یک عدد صحیح در محدوده‌ی ۲ تا ۱۲۶ است.

یادآوری ۱– داشتن بیش از یک SA که شناسه‌ی محلی یکسانی دارند، خطای جدی به حساب می‌آید.

ب- نشان‌گر اینکه آیا NLSPE راه‌اندازی شده است یا به برقراری SA پاسخ داده است:

راه‌انداز: بولی[2]
این صفت نشان می‌دهد که چگونه پرچم راه‌انداز به پاسخ‌دهنده باید تنظیم شود تا PDUهای بازتابیده شناسایی شوند.
مقدار این صفت، باید در زمان برقراری SA تنظیم شود.

پ- نشانی UN هستار NLSP همتا:

Peer_Adr: رشته هشت‌تایی به شکلی که در توصیه‌نامه‌ی ISO/IEC 8348 | CCITT X.213 تعریف شده است.
مقدار این صفت، باید در زمان برقراری SA تنظیم شود.

ت- نشانی NLSP هستارهای تأمین‌شده از طریق همتای راه دور:

1- Mnemonics
2 - Boolean

Adr_Served: رشته‌های هشت‌تایی به شکلی که در توصیه‌نامه‌ی ISO/IEC 8348 | CCITT X.213 تعریف شده است.

مقدار این صفت، باید در زمان برقراری یا قبل از برقراری SA تنظیم شود.

ث- خدمات امنیتی انتخاب شده برای SA:

AC: عدد صحیح در محدوده‌ای که توسط ASSR محدود می‌شود.

TF-Conf عدد صحیح در محدوده‌ای که توسط ASSR محدود می‌شود.

ج- محافظت پارامتر:

Param_Prot بولی

از تمام پارامترهای خدمت NLSP به غیر از آن‌هایی که ممکن است توسط شبکه‌ی اصلی تغییر پیدا کنند (یعنی QOS، انتخاب تأیید دریافت و انتخاب داده پیشتاز)، محافظت می‌کند.

چ- صفات سازوکار برچسب:

عنوان: بولی

برچسب‌گذاری صریح PDUهای اتصال/بی‌اتصال.

Label_Set: مجموعه‌ای از

{Label_Ref: عدد صحیح

Label_Auth: شناسه‌ی شئ

Label_Content: برای شکل‌دهی که به‌وسیله‌ی Lanel_Auth تعریف شده است.}

مقدار این صفات باید در زمان برقراری یا قبل از برقراری SA تنظیم شوند.

یادآوری ۲– انتظار می‌رود که این برچسب‌ها براساس رویه‌های تعریف‌شده توسط ISO/IEC و ITU-T ثبت شوند.

۶-۳ کارکردهاي معمول در زمان درخواست برای یک نمونه از ارتباط

۶-۳-۱ وارسی‌های اولیه

یک NLSPE که درخواستی را برای یک نمونه ارتباطی دریافت می‌کند، (یعنی یک درخواست NLSP-CONNECT یا UNITDATA) باید وارسی کند که:

الف- فراخوانی NLSP یا نشانی منبع، یک نشانی NLSP است که توسط این NLSPE خدمت‌رسانی می‌شود.

ب- خدمات امنیتی مورد نیازی که می‌تواند توسط این NLSPE فراهم شوند.

۶-۳-۲ شناسایی همبستگي امنیتی

یک NLSPE که درخواستی را برای یک نمونه‌ی ارتباطی دریافت می‌کند (مانند یک درخواست NLSP-CONNECT یا UNITDATA)، درمیان SAهای در دسترس خود، SAای که صفات آن مطابق شرایط زیر است را شناسایی می‌کند:

الف- هر یک از الزامات خدمت امنیتی مشتق‌شده به‌صورت محلی با خدمات امنیتی انتخاب‌شده برای SA منطبق باشد؛

ب- NLSP فراخوانی‌شده یا نشانی مقصد در مجموعه‌ی نشانی‌های NLSP در Adr_Served قرار داشته باشد؛

پ- هیچ اتصال NLDPای در حال استفاده از این SA نباشد. (تنها در مورد NLSP-CO)

اگر بیش از یک SA در این شرایط صدق کند، رویه‌ای که باید طی شود، یک مسأله محلی است. اگر این‌چنین SA وجود نداشته باشد و اگر از برقراری درون باند SA پشتیبانی شود، گزینه SA (پروتکل SA) مجاز است انتخاب شود. (مطابق تعریف بند ۷ و ۸) در غیر این‌صورت، رویه‌های برقرارشده برون باند می‌توانند پیگیری شوند. اگر هیچ یک از این رویه‌ها در یک مهلت زمانی تعریف شده‌ی محلی، به‌صورت موفقیت‌آمیز کامل نشوند، رویه‌های بازیابی خطای مناسب با حالت ارتباطات (که در زیربندهای ۷-۴ و ۸-۴ تعریف شده‌اند)، اجرا خواهند شد.

۶-۴ کارکردهاي پروتکل انتقال داده‌ي امن

۶-۴-۱ تولید کردن

۶-۴-۱-۱ SDT مبتنی بر PDU

موارد زیر باید همان‌گونه‌که در بندهای ۷ و ۸ به‌کار رفته‌اند، انجام شوند:

الف- بیت ۸ فیلد نوع داده باید به مقدار راه‌انداز صفت SA تنظیم شود.

ب- اگر این رویه‌ها از زیربند ۸-۶ فراخونی شوند (NLSP-DATA)، بیت ۷ فیلد نوع داده باید براساس این رویه‌ها تنظیم شود، در غیر این‌صورت در این بیت، مقدار «آخر» قرار می‌گیرد.

پ- در بیت‌های ۱ تا ۶ فیلد نوع داده باید مقداری که در زیربند ۱۳-۳-۴-۲ تعریف شده است و مناسب با رویه‌های بندهای ۷ و ۸ است، قرار گیرد.

ت- داده‌های مربوط به پارامترهای خدمت NLSP یا دیگر تبادلات پروتکل (برای مثال داده‌های آزمایشی)، آن‌گونه‌که مطابق با رویه‌های بندهای ۷ و ۸ نیاز است، در فیلدهای محتوای مناسب قرار داده می‌شوند. (زیربند ۱۳-۳-۴-۳ ملاحظه شود.)

ث- اگر (برچسب TRUE باشد)، و در مورد NLSP-CO، این اولین SDT PDUای باشد که روی اتصال جاری ارسال شده، آنگاه باید یکی از موارد زیر انجام شود:

۱- یک برچسب امنیتی، همراه با صادر کننده‌ی تعریف، باید در فیلد محتوای برچسب قرار گیرد و در PDU گنجانده شود؛

ب- یک مرجع برچسب امنیتی باید در فیلد محتوای مرجع برچسب قرار گیرد و در PDU گنجانده شود. برچسب انتخاب‌شده باید یکی از مقادیر Label-Set موجود در صفات SA باشد.

یادآوری ۱– SA-ID در NLSP-CO وجود نـدارد. در حالت NLSP CO، در صـورتی که Protect_Content_Params باشد، فقط SDT PDU حامل پارامترهای NLSP CONNECT برچسب‌گذاری خواهد شد، و در غیر این‌صورت اولین SDT PDU ارسال شده در هر جهتی در طی مرحله‌ی انتقال داده‌ی NLSP، برچسب‌گذاری خواهد شد.

ج- یک کارکرد کپسوله‌سازی (برای مثال، همانی که در بند ۱۱ توصیف شده است) باید با آرگومان[1]های زیر فراخوانی شود:

۱- SA-ID باید به My-SA-ID تنظیم شود؛

۲- unit-data-type باید به یکی از موارد زیر تنظیم شود:

- «پیشتاز»، اگر داده‌ای که قرار است محافظت شود شکلی از یک نخستینه‌ی NLSP-EXPEDITED-DATA باشد؛
- «عادی»، در غیر این‌صورت؛

۳- رشته‌ی هشت‌تایی قبل از کپسوله‌شدن (Octet-String-Before-Encapsulation) باید به فیلدهای PDU ساخته‌شده تنظیم شود.

چ- کارکرد کپسوله‌سازی باید یا یک خطا یا یک رشته هشت‌تایی encapsulated-octet-string را برگرداند. به‌محض تکمیل موفق یک کارکرد کپسوله‌سازی، سرآیند محافظت‌نشده‌ی SDT PDU باید همان‌طورکه در زیربند ۱۳-۳-۲ تعریف شده است با encapsulated-octet-string (رشته‌ی هشت‌تایی کپسوله‌شده‌ی متصل به سرآیند) ایجاد شود.

یادآوری۲- SA-ID در NLSP-CO وجود ندارد.

۶-۴-۱-۲ بدون حضور سرآیند (فقط NLSP-CO)

موارد زیر باید همان‌گونه‌که در بند ۸ به‌کار رفته‌اند، انجام شوند:

الف- یک کارکرد کپسوله‌سازی که اندازه‌ی داده را تغییر نمی‌دهد، (برای مثال، همانی که در بند ۱۲ توصیف شده است) باید با آرگومان‌های زیر فراخوانی شود.

۱- SA-ID باید برابر با My-SA-ID تنظیم شود؛

۳- unit-data-type باید به یکی از موارد زیر تنظیم شود:

1 - Argument

- «پیشتاز»، اگر داده‌ای که قرار است محافظت شود شکلی از یک **NLSP-EXPEDITED-DATA** باشد؛
- «عادی»، در غیر این‌صورت؛

۳- رشته‌ی هشت‌تایی قبل از کپسوله‌شدن (Octet-String-Before-Encapsulation) باید برابر با پارامتر NLSP-Userdata تنظیم شود.

ب- کارکرد کپسوله‌سازی باید یک خطا یا یک encapsulated-octet-string را برگرداند.

۶-۴-۲ وارسی

۶-۴-۲-۱ SDT مبتنی بر PDU

موارد زیر باید آن‌گونه‌که در بندهای ۷ و ۸ به‌کار رفته‌اند، انجام شود:

الف- سرآیند محافظت‌نشده‌ی PDU دور انداخته می‌شود.

ب- یک کارکرد واکپسوله‌سازی (برای مثال، همانی که در بند ۱۱ توصیف شده است) باید با آرگومان‌های زیر فراخوانی شود.

۱- SA-ID باید برابر با My-SA-ID تنظیم شود؛

۲- unit-data-type باید به یکی از موارد زیر تنظیم شود:

- «پیشتاز»، اگر داده‌ای که قرار است واکپسوله شود، شکلی از یک UN-EXPEDITED-DATA باشد؛
- «عادی»، در غیر این‌صورت؛

۳- encapsulated-octet-string باید به باقیمانده‌ی PDU تنظیم شود.

پ- کارکرد واکپسوله‌سازی باید یک خطا یا یک رشته‌ی هشت‌تایی قبل از کپسوله‌شدن (Octet-String-Before-Encapsulation) را برگرداند. به‌محض تکمیل موفق یک کارکرد واکپسوله‌سازی، پردازش بعدی باید انجام شود.

ت- فیلد نوع داده، بیت ۸ پرچم (راه‌انداز یا پاسخ‌دهنده) باید وارسی شود تا برابر با مقدار راه‌انداز صفت SA نباشد.

ث- بیت ۱ تا ۶ و بیت ۷ فیلد نوع داده وارسی خواهد شد تا مقدار مناسبی برای رویه‌های مفروض بندهای ۷ و ۸ داشته باشد.

ج- اگر (برچسب برابر TRUE باشد)، و در حالت NLSP-CO، این اولین SDT PDU دریافتی روی اتصال جاری باشد، PDU باید وارسی شود تا این اطمینان حاصل شود که یک و تنها یک برچسب یا فیلد محتوای مرجع برچسب موجود است. اگر موجود باشد، مقدار برچسب باید وارسی شود تا این اطمینان حاصل شود که در مجموعه‌ی Label-Set قرار دارد.

چ- فیلدهای محتوای مربوط به پارامترهای خدمت NLSP یا دیگر کارکردهای پروتکل باید وارسی شوند که موجود باشند. (مطابق با رویه‌های بندهای ۷ و ۸ نیاز است.) داده از این فیلدها بازیابی می‌شود و مطابق با رویه‌های بندهای ۷ و ۸ با آن‌ها رفتار می‌شود.

۶-۴-۲-۲ بدون حضور سرآیند (تنها NLSP-CO)

موارد زیر باید همان‌طورکه در بند ۸ به‌کار رفته‌اند، انجام شوند:

الف- کارکرد واکپسوله‌سازی تعریف‌شده برای استفاده‌ی این SA (برای مثال، همانی که در بند ۱۲ توصیف شده است) باید با آرگومان‌های زیر فراخوانی شود.

۱- SA-ID باید برابر با My-SA-ID تنظیم شود؛

۲- unit-data-type باید با مقادیر زیر تنظیم شود:

- «پیشتاز»، اگر داده‌ای که قرار است واکپسوله شود از یک نخستینه **UN-EXPEDITED-DATA** باشد؛
- «عادی»، در غیر این‌صورت؛

۳- رشته هشت‌تایی کپسوله شده (encapsulated-octet-string) باید برابر با پارامتر UN-Userdata تنظیم شود.

ب- کارکرد واکپسوله‌سازی باید یک خطا یا یک رشته‌ی هشت‌تایی قبل از کپسوله‌شدن (Octet-String-Before-Encapsulation) را برگرداند.

۶-۵ استفاده از پروتکل همبستگي امنیتی

زمانی که دو NLSPE، یک SA برقرار شده نداشته باشند، آن‌ها می‌توانند با استفاده از یک پروتکل همبستگی امنیتی (SA-P) یا برخی روش‌های دیگر، یک SA برقرار کنند. یک SA-P، مبادله‌ی SA PDUها یا SDT PDU با نوع داده‌ی محتوا که برابر SA-P تنظیم شده است را بین NLSPEها انجام می‌دهد تا یک SA را برقرار سازد، تغییر، یا پایان دهد.

بندهای ۷ و ۸ NLSP نشان می‌دهند که چگونه SA-P می‌تواند بدون رویه‌های SA به‌کار گرفته شود. رویه‌های SA-P و PCI که در SA PDU/SDT PDU قرار دارد، به سازوکارهای مشخصی که برای فراهم کردن SAP (یک سازوکار پروتکل مناسب در پیوست پ تعریف شده است) استفاده می‌شوند، بستگی دارند.

هر SA-P باید ویژگی‌های زیر را فراهم کند:

الف- اشتقاق[1] از تمام صفات مورد نیاز برای حالت انتخاب‌شده‌ی محافظت؛

ب- کلیدهایی که از یک منبع معتبر می‌آیند؛

پ- در صورت نیاز، برقراری اطلاعات اولیه برای احراز هویت و یکپارچگی.

اگر SA-P مشخصی پشتیبانی نشود، یک NLSPE باید SA PDUها را دور بریزد.

1 - Derivation

یک SA-P می‌تواند هم مبتنی بر الگوریتم‌های متقارن و هم مبتنی بر الگوریتم‌های نامتقارن باشد. توصیه می‌شود که یک الگوریتم نامتقارن استفاده شود. پیوست پ شامل مثالی از چنین سازوکاری است.

۷ کارکردهاي پروتکلی برای NLSP-CL

۷-۱ خدمات فراهم شده توسط NLSP-CL

به خدمات فراهم شده توسط NLSP با پیشوند «NLSP» اشاره خواهد شد. نخستینه‌ها به‌صورت زیر هستند:

نخستینه‌ها	پارامترها
درخواست[1] NLSP-UNITDATA	نشانی مقصد NLSP (NLSP Destination Address)
نشانه[2] NLSP-UNITDATA	نشانی منبع NLSP (NLSP Source Address)
	کیفیت خدمات NLSP (NLSP Quality of Service)
	داده‌ی کاربر NLSP (NLSP Userdata)

نخستینه‌ها و پارامترهای خدمت به‌طور مستقیم معادل آن‌هایی هستند که در توصیه‌نامه‌ی CCITT X.213 | ISO/IEC 8348 تعریف شده است.

۷-۲ خدمات مفروض

خدمات مفروض به‌وسیله‌ی NLSP در قلمرو پایین‌تر آن با پیشوند «UN» می‌آیند. (برای «شبکه‌ی اصلی») نخستینه‌ها به‌صورت زیر هستند:

نخستینه	پارامترها
درخواست UN-UNITDATA	نشانی فراخوانی‌شده UN (UN Called Address)
نشانه UN-UNITDATA	نشانی فراخواننده UN (UN Calling Address)
	کیفیت خدمت UN (UN Quality of Service)
	داده‌ی کاربر UN (UN Userdata)

نخستینه‌ها و پارامترهای خدمت مفروض معادل آن‌هایی هستند که در CLNS (توصیه‌نامه‌ی X.213 CCITT | ISO 8348/AD1 ملاحظه شود) تعریف شده‌اند.

۷-۳ صفات همبستگی امنیتی

صفات زیر عملیات NLSP-CL را کنترل می‌کنند. توصیف آن‌ها شامل یادمان‌های استفاده شده برای استفاده از این صفات در این استاندارد است:

یادآوری- جایی که یک صفت SA «توسط ASSR محدود شده» است، این محدودیت می‌تواند یک مقدار منفرد یا یک مجموعه از مقادیر را تعریف کند. جایی که ASSR یک محدوده از مقادیر را تعریف می‌کند، مقدار صفت می‌تواند به‌وسیله‌ی مدیریت سامانه OSI، یک تبادل SA-P یا با ابزارهای دیگر در خارج از حیطه‌ی این استاندارد برقرار شود.

1 - Request
2 - Indication

- خدمات امنیتی انتخاب‌شده برای SA:

DOAuth: عدد صحیح در محدوده‌ای که توسط سطح احراز هویت مبدأ داده‌ی ASSR محدود می‌شود.
مقدار این صفت باید از قبل تعیین شود یا در زمان برقراری SA تنظیم شود.

CLConf: عدد صحیح در محدوده‌ای که توسط سطح محرمانگی بی‌اتصال ASSR محدود می‌شود.
مقدار این صفت باید از پیش برقرار شده باشد یا در زمان برقراری SA تنظیم شود.

CLInt: عدد صحیح در محدوده‌ای که توسط سطح یکپارچگی بی‌اتصال ASSR محدود می‌شود.
مقدار این صفت باید از پیش برقرار شده باشد یا در زمان برقراری SA تنظیم شود.

۷-۴ وارسی‌ها

در بسیاری از نقاط در توضیحات زیر، هستار NLSP-CL وارسی می‌کند که برخی از شرایط برقرار باشد. در غیر این‌صورت (زمانی که چنین وارسی به شکست بیانجامد)، هستار NLSP-CL باید داده‌ای را که در حال پردازش است دور بریزد. هم‌چنین، هستار می‌تواند به‌صورت اختیاری یک گزارش ممیزی را ثبت کند. اینکه چه شکست‌هایی ثبت شوند یک مسأله محلی به‌حساب می‌آید.

۷-۵ برقراری SA درون باند

یک SA می‌تواند با استفاده از پروتکل همبستگی امنیتی (SA-P) در درون باند برقرار شود. PA-P در پیوست پ از این مشخصات تعریف شده است.

یادآوری– در حال حاضر، SA-P شامل هیچ رویه بازیابی نمی‌شود و در نتیجه، هنگام استفاده از این پروتکل به‌همراه NLSP-CL، باید مراقب بود که اطمینان‌پذیری[1] مورد نیاز فراهم شود.

۷-۶ پردازش درخواست NLSP-UNITDATA

۷-۶-۱ وارسی‌های اولیه و شناسایی SA

در زمان دریافت یک درخواست NLSP-UNITDATA، NLSPE وارسی می‌کند که ارتباطات محافظت‌نشده بر پایه‌ی نیازی‌های خدمات امنیتی محلی و زوج نشانی مبدا/مقصد، مجاز باشند. اگر ارتباطات محافظت‌نشده مجاز باشند، پارامترهای خدمت NLSP به‌طور مستقیم به پارامترهای خدمت UN معادل در یک درخواست UN-UNITDATA رونوشت (کپی) می‌شوند و هیچ عمل دیگری به‌وسیله‌ی NLSPE انجام نمی‌شود.
اگر ارتباطات محافظت‌شده مورد نیاز باشند، وارسی‌های اولیه و شناسایی‌های رویه SA همان‌طورکه در زیربند ۶-۳ توصیف شده است، باید تکمیل شود. در ادامه رویه‌های زیر می‌آیند:

1- Reliability

۷-۶-۲ محافظت از NLPS-UNITDATA

همان‌طورکه در زیربند ۶-۴-۱-۱ تعریف شده است، NLSPE باید «تولید کارکردهای SDT PDU» را با نوع داده «NLSP-UNITDATA req/in» که شامل موارد زیر است، انجام دهد:

الف- اگر Param_Prot برابر TRUE است، نشانی NLSP مبدأ؛

ب- اگر Param_Prot برابر TRUE است، نشانی NLSP مقصد؛

پ- پارامتر NLSP-Userdata.

پرچم Last/Not Last باید به Last تنظیم شود. (یعنی بیت ۷ از فیلد نوع داده=۰)

۷-۶-۳ درخواست شبکه

انتقال داده‌ی امن PDU باید به‌عنوان پارامتر UN-Userdata از یک درخواست UN-UNITDATA به پروتکل پایین‌تر بعدی گذر کند.

اگر Param_Prot برابر TRUE باشد، نشانی مبدأ UN باید UN-Address هستار NLSP محلی باشد، در غیر این‌صورت، نشانی مبدأ NLSP باید به نشانی مبدأ UN رونوشت شود.

اگر Param_Prot برابر TRUE باشد، نشانی مقصد UN باید Peer_Adr باشد، در غیر این‌صورت، نشانی مقصد NLSP باید به نشانی مقصد UN رونوشت شود.

کیفیت خدمت UN باید به‌وسیله‌ی خط‌مشی محلی مشخص شود، اما مجاز است که از NLSP QOS رونوشت شود.

یادآوری– اگر پارامترهای ثبت مسیر و مسیر مبدأ در پارامترهای NLSP QOS باشند و به‌عنوان پارامترهای UN QOS عبور داده نشوند، QOS مشخص شده می‌تواند برای قسمتی از مسیر بین هستارهای منبع و مقصد NLSP-CL فراهم نشود.

۷-۷ پردازش نشان UN-UNITDATA

۷-۷-۱ وارسی‌ها و پردازش اولیه

اگر هیچ SDT PDU وجود نداشته باشد، NLSP بر پایه‌ی الزامات خدمات امنیتی محلی و زوج نشانی منبع/مقصد، وارسی می‌کند که ارتباطات محافظت‌نشده مجاز باشند. اگر ارتباطات محافظت‌نشده مجاز باشند، پارامترهای خدمت UN به‌طور مستقیم به پارامترهای خدمت NLSP معادل آن در یک درخواست NLSP UNITDATA رونویسی می‌شوند و هیچ عمل اضافی به‌وسیله‌ی NLSPE انجام نمی‌شود. اگر ارتباطات محافظت‌نشده، مجاز نباشند، رویه‌های توصیف شده در زیربند ۷-۴ انجام می‌گیرند. هیچ عمل اضافی دیگری به‌وسیله‌ی NLSPE انجام نمی‌شود.

اگر یک SDT PDU حضور داشته باشد، NLSP باید در میان SAهای در دسترس خود، یک SA با My_SA_ID برابر با فیلد SA_ID را در SDT-PDU دریافتی شناسایی کند. تمامی عملیات دیگر به این SA شناسایی شده ارجاع می‌کنند.

هستار NLSP باید پردازش‌های عمومی را که در زیربند ۶-۴-۲-۱ تعریف شده‌اند انجام دهد. علاوه‌براین، وارسی‌های زیر نیز باید انجام گیرند:

الف- اگر فیلد نوع داده برابر با «به هیچ یک از نخستینه‌های خدمت NLSP مرتبط نیست» باشد، SDT PDU نباید بیش از این تحت این رویه‌ها پردازش شود. در غیر این‌صورت، فیلد نوع داده باید وارسی شود که NLSP-UNITDATA باشد.

یادآوری ۱- مقدار «آخرین پرچم/غیرآخرین پرچم» (یعنی بیت ۷ از فیلد نوع داده) می‌تواند چشم‌پوشی شود.

یادآوری۲- پشتیبانی از لت‌گذاری ترافیک یا تبادلات آزمون در مد بی‌اتصال خارج از حیطه‌ی NLSP است.

ب- اگر Param_Prot برابر TRUE باشد، SDT PDU باید برای اطمینان از این‌که فیلدهای زیر حاضر باشند، وارسی شود:

۱- نشانی مقصد؛

۲- نشانی مبدأ.

یک نشان NLSP UNITDATA باید با پارامترهای تنظیم‌شده و نشانی‌های وارسی‌شده مطابق آن‌چه در زیربند ۷-۷-۲ تعریف شده، به NLSP User تحویل داده شود.

۷-۷-۲ پارامترهای نشان NLSP-CL

۷-۷-۲-۱ پارامترهای نشانی

اگر Param_Prot برابر با TRUE باشد، NLSPE باید پارامترهای خدمت NLSP را به مقادیری که در SDT PDU قرار دارند، تنظیم کند.

اگر Param_Prot برابر با FALSE باشد، مقادیر باید مطابق زیر، از پارامترهای نشان UN گرفته شوند:

الف- نشانی مبدأ NLSP = نشانی منبع UN؛ و

ب- نشانی مقصد NLSP = نشانی مقصد UN.

نشانی مقصد NLSP، که مطابق بالا تنظیم شده است، باید وارسی شود تا نشانی NLSPای باشد که توسط این هستار NLSP به‌کار می‌رود. (همان‌گونه‌که توسط خط‌مشی امنیتی محلی تعیین شده است.)

نشانی مبدأ NLSP، که مطابق بالا تنظیم شده است، باید وارسی شود تا نشانی NLSPای باشد که در صفت Adr_Served SA قرار دارد.

۷-۷-۲-۲ QOS

پارامترهای QOS از خدمت UN به خدمت NLSP رونوشت می‌شوند.

۷-۷-۲-۳ داده‌ی کاربر

داده‌ی موجود در فیلد داده‌ی کاربر از Octet-String-Before-Encapsulation مربوط به SDT PDU باید به کاربر NLSP در پارامتر NLSP-Userdata از نشان NLPS-UNITDATA داده شود.

۸ کارکردهای پروتکل برای NLSP-CO

۸-۱ خدمات فراهم شده به‌وسیله‌ي NLSP-CO

نخستینه‌های خدمات فراهم‌شده به‌وسیله‌ی NLSP-CO به‌صورت زیر هستند:

نخستینه‌ها		پارامترها
NLSP-CONNECT	درخواست	نشانی فراخوانی‌شده‌ی NLSP
	نشانه	نشانی فراخواننده‌ی NLSP
		انتخاب تأیید دریافت NLSP
		انتخاب داده‌ی پیشتازی NLSP
		مجموعه پارامترهای NLSP QOS
		داده‌ی کاربر NLSP
NLSP-CONNECT	پاسخ	نشانی پاسخ NLSP
	تأیید	انتخاب تأیید دریافت NLSP
		انتخاب داده‌ی پیشتاز NLSP
		مجموعه پارامتر NLSP QOS
		داده‌ی کاربر NLSP
NLASP-DATA	درخواست	داده‌ی کاربر NLSP
	نشانه	درخواست تأیید NLSP
NLSP-DATA-ACKNOWLEDGE	درخواست	
	نشانه	
NLSP-EXPEDITED DATA	درخواست	داده‌ی کاربر NLSP
	نشانه	
NLSP-RESET	درخواست	دلیل NLSP
NLSP-RESET	نشانه	آغازگر NLSP
		دلیل NLSP
NLSP-RESET	پاسخ	
	تأیید	
NLSP-DICONNECT	درخواست	آغازگر NLSP
	نشانه	دلیل NLSP
		داده‌ی کاربر NLSP
		نشانی پاسخ NLSP

یادآوری- آغازگر، کاری به درخواست ندارد.

نخستینه‌ها و پارامترهای خدمت به‌طور مستقیم معادل با آن‌هایی هستند که در توصیه‌نامه‌ی X.213 CCITT | ISO 8348 تعریف شده‌اند.

۸-۲ خدمات مفروض

به خدمات مفروض به‌وسیله‌ی NLSP در قلمرو پایین‌تر آن با پیشوند «UN» («شبکه‌ی اصلی») ارجاع خواهد شد. این یک واسط ادراکی است. (به زیربند ۵-۱ مراجعه شود.)

واسط UN در دو قسمت مدل‌سازی شده است:

الف- تعریفی از نخستینه‌ها و پارامترهای خدمات UN (توضیحات زیر ملاحظه شود)؛

ب- نگاشتی از خدمت UN (به زیربند ۵-۱مراجعه شود) چه به یک خدمت شبکه استاندارد و چه به‌طور مستقیم به توصیه‌نامه‌ی ISO/IEC 8208/CCITT X.25.

پیوست‌های الف و ب نگاشتی از واسط خدمت ادراکی به خدمت شبکه و به ISO/IEC 8208 یا ITU X.25 را تعریف می‌کنند.

نخستینه‌های UN فرض شده برای NLSP-CO به‌صورت زیر است:

نخستینه‌ها		پارامترها
UN-CONNECT	درخواست	نشانی فراخوانی شده‌ی UN
	نشانه	نشانی فراخواننده‌ی UN
		انتخاب تأیید دریافت UN
		انتخاب داده‌ی پیشتازی UN
		مجموعه پارامترهای UN QOS
		داده‌ی کاربر UN
		احراز هویت UN
UN-CONNECT	پاسخ	نشانی پاسخ دهنده‌ی UN
	تأیید	انتخاب تأیید دریافت UN
		انتخاب داده‌ی پیشتازی UN
		مجموعه پارامتر UN QOS
		داده‌ی کاربر UN
		احراز هویت UN
NLASP-DATA	درخواست	داده‌ی کاربر UN
	نشانه	درخواست تأیید UN
UN-DATA-	درخواست	

ACKNOWLEDGE	نشانه	
UN-EXPEDITED-DATA	درخواست نشانه	داده‌ی کاربر UN
UN-RESET	درخواست	دلیل UN
UN-RESET	نشانه	آغازگر UN دلیل UN
UN-RESET	پاسخ تأیید	
UN-DISCONNECT Request	درخواست	دلیل UN داده‌ی کاربر UN نشانی پاسخ‌دهنده‌ی UN
UN-DISCONNECT	نشانه	آغازگر UN دلیل UN داده‌ی کاربر UN نشانی پاسخ دهنده‌ی UN

پیوست‌های الف و ب نگاشتی از احراز هویت UN به توصیه‌نامه‌ی CCITT X.213 | ISO/IEC 8348 و ISO/IEC 8208 یا X.25 را تعریف می‌کنند.

یادآوری– زمانی که NLSP در یک ارتباط محکم با توصیه‌نامه‌ی CCIT X.25 | ISO/IEC 8208 استفاده می‌شود، ممکن است بتواند از کدبندی‌های جایگزینی که مزایای کاملی را از پروتکل اصلی بهره می‌برند، استفاده کند؛ در حالی که نگاشت به توصیه‌نامه‌ی ISO/IEC 8348 | CCIT X.213 فقط از یک خدمت شبکه‌ی اصلی استفاده می‌کند.

۸-۳ صفات همبستگی امنیتی

صفات زیر عملیات NLSP-CO را کنترل می‌کنند. توصیف‌های آن‌ها شامل یادمان‌هایی است که برای ارجاع به این صفات در این استاندارد استفاده می‌شوند.

یادآوری ۱– وقتی یک صفت SA «به‌وسیله‌ی ASSR محدود شده» باشد، این محدودیت می‌تواند یک مقدار منفرد یا مجموعه‌ای از مقادیر را تعریف کند. جایی که ASSR محدوده‌ای از مقادیر را تعریف می‌کند، مقدار صفت می‌تواند به‌وسیله‌ی مدیریت سامانه‌های OSI، یک مبادله‌ی SA-P یا از طریق راه‌های دیگری که در حیطه‌ی این مشخصات نیست، برقرار شود.

الف- خدمات امنیتی انتخاب شده برای SA:

PE Auth: عدد صحیح در محدوده‌ای که به‌وسیله‌ی سطح احراز هویت هستار همتای ASSR محدود می‌شود.

CO Conf: عدد صحیح در محدوده‌ای که به‌وسیله‌ی سطح محرمانگی اتصال ASSR محدود می‌شود.

CO Int: عدد صحیح در محدوده‌ای که به‌وسیله‌ی یکپارچگی اتصال بدون بازیابی ASSR محدود می‌شود. مقادیر این صفات باید از قبل برقرار شوند یا زمان برقراری SA راه‌اندازی شوند.

ب- صفات مرتبط با پروتکل CO

Retain_On_Disconnect: بولی

اینکه صفات SA در قطع اتصال حفظ شوند.

مقادیر این صفات باید از قبل برقرار شوند یا زمان برقراری SA راه‌اندازی شوند.

Protect_Connect_Params: بولی

محافظت NLSP-Userdata در NLSP-CONNECT و NLSP-DISCONNECT، همچنین دیگر پارامترهای خدمت در NLSP-CONNECT و NLSP-DISCONNECT اگرکه Param_Prot، TRUE باشد.

مقدار این صفت باید به‌وسیله‌ی ASSR محدود شود.

یادآوری ۲– اگر Protect_Connect_Params برابر FALSE باشد، Param_Prot نمی‌تواند TRUE باشد.

No_Header: بولی

اگر True باشد، محافظت مبتنی بر No_Header برای محافظت داده (برای مثال با استفاده از رویه‌هایی تعریف شده در بند ۱۲) استفاده خواهد شد.

مقدار این صفت باید به‌وسیله‌ی ASSR محدود شود.

۸-۴ وارسی‌ها و دیگر کارکردهاي مشترک

در بسیاری از نکات در توصیفات زیر، بیان شده است که بعضی شرایط برقرار باشند. هرگاه چنین وارسی در طی رویه‌های NLSP-CONNECT یا NLSP-DISCONNECT با شکست مواجه شود (درصورتی‌که طور دیگری تعیین نشده باشد)، درخواست UN-DISCONNECT و نشانNLSP-DISCONNECT باید به‌صورت مناسب انتشار داده شوند. اگر این امر پس از برقراری اتصال اتفاق بیفتد, NLSP باید داده‌ای را که در حال پردازش است دور بریزد و براساس تصمیم محلی یکی از موارد زیر را به‌کار گیرد:

- همان‌طورکه در زیربند ۸-۸-۵ تعریف شده است، رویه‌های UN_RESETای که توسط NLSP راه‌اندازی شده‌اند.
- یک درخواست UN-DISCONNECT و یک نشان NLSP-DISCONNECT.

به‌طور اختیاری، هستار مجاز است که یک گزارش ممیزی را ثبت کند. تصمیم‌گیری درباره این که کدام یک از اطلاعات ممیزی باید ثبت شوند، یک مسئله‌ی محلی است.
به‌طور مشابه، یک دنباله‌ی مورد انتظار از رویدادها در رویه‌هایی که در زیر توصیف شده‌اند، داده می‌شود. اگر از این دنباله پیروی نشود، به روش مشابه وارسی شکست، یک رویداد غیر منتظره تلقی شود.
جایی که در توصیفات زیر به تولید یا وارسی CSC-PDUها یا انتقال داده‌ی امن PDU اشاره می‌شود، باید رویه‌های مختص سازوکار مناسب، برای مثال رویه‌هایی که در بندهای ۹ تا ۱۲ این استاندارد توضیح داده می‌شود، انجام شوند.

۸-۵ کارکردهاي NLSP-Connect

۸-۵-۱ رویه‌های اولیه

۸-۵-۱-۱ وارسی‌های اولیه - درخواست NLSP CONNECT

در زمان دریافت یک فراخوانی NLSP-CONNECT، NLSPE باید وارسی کند که آیا امکان ارتباطات محافظت‌نشده وجود دارد. (مبتنی بر الزامات خدمت امنیتی محلی و زوج نشانی‌های فراخوانی‌شده/فراخواننده) اگر اجازه ارتباط محافظت‌نشده داده شده باشد، پارامترهای خدمات NLSP و UN به‌طور مستقیم در پارامترهای خدمت UN و NLSP معادل رونوشت می‌شوند. (برای تمام نخستینه‌های خدمت UN و NLSP بعدی تا زمانی که یک نشان UN-DISCONNECT دریافت شود.) هیچ اقدام دیگری توسط NLSPE در طول اتصال انجام نمی‌گیرد.

اگر ارتباطات محافظت‌شده مورد نیاز باشند، NLSPE باید رویه‌هایی را برای وارسی‌های اولیه و شناسایی همبستگی امنیتی همان‌طورکه به ترتیب در زیربندهای ۶-۳-۱ و ۶-۳-۲ بیان شد، دنبال کند. این امر توسط رویه‌های معرفی‌شده در زیربندهای ۸-۵-۲، ۸-۵-۳ یا ۸-۵-۴، دنبال می‌شود. رویه‌های مناسب به حالت برقراری اتصال انتخاب‌شده که در زیربند ۸-۵-۱-۲ تعریف شده‌اند، بستگی دارد. سپس زیربندهای مشابه برای نخستینه‌ی خدمت UN-CONNECT و NLSP-CONNECT بعدی برای آن اتصال UN استفاده می‌شود.

۸-۵-۱-۲ حالت برقراری اتصال NLSP

اگر یک SA با مشخصه‌های مورد نیاز در آن لحظه وجود داشته باشد، می‌تواند برای محافظت از اتصال استفاده شود. در غیر این‌صورت، یک SA جدید باید (به شکل درون باند به‌عنوان قسمتی از کارکردهای NLSP-CONNECT یا برون باند در مهلت زمانی مفروض) برقرار شود. اگر هیچ یک از این دو نتواند اجرا شود، یک NLSP-DISCONNECT باید بازگردانده شود.

دو حالت پایه برای برقراری یک اتصال NLSP وجود دارد که همراه با گونه‌هایی برای پشتیبانی از برقراری SA درون باند عبارتند از:
الف- NLSP-CONNECT در UN-CONNECT که درآن تبادلات پروتکل (برای فراهم‌کردن احراز هویت و مبادله‌ی پارامترهای NLSP-CONNECT) در پارامترهای UN-CONNECT حمل می‌شوند؛

ب- NLSP-CONNECT در UN-CONNECT با SA-P که درآن برقراری SA درون باند در UN-DATA اتصال قبلی پیش از برقراری اتصال UN دوم با احراز هویت، حمل می‌شود و پارامترهای NLSP-CONNECT در UN-CONNECT مانند مورد بالا حمل می‌شود؛

پ- NLSP-CONNECT در UN-DATA که در آن یک تبادل احراز هویت که در UN-CONNECT حمل شده است به‌وسیله‌ی تبادل پارامترهای NLSP-CONNECT در UN-DATA دنبال می‌شود؛

ت- NLSP-CONNECT در UN-DATA با SA-P که در آن یک تبادل SA-P که به UN-DATA حمل شده است به‌وسیله‌ی تبادل پارامترهای NLSP-CONNECT در UN-DATA دنبال می‌شود.

انتخاب مناسب‌ترین حالت، یک تصمیم محلی است که با فراخوانی NLSPE مبتنی بر الزامات (یا الزامات مورد انتظار) برای برقراری اتصال NLSP و محیطی که NLSP در آن عمل می‌کند، گرفته می‌شود.

انتخاب یک SA-P به‌وسیله‌ی پرچم SA-P در CSC-PDU نشان داده می‌شود. انتخاب NLSP-CONNECT در UN-CONNECT یا NLSP-CONNECT در UN-DATA برای NLSPE راه دور به‌وسیله‌ی پرچم UNC-UND نشان داده می‌شود. (به جدول ۸-۲ مراجعه شود.)

در دو حالت آخر (NLSP-CONNECT در UN-DATA با/یا بدون SA-P)، پارامترهای NLSP-CONNECT در داخل یک SDT-PDU کدبندی می‌شوند و در نتیجه این حالت‌ها نمی‌توانند در حالت No_Header استفاده شوند.

در دو حالت اول (NLSP-CONNECT در UN-CONNECT با/یا بدون SA-P)، پارامترهای NLSP-CONNECT (اگر No_Header برابر FALSE باشد و Protect_Connect_Prom برابر TRUE باشد) در یک SDT PDU محافظت می‌شوند. هرچند که اگر SDT PDU حاصل بزرگتر از فضای دردسترس UN-CONNECT UN Userdata باشد، این حالت‌ها نمی‌توانند استفاده شوند.

جدول ۸-۱ محدودیت‌های حالات مختلف از برقراری اتصال را که در بالا تعریف شده است نشان می‌دهد. این جدول مشخص می‌کند که کدام رویه‌ها برای فراخوانی راه‌اندازی نمایه‌ی داده‌شده مناسب هستند:

جدول ۸-۱- جدولی که محدودیت‌ها را برای حالت برقراری اتصال NLSP می‌دهد.

رویه‌های تنظیم ارتباطات	حالت	محدودیت‌های طول SDT PDU (یادآوری‌ها ملاحظه شوند)	Protect-Connect-Params	No Header	SAP
۸-۵-۳ در ادامه ۸-۵-۲-۲ تا ۸-۵-۲-۴	NLSP-CONNECT در UN-CONNECT با SA-P		EITHER	TRUE	TRUE
۸-۵-۳ در ادامه ۸-۵-۲-۲ تا ۸-۵-۲-۴	NLSP-CONNECT در UN-CONNECT با SA-P	SDT <= max UN Userdata	TRUE	FALSE	
۸-۵-۳ در ادامه ۸-۵-۲-۲ تا ۸-۵-۲-۴	NLSP-CONNECT در UN-CONNECT با SA-P		FALSE	FALSE	TRUE
۸-۵-۴	NLSP-CONNECT در UN-CONNECT با SA-P		EITHER	FALSE	TRUE

FALSE	TRUE	EITHER		NLSP-CONNECT در UN-CONNECT	۸-۵-۲
FALSE	FALSE	TRUE	SDT <= max UN Userdata	NLSP-CONNECT در UN-CONNECT	۸-۵-۲
FALSE	FALSE	FALSE		NLSP-CONNECT در UN-CONNECT	۸-۵-۲
FALSE	FALSE	EITHER		NLSP-CONNECT در UN-DATA	۸-۵-۴

EITHER تحت پارامتر Protect_Connect_Params استفاده می‌شود تا مشخص کند که می‌تواند TRUE یا FALSE باشد.

یادآوری ۱- SDT به حداکثر طول ممکن SDT PDU اشاره دارد که مجاز است که درطی برقراری اتصال برای محیط نمایه که در آن NLSP عمل می‌کند، تولید شود.

یادآوری ۲- فرض شده است که همان محدودیت‌هایی به طول NLSP-Userdata اعمال می‌شود که به UN-Userdata اعمال می‌شود.

یادآوری ۳- برای نگاشت UN به توصیه‌نامه‌ی CCITT X.213 | ISO 8348 «max UN Userdata» برابر حداکثر داده‌ی کاربر است که می‌تواند در خدمت شبکه، نخستینه‌های خدمت N-CONNECT (مانند ۱۲۸ برای توصیه‌نامه‌ی CCITT X.233 | ISO 8879 و ISO 8208 | X.25) کمتر از طول CSC-PDU، حمل شود.

یادآوری ۴- برای نگاشت مستقیم UN به X.25 | ISO 8208 «max UN Userdata» برابر ۱۲۸ است.

۸-۵-۱-۳ وارسی‌های اولیه – نشان UN-CONNECT

در زمان دریافت یک نشان UN-CONNECT بدون حضور CSC-PDU در پارامتر احراز هویت UN، NLSPE باید وارسی کند که آیا ارتباطات محافظت‌نشده مجاز هستند. (مبتنی بر الزامات خدمت امنیتی محلی و زوج نشانی فراخوانی شده/فراخواننده) اگر ارتباطات محافظت‌نشده مجاز باشند، پارامترهای خدمت **NLSP** و **UN** به‌طور مستقیم در پارامترهای خدمت **UN** و **NLSP** معادل (برای همه‌ی **NLSP** و نخستینه‌های خدمت **UN** بعدی تا زمانی که یک نشان **UN-DISCONNECT** دریافت شود) رونوشت می‌شوند. هیچ اقدام بیشتری به‌وسیله‌ي **NLSPE** در طول اتصال انجام نمی‌شود.

اگر ارتباطات محافظت‌نشده مجاز نباشند و هیچ CSC-PDU حاضر نباشد، رویه‌های تعریف شده در زیربند ۸-۴ برای وارسی شکست اجرا می‌شوند.

اگر یک CSC-PDU حاضر باشد، بسته به مقدار SA-P و پرچم‌های UNC-UND در فیلد نوع PDU که در جدول ۸-۲ داده شده است، رویه‌های تعریف شده در زیربندهای ۸-۵-۲، ۸-۵-۳ یا ۸-۵-۴ اجرا می‌شوند. درصورتی‌که پرچم به SA-P تنظیم شده باشد، نشان می‌دهد که تبادلات درون باند SA-P قرار است به‌وسیله‌ی NLSP حمل شوند. درصورتی‌که پرچم به UNC-UND تنظیم شده باشد، نشان می‌دهد که NLSP-CONNECT قرار است به جای UN-CONNECT در UN-DATA حمل شود. سپس زیربند مشابهی برای نخستینه‌های خدمت بعدی UN-CONNECT و NLSP-CONNECT در آن اتصال UN، استفاده می‌شوند.

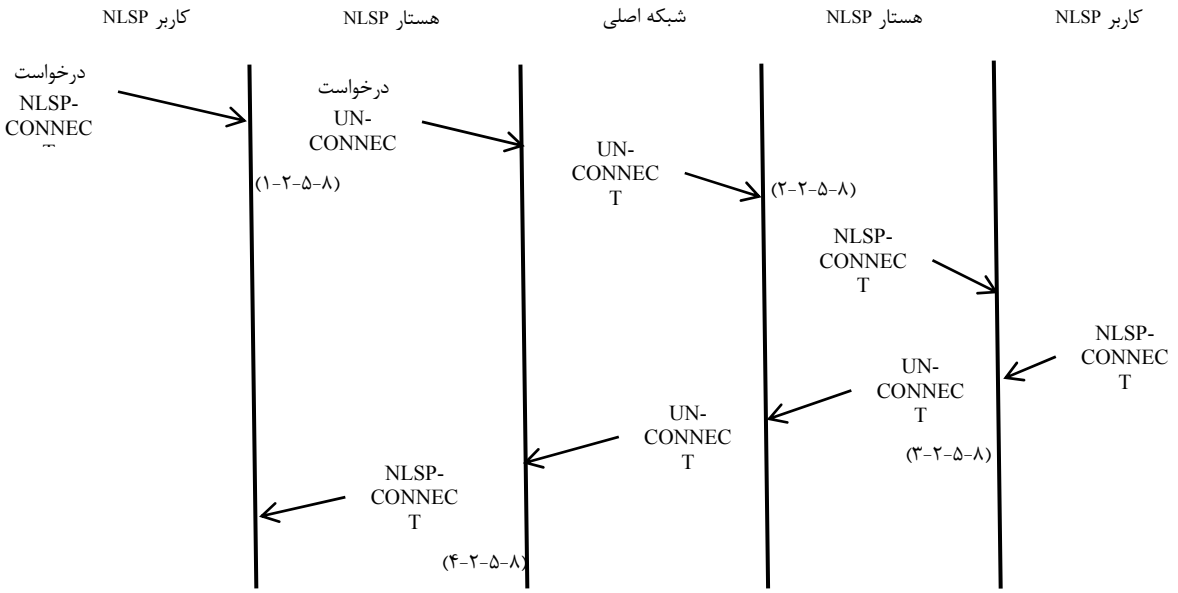
جدول ۸-۲- پرچم‌های CSC-PDU که رویه‌های راه‌اندازی اتصال NLSP را شناسایی می‌کنند.

رویه‌های راه‌اندازی اتصال NLSP	پرچم SA-P	پرچم UNC-UND
(NLSP-CONNECT در UN-DATA) ۸-۵-۴	Set	Set

Set	Clear	۸-۵-۴ (NLSP-CONNECT در UN-DATA)
Clear	Set	۸-۵-۳ (NLSP-CONNECT در UN-DATA با SA-P)
Clear	Clear	۸-۵-۲ (NLSP-CONNECT در UN-DATA)

۸-۵-۲ NLSP-CONNECT در UN-CONNECT

دنباله مورد انتظار از رویدادهای برقراری اتصال NLSP با پارامترهای NLSP-CONNECT در UN-CONNECT در شکل ۸-۱ نشان داده شده است.



شکل ۸-۱ – نمودار دنباله زمانی نخستینه خدمات برای NLSP-CONNECT در UN-CONNECT

۸-۵-۲-۱ درخواست NLSP-CONNECT

در یک درخواست NLSP-CONNECT اگر پارامترهای NLSP-CONNECT قرار باشد در UN-CONNECT حمل شوند، رویه‌های زیر باید انجام گیرند:

الف- اگر Protect_Connect_Params برابر TRUE باشد و No_Header برابر TRUE باشد، هر داده‌ی کاربر NLSP باید مطابق آن‌چه در زیربند ۶-۴-۱-۲ توصیف شده است، کپسوله شود. این در UN-Userdata قرار داده شده است.

ب- اگر Protect_Connect_Params برابر TRUE باشد، No_Header برابر FALSE باشد و Param_Prot برابر TRUE باشد، یک SDT PDU تولید می‌شود که شامل نشانی فراخوانی شده‌ی NLSP، نشانی فراخواننده‌ی NLSP، و NLSP-Userdata است. (که در زیربند ۶-۴-۱-۱ توصیف شده است با نوع داده «NLSP-CONNECT req/inf» است.) این در UN-Userdata قرار داده شده است.

پ- اگر Protect_Connect_Params برابر TRUE ، No_Header برابر FALSE و Param_Prot برابر FALSE باشد، یک SDT PDU تولید می‌شود که شامل NLSP-Userdata (در صورت وجود) است. (و

همان‌طورکه در زیربند ۶-۴-۱-۱ توصیف شد همراه با نوع داده «NLSP-CONNECT req/inf» است.) این SDT PDU در UN-Userdata قرار داده شده است.

ت- اگر Protect_Connect_Params برابر FALSE باشد، سپس NLSP-Userdata در UN-Userdata قرار داده می‌شود.

ث- یک CSC-PDU با موارد زیر ساخته می‌شود:

۱- پرچم UNC-UND صفر می‌شود؛

۲- SA-ID مرتبط به SA جاری در فیلد SA-ID قرار داده می‌شود؛

۳- پرچم SA-ID به صفر تنظیم می‌شود؛

۴- محتوای CSC به تبادل اول CSC تنظیم می‌شود که برای رویه‌های مختص سازوکار (مانند آن‌هایی که در زیربند ۱۰-۳ توصیف شد) مورد نیاز است.

ج- یک درخواست UN-CONNECT باید با موارد زیر فراخوانی شود:

۱- اگر Param_Prot، true باشد، نشانی فراخوانی شده‌ی UN به Peer_Adr و درغیر این‌صورت به نشانی فراخوانی شده‌ی NLSP؛

۲- اگر Param_Prot، true باشد، نشانی فراخواننده‌ی UN به NLSPE UN-address محلی تنظیم شود و درغیر این‌صورت به نشانی فراخواننده‌ی NLSP تنظیم خواهد شد؛

۳- انتخاب تأیید دریافت UN و انتخاب داده‌ی پیشتاز به مقادیری که به‌صورت محلی از انتخاب تأیید دریافت NLSP و انتخاب داده‌ی پیشتاز تعیین می‌شود، تنظیم می‌شود.

۴- تنظیم پارامتر UN QOS به مقداری که به‌صورت محلی توسط پارامتر NLSP QOS تعیین می‌شود؛

۵- تنظیمUN-Userdata به‌صورتی که در ردیف‌های الف تا ت توصیف شده در بالا عنوان شده است.

۶- تنظیم احراز هویت UN به SCS PDU به‌صورتی‌که در ردیف ث توصیف شده در بالا عنوان شده است.

چ- NLSPE فراخواننده منتظر تأیید UB-CONNECT که در زیربند ۸-۲-۵-۴ توصیف شده، یا یک نشان UN-DISCONNECT که در زیربند ۸-۱۰ توصیف شده می‌ماند.

۸-۵-۲-۲ نشان UN-CONNECT - صفر کردن UNCD-UND و صفر کردن SA-P

در زمان دریافت یک نشان UN-CONNECT همراه با احراز هویت UN که شامل یک CSC-PDU همراه با صفر کردن پرچم UNC-UND و صفر کردن پرچم SA-P است:

الف- NLSPE باید در میان SAهای موجود خود، یک SA با My_SA_ID برابر با فیلد SA-ID در CSC-PDU دریافتی را شناسایی کند. تمام عملیات بعدی به این SA شناسایی شده ارجاع می‌کند.

ب- محتوای CSC-PDU باید آن‌گونه که برای رویه‌های مختص سازوکار مورد نیاز است، (مانند رویه‌های که در زیربند ۱۰-۳ توصیف شده است) وارسی شود. محتوای CSC-PDU پاسخ برگشتی باید برای استفاده در پردازش پاسخ NLSP-CONNECT که در زیربند ۸-۵-۲-۳ توصیف شده‌است، نگه داشته شود.

پ- اگر Protect_Connect_Params برابر TRUE و No_Header برابر TRUE باشد، آنگاه UN-Userdataها باید مطابق آن‌چه که در زیربند ۶-۴-۲-۲ توصیف شده است، واکپسوله شوند. بقیه پارامترهای نشان NLSP-CONNECT از پارامترهای نشان UN-CONNECT رونوشت می‌شوند.

ت- اگر Protect_Connect_Params برابر TRUE، No_Header برابر FALSE و Param_Prot برابر TRUE باشد، آنگاه SDT PDU در UN-Userdata مطابق زیربند ۶-۴-۲-۲ وارسی می‌شود. فیلد نوع داده باید وارسی شود که NLSP-CONNECT req/ind باشد. نشانی فراخوانی‌شده‌ی NLSP، نشانی فراخواننده‌ی NLSP و فیلدهای محتوای NLSP-Userdata در SDT PDU باید در پارامترهای نشان NLSP-CONNECTقرار گیرند. انتخاب تأیید دریافت UN و انتخاب داده‌ی پیشتاز، همچنین مجموعه‌ی پارامتر UN QOS باید به پارامترهای نشان NLSP-CONNECT معادل رونوشت شوند.

ث- اگر Protect_Connect_Params برابر TRUE، No_Header برابر FALSE و Param_Prot برابر FALSE باشد، آنگاه در صورت وجود، SDT PDU در UN-Userdata مطابق زیربند ۶-۴-۲-۱ وارسی خواهد شد. فیلد نوع داده باید وارسی شود که NLSP-CONNECT req/ind باشد. فیلد محتوای داده‌ی کاربر در SDT-PDU باید در NLSP-Userdata قرار داده شود. بقیه پارامترهای نشان NLSP-CONNECT باید از پارامترهای نشان UN-CONNECT رونوشت شوند.

ج- اگر Protect_Connect_Params برابر FALSE باشد، آنگاه تمام پارامترهای نشان UN-CONNECT به پارامترهای نشان NLSP-CONNECT رونوشت می‌شوند.

چ- نشانی فراخوانی‌شده‌ی NLSP که مطابق آن‌چه در بالا توصیف شد، تنظیم شده است، باید وارسی شود تا نشانی NLSPی باشد که به‌وسیله‌ی این هستار NLSP (که به‌صورت محلی تعیین شده است)، به‌کار می‌رود.

ح- نشانی فراخواننده‌ی NLSP که مطابق آن‌چه در بالا توصیف شد، تنظیم شده است ، باید وارسی شود تا یک نشانی NLSP در صفت Adr_Served SA باشد.

خ- اگر برچسب امنیتی برای اتصال برقرار شده باشد، باید با مجموعه‌ی برچسب‌های احراز هویت شده در صفت Label_Set SA وارسی شود.

د- نشان NLSP-CONNECTION باید به کاربر NLSP گذر داده شود.

یادآوری– انتخاب تأیید دریافت NLSP، انتخاب داده‌ی پیشتاز و مجموعه پارامتر NLSP QOS می‌توانند قبل از گذردهی به کاربر NLSP به یک مقدار معین محلی تغییر داده شوند.

ه- NLSPE فراخوانی‌شده منتظر یک پاسخ NLSP-CONNECT که در زیربند ۸-۵-۲-۳ توصیف شده است یا یک درخواست NLSP-DISCONNECT یا نشان UN-DISCONNECT که در زیربند ۸-۱۰ توصیف شده است می‌ماند.

۸-۵-۲-۳ پاسخ NLSP CONNECT

در زمان دریافت یک پاسخ NLSP-CONNECT:

الف- اگر Protect_Connect_Params برابر TRUE و No_Header برابر TRUE باشد، آنگاه هر NLSP Userdata باید مطابق آن‌چه در زیربند ۶-۴-۱-۲ توصیف شده است، کپسوله شود. این NLSP Userdata در UN-Userdata قرار داده شده است.

ب- اگر Protect_Connect_Params برابر TRUE، No_Header برابر FALSE و Param_Prot برابر TRUE باشد، آنگاه یک SDT PDU تولید می‌شود که نشانی فراخوانی‌شده‌ی NLSP، نشانی فراخواننده‌ی NLSP و NLSP-Userdata (که در زیربند ۶-۴-۱-۱ توصیف شده است) که با نوع داده «NLSP-CONNECT req/inf» همراه است را در بر می‌گیرد. این SDT PDU در UN-Userdata قرار داده شده است.

پ- اگر Protect_Connect_Params برابر TRUE، No_Header برابر FALSE و Param_Prot برابر FALSE باشد و NLSP-Userdata وجود داشته باشد، آنگاه یک SDT PDU تولید می‌شود که شامل NLSP Userdataی است که در زیربند ۶-۴-۱-۱ توصیف شده و با نوع داده «NLSP-CONNECT req/inf» همراه است. این SDT PDU در داده‌ی کاربر UN قرار داده شده است.

ت- اگر Protect_Connect_Params برابر FALSE باشد، NLSP-Userdata در UN-Userdata قرار داده می‌شود.

ث- اگر نتوان داده‌ی تولید شده در الف تا ت را در UN-Userdata گنجاند، این رویه‌ها باید مطابق آن‌چه در زیربند ۸-۴ تعریف شده لغو شوند.

ج- یک CSC-PDU باید به‌وسیله موارد زیر تولید شود:

۱- صفر کردن پرچم‌های SA-P و UNC-UND؛

۲- SA-ID به SA-ID مانند CSC-PDU دریافت‌شده در نشان UN-CONNECT ؛

۳- محتوای CSC به مقداری تنظیم می‌شود که از فراخوانی قبلی رویه‌های مختص سازوکار در زیربند ۸-۵-۲-۲، قسمت ب برگردانده می‌شود.

چ- یک پاسخ UN-CONNECT باید با موارد زیر فرستاده شود:

۱- اگر Param_Prot برابر TRUE باشد، نشانی پاسخ‌دهی UN به نشانی UN هستار NLSP محلی و در غیر این‌صورت به پارامتر نشانی پاسخ‌دهی NLSP تنظیم می‌شود.

۲- انتخاب تأیید دریافت UN و انتخاب داده‌ی پیشتاز برابر مقادیری تنظیم می‌شوند که به‌صورت محلی از انتخاب تأیید دریافت NLSP و انتخاب داده‌ی پیشتاز تعیین می‌شوند.

۳- پارامتر UN QOS برابر مقادیری تنظیم می‌شود که به‌صورت محلی از پارامتر NLSP QOS تعیین می‌شوند.

۴- UN-Userdata که در الف تا ث بالا توصیف شده است.

۵- احراز هویت UN که مطابق توصیف خ در بالا به CSC-PDU تنظیم شده است.

ح- اگر تحت رویه‌های مختص سازوکار به احراز هویت و تبادل CSC نیاز باشد (مانند آن‌چه که در زیربند ۱۰-۳ توصیف شده است)، NLSPE فراخوانی‌شده می‌تواند برای یک SDT PDU در UN-DATA قبل از آنکه برقراری اتصال NLSP و پردازش‌های نخستینه‌های NLSP-DATA از کاربر NLSP کامل شود، منتظر بماند. در غیر این‌صورت، NLSPE فراخوانی شده مجبور است که رویه‌های برقراری اتصال NLSP را کامل کند و می‌تواند وارد مرحله‌ی انتقال داده شود.

یادآوری– اگر سازوکار مبادله CSC نیاز به مبادله‌ی بیش از دو CSC-PDU داشته باشد، در این صورت آن‌ها قبل از اینکه برقراری اتصال کامل شود، در UN-DATA مبادله می‌شوند.

۸-۵-۲-۴ تأیید UN-CONNECT - UNCD-UND Clear و SA-P Clear

در زمان دریافت یک تأیید UN-CONNECT با احراز هویت UN که شامل یک CSC-PDU است که هر دو پرچم UNC-UND و SA-P آن صفر هستند:

الف- محتوای CSC-PDU با استفاده از رویه‌های مختص سازوکاری که در زیربند ۱۰-۳ توصیف شده‌اند، وارسی می‌شود.

ب- اگر Protect_Connect_Params برابر TRUE و No_Header برابر TRUE باشد، در این صورت هر UN-Userdata باید مطابق آن‌چه در زیربند ۶-۴-۲-۲ توصیف شده است، واکپسوله شود. این در UN-Userdata قرار داده شده است. بقیه پارامترهای تصدیق NLSP-CONNECT از پارامترهای تأیید UN-CONNECT رونوشت می‌شوند.

پ- اگر Protect_Connect_Params برابر TRUE، No_Header برابر FALSE و Param_Prot برابر TRUE باشد، در این‌صورت مطابق زیربند ۶-۴-۲-۱، SDT PDU در UN-Userdata وارسی می‌شود. فیلد نوع داده باید وارسی شود که NLSP-CONNECT req/ind باشد. نشانی پاسخ NLSP، و فیلدهای محتوای NLSP Userdata در SDT PDU باید در پارامترهای تصدیق NLSP-CONNECT قرارگیرند. پارامترهای انتخاب تصدیق دریافت UN و انتخاب داده‌ی مورد انتظار، مانند مجموعه‌ی پارامتر UN QOS باید به پارامترهای تصدیق NLSP-CONNECT رونوشت شوند.

ت- اگر Protect_Connect_Params برابر TRUE، No_Header برابر FALSE و Param_Prot برابر FALSE باشد، مطابق زیربند ۶-۴-۲-۱ SDT PDU، در صورت وجود، در NLSP Userdata وارسی می‌شود. فیلد محتوای داده کاربر در SDT-PDU باید در NLSP-Userdata قرار داده شود. بقیه پارامترهای تأیید NLSP-CONNECT باید به پارامترهای تأیید UN-CONNECT رونوشت شوند.

ث- اگر Protect_Connect_Params برابر FALSE باشد، در این‌صورت تمام پارامترهای تأیید UN-CONNECT باید به پارامترهای تأیید NLSP-CONNECT رونوشت شوند.
ج- اگر نشانی پاسخ‌دهی NLSP وجود داشته باشد باید وارسی شود که یک نشانی NLSP در صفت SA از Adr_Seved موجود باشد.
چ- تأیید اتصال NLSP باید به کاربر NLSP واگذار شود.
ح- اگر نیاز باشد، در رویه‌های مختص سازوکار برای احراز هویت و مبادله CSC (مانند رویه‌هایی که در زیربند ۱۰-۳ توصیف شد)، یک SDT PDU مجاز است (مطابق توصیف زیربند ۶-۴-۱-۱) با نوع داده‌ی «غیرمرتبط با نخستینه‌های خدمت NLSP» (که شامل هیچ فیلد محتوایی به جز موارد مورد نیاز در بند ۶، نیست)، ایجاد شود. این باید در داخل UN-Userdata از یک نخستینه‌ی UN-DATA فرستاده شود.

یادآوری– اگر سازوکار مبادله‌ی CSC نیاز به مبادله‌ی بیش از دو CSC-PDU داشته باشد، در این صورت آن‌ها قبل از اینکه برقراری اتصال کامل شود، در UN-DATA مبادله می‌شوند.

حال رویه‌های برقراری اتصال NLSP کامل است.

۸-۵-۳ NLSP-CONNECT در UN-CONNECT با SA-P

دنباله‌ی مورد انتظار رویدادها در شکل ۸-۳ نشان داده شده است:

۸-۵-۳-۱ درخواست NLSP-CONNECT

در هنگام درخواست NLSP-CONNECT، اگر NLSP-CONNECT قرار است در داخل UN-CONNECT حمل شود و برقراری SA درون باند انتخاب‌شده باشد، رویه زیر باید اجرا شود:
الف- یک CSC-PDU باید به‌وسیله‌ی موارد زیر آماده شود:

۱- صفر کردن پرچم UNC-UND؛

۲- پرچم SA-P، ۱ است و SA-ID، طول محتوا و محتوای CSC-PDU حضور ندارند.
ب- یک درخواست UN-CONNECT باید به‌وسیله‌ی موارد زیر فرستاده شود:

۱- تنظیم نشانی فراخوانی‌شده‌ی UN به Peer_Adr؛

۲- نشانی فراخواننده‌ی UN به UN-Address هستار NLSP محلی تنظیم شده است؛

۳- انتخاب تأیید دریافت UN به مقداری تنظیم می‌شود که به‌صورت محلی تعیین شده است؛

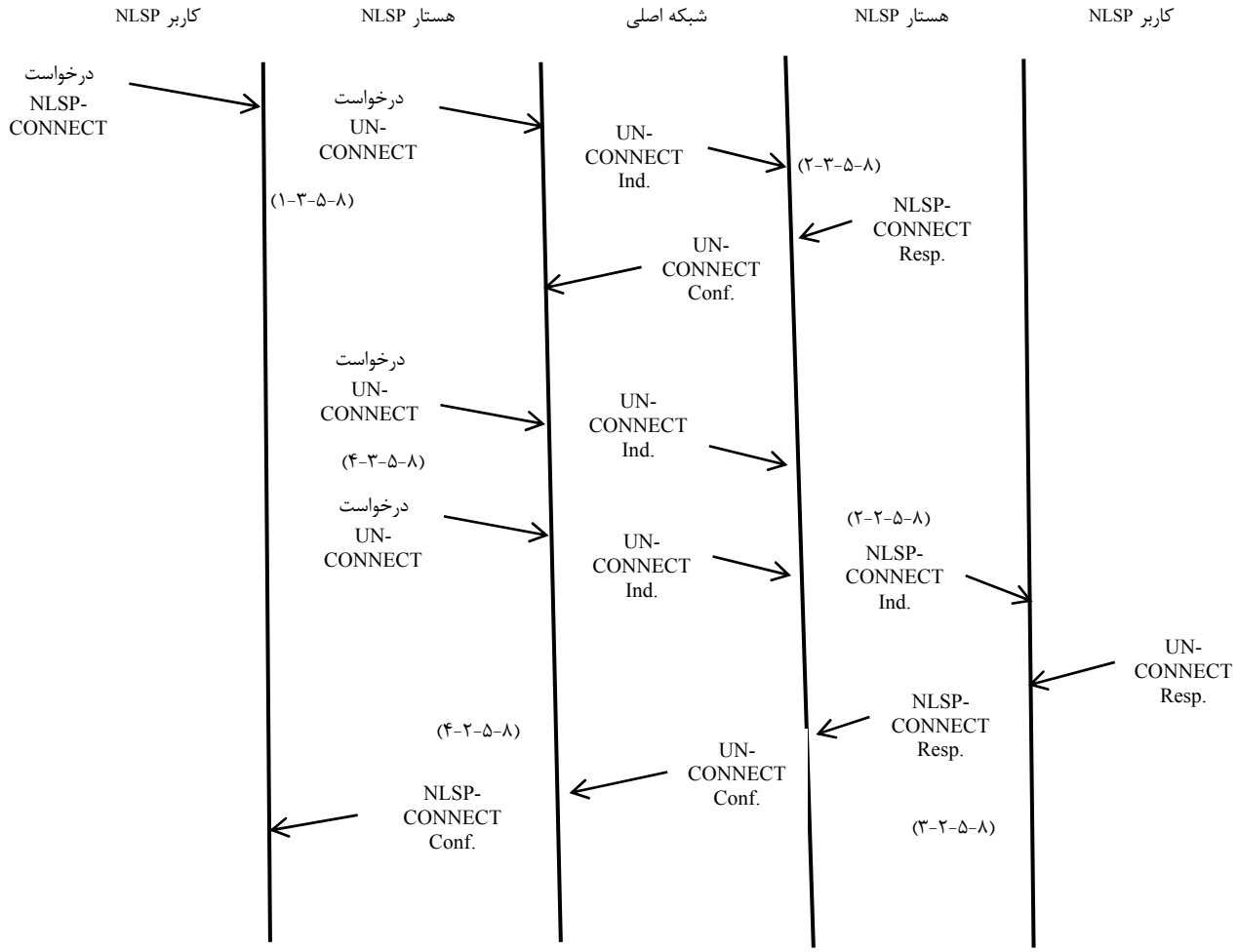
۴- انتخاب داده‌ی پیشتازی UN به مقداری تنظیم می‌شود که به‌صورت محلی تعیین شده است؛

۵- پارامتر UN QOS به مقداری تنظیم می‌شود که به‌صورت محلی تعیین شده است؛

۶- UN-Userdata خالی؛

۷- احراز هویت UN به CSC-PDU.

پ- NLSPE فراخواننده، باید برای تأیید UN-CONNECT که در زیربند ۸-۵-۳-۳ توصیف شده یا نشان UN-DISCONNECT که در زیربند ۸-۱۰ توصیف شده است، منتظر بماند.



شکل ۸-۲– نمودار دنباله زمانی نخستینه خدمت برای NLSP-CONNECT در UN-CONNECT با SA-P

۸-۵-۳-۲ نشان UN-CONNECT– صفر کردن UNC-UND و تنظیم مقدار SA-P به ۱

در زمان دریافت یک نشان UN-CONNECT با احراز هویت UN که در برگیرنده‌ی CSC-PDUی است که پرچم UNC-UND آن صفر و پرچم SA-P آن ۱ است:

الف- NLSP باید یک CSC-PDU با موارد زیر را آماده کند:

۱- صفر کردن پرچم UNC-UND؛

۲- یک کردن پرچم SA-P؛

۳- محتوای خالی CSC.

ب- سپس NSPE باید با یک پاسخ UN-CONNECT موارد زیر را پاسخ دهد:

۱- نشانی پاسخ UN که به UN-Address محلی تنظیم شده است؛

۲- انتخاب تأیید دریافت UN و انتخاب داده پیشتاز به مقادیری که به‌صورت محلی از پارامترهای نشان UN-CONNECT تعیین شده است، تنظیم می‌شوند؛

۳- پارامتر QOS به مقداری تنظیم می‌شود که به‌صورت محلی از پارامتر UN QOS در نشان UN-CONNECT تعیین می‌شود؛

۴- UN-Userdata خالی؛

۵- تنظیم احراز هویت UN به CSC PNU.

NLSPE فراخوانی‌شده باید منتظر یک تبادل SA-P یا یک نشان UN-DISCONNECT که در زیربند ۸-۱۰ توصیف شده است، بماند.

۸-۵-۳-۳ تأیید UN-CONNECT - صفر کردن UNC-UND و ۱ کردن SA-P

در زمان دریافت یک تأیید UN-CONNECT با احراز هویت UN شامل یک CSC-PDU پاسخ که پرچم UNC-UND آن صفر و پرچم SA-P آن یک است:

الف- SA-P باید درون باند انجام شود؛

ب- NPLSE فراخوانده برای تکمیل SA-P که در زیربند ۸-۵-۳-۴ توصیف شده است یا یک UN-DISCONNECT که در زیربند ۸-۱۰ توصیف شده است، منتظر می‌ماند.

۸-۵-۳-۴ تکمیل SA-P

زمانی که SA-P تکمیل می‌شود (همان‌طورکه در زیربند ۸-۵-۳-۳ توصیف شده است)، NLSPE فراخواننده باید رویه‌هایی که در ادامه می‌آید را انجام دهد:

الف- یک درخواست UN-DISCONNECT باید به‌وسیله‌ی NLSPE فراخواننده با تنظیم دلیل آن به «disconnect-normal-condition» فرستاده شود و با یک درخواست UN-CONNECT با پارامترهای خدمت که مطابق آن‌چه در ادامه می‌آید تنظیم شده‌اند، دنبال شود.

ب- اگر Protect_Connect_Params برابر TRUE و No_Header برابر TRUE باشد، در این‌صورت تمام NLSP Userdataها باید مطابق آن‌چه در زیربند ۶-۴-۱-۲ توصیف شده است، در کپسول گذارده شوند. این در UN-userdata قرار داده می‌شود.

پ- اگر Protect_Connect_Params برابر TRUE، No_Header برابر FALSE و Param_Prot برابر TRUE باشد، در این‌صورت یک SDT PDU تولید می‌شود که شامل نشانی فراخواننده‌ی NLSP، نشانی فراخوانی‌شده‌ی NLSP و NLSP-Userdata که در زیربند ۶-۴-۱-۱ توصیف شده به همراه نوع داده‌ی «NLSP-CONNET req/ind»، است. این در UN-Userdata قرار داده می‌شود.

ت- اگر Protect_Connect_Params برابر TRUE، No_Header برابر FALSE و Param_Prot برابر FALSE باشد، در این‌صورت یک SDT PDU تولید می‌شود که شامل NLSP-Userdata که در زیربند

۶-۴-۱-۱ توصیف شده است همراه با نوع داده‌ی «NLSP-CONNET req/ind» است. این در UN-Userdata قرار داده می‌شود.

ث- گر Protect_Connect_Params برابر FALSE باشد، آن‌گاه NLSP Userdata در UN-Userdata قرار داده می‌شود.

ج- یک CSCPDU با اجزای زیر آماده می‌شود:

۱- پرچم UNC-UND صفر می‌شود؛

۲- SA-ID مربوط به SA جاری در فیلد SA-ID قرار می‌گیرد؛

۳- پرچم SA-P صفر می‌شود.

۴- محتوای CSC به اولین مبادله‌ی CSC، همان‌طوری‌که در رویه‌های مختص سازوکارها مورد نیاز است (مانند رویه‌هایی که در زیربند ۱۰-۳ توصیف شده‌اند)، تنظیم می‌شود.

چ- یک درخواست UN-CONNECT باید فراخوانی شود:

۱- اگر Param_Prot برابر true باشد، نشانی فراخوانی‌شده‌ی UN به Peer_Adr تنظیم می‌شود، در غیر این‌صورت به نشانی فراخواننده‌ی NLSP تنظیم خواهد شد؛

۲- اگر Param_Prot برابر true باشد، نشانی فراخواننده‌ی UN به UN-Adress هستار NLSP محلی تنظیم می‌شود، در غیر این‌صورت به نشانی فراخواننده‌ی NLSP تنظیم خواهد شد؛

۳- انتخاب تأیید دریافت UN و انتخاب داده‌ی پیشتاز به مقادیری تنظیم می‌شود که به‌صورت محلی از تأیید دریافت NLSP و انتخاب داده‌ی پیشتاز تعیین شده‌اند؛

۴- پارامتر UN QOS به مقداری تنظیم می‌شود که به‌صورت محلی از پارامتر NLSP QOS تعیین شده است؛

۵- UN-userdata همان‌طوری‌که در الف و ت توضیح داده شد، تنظیم می‌شود؛

۶- احراز هویت UN به CSC-PDU که در ث توضیح داده شد، تنظیم می‌شود.

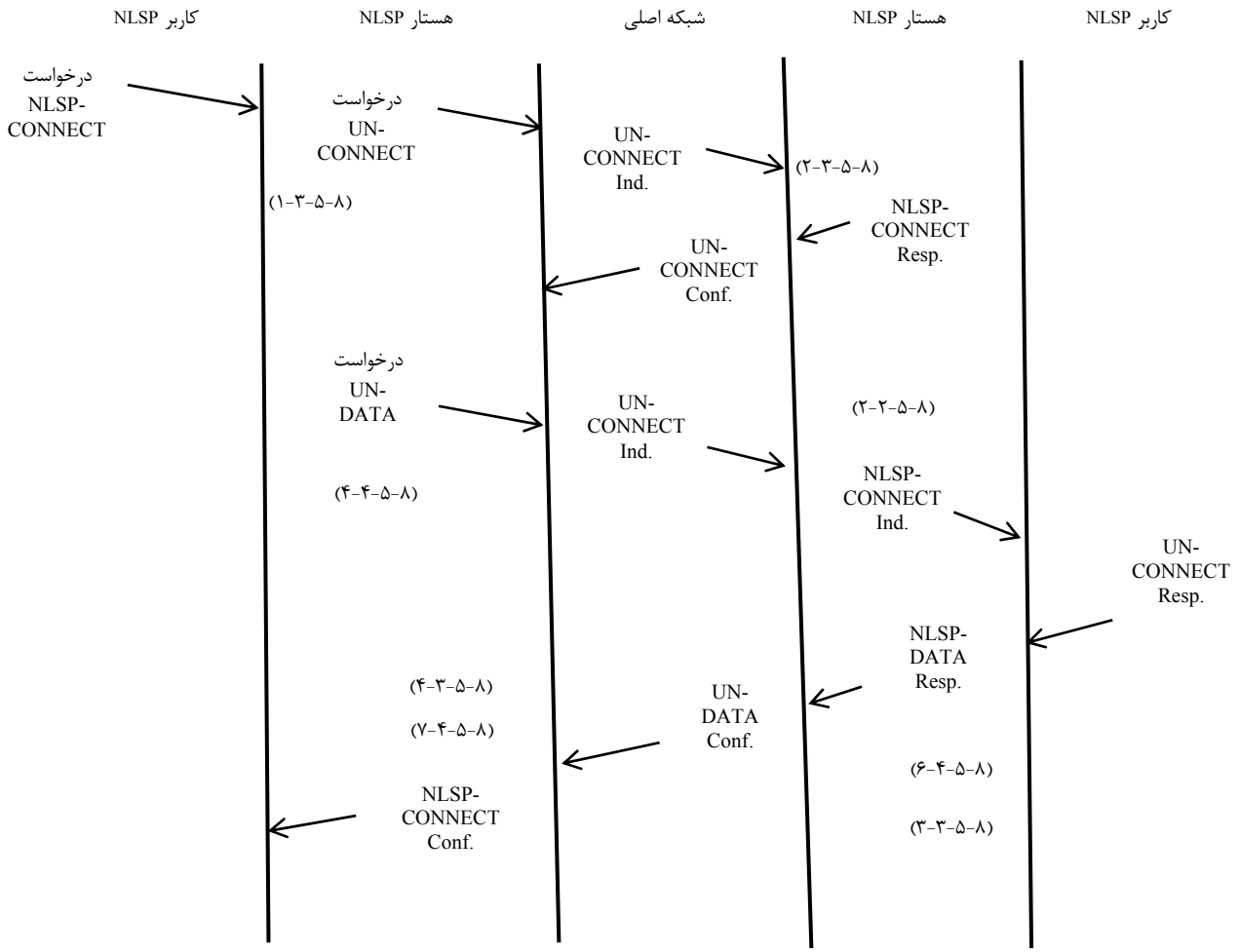
ح – NLSP فراخواننده منتظر یک تأیید UN-CONNECT (همان‌طورکه در زیربند ۸-۵-۲-۴ توضیح داده شده است) یا یک نشان UN-DISCONNECT (همان‌طورکه در زیربند ۱۰-۸ توضیح داده شده است) می‌ماند.

در زمان تکمیل SA-P، NLSP منتظر یک UN-DISCONNECT می‌شود و دلیل آن را به «disconnect-normal-condition» تنظیم می‌کند. بر روی این نشان UN-CONNECT، NLSP فراخوانی‌شده سپس منتظر یک نشان UN-CONNECT (همان‌طورکه در زیربند ۸-۵-۲-۲ توضیح داده شده است) می‌ماند.

NLSPE فراخوانی‌کننده و فراخوانی‌شده همان‌طوری‌که در زیربندهای ۸-۵-۲-۲ و ۸-۵-۲-۴ توصیف شده است NLSP و UN-CONNECT نخستینه را پردازش می‌کنند.

۸-۵-۴ NLSP-CONNECT در UN-Data

دنباله‌ی مورد انتظار از رویدادها در شکل ۸-۳ نشان داده شده است.



شکل ۸-۳ – نمودار دنباله زمانی نخستینه خدمات برای NLSP-CONNECT در UN-DATA

۸-۵-۴-۱ درخواست NLSP-CONNECT

در هنگام درخواست NLSP-CONNECT اگر پارامترهای NLSP-CONNECT قرار باشد در UN-DATA حمل شوند، رویه زیر باید اجرا شود:

الف- یک SCS PDU باید به‌وسیله‌ی موارد زیر آماده شود:

۱- پرچم UNC-UND یک شود؛

۲- اگر SA-P درون باند انتخاب شده باشد، در این صورت پرچم SA-P به ۱ تنظیم شده و پرچم SA-ID، طول محتوا و محتوای CSC-PDU حضور ندارند؛

۳- اگر SA-P درون باند انتخاب نشده باشد، SA-ID به Your_SA_ID تنظیم می‌شود و محتوای CSC-PDU به اولین مبادله‌ی CSC آن‌گونه که برای رویه‌های مختص سازوکار نیاز است، تنظیم می‌شود. (مانند آن‌هایی که در زیربند ۳-۱۰ توصیف شده است.)

ب- یک درخواست UN-CONNECT باید به‌وسیله‌ی موارد زیر فرستاده شود:

۱- تنظیم نشانی فراخوانی‌شده‌ی UN به Peer_Adr ؛

۲- تنظیم نشانی فراخواننده‌ی UN به UN-Address هستار NLSP محلی؛
۳- انتخاب تأیید دریافت UN به مقداری تنظیم می‌شود که به‌صورت محلی از تأیید دریافت NLSP تعیین شده است؛
۴- انتخاب داده‌ی پیشتاز UN به مقداری تنظیم می‌شود که به‌صورت محلی از انتخاب داده‌ی پیشتاز NLSP تعیین می‌شود؛
۵- پارامتر UN QOS به مقداری تنظیم می‌شود که به‌صورت محلی از NLSP QOS تعیین می‌شود.
۶- UN-Userdata خالی؛
۷- احراز هویت UN به CSC-PDU.

پ- NLSPE فراخواننده باید منتظر یک تأیید UN-CONNECT آن‌گونه که در زیربند ۸-۵-۴-۳ توصیف شده یا یک نشان UN-DISCONNECT آن‌گونه که در زیربند ۱۰-۸ توصیف شده، بماند.

۸-۵-۴-۲ نشان UN-CONNECT– تنظیم UNC-UND

در زمان دریافت یک نشان UN-CONNECT با احراز هویت UN دربرگیرنده‌ی یک CSC-PDU با پرچم UNC-UND که مقدارش ۱ است:

الف- اگر پرچم SA-P صفر باشد، آنگاه:
۱- NLSPE باید در میان SAهایی که برای آن دردسترس است، یک SA که My_SA-ID آن برابر فیلد SA-ID در CSC-PDU دریافتی است را شناسایی کند. تمام عملیات بعدی به این SA شناسایی شده، ارجاع می‌دهند؛
۲- محتوای CSC-PDU باید به‌طوری که برای رویه‌های مختص سازوکار مورد نیاز است، (مانند آن‌هایی که در زیربند ۱۰-۳ توصیف شده است) وارسی شود.

در صورتی که پرچم SA-P ۱ باشد یا نباشد، رویه‌های ذیل در این زیربند اجرا می‌شوند.

ب- NLSPE باید یک CSC-PDU را به‌وسیله‌ی موارد زیر آماده کند:
۱- ۱ کردن پرچم UNC-UND؛
۲- اگر SA-P درون باند انتخاب‌شده باشد، آنگاه فیلد SA-ID باید غایب باشد، در غیر این‌صورت باید به SA-ID دریافت‌شده در CSC-PDU تنظیم شود؛
۳- اگر SA-P درون باند انتخاب‌شده باشد، آنگاه مقدار پرچم SA-P ۱ است، در غیر این‌صورت صفر است؛
۴- اگر SA-P درون باند انتخاب‌شده باشد، محتوای CSC-PDU و فیلدهای طول محتوا حضور ندارند، در غیر این‌صورت، محتوای CSC-PDU به تبادل CSCی تنظیم می‌شود که از رویه‌های مختص سازوکاری که در زیربند ۱۰-۳ تعریف شده است، برگشته است.

یادآوری– رویه‌های جاری از سازوکارهای مبادله CSC که نیازمند بیش از یک مبادله دو-طرفه از CSC-PDUهای اختیاری که با یک SDT-PDU دنبال می‌شوند، پشتیبانی نمی‌کنند.

پ- سپس NLSPE باید با یک پاسخ UN-CONNECT، توسط موارد زیر پاسخ دهد:
۱- نشانی پاسخ‌دهی UN که به UN-Address محلی تنظیم شده است؛

۲- انتخاب تأیید دریافت UN و انتخاب داده‌ی پیشتاز به مقادیری تنظیم می‌شوند که به‌صورت محلی از پارامترهای داخل نشان UN-CONNECT تعیین می‌شود؛

۳- پارامتر UN QOS به مقداری تنظیم می‌شود که به‌صورت محلی از پارامتر UN QOS در نشان UN- CONNECT تعیین شده است؛

۴- فیلد UN-Userdata خالی شود؛

۵- احراز هویت UN که به CSC-PDU تنظیم شده است.

ت- NLSPE فراخوانی‌شده باید منتظر یک مبادله‌ی SA-P یا نشان UN-DATA که دربرگیرنده‌ی یک SDT PDU (آن‌گونه که در زیربند ۸-۵-۴-۵ توصیف شده است) یا یک نشان UN-DISCONNECT (آن‌گونه که در زیربند ۸-۱۰ توصیف شده است) یا یک UN-RESET (آن‌گونه که در زیربند ۸-۹ توصیف شده است) بماند.

۸-۵-۴-۳ تأیید UN-CONNECT – تنظیم UNC-UND

در زمان دریافت یک تأیید UN-CONNECT با UN-Authentication که دربرگیرنده‌ی یک CSC-PDU پاسخ با پرچم UNC-UND برابر با مقدار ۱ است:

الف- پرچم SA-P در CSC-PDU وارسی می‌شود تا با انتخاب SA-P درون باند، انطباق داشته باشد.

ب- اگر SA-P انتخاب نشده باشد:

۱- محتوای CSC-PDU با استفاده از رویه‌های مختص سازوکار (مانند آن‌هایی که در زیربند ۱۰-۳ توصیف شده است)، وارسی می‌شود؛

۲- رویه‌ها مانند آن‌چه در زیربند ۸-۵-۴-۴ قسمت پ توصیف شده است، ادامه می‌یابد.

یادآوری– اگر SA-P انتخاب نشده باشد و سازوکار مبادله CSC نیاز به تبادل بیش از دو CSC-PDU داشته باشد، در این صورت این موارد قبل از ادامه دادن با رویه‌های برقراری اتصال در UN-DATA مبادله می‌شوند.

پ- SA-P درون باند انتخاب شده است:

۱- تبادل SA-P باید انجام شود؛

۲- NLSPE فراخواننده منتظر تکمیل SA-P (آن‌گونه که در زیربند ۸-۵-۴-۴ توصیف شده است) یا یک نشان UN-DISCONNECT (آن‌گونه که در زیربند ۸-۱۰ توصیف شده است) یا یک نشان UN-RESET (آن‌گونه که در زیربند ۸-۹ توصیف شده است) بماند. با هر خطایی در SA-P باید مانند خطایی که در زیربند ۸-۴ توصیف شده است، رفتار شود.

۸-۵-۴-۴ تکمیل SA-P/ بدون SA-P

در تکمیل SA-P:

الف- اگر SA-P موفق شود، پس از آن، SA برقرارشده برای تکمیل برقراری اتصال NLSP و ارتباطات امن که در زیربندهای ذیل توصیف شده است، استفاده می‌شود.

ب- اگر SA-P ناموفق باشد، NLSPE فراخوانی‌شده و فراخواننده باید یک UN-DISCONNECT را به‌کار گیرد و رویه‌های برقراری اتصال NLSP باید لغو شوند.

در تکمیل SA-P یا به دنبال یک تأیید UN-CONNECT بدون SA-P که در زیربند ۸-۵-۴-۳ قسمت ب توصیف شده است:

پ – سپس پارامترهای NLSP-CONNECT ذیل که به NLSP فراخواننده در رویداد توصیف‌شده مطابق زیربند ۸-۵-۴-۱ عبور داده شده است، باید در یک SDT PDU قرار داده شود. (آن‌طور که با نوع داده‌ی «NLSP-CONNECT req/ind» در زیربند ۶-۴-۱-۱ توصیف شده است.)

- نشانی فراخواننده‌ی NLSP؛
- نشانی فراخوانی‌شده‌ی NLSP؛
- فیلد NLSP Userdata.

یادآوری ۱– پارامترهای نشانی NLSP به یک شکل محافظت‌شده حمل می‌شوند حتی اگر Param_Prot برابر FALSE باشد.

ت- SDT PDU باید به فراهم‌آورنده‌ی خدمت UN در UN-Userdata مربوط به درخواست UN-DATA تحویل داده شود.

یادآوری ۲– این موضوع می‌تواند قسمت سوم تبادل احراز هویت هستار همتا را فراهم کند.

ث- NLSPE فراخوانی منتظر نشان UN-DATA که دربرگیرنده‌ی یک SDT PDU که در زیربند ۸-۵-۴-۷ توصیف شده یا یک نشان UN-DISCONNECT که در زیربند ۸-۱۰ توصیف شده یا یک نشان UN-RESET که در زیربند ۸-۹ توصیف شده است، می‌ماند.

در زمان تکمیل SA-P، NLSPE فراخوانی‌شده منتظر یک نشان UN-DATA که دربرگیرنده‌ی یک SDT-PDU که در زیربند ۸-۵-۴-۵ توصیف شده یا یک نشان UN-DISCONNECT که در زیربند ۸-۱۰ توصیف شده یا یک نشان UN-RESET که در زیربند ۸-۹ توصیف شده است، می‌ماند.

۸-۵-۴-۵ UN-DATA دربرگیرنده‌ی یک SDT PDU در NLSPE فراخوانده

در زمان دریافت یک نشان UN-DATA دربرگیرنده‌ی یک PDU انتقال داده امن در NLSPE فراخوانی‌شده مطابق آن‌چه در زیربند ۶-۴-۲-۲ توصیف شده است باید وارسی شود.

یادآوری– این وارسی می‌تواند قسمت سوم تبادل احراز هویت هستار همتا را فراهم کند.

باید وارسی شود که فیلد نوع داده در SDT PDU، NLSP-CONNECT req/ind باشد.

باید وارسی شود که نشانی فراخوانی‌شده‌ی NLSP یک نشانی NLSP باشدکه به‌وسیله‌ی این هستار NLSP که به‌صورت محلی تعیین شده، خدمت رسانی می‌شود.

باید وارسی شود که نشانی فراخواننده‌ی NLSP یک نشانی NLSP قرار گرفته در صفت SA، Adr_Served باشد.

اگر برچسب امنیتی برای اتصال برقرار شده باشد، این برچسب با مجموعه مجاز از برچسب‌ها در صفت Label_Set SA وارسی می‌شود.

نشان NLSP-CONNECT باید با مجموعه پارامترهای زیر به کاربر NLSP فراخوانی‌شده تحویل داده شود:

الف- نشانی فراخواننده‌ی NLSP، نشانی فراخوانی‌شده‌ی NLSP، مجموعه NLSP Userdata به‌عنوان فیلدهای محتوای SDT PDU دریافتی؛
ب- انتخاب تأیید دریافت NLSP و انتخاب داده‌ی پیشتازی NLSP که به تنظیمات پارامترهای UN معادل در پاسخ UN-CONNECT ارسالی توسط رویه‌های اشاره شده در زیربند ۸-۵-۴-۲، تنظیم شده‌اند.
پ- NLSP QOS «در دسترس» به UN QOS «انتخاب شده» توسط NLSPE فراخوانی‌شده در پاسخ UN-CONNECT ارسال شده تحت رویه‌های اشاره شده در زیربند ۸-۵-۴-۲ (همراه با «هدف» و «کمینه‌ی قابل قبول» نامشخص)، تنظیم شده است.
NLSP فراخوانی‌شده باید منتظر یک پاسخ NLSP-CONNECT که در زیربند ۸-۵-۴-۶ توصیف شده یا یک درخواست NLSP-DISCONNECT که در زیربند ۸-۱۰ توصیف شده یا یک نشان UN-DISCONNECT که در زیربند ۸-۱۰ توصیف شده یا یک نشان UN-RESET که در زیربند ۸-۹ توصیف شده است، بماند.

۸-۵-۴-۶ پاسخ NLSP-CONNECT

در زمان دریافت یک پاسخ NLSP-CONNECT، نشانی پاسخ‌دهی NLSP، پارامترهای NLSP Userdata باید همراه با نوع داده‌ی «NLSP-CONNECT res/conf» در یک SDT PDU که در زیربند ۶-۴-۱-۱ توصیف شده است قرار داده شوند.
این SDT PDU باید به فراهم‌کننده‌ی خدمت UN در UN-Userdata از یک درخواست UN-DATA تحویل داده شود.
اکنون NLSPE فراخوانی‌شده، رویه‌های برقراری اتصال NLSP خود را کامل کرده است.

۸-۵-۴-۷ UN-DATA شامل یک SDT PDU در NLSPE فراخواننده

در زمان دریافت یک نشان UN-DATA دربرگیرنده‌ی یک انتقال داده امن، SDT PDU باید مطابق توضیحات اشاره شده در زیربند ۶-۴-۲-۱ وارسی شود. جای درج نوع داده در SDT PDU باید وارسی شود تا NLSP-CONNECT req/conf باشد.
نشانی پاسخ‌دهی NLSP باید وارسی شود تا یک نشانی NLSP در محتوای صفت SA، Adr_Served باشد.
یک تأیید NLSP-CONNECT با تنظیم کردن پارامترها مطابق ذیل، به کاربر NLSP فرستاده می‌شود:
الف- نشانی پاسخ‌دهی NLSP، NLSP Userdata، (در صورت حضور) به‌عنوان فیلدهای محتوای SDT PDU دریافتی تنظیم می‌شود؛
ب- انتخاب تأیید دریافت NLSP و انتخاب داده‌ی پیشتاز NLSP به تنظیمات پارامترهای UN معادل در تأیید UN-CONNECT ارسالی تحت رویه‌های اشاره شده در زیربند ۸-۵-۴-۳، تنظیم می‌شود.
پ- NLSP QOS به UN QOS دریافتی در تأیید UN-CONNECT تنظیم شده که تحت رویه‌های اشاره شده در زیربند ۸-۵-۳ دریافت شده است.
اکنون NLSPE فراخواننده، رویه‌های برقراری اتصال NLSP را کامل کرده است.

۸-۶ کارکردهاي NLSP-DATA

۸-۶-۱ درخواست NLSP-DATA

در زمان دریافت یک درخواست NLSP-DATA، اگر No_Header برابر TRUE باشد، در این صورت NLSP Userdata باید مطابق آن‌چه در زیربند ۶-۴-۱-۲ توصیف شده است، در کپسول‌گذاشته شود. این در UN-Userdata از یک درخواست UN-DATA قرار داده می‌شود و پارامتر درخواست تأیید NLSP به پارامتر UN-DATA معادل آن رونوشت می‌شود. سپس UN-DATA باید به فراهم‌کننده خدمت UN تحویل داده شود.

در زمان دریافت یک درخواست NLSP-DATA، اگر No_Header برابر FALSE باشد، در این صورت:
الف- به‌عنوان یک مسأله محلی، NLSPE باید NLSP Userdata را قطعه‌بندی کند. (اگر مورد نیاز SA باشد.)
ب- برای هر قطعه، SDT PDU باید مطابق آن‌چه در زیربند ۶-۴-۱-۱ توصیف شده، تولید شود که همراه با نوع داده «NLSP-DATA req/ind» بوده و دربرگیرنده‌ی موارد زیر است:

۱- قطعه‌ی NLSP Userdata؛

۲- پرچم Last/No Last که برای آخرین قطعه به صفر و برای تمام قطعه‌های ماقبل به ۱ تنظیم شود.

۳- فیلد محتوای درخواست تأیید NLSP اگر:
- درخواست تأیید NLSP حاضر باشد، نشان‌دهنده‌ی «تأیید دریافت درخواست‌شده» در درخواست NLSP-DATA است؛ و
- این آخرین قطعه است؛ و
– Param_Prot برابر TRUE است.

پ- SDT PDU برای هر قطعه باید در پارامتر UN-Userdata از یک درخواست UN-DATA قرار داده شود.
ت- پارامتر درخواست تأیید UN از UN-DATA باید حاضر باشد که نشان‌دهنده‌ی «تأیید دریافت درخواست شده» است اگر:

۱- درخواست تأیید NLSP در درخواست NLSP-DATA نشان‌داده شده باشد؛ و

۲- این آخرین قطعه باشد؛ و

۳- Param_Prot برابر FALSE باشد.

درغیراین‌صورت، پارامتر درخواست UN-Confirm باید «تأیید دریافت درخواست‌نشده است» را نشان دهد.
ث – نخستینه‌ی درخواست UN-DATA برای هر قطعه باید به فراهم‌کننده‌ی خدمت UN تحویل داده شود.

۸-۶-۲ داده‌ي محافظت‌شده در نشان UN-DATA در ادامه‌ي برقراری اتصال

در زمان دریافت یک نشان UN-DATA، اگر No_Header برابر TRUE باشد، در این صورت UN Userdata باید مطابق آن‌چه در زیربند ۶-۴-۲-۲ توصیف شده است، واکپسوله شود. این در NLSP-Userdata از یک

نشان NLSP-DATA قرار داده می‌شود و پارامتر درخواست تأیید UN به پارامتر نشان NLSP-DATA معادل رونوشت می‌شود. سپس نشان NLSP-DATA باید به کاربر خدمت NLSP تحویل داده شود.

در صورت دریافت یک نشان UN-DATA، اگر No_Header برابر FALSE باشد:

الف- SDT PDU در UN Userdata باید مطابق آن‌چه در زیربند ۶-۴-۲-۱ توصیف شده است، وارسی شود.

ب- اگر فیلد نوع داده «نامرتبط با هیچ یک از نخستینه‌های خدمت NLSP» باشد، در این‌صورت SDT PDU باید مطابق زیربند ۸-۱۱ و نه مانند آن‌چه در زیر توصیف شده، پردازش شود.

پ- اگر فیلد نوع داده NLSP-DATA-ACKNOWLEDGE req/ind باشد، SDT PDU باید مطابق زیربند ۸-۹-۲ و نه مانند آن‌چه در زیر توصیف شده، پردازش شود.

ت- اگر فیلد نوع داده، NLSP-DISCONNECT req/ind باشد، SDT PDU باید مطابق زیربند ۸-۱۰-۲ و نه مانند آن‌چه در زیر توصیف شده، پردازش شود.

ث- در غیر این‌صورت، فیلد نوع داده باید به‌عنوان NLSP-DATA و مطابق ذیل پردازش شود.

ج- اگر پرچم Last/Not Last در SDT PDU به ۱ تنظیم شده باشد (Not Last)، فیلد محتوای NLSP Userdata در SDT PDU به هر NLSP Userdata قبلی که قسمتی از درخواست/نشان NLSP-DATA یکسان است افزوده می‌شود و توسط NLSPE برای استفاده بعدی نگه‌داشته می‌شود.

چ- اگر پرچم Last/Not Last در SDT PDU به صفر تنظیم شده باشد (Last):

۱- فیلد محتوای NLSP Userdata در SDT PDU به تمام NLSP Userdata قبلی که قسمتی از درخواست/ نشان NLSP-DATA یکسان است افزوده می‌شود و در پارامتر NLSP Userdat از یک نشان NLSP-DATA قرار داده می‌شود.

۲- اگر Param_Prot برابر TRUE باشد، درخواست تأیید NLSP در نشان NLSP-DATA باید نشان‌دهنده‌ی «تأیید دریافت درخواست شده» باشد. (اگر فیلد محتوای درخواست تأیید در SDT PDU حاضر باشد.)

۳- اگر Param_Prot برابر FALSE باشد، درخواست تأیید UN در نشان UN-DATA دریافت‌شده به پارامتر معادل در نشان NLSP-DATA رونوشت می‌شود.

۴- نشان NLSP-DATA به کاربر NLSP-DATA تحویل داده می‌شود.

۸-۷ کارکردهاي NLSP-DATA

۸-۷-۱ درخواست NLSP-DATA

در زمان دریافت یک درخواست NLSP-EXPEDITED DATA، اگر No_Header برابر TRUE باشد، NLSP Userdata باید مطابق آن‌چه در زیربند ۶-۴-۱-۲ توصیف شده است، کپسوله و در UN-Userdata از یک درخواست UN-EXPEDITED_DATA قرار داده شود. سپس باید درخواست UN-EXPEDITED-DATA به فراهم‌کننده‌ی خدمت UN تحویل داده شود.

در زمان دریافت یک درخواست NLSP-EXPEDITED DATA اگر No_Header برابر FALSE باشد:
الف- به‌عنوان یک مسأله محلی، NLSPE باید NLSP Userdata را قطعه‌بندی[1] کند. (اگر SA نیاز داشته باشد.)
ب- برای هر قطعه، یک SDT PDU باید مطابق آن‌چه در زیربند ۶-۴-۱-۱ توصیف شده است، تولید شود همراه با نوع داده «NLSP-EXPEDITED_DATA req/ind» بوده و دربرگیرنده‌ی موارد زیر است:

۱- قطعه‌ی NLSP Userdata؛

۲- پرچم Last/No Last که برای آخرین قطعه به صفر و برای تمام قطعه‌های ماقبل به ۱ تنظیم می‌شود.

۳- برای هر قطعه SDT PDU باید در پارامتر UN-Userdata از یک UN-EXPEDITED-DATA قرار داده شود.

پ- نخستینه درخواست UN-EXPEDITED-DATA برای هر قطعه باید به فراهم‌کننده خدمات UN عبور داده شود.

یادآوری– هنگام استفاده از SDT PDU، به‌دلیل اینکه کارکرد کپسوله‌سازی ممکن است اندازه‌ی داده را گسترش دهد، اندازه-ی محدود شده‌ی فیلد Userdata ممکن است نیازمند این باشد که داده‌ی پیشتازی محافظت‌شده هنگام گذر از شبکه اصلی، بیشتر قطعه‌بندی شود.

۸-۷-۲ نشان UN-EXPEDITED-DATA

در زمان دریافت یک نشان UN-EXPEDITED-DATA اگر No_Header برابر TRUE باشد، در این‌صورت UN Userdata باید مطابق آن‌چه در زیربند ۶-۴-۲-۲ توصیف شده است، واکپسوله شود. این در NLSP-Userdata از یک نشان NLSP-XPEDITED-DATA قرار داده می‌شود. آنگاه باید نشان NLSP-EXPEDITED-DATA به فراهم‌کننده خدمت NLSP تحویل داده شود.

در هنگام دریافت یک نشانه UN-EXPEDITED-DATA، اگر No_Header برابر FALSE باشد، در این‌صورت:

یادآوری – هنگام استفاده از SDT PDU، به دلیل اینکه کارکرد کپسوله‌سازی می‌تواند اندازه‌ی داده را گسترش دهد، اندازه‌ی محدودشده‌ی فیلد Userdata ممکن است نیازمند این باشد که SDT PDU ، قبل از اینکه به‌طور کامل پردازش شود از چندین درخواست NLSP-EXPEDITED-DATA هم‌گذاری مجدد شود.

الف- SDT PDU در UN Userdata باید مطابق آن‌چه در زیربند ۶-۴-۲-۱ توصیف شده است، وارسی شود. باید وارسی شود که نوع داده در SDT PDU، NLSP-EXPEDITED Data req/ind باشد.
ب- اگر پرچم Last/Not Last در SDT PDU به ۱ تنظیم شده باشد (Not Last)، فیلد محتوای NLSP Userdata در SDT PDU به تمام NLSP Userdataهای قبلی که قسمتی از درخواست/نشان

1 - Segmentation

NLSP-EXPEDITED-DATA یکسان، است و برای استفاده بعدی به‌وسیله‌ی NLSPE نگهداری شده است، افزوده می‌شود.

پ- اگر پرچم Last/Not Last در SDT PDU به صفر تنظیم شده باشد (Last)،:

۱- فیلد محتوای NLSP Userdata در SDT PDU به تمام NLSP Userdataهای قبلی که قسمتی از درخواست/ نشان NLSP-EXPEDITED-DATA است، افزوده شده و در پارامتر NLSP Userdata از یک نشان NLSP-EXPEDITED-DATA قرار داده می‌شود.

۲- نخستینه‌ی خدمت نشان NLSP-EXPEDITED-DATA به کاربر NLSP تحویل داده می‌شود.

۸-۸ کارکردهای تنظیم مجدد (RESET)

NLSPها یا رویدادهای مرتبط با UN-RESET که در زیر فهرست شده‌اند، بر هر تبادل CSC-PDU، تبادل SA-P، یا تبادل ارزیابی در جریان، مقدم[1] هستند.

۸-۸-۱ درخواست NLSP-RESET

در زمان دریافت یک درخواست NLSP-RESET، یک درخواست UN-RESET باید با مقادیر پارامتر یکسان صادر شود.

هر NLSP-Userdata قطعه‌بندی‌شده‌ای که تحت رویه‌هایی که در زیربندهای ۸-۶ یا ۸-۷ توصیف شده‌اند، نگه داشته شده باید دور انداخته شود.

NLSP باید منتظر یک تأیید UN-RESET که در زیربند ۸-۸-۲ توصیف شده است یا یک درخواست NKSP-DISCONNECT، یا یک نشان UN DISCONNECT که در زیربند ۸-۱۰ توصیف شده است، بماند. NLSPE تمام UN-DATA و نخستینه‌های UN-DATA-ACKNOWLEDGE را تا زمانی که یک تأیید UN-RESET یا DISCONNECT دریافت شود، دور می‌اندازد.

۸-۸-۲ تأیید UN-RESET در ادامه‌ي درخواست NLSP-RESET

در زمان دریافت تأیید UN-RESET، به دنبال یک درخواست NLSP-RESET که در زیربند ۸-۸-۱ توصیف شده است، باید یک تأیید NLSP-RESET با مقادیر پارامتر مشابه صادر شود.

یادآوری– ممکن است لازم باشد که برخی سازوکارهای امنیتی دوباره راه‌اندازی شوند، چون ممکن است که داده مفقود شده باشد. به‌ویژه، سازوکارهای دنباله یکپارچگی باید توانایی جلوگیری از حملات بازپخش را حتی بعد از مفقود شدن داده داشته باشند. این امر می‌تواند با استفاده از تبادل CSC-PDU که در زیر توصیف شده است، به‌دست آید.

اگر راه‌انداز صفت SA برابر TRUE باشد، در این‌صورت NLSPE باید یک تبادل CSC را آن‌گونه که در زیربند ۸-۱۲-۱ توصیف شده است، راه‌اندازی کند. در غیر این‌صورت NLSPE باید منتظر UN-DATA که دربرگیرنده‌ی یک CSC-PDU است (همان‌طورکه در زیربند ۸-۱۲-۲ توصیف شده است) بماند.

1- Pre-empts

۸-۸-۳ نشان UN-RESET

در زمان دریافت یک نشان UN-RESET در طی رویه‌های برقـراری اتصال NLSP مطابق آن‌چه در زیربنـد ۸-۵ توصیف شده است، یک UN-DISCONNECT و نشان NLSP-DISCONNECT باید در انطباق با خدمت شبکه‌ی OSI صادر شود و رویه‌های برقراری اتصال لغو می‌شوند.

در زمان دریافت یک نشان UN-RESET دنباله‌رو تکمیل برقراری اتصال NLSP:

۱- یک نشان NLSP-RESET باید با مقادیر پارامتر یکسان صادر شود.

۲- تمام NLSP-Userdataهای قطعه‌بندی‌شده که تحت رویه‌های توصیف شده در زیربندهای ۸-۶ یا ۸-۷ نگه‌داری شده‌اند، باید دور انداخته شوند.

۳- NLSPE باید منتظر یک پاسخ NLSP-RESET که در زیربند ۸-۸-۴ توصیف شده یا یک درخواست NLSP-DISCONNECT یا یک نشان UN DISCONNECT که در زیربند ۸-۱۰ توصیف شده است، بماند. تا زمانی که NLSPE یک پاسخ NLSP-RESET یا DISCONNECT دریافت کند، تمام UN-DATA و نخستینه‌های UN-DATA-KNOWLEDGE را دور می‌اندازد.

۸-۸-۴ پاسخ NLSP-RESET دنباله‌روی نشان UN-RESEST

در زمان دریافت یک پاسخ NLSP-RESET که دنباله‌رو یک نشان UN-RESET است و در زیربند ۸-۸-۳ توصیف شده است، یک پاسخ UN-RESET باید صادر شود.

یادآوری - ممکن است لازم باشد که برخی سازوکارهای امنیتی دوباره راه‌اندازی شوند، چون ممکن است که داده مفقود شده باشد. به‌ویژه، سازوکارهای دنباله یکپارچگی باید توانایی جلوگیری از حملات بازپخش را حتی بعد از مفقود شدن داده داشته باشند. این امر می‌تواند با استفاده از تبادل CSC-PDU که در زیر توصیف شده است، به‌دست آید.

اگر راه‌انداز صفت SA برابر TRUE باشد، NLSPE باید یک تبادل CSC را مطابق آن‌چه در زیربند ۸-۱۲-۱ توصیف شده است، راه‌اندازی کند. درغیر این‌صورت، NLSPE باید منتظر یک UN-DATA که در برگیرنده‌ی یک CSC-PDU است، بماند. (همان‌طورکه در زیربند ۸-۱۲-۲ توصیف شده است.)

۸-۸-۵ راه‌اندازی تنظیم مجدد توسط NLSP

در زمان تنظیم مجدد به‌علت یک رویداد مرتبط به پروتکل NLSP (برای مثال یک شکست وارسی که در زیربند ۸-۴ توصیف شده است) خواهیم داشت:

الف- تمام NLSP-Userdataهای قطعه‌بندی‌شده که تحت رویه‌هایی توصیف شده در زیربندهای ۸-۶ و ۸-۷ نگه‌داشته شده‌اند، باید دور انداخته شود.

ب- یک نشان NLSP-RESET باید به کاربر خدمت NLSP همراه با راه‌انداز NLSP و دلیل NLSPی که به مقداری تنظیم شده‌اند که به‌صورت محلی تعیین شده، تحویل داده شود.

پ- یک درخواست UN-RESET باید به فراهم‌کننده خدمت UN همراه با دلیل UNی که به مقداری تنظیم شده‌است که به‌صورت محلی تعیین شده، تحویل داده شود.

ت- NLSPE باید منتظر یک پاسخ NLSP-RESET که در زیربند ۸-۸-۶ توصیف شده است و یک تأیید UN-RESET که در زیربند ۸-۸-۷ توصیف شده است، بماند. همچنین ممکن است یک درخواست NLSP-DISCONNECT یا یک نشان UN DISCONNECT که در زیربند ۸-۱۰ توصیف شده است، دریافت شود.

ث- NLSPE باید تمام UN-DATA و نخستینه‌های UN-DATA-KNOWLEDGE را تا زمانی که یک تأیید UN-RESET یا هر DISCONNECTای دریافت شود، دور بریزد.

ج- NLSPE باید تمام UN-DATA و نخستینه‌های UN-DATA-KNOWLEDGE را تا زمانی که یک پاسخ NLSP-RESET یا هر DISCONNECTای دریافت شود، دور بریزد.

۸-۸-۶ پاسخ NLSP-RESET در ادامه‌ي یک تنظیم مجدد راه‌اندازی شده توسط NLSP

هیچ عملیات اضافی بر روی NLSP-RESET دنباله‌رو یک تنظیم مجدد راه‌اندازی‌شده توسط NLSP نیاز نیست.

۸-۸-۷ تأیید UN-RESET در ادامه یک تنظیم مجدد راه‌اندازی شده توسط NLSP

یادآوری– ممکن است نیاز باشد که برخی از سازوکارهای امنیتی دوباره راه‌اندازی شود، به دلیل آن که داده‌ها ممکن است مفقود شده باشند. به‌ویژه، سازوکارهای ترتیب‌دهی یکپارچگی باید بتوانند از حملات بازپخش، حتی بعد از مفقود شدن داده‌ها، جلوگیری کنند. این امر می‌تواند با استفاده از تبادل CSC-PDU به‌دست آید که در زیر توصیف شده است.

در یک تأیید UN-RESET که دنباله‌رو یک تنظیم مجدد راه‌اندازی‌شده توسط NLSP است، اگر راه‌انداز صفت SA برابر TRUE باشد، NLSPE باید یک تبادل CSC را آغاز کند که در زیربند ۸-۱۲-۱ توصیف شده است. درغیر این‌صورت، NLSPE باید منتظر UN-DATAای که دربرگیرنده‌ی یک CSC-PDU که در زیربند ۸-۱۲-۲ توصیف شده است، بماند.

۸-۹ NLSP-DATA ACKNOWLEDGE

۸-۹-۱ درخواست NLSP-DATA-ACKNOWLEDGE

در زمان دریافت یک درخواست NLSP-DATA-ACKNOWLEDGMENT، اگر No_Header برابر TRUE باشد یا Param_Prot برابر FALSE باشد، در این‌صورت یک درخواست NLSP-DATA-ACKNOWLEDGMENT به فراهم‌کننده خدمت UN تحویل داده می‌شود.

در زمان دریافت یک NLSP-DATA-ACKNOWLEDGMENT، اگر No_Header برابر FALSE و Param_Prot برابر TRUE باشد:

الف- همان‌طورکه در زیربند ۶-۴-۱-۱ توصیف شده است، یک SDT PDU باید همراه با نوع داده «NLSP-DATA-ACKNOWLEDGMENT req/ind» تولید شود که دربرگیرنده‌ی هیچ درج محتوای اضافی نیست.

ب- یک SDT PDU باید به‌عنوان UN-Userdata در یک نخستینه درخواست UN-DATA به فراهم‌کننده خدمت UN تحویل داده شوند.

۸-۹-۲ NLSP-DATA-ACKNOWLEDGE محافظت‌شده در نشان UN-DATA

اگر یک SDT PDU در نشان UN-DATA با نوع داده تنظیم‌شده به NLSP-DATA-ACKNOWLEDGMENT دریافت شده باشد همان‌طورکه در زیربند ۸-۶-۲، قسمت ث توصیف شده است، در این‌صورت:

الف- باید وارسی شود که SDT PDU شامل هیچ فیلد محتوای مرتبط با پارامترهای خدمت NLSP نباشد؛

ب- یک نشان NLSP-DATA-ACKNOWLEDGMENT باید به کاربر NLSP تحویل داده شود.

۸-۹-۳ نشان NLSP-DATA-ACKNOWLEDGE

در زمان دریافت یک UN DATA-ACKNOWLEDGMENT:

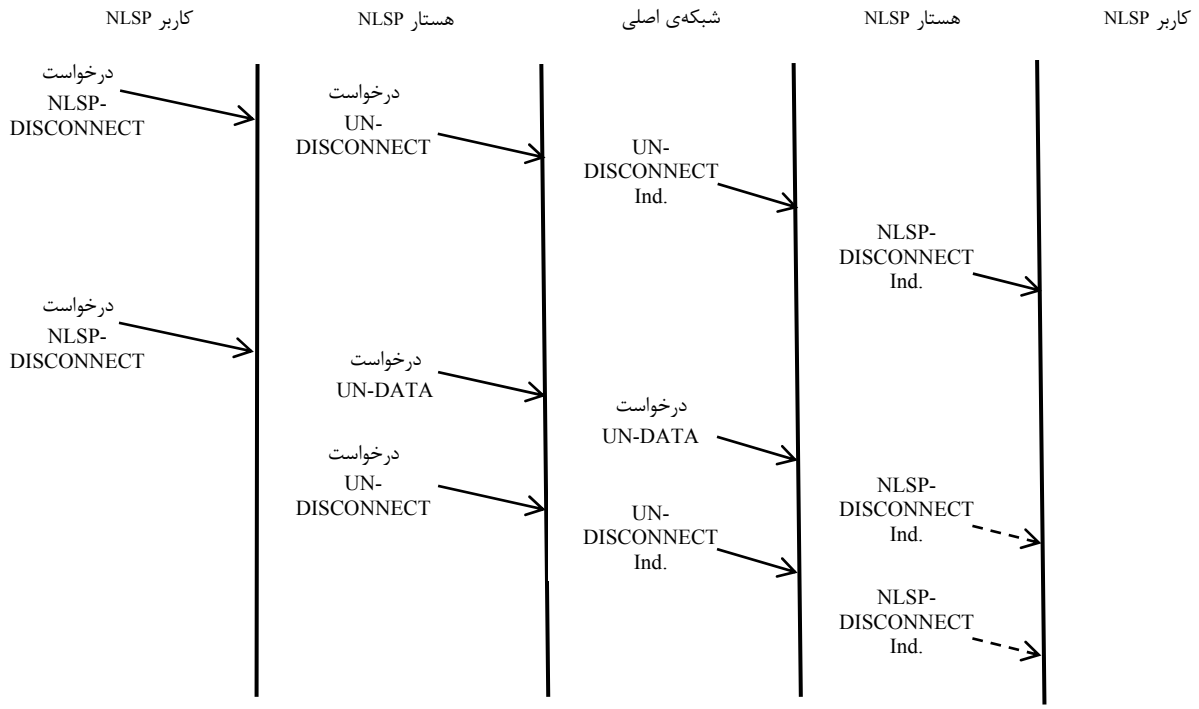
الف- NLSPE باید وارسی کند که No_Header برابر TRUE یا Param_Prot برابر FALSE باشد.

ب- یک نشان NLSP-DATA-ACKNOWLEDGMENT باید به کاربر NLSP تحویل داده شود.

۸-۱۰ NLSP-DISCONNECT

هر یک از رویدادهای مرتبط با NLSP یا UN-DISCONNECT که در زیر فهرست شده است بر هر تبادل CSC-PDU، تبادل SA-P یا تبادل آزمایشی که در حال انجام است، تقدم دارد.

رویه‌ها برای قطع NLSP توسط کاربر در شکل ۸-۴ نشان داده شده است.



شکل ۸-۴ - نمودار دنباله زمانی نخستینه خدمت برای NLSP-DISCONNECT

یادآوری– ممکن است که NLSP DISCONNECT در هر یک از نقاط نشان داده شده، رخ دهد.

۸-۱۰-۱ درخواست NLSP-DISCONNECT

در زمان دریافت یک درخواست NLSP-CONNECT درطی رویه‌های برقراری اتصال NLSP که در زیربند ۸-۵ توصیف شده است، یک درخواست UN-DISCONNECT باید در تطابق با خدمت شبکه OSI (یعنی اگر برقراری یک اتصال UN شروع شده باشد) صادر شود و رویه‌های برقراری اتصال لغو شوند. اگر Protect_Connect_Params برابر TRUE باشد، پارامترهای هر درخواست UN-DISCONNECT باید به‌صورت محلی تعیین شود در غیر این‌صورت پارامترهای درخواست NLSP-DISCONNECT باید درتمام پارامترهای درخواست UN-DISCONNECT معادل رونوشت شوند.

یادآوری– اگر یک درخواست NLSP-DISCONNECT در طی برقراری اتصال رخ دهد و Protect_Connect_Params انتخاب شده باشد، پارامترهای درخواست NLSP-CONNECT دور انداخته خواهد شد.

در زمان دریافت یک درخواست NLSP-DISCONNECT، به دنبال برقراری اتصال NLSP:

الف- اگر Protect_Connect_Params برابر TRUE باشد و No_Header برابر TRUE باشد، هر یک از NLSP Userdataها باید مطابق آن‌چه در زیربند ۶-۴-۱-۲ توصیف شده است، در کپسول گذاشته شوند. این در UN-Userdata مربوط به یک درخواست UN-DISCONNECT قرار داده می‌شود. بقیه پارامترهای درخواست NLSP-CONNECT از پارامترهای درخواست UN-DISCONNECT معادل رونوشت می‌شوند.

ب- اگر Protect_Connect_Params برابر TRUE، No_Header برابر FALSE و Param_Prot برابر TRUE باشد، در این‌صورت یک SDT PDU شامل تمام پارامترهای درخواست NLSP-DISCONNECT که در زیربند ۶-۴-۱-۱ توصیف شده است همراه با نوع داده «NLSP-DISCONNET req/ind» است، تولید می‌شود. این در UN-Userdata قرار داده شده است. بقیه پارامترهای UN-DISCONNECT به‌صورت محلی تعیین شده‌اند.

پ- اگر NLSP Userdata حاضر باشد، Protect_Connect_Params برابر TRUE، No_Header برابر FALSE و Param_Prot برابر FALSE باشد، در این‌صورت یک SDT PDU تولید می‌شود که شامل NLSP Userdata که در زیربند ۶-۴-۱-۱ توصیف شده و همراه با نوع داده «NLSP-DISCONNET req/ind» است. این در UN-Userdata قرار داده شده است. بقیه پارامترهای درخواست NLSP-DISCONNECT از طریق پارامترهای درخواست UN-DISCONNECT معادل رونوشت می‌شوند.

ت- اگر Protect_Connect_Params برابر FALSE باشد، تمام پارامترهای NLSP-DISCONNECT به پارامترهای درخواست UN-DISCONNECT معادل رونوشت می‌شوند.

یادآوری- فرض می‌شود محدودیت‌هایی که به طول NLSP Userdata اعمال می‌شود، به UN Userdata نیز اعمال شود.

ث- در صورت پیروی از قسمت‌های ب یا پ، پارامتر UN-Userdata به‌دست آمده بزرگتر از بیشترین طول داده UN-Userdata مربوط به درخواست UN-DISCONNECT است، در نتیجه این باید در یک پارامتر UN-Userdata درخواست UN-DATA فرستاده شده و به فراهم‌کننده‌ی خدمت UN تحویل داده شود. UN-Userdata در درخواست UN-DISCONNECT باید خالی باشد.

یادآوری– یک پیاده‌سازی باید منتظر بماند این UN-DATA قبل از اعلام UN-DISCONNECT، شبکه اصلی را پیمایش کند، آن‌گونه که در پارگراف ذیل توصیف شده است. مدت زمان این انتظار به‌صورت محلی تعیین شده است.

ج- یک درخواست UN-DISCONNECT باید با مجموعه پارامترهایی که در بالا توصیف شد، فرستاده شود.

۸-۱۰-۲ NLSP-DISCONNECT محافظت‌شده در نشان UN-DATA

اگر یک SDT PDU در نشان UN-DATA با نوع داده تنظیم‌شده روی NLSP-DISCONNECT دریافت شود، همان‌گونه که در زیربند ۸-۶-۲ قسمت ت- توصیف شد:

الف- NLSPE وارسی می‌کند که Protect_Connect_Params برابر TRUE و No_Header برابر FALSE باشد؛

ب- هر فیلد محتوا شامل پارامترهای خدمت NLSP، به پارامترهای NLSP DISCONNECT معادل رونوشت می‌شود و آغازگر NLSP به کاربر NS تنظیم می‌شود.

پ- NLSPE پارامترهای NLSP-DISCONNECT که مطابق بالا تنظیم شده‌اند را نگه می‌دارد و منتظر یک نشان UN-DISCONNECT می‌ماند یا بلافاصله یک نشان NLSP-DISCONNECT را صادر می‌کند. این انتخاب یک تصمیم محلی است.

۸-۱۰-۳ نشان UN-DISCONNECT

در زمان دریافت یک نشان UN-DISCONNECT در طول رویه‌های برقراری اتصال NLSP مطابق آن‌چه در زیربند ۸-۵ توصیف شد، باید یک نشان NLSP-DISCONNECT در انطباق با خدمت شبکه OSI صادر شود و رویه‌های برقراری اتصال لغو شوند. پارامترهای نشان UN-DISCONNECT باید در سراسر پارامترهای معادل هر نشان NLSP-DISCONNECT رونوشت شوند یا اگر Protect_Connect_Params برابر TRUE باشد، مطابق آن‌چه به‌صورت محلی تعیین شده است تنظیم شوند.

در غیر این‌صورت، برای یک نشان UN-DISCONNECT به دنبال برقراری اتصال NLSP با UN Userdata غیر خالی:

الف- اگر Protect_Connect_Params برابر TRUE و No-Header برابر TRUE باشد، آنگاه باید Userdata UN مطابق آن‌چه در زیربند ۶-۴-۲-۲ توصیف شد واکپسوله شود. نتیجه در NLSP Userdata مربوط به نشان NLSP-DISCONNECT قرار داده می‌شود. دیگر پارامترهای نشان NLSP-DISCONNECT باید به پارامترهای معادل نشان UN-DISCONNECT تنظیم شوند.

ب- اگر Protect_Connect_Params برابر TRUE، No-Header برابر FALSE و Param-Port برابر TRUE باشد آنگاه باید SDT PDU در UN Userdata مطابق آن‌چه در زیربند ۶-۴-۲-۱ توصیف شد وارسی شود. باید وارسی شود که نوع داده NLSP-DISCONNECT req/ind باشد. هر فیلد محتوای مرتبط با پارامترهای NLSP-DISCONNECT به این پارامترها رونوشت می‌شوند.

پ- اگر Protect_Connect_Params برابر TRUE، No-Header برابر FALSE و Param-Prot برابر FALSE باشد آنگاه باید SDT PDU در UN Userdata مطابق آن‌چه در زیربند ۶-۴-۲-۱ توصیف شد وارسی شود. باید وارسی شود که نوع داده NLSP-DISCONNECT باشد. باید حضور فیلد محتوای داده‌ی

کاربر وارسی شود و آنگاه به NLSP Userdata مربوط به نشان NLSP-DISCONNECT رونوشت شود. دیگر پارامترهای نشان UN-DISCONNECT به پارامترهای نشان NLSP-DISCONNECT معادل رونوشت می‌شوند.

ت- اگر Protect_Connect_Params برابر FALSE باشد آنگاه همه‌ی پارامترهای نشانه UN-DISCONNECT به پارامترهای نشان NLSP-DISCONNECT معادل رونوشت می‌شوند.

ث- باید نشان NLSP-DISCONNECT به کاربر NLSP تحویل داده شود.

در غیر این‌صورت، برای نشان UN-DISCONNECT به دنبال برقراری اتصال NLSP با NLSP Userdata خالی:

الف- اگر NLSPE در انتظار یک نشان UN-DISCONNECT دنباله‌رو یک NLSP-DISCONNECT محافظت‌شده در نشان UN-DATA باشد (به زیربند ۸-۱۰-۲ قسمت پ مراجعه شود) آنگاه باید فیلدهای پارامتر NLSP محافظت‌شده در نشان NLSP-DISCONNECT قرار داده شوند. دیگر پارامترهای نشان NLSP-DISCONNECT باید به پارامترهای معادل نشان UN-DISCONNECT تنظیم شوند.

ب- در غیر این‌صورت، باید پارامترهای نشان UN-DISCONNECT به پارامترهای نشان NLSP-DISCONNECT معادل رونوشت شوند.

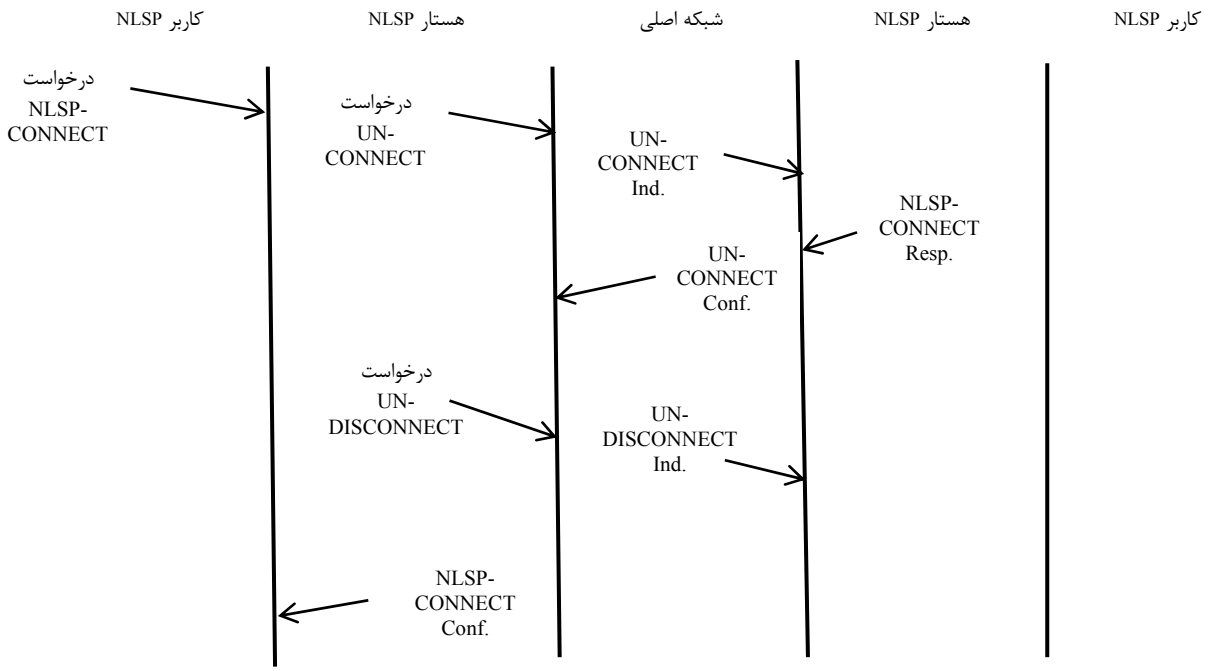
پ- باید نشان NLSP-DISCONNECT به کاربر NLSP تحویل داده شود مگر اینکه یکی پیش از این صادر شده باشد.

صفات SA ممکن است به دنبال هر UN-DISCONNECT اگر Retain-On_ Disconnect برابر FALSE باشد، به‌صورت محلی صفر شوند.

۸-۱۰-۴ قطع اتصال آغاز شده به‌وسیله NLSP

در صورت شکست یک SA-P یا هر وارسی دیگری، نشان‌های NLSP-DISCONNECT و درخواست‌های UN-DISCONNECT به کاربر NLSP و شبکه‌ی اصلی آن‌طورکه در زیربند ۸-۴ تعریف شده، تحویل داده می‌شوند.

شکل ۸-۵ یک مثال گویا از قطع اتصال راه‌اندازی‌شده توسط NLSP به دلیل SA-P ناموفق است.



شکل ۸-۵ - قطع اتصال راه‌اندازی شده توسط NLSP به دلیل SA-P ناموفق

۸-۱۱ کارکردهای دیگر NLSP-CO

رویه‌های زیر در رویدادهای زمانی یا دیگر رویدادهای خارجی راه‌اندازی می‌شوند.

۸-۱۱-۱ تغییر صفات-SA پویا

ممکن است که NLSPE صفات SA پویا را (به پیوست چ مراجعه شود) در هر زمانی در طول دوره‌ی حیات یک اتصال تغییر دهد. هر تغییری به صفات SA پویا نباید خدمات امنیتی فراهم‌شده را تغییر بدهد. این باید از طریق تبادل CSC-PDUها یا یک تبادل SA-P (یا با استفاده از SA-PDUها یا با استفاده از SDT PDUها با نوع داده محتوای پروتکل SA) در UN-DATA Userdata یا به‌وسیله‌ی ابزارهای خارجی حاصل شود. کاربر NLSP متوجه این تبادل نخواهد شد و هیچ نخستینه NLSP برای فراخوانی آن تعریف نشده است.

یادآوری– برای مثال، این تبادل می‌تواند در طی یک اتصال به‌صورت منظم رخ دهد (برای مثال، هر ساعت یا هر ۱۰ ۰۰۰ PDU داده‌ی امن) تا کلیدها را مبادله کند.

زمانی‌که انتقال داده با No_Header انجام می‌شود، یک UN-RESET باید قبل از مبادله‌ی CSC-PDUها که در زیربند ۸-۸-۵ تعریف شده است، فرستاده شود.

رویه‌های تبادل CSC-PDU باید مطابق آن‌چه در زیربند ۸-۱۲ توصیف شده است باشند. یک SA-P نمونه که شامل رویه‌هایی برای تغییر صفات SA است، در پیوست پ ارائه شده است.

۸-۱۱-۲ تبادل آزمون امنیتی

این رویه‌ها باید برای آزمون عملیات جنبه‌های رمزنگاشتی یک SA استفاده شود.

این رویه‌ها تنها در حالت‌هایی می‌توانند فراخوانی شوند که نخستینه‌های NLSP-DATA می‌توانند در UN-DATA فرستاده شوند. (یعنی بعد از اینکه برقراری اتصال NLSP کامل شد، قبل از هر رویه قطع اتصال و نه در طی رویه‌های تنظیم مجدد)
تبادل‌های DISCONNECT، RESET، CSC-PDU یا تبادل SA-P، بر یک مبادله‌ی آزمایشی مقدم هستند.

یادآوری– استفاده از این امکان به‌صورت محلی معین می‌شود. حالت‌های امکان‌پذیر کاربرد عبارتند از:
الف- استفاده‌نشده؛
ب- به دنبال تبادل کلیدها؛
پ – به‌صورت دوره‌ای، در یک زمان معین محلی.

۸-۱۱-۲-۱ فراخوانی تبادل آزمایشی

در زمان فراخوانی تبادل آزمایشی:
الف- یک فیلد داده‌ی آزمون باید ایجاد شود که پرچم جهت[1] آن به ۰ تنظیم شده باشد و داده آزمون آن به داده تصادفی تنظیم شده باشد؛
ب- یک SDT PDU آنگونه که در زیربند ۶-۴-۱-۱ توصیف شده است، باید تولید شود که نوع داده‌ی آن «غیرمرتبط به هیچ یک از نخستینه‌های خدمت NLSP» و دربرگیرنده‌ی فیلد داده‌ی آزمون است؛
پ- این PDU باید در UN-DATA UN-Userdata با تأیید دریافت UN که نشان‌دهنده‌ی «تأیید دریافت مورد نیاز نیست» است، فرستاده شود.

۸-۱۱-۲-۲ UN-Data با SDT PDU دربرگیرنده‌ی داده‌ی آزمون

در زمان دریافت UN-DATA دربرگیرنده‌ی یک SDT PDU با نوع داده که به صفر تنظیم شده (نامرتبط با هیچ یک از نخستینه‌های خدمت NLSP) آن‌گونه که در زیربند ۸-۶-۲، قسمت ب توصیف شده است، اگر SDT PDU دربرگیرنده‌ی داده آزمون باشد، باید مطابق زیر پردازش شود:
الف- اگر پرچم جهت در فیلد داده آزمون صفر باشد، یک SDT PDU جدید باید همان‌گونه که در زیربند ۶-۴-۱-۱ توصیف شده، تولید شود که نوع داده‌ی آن «نامرتبط با هیچ یک از نخستینه‌های خدمت NLSP» و دربرگیرنده‌ی یک فیلد داده‌ی آزمون است که پرچم جهت آن ۱ و داده‌ی آن با داده‌ی تصادفی دریافتی تنظیم شده است.
ب- اگر پرچم جهت در داده آزمون ۱ باشد، آنگاه باید وارسی شود که داده‌ی آزمون دریافتی با داده آزمونی که از پیش فرستاده شده است، برابر باشد. اگر نه، NLSPE باید کارکردهای خطا را که در زیربند ۸-۴ تعریف شد، اجرا کند.

1 - Direction

۸-۱۱-۳ لت‌گذاری ترافیک

برای مخفی کردن حضور کاربر ممکن است نخستینه‌های UN-DATA اضافی در برگیرنده‌ی PDUهای انتقال داده امن فقط با لت‌گذاری ترافیک فرستاده شود.

تمام هستارهای NLSP باید توانایی دریافت PDUهای انتقال داده امن با چنین لت‌گذاری ترافیک را داشته باشند.

استفاده از این امکان با صلاح‌دید هستار NLSP محلی است و کاربر خدمت NLSP متوجه آن نمی‌شود.

۸-۱۱-۳-۱ فراخوانی لت‌گذاری ترافیک

در فراخوانی لت‌گذاری ترافیک:

الف- یک SDT PDU باید آن‌چنان‌که در زیربند ۶-۴-۱-۱ توصیف شده است، با نوع داده «غیرمرتبط به هیچ یک از نخستینه‌های خدمت NLSP»، که هیچ فیلد محتوای اضافی ندارد، (به‌جز آن‌هایی که به‌وسیله‌ی زیربند ۶-۴-۱-۱ مورد نیاز است) تولید شود.

ب- این PDU باید در UN-DATA UN-Userdata با تأیید دریافت UN که نشان‌دهنده‌ی «تأیید دریافت مورد نیاز نیست» است، فرستاده شود.

۸-۱۱-۳-۲ UN-DATA با SDT PDU بدون در برداشتن فیلدهای محتوای اضافی

در زمان دریافت UN-DATA دربرگیرنده‌ی یک SDT PDU که نوع داده آن به صفر تنظیم شده است (نامرتبط با هیچ یک از نخستینه‌های خدمت NLSP) آن‌گونه که در زیربند ۸-۶-۲، قسمت ب توصیف شده است، اگر SDT PDU شامل هیچ فیلد محتوا نباشد (به‌غیر از آن‌هایی که به‌صورت معمول در بند ۶ مورد نیاز است)، SDT PDU باید نادیده گرفته شود.

۸-۱۲ احراز هویت هستار همتا

رویه‌های تعریف شده در زیربندهای ۸-۱۲-۱ و ۸-۱۲-۲ ممکن است در موارد زیر فراخوانی شوند:

- به دنبال یک UN-RESET یا NLSP-RESET همان‌طورکه در زیربند ۸-۸ توصیف شده است و
- در فواصل زمانی که به‌صورت محلی تعیین شده‌اند،

برای انجام احراز هویت هستار همتا یا تغییر دادن صفات SA پویا.

تبادل CSC-PDUها در طی برقراری اتصال، در زیربند ۸-۵ توصیف شده است.

تا زمانی که تبادل CSC کامل شود، درخواست‌های NLSP-DATA یا NLSP-EXPEDITED-DATA نباید خدمت‌رسانی شوند.

هر نخستینه‌ی RESET یا DISCONNECT، مقدم بر تبادل CSC است.

۸-۱۲-۱ فراخوانی تبادل CSC

در فراخوانی تبادل CSC، یک CSC باید با موارد زیر ایجاد شود:

الف- پرچم‌های UNC-UND و SA-P صفر شوند؛

ب- فیلد SA-ID به Your_SA_ID تنظیم شود؛

پ- محتوا به اولین تبادل CSC آن‌چنان‌که برای رویه‌های مختص سازوکار مورد نیاز است، (مانند آن‌هایی که در زیربند ۱۰-۳ توصیف شده است) تنظیم می‌شود.

این CSC-PDU باید به UN-Userdata از یک UN DATA با «درخواست تأیید نیاز نیست» فرستاده شود.

NLSPE که تبادل CSC را فراخوانی می‌کند، باید منتظر یک UN-DATA که دربرگیرنده‌ی یک CSC-PDU است، بماند. به‌صورت تناوبی، تبادل CSC می‌تواند با یک UN-RESET یا NLSP-RESET که در زیربند ۸-۸ توصیف شده است، یا یک UN-DISCONNECT یا NLSP-DISCONNECT که در زیربند ۸-۱۰ توصیف شده است، pre-emted شود.

۸-۱۲-۲ UN-DATA دربرگیرنده‌ی یک CSC-PDU

در زمان دریافت UN-DATAی که دربرگیرنده‌ی یک CSC-PDU (چه راه‌انداز یا پاسخ‌دهنده به تبادل CSC) است، محتوا آن‌گونه که برای رویه‌های مختص سازوکاری که در زیربند ۱۰-۳ توصیف شده مورد نیاز است، وارسی می‌شود.

بسته به رویه‌های مختص سازوکار، NLSPE می‌تواند:

الف- با یک محتوای CSC-PDU بازگردد و نشان دهد تبادل CSC بیشتر، مورد نیاز است.

در حالتی که، پرچم‌های CSC-PDU UNC-UND و SA-P باید صفر شوند، SA-ID به Your_SA_ID تنظیم می‌شود و محتوا آن‌گونه که برای رویه‌های مختص سازوکار نیاز است، تنظیم می‌شود. CSC-PDU باید در UN-DATA Userdata فرستاده شود. NLSPE باید منتظر UN-DATA دیگری که دربرگیرنده‌ی یک CSC-PDU است، بماند. به‌صورت تناوبی، تبادل CSC می‌تواند به‌وسیله‌ی یک UN-RESET یا NLSP-RESET که در زیربند ۸-۸ توصیف شده است، یا یک UN-DISCONNECT یا NLSP-DISCONNET که در زیربند ۸-۱۰ توصیف شده است، pre-empted شود.

ب- یک محتوای CSC-PDU را بازگرداند و نشان‌دهد SDT PDU برای کامل کردن تبادل مورد نیاز است.

در حالتی که، پرچم‌های CSC UNC-UND و SA-P باید صفر باشند، SA-ID به Your_SA_ID تنظیم می‌شود و محتوا آن‌گونه که برای رویه‌های مختص سازوکار نیاز است، تنظیم می‌شود. CSC-PDU باید در UN-DATA Userdata فرستاده شود. NLSPE باید منتظر UN-DATA دیگری که دربرگیرنده‌ی یک CSC-PDU است (و به‌گونه‌ای که در زیربند ۸-۶ توصیف شده، پردازش می‌شود)، بماند. به‌صورت تناوبی، تبادل CSC می‌تواند به‌وسیله‌ی یک UN-RESET یا NLSP-RESET که در زیربند ۸-۸ توصیف شده، یا یک UN-DISCONNECT یا NLSP-DISCONNET که در زیربند ۸-۱۰ توصیف شده است، مقدم شود.

یادآوری ۱- فرض نمی‌شود که احراز هویت کامل است و در نتیجه درخواست‌های NLSP-DATA (یا NLSP EXPEDITED) نباید تا دریافت از یک SDT PDU، در این NLSPE پردازش شوند. این SDT PDU می‌تواند یا دربرگیرنده یک NLSP-DATA از کاربر NLSP راه دور باشد یا می‌تواند به هیچ یک از نخستینه‌های خدمت NLSP ربطی نداشته باشد.

یادآوری ۲- اگر No_Header برابر TRUE باشد، این گزینه پشتیبانی نمی‌شود.

پ- یک محتوای CSC-PDU را بازگرداند و تکمیل تبادل را نشان دهد.
در حالتی که، پرچم‌های CSC UNC-UND و SA-P باید صفر باشند، SA-ID به Your_SA_ID تنظیم می‌شود و محتوا آن‌گونه که برای رویه‌های مختص سازوکار نیاز است، تنظیم می‌شود. CSC-PDU باید در UN-DATA Userdata فرستاده شود.
ت- نشان دهد که در تکمیل تبادل CSC، یک SDT PDU باید فرستاده شود.
در هر حالت اگر درخواست NLSP-DATA (یا NLSP-EXPEDITED-DATA) منتظر فرستاده شدن است و No_Header برابر FALSE است، در این‌صورت باید مانند آن‌چه در زیربند ۸-۶ و ۸-۷ توصیف شده است، پردازش شود. در غیر این‌صورت، یک SDT PDU باید آن‌گونه که در زیربند ۶-۴-۱-۱ توصیف شده است، با نوع داده «نامرتبط به هیچ یک از نخستینه‌های خدمت NLSP»، که دربرگیرنده‌ی هیچ فیلد محتوایی نیست، (به جز آن‌هایی که به‌طور کلی در بند ۶ مورد نیاز هستند) ایجاد و در UN Userdata از نخستینه‌ی UN-DATA فرستاده شود.
ث- نشان دهد که تبادل CSC کامل است.
در حالتی که هیچ عمل بیشتری مورد نیاز نیست.

یادآوری ۳ – هیچ رویه عمومی برای حل تصادم بین دو تبادل CSC که در یک زمان راه‌اندازی می‌شوند، تعریف نشده است.

یادآوری ۴ – با سازوکار احراز هویتی که در بند ۱۰ تعریف شد، اگر استفاده از کارکردهای کپسوله‌سازی/واکپسوله‌سازی، مانند آن‌هایی که در بند ۱۱ معرفی شد، شامل ISNها نباشد، احراز هویت هستار همتا به‌صورت کامل فراهم نمی‌شود. علاوه بر این احراز هویت، اگر سازوکار کپسوله‌سازی No_Header (مانند آن‌هایی که در بند ۱۲ توصیف شده‌اند) استفاده شود، احراز هویت هستار همتا به‌طور کامل، فراهم نمی‌شود.

۹ مرور کلی سازوکارهای استفاده شده

بندهای ۹ تا ۱۲، سازوکارهای مخصوصی را تعریف می‌کنند که برای استفاده با پروتکل عمومی تعریف‌شده در بندهای ۱ تا ۸ هستند. این سازوکارها، تنها سازوکارهایی که می‌توانند برای فراهم کردن امنیت در NLSP عمومی استفاده شوند، نیستند. سازوکارهای دیگری نیز می‌توانند در آینده استاندارد شوند و این امکان برای سازوکارهای خصوصی وجود دارد که با NLSP استفاده شوند.

۹-۱ خدمات امنیتی و سازوکارها

NLSP-CL توسط سازوکارهای توصیف‌شده از خدمات امنیتی زیر (درصورتی‌که انتخاب شده باشند) پشتیبانی می‌کند:
الف- احراز هویت مبدأ داده – سازوکار استفاده‌شده برای فراهم کردن این خدمت، ICVها توأم با مدیریت کلید هستند.
ب- کنترل دسترسی - سازوکار استفاده‌شده برای فراهم کردن این خدمت، برچسب‌های امنیتی و/یا کنترل کلیدها و/یا استفاده از نشانی‌های احراز هویت‌شده هستند.
پ- محرمانگی بی‌اتصال - سازوکار استفاده‌شده برای فراهم کردن این خدمت، رمزگذاری است. این محافظت به‌صورت اختیاری، بسته به خدمات امنیتی انتخاب‌شده، شامل تمام پارامترهای خدمت NLSP می‌شود.

ت- محرمانگی جریان ترافیک- سازوکار استفاده‌شده برای فراهم کردن این خدمت، لت‌گذاری ترافیک و/یا پنهان‌کردن NLSP-addres است.

ث- یکپارچگی بی‌اتصال - سازوکار استفاده‌شده برای فراهم کردن این خدمت، یک ICV است. این محافظت به‌صورت اختیاری، بسته به خدمات امنیتی انتخاب‌شده، شامل تمام پارامترهای خدمت NLSP می‌شود.

NLSP-CO از خدمات امنیتی زیر (درصورتی‌که انتخاب شده باشند) توسط سازوکارهای توصیف‌شده پشتیبانی می‌کند:

الف- احراز هویت هستار همتا – سازوکار استفاده‌شده برای فراهم کردن این خدمت، یک تبادل از شماره‌های دنباله یکپارچگی رمزشده به همراه مدیریت کلید است.

ب- کنترل دسترسی - سازوکار استفاده‌شده برای فراهم کردن این خدمت، برچسب‌های امنیتی و/یا ازطریق کنترل کلیدها و/یا نشانی‌های احراز هویت‌شده هستند.

پ- محرمانگی اتصال - سازوکار استفاده‌شده برای فراهم کردن این خدمت، رمزگذاری است. این محافظت به‌صورت اختیاری شامل تمام پارامترهای اتصال NLSP می‌شود که وابسته به خدمات امنیتی انتخابی است.

ت- محرمانگی جریان ترافیک- سازوکار استفاده‌شده برای فراهم کردن این خدمت، لت‌گذاری ترافیک و/یا پنهان‌کردن نشانی است.

ث- یکپارچگی اتصال بدون بازگردانی - سازوکار استفاده‌شده برای فراهم کردن این خدمت، مقدار وارسی یکپارچگی و شماره‌های دنباله یکپارچگی است. این محافظت به‌صورت اختیاری شامل تمام پارامترهای اتصال NLSP می‌شود که وابسته به خدمات امنیتی انتخابی است.

۹-۲ کارکردهاي پشتیبانی‌شده

ویژگی ضروری سازوکار پشتیبانی‌شده به‌وسیله‌ی NLSP:

الف- یک کارکرد احراز هویت اتصال که از احراز هویت هستار همتا پشتیبانی می‌کند و مقادیر اولیه برای صفات SA «پویا» که از انتقال داده امن پشتیبانی می‌کند را برقرار می‌کند. این کارکرد تنها به‌وسیله‌ی NLSP-CO استفاده می‌شود.

ب- یک کارکرد کپسوله‌سازی مبتنی بر SDT PDU، که با استفاده از سازوکارهای زیر، از انتقال داده امن پشتیبانی می‌کند:

۱- شماره دنباله یکپارچگی؛

۲- لت‌گذاری برای محرمانگی جریان ترافیک، الگوریتم‌های یکپارچگی بستک[1]، و الگوریتم‌های رمزگذاری بستک،

۳- مقدار وارسی یکپارچگی؛

۴- رمزگذاری.

پ- یک کارکرد کپسوله‌سازی مبتنی بر شکل No_Header محافظت که از یک سازوکار رمزگذاری که طول داده را تغییر نمی‌دهد، استفاده می‌کند.

1 - Block

سازوکارها در ترتیبی که در بالا آورده شد، اجرا می‌شوند.

۱۰ کنترل امنیت اتصال (تنها NLSP-CO)

۱۰-۱ مرورکلی

رویه «کنترل امنیتی اتصال» از تبادل کنترل امنیتی اتصال (CSC) PDUها استفاده می‌کند تا:

الف- به‌صورت اختیاری، یک کلید رمزگذاری/یکپارچگی جدید را مشخص کند؛

ب- احراز هویت هستار همتا را انجام دهد؛

پ- یک عدد دنباله یکپارچگی را برقرار کند.

پشتیبانی برای یک سازوکار احراز هویت از طریق تبادل عددهای دنباله به‌وسیله‌ی این استاندارد ملی مشخص شده است. احراز هویت با استفاده از این سازوکار برای هستار راه‌انداز هنگامی که تبادل دو طرفه کامل شود، تکمیل خواهد شد. برای هستار پاسخ‌دهی، اگر یکپارچگی دنباله برای محافظت در مقابل حملات بازپخش (یعنی ISN برابر TRUE است) انتخاب شده باشد، احراز هویت تنها هنگام دریافت اولین SDT PDU از هستار راه‌انداز، کامل می‌شود.

۱۰-۲ صفات SA

صفات امنیتی زیر برای پشتیبانی رویه‌های کنترل امنیتی اتصال استفاده می‌شوند:

الف- *سازوکارهای انتخاب شده برای SA*:

احراز هویت: بولی

آیا قرار است از احراز هویت هستار همتا با استفاده از ISN رمزنگاری‌شده استفاده شود.

مقادیر این صفات توسط ASSR که خدمات امنیتی انتخاب‌شده در آن داده شده است، تعریف می‌شود.

ب- *صفات سازوکار توزیع کلید*:

kdm: حالت برای استفاده با این SA

مقدار این صفت توسط ASSR که خدمات امنیتی انتخاب‌شده در آن داده شده است، تعریف می‌شود.

این می‌تواند مقادیر زیر را داشته باشد:

kdm_mutual: توزیع به‌وسیله‌ی کلیدهای متقارن.

kdm_asymetric_single: توزیع با استفاده از کلید عمومی گیرنده‌ها.

kdm_asymmetric_double: توزیع با استفاده از هم کلیدهای عمومی دور و هم کلیدهای خصوصی محلی

kdm distributed: توزیع با استفاده از ارجاع به کلید از قبل توزیع‌شده یا کلید توزیع‌شده توسط راه‌کارهای دیگر.

kdm_other: از یک سازوکار توزیع که به‌صورت خصوصی تعریف شده، استفاده می‌شود.

پ- صفات سازوکار احراز هویت:

Auth_Alg: شناسه‌ی شئ که تحت ISO/IEC 9979 اختصاص یافته است.
مقدار این صفت باید توسط ASSR که خدمات امنیتی در آن داده شده است، تعریف شود.

Enc_Auth_Len: طول فیلد auth-data رمزگذاری در CSC-PDU.
مقدار این صفت باید توسط ASSR که خدمات امنیتی انتخاب‌شده در آن داده شده است، تعریف شود. Auth_Gen_Key: شکل محدودشده به‌وسیله‌ی ASSR
مقدار اولیه‌ی این صفت در زمان برقراری SA تنظیم می‌شود و می‌تواند در طی دوره‌ی حیات همبستگی تغییر کند.

Auth_Check_Key: شکل محدودشده به‌وسیله‌ی ASSR
مقدار اولیه‌ی این صفت در زمان برقراری SA تنظیم می‌شود و می‌تواند در طی دوره‌ی حیات همبستگی تغییر کند.

صفات زیر که به‌وسیله‌ی سازوکارهای انتقال داده امنیتی استفاده می‌شود می‌توانند توسط سازوکار احراز هویت اتصال برقرار شوند:

الف- صفات سازوکار ISN:

Data_My_ISN
Data_Your_ISN
Exp_My_ISN
Exp_Your_ISN

ب- صفات سازوکار رمزگذار:

Data_Enc_Key
Data_Dec_Key
Exp_Enc_Key
Exp_Dec_Key

پ- صفات سازوکار ICV:

Data_ICV_Gen_ISN
Data_ICV_Check_ISN
Exp_ICV_Gen_ISN
Exp_ICV_Check_ISN

یادآوری - صفات مختص سازوکار اضافی می‌توانند در نسخه‌های آتی این استاندارد ملی و برای سازوکارهای خصوصی مشخص شوند.

۳-۱۰ رویه‌ها

هستارهای NLSP، PDUهای کنترل امنیتی اتصال را در زمان برقراری اتصال یا به دنبال یک تنظیم مجدد یا در زمان دیگر رویدادهای زمان‌بندی‌شده به‌صورت خارجی مبادله می‌کنند تا:

الف- به‌صورت اختیاری، کلید یکپارچگی یا رمزگذاری را تعیین کنند؛

ب- احراز هویت هستار همتا را انجام دهند؛

پ- کلید دنباله‌ی یکپارچگی را ایجاد کنند.

احراز هویت هستار همتا ممکن است به‌صورت تعریف‌شده در زیر تأمین شود. اگر به یکپارچگی اتصال نیاز داشته باشیم، هر روش دیگری باید یک کلید دنباله‌ی یکپارچگی تحویل دهد.

کلید رمزگذاری/یکپارچگی به‌روش‌های زیر تعیین می‌شود:

الف- به‌وسیله‌ی یک نشانه که باید از کلید موجود استفاده شود.

ب- با فرستادن یک کلید جدید که با یک کلید مشترک رمزگذاری شده است.

پ- با فرستادن یک کلید جدید که با کلید عمومی دریافت‌کننده رمزگذاری شده است.

ت- با ارجاع به کلیدی که از پیش توزیع شده است.

یادآوری ۱ - اشتقاق کلید رمزگذاری میزان کمی از وارسی یکپارچگی را تأمین می‌کند که از بازپخش یک متن رمزگذاری‌شده که با کلید متفاوتی محافظت می‌شود جلوگیری می‌کند. الگوریتم اشتقاق کلید باید مختص هر الگوریتم رمزگذاری باشد تا از اشتقاق تصادفی کلیدهای ضعیف جلوگیری شود.

NLSP از یک روش احراز هویت هستار همتا مبتنی بر تبادل اعداد آغازین دنباله‌ی یکپارچگی (که با استفاده از یک کلید احراز هویت رمز شده‌اند)، استفاده می‌کند. این روش می‌تواند حتی درصورتی‌که اعداد دنباله برای خدمت یکپارچگی استفاده نشوند، به‌کار رود.

رویه‌های کنترل امنیت اتصال بر پایه‌ی تبادل دو PDUی CSC و PDUی انتقال داده‌ی امن هستند. (آن‌چنان‌که در زیر آمده است.)

یک PDUی CSC به‌وسیله‌ی راه‌انداز مبادله‌ی امنیتی آماده می‌شود:

الف- Auth-Data رمزگذاری‌شده که به یک مقدار انتخاب‌شده‌ی محلی مربوط به My-Initial-ISN و یک مقدار صفر برای Your-initial-ISN که هر دو با استفاده از یک Auth-Gen-Key رمزگذاری شده‌اند، تنظیم شده است. ISN انتخاب‌شده باید برای کلیدهای احراز هویت و یکپارچگی یکتا باشد؛

ب- اطلاعات کلید براساس نیازهای سازکارهای توزیع‌شده کلید تنظیم می‌شوند.

در زمان دریافت یک PDUی CSC به‌وسیله‌ی یک هستار NLSP که آغازگر مبادله‌ی CSCPDU نیست:

الف- Auth-Data رمزگذاری‌شده به‌وسیله‌ی Auth-Check-Key رمزگشایی می‌شود؛

ب- وارسی می‌شود که فیلد Your-Initial-Key صفر باشد؛

پ- صفات محلی SA، Data-Your-ISN و Exp-Your-ISN به فیلد دریافتی My-Initial-ISN تنظیم می‌شوند؛

ت- اطلاعات کلید براساس نیازهای سازکارهای توزیع کلید، پردازش می‌شوند.

سپس یک CSC-PDU توسط موارد زیر آماده می‌شود:

الف- Auth-Data رمزگذاری‌شده که به یک مقدار انتخاب‌شده‌ی محلی مربوط به My-Initial-ISN و Your-initial-ISN با مقدار دریافتی My-Initial-ISN تنظیم شده و هر دو با استفاده از یک Auth-Gen-Key رمزگذاری شده‌اند. ISN انتخاب‌شده باید برای کلیدهای احراز هویت و یکپارچگی یکتا باشد؛

ب- اطلاعات کلید براساس نیازهای سازکارهای توزیع کلید تنظیم می‌شوند.

در زمان رسیدن یک CSC PDU به راه‌انداز مبادله‌ی CSC :

الف- Auth-Data رمزگذاری‌شده به‌وسیله‌ی Auth-Check-Key رمزگشایی می‌شود؛

ب- فیلد Your-Initial-Key با فیلد My-Initial-ISN که از پیش فرستاده شده بود وارسی می‌شود؛

پ- صفات محلی SA، Data-Your-ISN و Exp-Your-ISN به فیلد دریافتی My-Initial-ISN تنظیم می‌شوند؛

ت- اطلاعات کلید براساس نیازهای سازوکارهای توزیع کلید، پردازش می‌شوند.

در ادامه‌ی وارسی موفقیت‌آمیز پاسخ، اگر هستار NLSP داده‌ی در حال انتظاری نداشته باشد و سازوکار ISN برای کپسوله‌سازی SDT PDU انتخاب شده باشد (به بند ۱۱ شود)، آنگاه یک PDUی انتقال داده‌ی امن که هیچ داده‌ای درون آن وجود ندارد ولی ISN را شامل می‌شود باید برای تکمیل احراز هویت فرستاده شود.

یادآوری ۲– SDT PDU می‌تواند حتی زمانی که داده منتظر تکمیل رویه‌های احراز هویت است، بدون نیاز به اجرای رویه‌های عادی انتقال داده فرستاده شود.

اگر احراز هویت با شکست مواجه شود، آنگاه بسته به تصمیم‌گیری محلی، همبستگی امنیتی ممکن است دوباره در داخل یا برون باند ایجاد شود و همچنین از رویه‌های بازیابی خطای توصیف‌شده در زیربند ۸-۴ استفاده شود.

۱۰-۴ فیلدهای CSC-PDU استفاده شده

فیلدهای محتوای CSC مختص سازوکار زیر که در زیربند ۱۳-۵-۶ تعریف شده است، به‌وسیله‌ی رویه‌های این بند استفاده می‌شوند:

الف- Auth-Data رمزگذاری‌شده؛

ب- اطلاعات کلید.

۱۱ کارکرد کپسوله‌سازی مبتنی بر SDT PDU

۱۱-۱ مرورکلی

NLSP-CL، و به‌صورت اختیاری NLSP-CO، از داده کاربر و اطلاعات کنترل پروتکل مرتبط با استفاده از یک کارکرد کپسوله‌سازی مبتنی بر SDT PDU محافظت می‌کنند. این بند چنین کارکرد کپسوله‌سازی را تعریف می‌کند. این کارکرد کپسوله‌سازی مبتنی بر چهار کارکرد است:

- ISN؛
- لت‌گذاری؛
- ICV؛ و

- رمزگذاری.

تصمیم برای به‌کارگیری یک کارکرد مخصوص باید مبتنی بر صفات SA باشد.
اگر شماره دنباله انتخاب شده باشد، یک فیلد ISN باید اضافه شود.

یادآوری ۱–انتظار نمی‌رود که سازوکار محافظت به همراه NLSP-CL استفاده شود.

اگر لت‌گذاری ترافیک انتخاب شده باشد، ممکن است یک فیلد لت‌گذاری ترافیک اضافه شود.
اگر از یک الگوریتم یکپارچگی بستک استفاده شود، ممکن است یک فیلد لت‌گذاری یکپارچگی اضافه شود.
اگر وارسی یکپارچگی انتخاب شده باشد، باید یک ICV محاسبه و به فیلدهای بالا اضافه شود.

یادآوری ۲– همچنین ICV می‌تواند برای فراهم کردن احراز هویت مبدأ داده استفاده شود.

اگر باید الگوریتم رمزگذاری بستک استفاده شود، ممکن است یک فیلد لت‌گذاری رمزگذاری اضافه شود.
اگر رمزگذار انتخاب شده باشد، فیلدهای بالا با استفاده از کلید رمزگذاری برای همبستگی امنیتی رمزگذاری می‌شوند.

رویه‌ای که در بالا توصیف شد، داده‌ی کاربر و دیگر پارامترهای پروتکل NLSP را جهت فراهم کردن محافظت برای انتقال روی یک شبکه، در کپسول می‌گذارد. در طرف راه دور، دریافت‌کننده‌ی یک PDU انتقال داده‌ی امن با معکوس‌کردن ترتیب رویه، محافظت را وارسی می‌کند.

۲-۱۱ صفات SA

الف- سازوکارهای انتخاب‌شده برای SA:

ISN: بولی
اعداد دنباله‌ی یکپارچگی که باید در هر رشته‌ی هشت‌تایی در کپسول گذاشته‌شده قرار داده شود.

Padd: بولی
لت‌گذاری در داخل رشته‌ی هشت‌تایی در کپسول گذاشته‌شده برای پشتیبانی سازوکار لت‌گذاری ترافیک.

ICV: بولی
یکپارچگی و/یا احراز هویت مبدأ داده‌ی محتوای رشته‌ی هشت‌تایی در کپسول گذاشته‌شده با استفاده از یک مقدار وارسی یکپارچگی.

Encipher: بولی
رمزگذاری یک رشته‌ی هشت‌تایی در کپسول گذاشته‌شده برای فراهم کردن محرمانگی.

مقادیر این صفات، توسط ASSR که خدمات امنیتی انتخاب‌شده در آن داده شده است، تعریف می‌شود.

ب- صفات سازوکار ISN:

ISN_Len: عدد صحیح

مقدار این صفت باید توسط ASSR که خدمات امنیتی انتخاب‌شده در آن داده شده است، تعریف شود.

Data_My_ISN: ISN برای آخرین داده‌ی عادی فرستاده شد.

Data_Your_ISN: ISN برای آخرین داده‌ی عادی دریافت شد.

Exp_My_ISN: ISN برای آخرین داده‌ی پیشتاز فرستاده شد.

Exp_Your_ISN: ISN برای آخرین داده‌ی پیشتاز دریافت شد.

مقدار اولیه‌ی این صفات «کلید» باید در زمان برقراری SA راه‌اندازی شود و می‌تواند درطی زمان حیات همبستگی تغییر کند.

یادآوری ۱– صفات ISN داده‌ی پیشتاز تنها به NLSP-CO قابل اعمال هستند.

پ- صفات سازوکار لت‌گذاری:

Traff_Padd: شکل آن به‌وسیله‌ی ASSR محدود شده است.

الزامات لت‌گذاری ترافیک.

ت- صفات سازوکار ICV:

ICV_Alg: شناسه‌ی شئ

مقدار این صفت توسط ASSR که خدمات امنیتی انتخاب‌شده در آن داده شده است، محدود شود. این صفت بر صفات مشخصی از سازوکار یکپارچگی مانند تولید منفرد و الگوریتم‌های وارسی، بردارهای راه‌اندازی و غیره دلالت دارد.

ICV_Blk: عدد صحیح

اندازه‌ی بستک پایه‌ای که الگوریتم ICV بر روی آن عمل می‌کند.

مقدار این صفت باید توسط ASSR که خدمات امنیتی انتخاب‌شده در آن داده شده است، محدود شود.

ICV_Len: عدد صحیح

طول خروجی سازوکار ICV.

مقادیر این صفت، توسط ASSR که خدمات امنیتی انتخاب‌شده در آن داده شده است، تعریف می‌شود. ضروری نیست که ICV_Len برابر ICV_Blk باشد.

Dara_ICV_Gen_Key: شکل آن به‌وسیله‌ی ASSR محدود می‌شود.

مرجع کلید تولید ICV برای داده‌ی معمولی.

Data_ICV_Check_Key: شکل آن به‌وسیله‌ی ASSR محدود می‌شود.

مرجع کلید وارسی ICV برای داده‌ی معمولی.

Exp_ICV_Gen_Key: شکل آن به‌وسیله‌ی ASSR محدود می‌شود.
مرجع کلید تولید ICV برای داده‌ی پیشتاز.

Exp_ICV_Check_Key: شکل آن به‌وسیله‌ی ASSR محدود می‌شود.
مرجع کلید وارسی ICV برای داده‌ی پیشتاز.
مقدار اولیه این صفات «کلید» باید در زمان برقراری SA تنظیم شود و می‌تواند درطی حیات همبستگی تغییر کند.

یادآوری ۲– صفات کلید داده‌ی پیشتاز تنها به NLSP-CO قابل اعمال هستند.

ث- صفات سازوکار رمزگذاری:

Enc_Alg: شناسه‌ی شئ که تحت ISO/IEC 9979 اختصاص یافته است
مقدار این صفت باید توسط ASSR که خدمات امنیتی انتخاب‌شده در آن داده شده است، محدود شود. این صفت بر صفات مشخصی از سازوکار رمزگذاری مانند شکل و طول فیلد همگام‌سازی، رمزگذاری مجزا و الگوریتم‌های رمزگشایی، راه‌اندازی و غیره دلالت دارد.

Enc_Blk: عدد صحیح
اندازه‌ی بستک الگوریتم رمزگذاری.
مقدار این صفت باید توسط ASSR که خدمات امنیتی انتخاب‌شده در آن داده شده است، محدود شود.

Dara_Enc_Key: شکل آن به‌وسیله‌ی ASSR محدود می‌شود.
مرجع کلید رمزگذاری برای داده‌ی معمولی.

Data_Dec_Key: شکل آن به‌وسیله‌ی ASSR محدود می‌شود.
مرجع کلید رمزگشایی برای داده‌ی معمولی.

Exp_Enc_Key: شکل آن به‌وسیله‌ی ASSR محدود می‌شود.
مرجع کلید رمزگذاری برای داده‌ی پیشتاز.

یادآوری ۳ – این Exp_Enc_Key تنها به‌وسیله‌ی NLSP-CO استفاده می‌شود.

Exp_Dec_Key: شکل آن به‌وسیله‌ی ASSR محدود می‌شود.
مرجع کلید رمزگشایی برای داده‌ی پیشتاز.

یادآوری ۴ - این Exp_Dec_Key تنها به‌وسیله‌ی NLSP-CO استفاده می‌شود.

مقدار اولیه‌ی این صفات «کلید» باید در زمان برقراری SA راه‌اندازی شود و می‌تواند درطی حیات همبستگی تغییر کند.

یادآوری ۵ – صفات مختص سازوکار اضافی می‌توانند در نسخه‌های آتی این استاندارد ملی و برای سازوکارهای خصوصی شناسایی شوند.

۳-۱۱ رویه‌ها

هنگامی که کپسوله‌سازی اتفاق می‌افتد، یک PDU باید به‌وسیله‌ی فیلدهایی که در ابتدا یا انتهای آن اضافه می‌شود، ایجاد شود. این فیلدها ممکن است اختیاری باشند. به یک PDU که به صورت کامل تشکیل نشده است به اصطلاح «فیلدهای موجود» می‌گوییم. در طی واکپسوله‌سازی، یک PDU باید به‌وسیله‌ی حذف فیلدها، تجزیه شود. یک PDU که به‌صورت جزیی تجزیه شده باشد، در زیر با عنوان «داده‌ی باقیمانده» اشاره شده است.

یادآوری ۱- فیلدهایی که قبل و بعد از PDU اضافه می‌شوند به‌منظور محدود کردن پیاده‌سازی NLSP نیست، بلکه برای مشخص کردن بدون ابهام پروتکل است.

یادآوری ۲- کارکرد کپسول‌گذاری از گزینه‌ی No_Header پشتیبانی نمی‌کند. این گزینه توسط رویه‌های تعریف شده در بند ۱۲ پشتیبانی می‌شود.

۱-۳-۱۱ کارکرد کپسوله‌سازی

SA-ID باید برای ارجاع به یک همبستگی امنیتی استفاده شود. اگر همبستگی امنیتی وجود نداشته باشد، باید خطای SA-not-available بازگردانده شود و مقدار رشته‌ی هشت‌تایی در کپسول گذاشته‌شده باید تعیین نشده باشد.

اگر ISN برابر TRUE باشد در این‌صورت:

الف- اگر (data-unit-type = normal) در این‌صورت Data_Your_ISN باید پیش‌برده شود و در فیلد محتوای عدد دنباله قرار داده شده و به فیلدهای موجود در Octet-String-Before-Encapsulation پیوست شود.

ب- اگر (data-unit-type = expedited) آنگاه Exp_Your_ISN باید پیش‌برده شود و در فیلد محتوای عدد دنباله قرار داده شده و به فیلدهای موجود در Octet-String-Before-Encapsulation پیوست شود.

یادآوری ۱- ISN ممکن است با افزایش یک عدد دنباله یا با انتخاب عدد بعدی از یک دنباله بدون-تکرار پیش‌برده شود. همچنین نشان‌های زمانی نیز می‌توانند به‌عنوان یک دنباله بدون تکرار قلمداد شوند.

یادآوری ۲- انتظار نمی‌رود که سازوکار ISN با NLSP-CL استفاده شود.

یادآوری ۳- Exp_My_ISN تنها به NLSP-CO قابل اعمال است.

اگر لت[1] برابر TRUE باشد، آنگاه مقدار و شکل لت‌گذاری که به‌صورت محلی به‌وسیله‌ی قواعد ASSR که به Traff_Padd اشاره دارد، تعیین شده است باید در یک فیلد محتوای لت‌گذاری ترافیک قرار داده شود و به فیلدهای موجود در **Octet-String-Before-Encapsulation** افزوده شود. اگر یک هشت‌تایی منفرد از لت‌گذاری مورد نیاز باشد، در این‌صورت فیلد محتوای لت‌گذاری هشت‌تایی منفرد باید استفاده شود.

1 - Pad

اگر **ICV** برابر **TRUE** باشد و **ICV_Blk > 1** باشد، آنگاه درصورت نیاز یک فیلد لت‌گذاری یکپارچگی باید به فیلدهای موجود افزوده شود، به‌نحوی که طول فیلدهای موجود با فیلد لت‌گذاری یکپارچگی (شامل فیلد محتوای محافظت‌شده)، مضرب صحیحی از اندازه بستك **ICV** (یعنی **ICV_Blk**) شود. سپس مقدار و شکل لت‌گذاری که به‌صورت محلی تعیین شده است، باید در فیلد محتوای لت یکپارچگی قرار داده شود. اگر یک هشت‌تایی منفرد از لت‌گذاری مورد نیاز باشد، آنگاه فیلد محتوای لت هشت‌تایی منفرد باید استفاده شود. مقدار طول محتوا باید با مقدار لت‌گذاری اضافه‌شده، افزایش یابد.

یک طول محتوا باید قبل از فیلدهای موجود قرار داده شود. طول تمام فیلدهای موجود باید تعیین و در طول محتوا قرار داده شود.

اگر ICV برابر TRUE باشد، یک ICV از طول ICV_Len باید بر روی آن محاسبه و به فیلدهای موجود پیوست شود. الگوریتم استفاده‌شده باید به‌وسیله‌ی ICV_Alg شناسایی شود و کلید استفاده‌شده باید یکی از موارد زیر باشد:

الف- Data_ICV_Gen اگر data-unit-type = normal؛ یا

ب- Exp_ICV_Gen اگر data-unit-type = expedited.

اگر رمزگذاری برابر TRUE باشد، یک فیلد همگام‌سازی مخفی با شکل و طولی که به‌وسیله‌ی Enc_Alg تعیین شده است باید تولید و به ابتدای فیلدهای موجود اضافه شود.

اگر رمزگذاری برابر TRUE باشد، یک لت رمزگذاری باید به فیلدهای موجود افزوده شود، به نحوی که طول فیلدهای موجود (یعنی، طول داده‌ی محافظت‌شده، Octet-String-Before-Encapsulation، ISN، لت یکپارچگی و فیلدهای ICV) به‌اضافه‌ی طول لت رمزگذاری باید مضرب صحیحی از اندازه بستک رمزگذاری (یعنی Enc_Blk) باشد. سپس مقدار و شکل لت‌گذاری که به‌صورت محلی تعیین شده است، باید در محتوای لت رمزگذاری قرار داده شود. اگر یک هشت‌تایی منفرد لت‌گذاری مورد نیاز باشد، فیلد محتوای لت‌گذاری هشت‌تایی منفرد باید استفاده شود.

اگر رمزگذاری برابر TRUE باشد، فیلدهای موجود رمزگذاری می‌شوند. الگوریتم استفاده‌شده باید به‌وسیله‌ی Enc_Alg شناسایی شود و کلید استفاده‌شده باید یکی از موارد زیر باشد:

الف- Data_Enc_Key اگر data-unit-type = normal؛ یا

ب- Exp_Enc_Key اگر data-unit-type = expedited.

PDU ساخته‌شده باید به‌عنوان نتیجه در رشته‌ی هشت‌تایی در کپسول گذاشته شده بازگردانده شود.

۱۱-۳-۲ کارکرد واکپسوله‌سازی

اگر هر یک از وارسی‌های زیر شکست بخورد، تمام اطلاعات وضعیت مربوط به امنیت، قبل از دریافت این پیام، به اطلاعات وضیعت امنیتی تنظیم خواهند شد، به‌جز برای هشدار، رسیدگی کردن، و/یا اطلاعات حسابداری.

آرگومان SA-ID باید برای ارجاع به یک همبستگی امنیتی استفاده شود. اگر همبستگی امنیتی وجود نداشت در این‌صورت خطای SA-not-available باید بازگردانده شده و مقدار Octet-String-Before-Encapsulation باید تعیین نشده باشد.

اگر رمزگذاری برابر TRUE باشد، گام‌های زیر برداشته می‌شوند:

الف- رشته‌ی هشت‌تایی در کپسول گذاشته‌شده باید رمزگشایی شود. الگوریتم رمزگشایی استفاده‌شده باید به‌وسیله‌ی Enc-Alg شناسایی شود و کلید استفاده‌شده باید یکی از موارد زیر باشد:

۱- Data_Dec_Key اگر که data-unit-type=normal باشد؛ یا

۲- Exp_Dec_Key اگر که data-unit-type=expedited.

ب- فیلد همگام‌سازی مخفی باید با دورانداختن تعدادی از هشت‌تایی‌ها، که به‌وسیله‌ی Enc_Alg تعیین می‌شود از جلوی داده‌ی رمزگشایی‌شده، حذف شود.

پ- لت رمزگذاری یا فیلد محتوای لت هشت‌تایی منفرد باید با افزوردن طول محتواها و ICN_Len حذف شود، سپس هر یک از هشت‌تایی‌ها در داده‌ی رمزگشایی‌شده‌ی باقیمانده که خارج از محدوده طول محاسبه شده است، دور انداخته می‌شود.

اگر ICV برابر TRUE باشد، گام‌های زیر برداشته می‌شود:

الف- درستی فیلد ICV باید با وارسی آخرین هشت‌تایی‌های ICV_Len مربوط به داده‌ی باقیمانده وارسی شود. الگوریتم استفاده‌شده باید به‌وسیله‌ی ICV_Alg شناسایی شود و اگر مبتنی بر رمزنگاری باشد، کلید استفاده‌شده برای محاسبه‌ی ICV باید یکی از موارد زیر باشد:

۱- Data_ICV_Check_Key اگر که data-unit-type=normal باشد؛ یا

۲- Exp_ICV_Check_Key اگر که data-unit-type=expedited.

ب- اگر درستی‌سنجی ICV شکست بخورد، خطای data-unit-integrity-failure باید بازگردانده شود و مقدار Octet-String-Before-Encapsultion باید تعیین نشده باشد.

ICV باید با دور انداختن هر یک از هشت‌تایی‌ها در داده‌ی باقیمانده (که خارج از محدوده طول قرار گرفته در طول محتوا بعد از فیلد طول محتوا است) حذف شود.

فیلد طول محتوا باید با دورانداختن اولین دو هشت‌تایی از داده‌ی باقیمانده، حذف شود.

لت‌گذاری ترافیک، لت‌گذاری یکپارچگی، یا فیلدهای محتوای لت‌گذاری هشت‌تایی منفرد از داده‌ی باقیمانده به‌وسیله‌ی حذف کردن داده‌ی خارج از محدوده Octet-String-Before-Encapsulation، حذف می‌شوند.

یادآوری ۱– فیلدهای محتوا به‌وسیله‌ی کدگشایی محتوای Octet-String-Before-Encapsulation جایابی می‌شوند، که یک فیلد از نوع یک- هشت‌تایی[1] است که در ادامه‌ی تعدادی از فیلدهای TLV می‌آید.

1 - One-octet

اگر ISN برابر TRUE باشد، داده‌ی باقیمانده باید برای اطمینان از اینکه یک و تنها یک فیلد محتوای ISN حاضر است، وارسی شود؛ یا در غیر این‌صورت داده‌ی باقیمانده باید برای اطمینان از اینکه هیچ فیلد محتوای ISN حاضر نباشد، وارسی شود. اگر حاضر باشد:

الف- اگر (data-unit-type = normal)، سپس Data_My_ISN باید پیش برده شود و مقدار توسط پنجره‌ی مقادیر مورد انتظار که به‌وسیله‌ی Data_My_ISN تعیین می‌شود، وارسی شود.

ب- اگر (data-unit-type = expedited)، سپس Exp_My_ISN باید پیش برده شود و مقدار توسط پنجره-ی مقادیر مورد انتظار که به‌وسیله‌ی Exp_My_ISN تعیین می‌شود، وارسی شود.

در هر دو قسمت الف و ب، ISN قبل از وارسی ، پیش برده می‌شود.

یادآوری ۲– پیش‌رفت[1] ممکن است با افزایش یک عدد دنباله یا با انتخاب عدد بعدی از یک دنباله‌ی شبه تصادفی و بدون تکرار به‌دست آید.

مقدار Octet-String-Before-Encapsulation باید به‌عنوان نتیجه در Octet-String-Before-Encapsulation بازگردانده شود.

۱۱-۴ فیلدهای PDU استفاده‌شده

این رویه‌ها از فیلدهای زیر مربوط به یک SDT PDU که در زیربند ۱۳-۳ تعریف شده است، استفاده می‌کنند:

الف- رشته- هشت‌تایی- در کپسول گذاشته شده؛

ب- همگام‌سازی مخفی؛

پ- ICV؛

ت- فیلدهای محتوا:

۱- لت رمزگذاری؛

۲- عدد دنباله؛

۳- لت هشت‌تایی منفرد؛

۴- لت ترافیک؛

۵- لت یکپارچگی.

۱۲ کارکرد کپسوله‌سازی No-Header (فقط NLSP-CO)

۱۲-۱ مرورکلی

NLSP-CO می‌تواند، تنها با استفاده از گزینه No_Header، محرمانگی داده‌ی کاربر را فراهم کند. گزینه‌ی No_Header از یک کارکرد کپسوله‌سازی مانند آن‌چه در این بند توصیف شده است، استفاده می‌کند. این کارکرد کپسوله‌سازی باید مبتنی بر یک سازوکار رمزگذاری باشد.

1 - Advancement

استفاده از گزینه No_Header دلالت بر این دارد که سازوکار رمزگذاری بر روی یک بستک به طول یک هشت‌تایی عمل می‌کند و اینکه الگوریتم اندازه‌ی داده‌ی رمزشده را تغییر نمی‌دهد.

۲-۱۲ صفات SA

الف- سازوکارهای انتخاب‌شده برای SA:

Encipher: بولی

رمزگذاری یک رشته‌ی هشت‌تایی در کپسول گذاشته شده برای فراهم کردن محرمانگی.

مقادیر این صفت توسط ASSR که خدمات امنیتی انتخاب‌شده در آن داده شده است، تعریف می‌شود.

ب- صفات سازوکار رمزگذاری:

Enc_Alg: شناسه‌ی شئ که تحت ISO/IEC 9979 اختصاص یافته است.

مقدار این صفت باید توسط ASSR که خدمات امنیتی انتخاب‌شده در آن داده شده است، تعریف شود. این صفت به صفات معین سازوکار رمزگذاری مانند شکل و طول هر فیلد همگام‌سازی، الگوریتم‌های رمزگذاری و رمزگشایی مجزا، بردارهای راه‌اندازی و غیره اشاره می‌کند.

Data_Enc_Key: شکل آن به‌وسیله‌ی ASSR محدود می‌شود.

مرجع کلید رمزگذاری برای داده‌ی عادی.

Data_Dec_Key: شکل آن به‌وسیله‌ی ASSR محدود می‌شود.

مرجع کلید رمزگشایی برای داده‌ی پیشتاز.

Exp_Enc_Key: شکل آن به‌وسیله‌ی ASSR محدود می‌شود.

مرجع کلید رمزگذاری برای داده‌ی پیشتاز.

Exp_Dec_Key: شکل آن به‌وسیله‌ی ASSR محدود می‌شود.

مرجع کلید رمزگشایی برای داده‌ی پیشتاز.

مقدار آغازین این صفات «کلید» باید در زمان برقراری SA تنظیم شود و می‌تواند در طی زمان حیات همبستگی عوض شود.

یادآوری- صفات مشخص سازوکار اضافی برای دریافت‌های آینده‌ی این استاندارد ملی و برای سازوکارهای خصوصی مجاز است.

۳-۱۲ رویه‌ها

۱-۳-۱۲ کارکرد کپسوله‌سازی

آرگومان SA-ID برای ارجاع به یک همبستگی امنیتی استفاده می‌شود. اگر همبستگی امنیتی وجود نداشته باشد، آنگاه خطای SA-not-available باید بازگردد و مقدار رشته‌ی هشت‌تایی در کپسول گذاشته‌شده نباید تعیین شود.

اگر رمزگذاری برابر TRUE باشد، Octet-String-Before-Encapsulation باید رمزگذاری شود. الگوریتم استفاده‌شده باید به‌وسیله‌ی End-Alg شناسایی و کلید استفاده‌شده باید یکی از موارد زیر باشد:

الف- Data-Enc-Key اگر data-unit-type=normal؛ یا

ب- Exp_Enc_Key اگر data-unit-type=expedited.

داده‌ی رمزگذاری‌شده باید به‌عنوان نتیجه در رشته‌ی هشت‌تایی در کپسول گذاشته شده، بازگردانده شود.

۱۲-۳-۲ کارکرد واکپسوله‌سازی

اگر هر یک از وارسی‌های زیر با شکست مواجه شوند، تمام اطلاعات وضعیت مرتبط با امنیت، به اطلاعات وضعیت امنیتی، قبل از پذیرش این پیام (به‌جز برای هشدار، رسیدگی و/یا اطلاعات حسابداری)، تنظیم می‌شود.

آرگومان SA-ID باید برای ارجاع به یک همبستگی امنیتی استفاده شود. اگر همبستگی امنیتی وجود نداشته باشد، آنگاه خطای SA-not-available باید برگردانده شود و مقدار Octet-String-Before-Encapsulation نباید تعیین شود.

اگر رمزگذاری برابر TRUE باشد، رشته‌ی هشت‌تایی در کپسول گذاشته‌شده باید رمزگشایی شود. الگوریتم رمزگشایی استفاده‌شده باید به‌وسیله‌ی Enc_Alg شناسایی شود و کلید استفاده‌شده باید یکی از موارد زیر باشد:

الف- Data_Dec_Key اگر data-unit-type = normal؛ یا

ب- Exp_Dec_Keu اگر data-unit-type-expedited.

مقدار داده‌ی رمزگشایی‌شده باید به‌عنوان نتیجه در Octet-String-Before-Encapsulation برگردانده شود.

۱۳ ساختار و کدبندی PDUS

۱۳-۱ مقدمه

پروتکل NLSP از ۳ نوع PDU استفاده می‌کند:

الف- انتقال داده امن PDU؛

ب- همبستگی امنیتی PDU؛

پ- کنترل امنیت اتصال PDU.

یک قالب داده فاقد ساختار اضافی بدون PCI به همراه گزینه No-Header برای داده‌ی محافظت‌شده استفاده می‌شود.

تمام PDUها باید شامل تعداد صحیحی از هشت‌تایی‌ها باشند. شماره‌گذاری هشت‌تایی‌ها داخل یک PDU از یک (۱) شروع می‌شود و به ترتیبی که در درخواست «شبکه‌ی اصلی» مناسب قرار داده می‌شوند، افزایش پیدا می‌کند. وقتی که برای نمایش یک عدد دودویی، هشت‌تایی‌های متوالی استفاده می‌شود، عدد هشت‌تایی پایین‌تر، با ارزش‌ترین مقدار را دارد. بیت‌های داخل یک هشت‌تایی از یک (۱) تا هشت (۸) شماره‌گذاری می‌شوند که بیت یک (۱)، کم ارزش‌ترین بیت است.

زمانی که کدبندی یک PDU با استفاده از یک نمودار در این بند نشان داده می‌شود:
الف- هشت‌تایی‌ها با هشت‌تایی کمترین شماره در چپ یا بالا، نشان داده می‌شوند؛
ب- داخل یک هشت‌تایی، بیت‌ها با بیت هشت (۸) در چپ و بیت (۱) در راست، نشان داده می‌شوند.
در نشان‌گذاری‌های زیر، یک جعبه، طول هر فیلد در هشت‌تایی‌ها را نشان می‌دهد؛ «var» نشان‌دهنده این است که طول فیلد متغیر است.
حضور یا غیاب یک فیلد «اختیاری» باید به‌وسیله‌ی صفات موجود در همبستگی امنیتی مشخص شود.

یادآوری– فیلدهای اختیاری در صورتی اختیاری هستند که یک همبستگی امنیتی مفروض به حضور یا عدم حضور برخی فیلدها نیاز داشته باشد. وقتی که همبستگی امنیتی تعیین شد، حضور یا عدم حضور هر فیلد به‌وسیله‌ی صفات SA تعیین می‌شود.

۱۳-۲ قالب فیلد محتوا

فیلد محتوا یک قالب فیلد عمومی برای مقادیر داده است که باید در PDUهای تعریف‌شده در این بند قرار گیرند. (به شکل ۱۳-۱ مراجعه شود.)

مقدار	طول	نوع
متغیر	۱-۳	۱

شکل ۱۳-۱- فیلد محتوا

نوع فیلد محتوا باید به یکی از مقادیر زیر تنظیم شود:

مقدار	نوع فیلد محتوا
00-5F	ذخیره‌شده برای استفاده خصوصی
60-9F	ذخیره‌شده برای استفاده در آینده
A0-BF	ذخیره‌شده برای استفاده SA-P (به پیوست پ مراجعه شود.)
C0-CF	ذخیره‌شده برای استفاده‌ی مستقل از سازوکار (به زیربند ۱۳-۳-۴-۳ مراجعه شود.)
D0-FF	ذخیره‌شده برای استفاده‌ی وابسته به سازوکار (به زیربند ۱۳-۳-۵ مراجعه شود.)

طول فیلد محتوا باید شامل طول مقدار فیلد محتوا در هشت‌تایی‌ها باشد. طول فیلد محتوا باید دارای طول‌های یک، دو یا سه هشت‌تایی باشد.
الف- اگر طول آن یک هشت‌تایی باشد، بیت ۸ باید صفر باشد و ۷ بیت باقی‌مانده یک مقدار با طول تا حداکثر ۱۲۷ هشت‌تایی را تعریف می‌کنند.

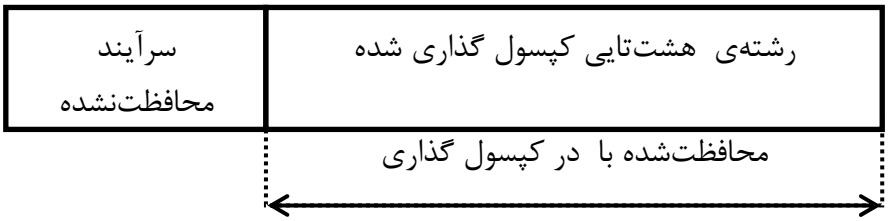
ب- اگر طول آن دو هشت‌تایی باشد، اولین هشت‌تایی باید به‌صورت 1000 0001 کدبندی شود و هشت‌تایی باقی‌مانده طول فیلدها را تا حداکثر ۲۵۵ هشت‌تایی تعریف می‌کند.
پ- اگر طول آن سه هشت‌تایی باشد، هشت‌تایی اول باید به‌صورت 1000 0010 کدبندی شود و دو هشت‌تایی باقی‌مانده طول فیلد را تا حداکثر ۶۵۵۳۶ هشت‌تایی تعریف می‌کند.
دیگر مقادیر از اولین هشت‌تایی برای استفاده در آینده ذخیره می‌شوند.
مقدار فیلد محتوا، شامل داده برای فیلد PDU است.

۱۳-۳ داده‌ي محافظت‌شده

این زیربند، PDUهای استفاده‌شده برای انتقال داده‌ی محافظت‌شده را توصیف می‌کند. این توصیف شامل دو جنبه از PDUها می‌شود: آن‌هایی که مستقل از سازوکار استفاده‌شده هستند (که نشان عمومی دارند) و آن‌هایی که مختص سازوکارهای پشتیبانی‌شده به‌وسیله‌ی رویه‌های کپسوله‌سازی که در بند ۱۱ تعریف شده، هستند. (که نشان مختص سازوکار دارند.) آن‌هایی که هم شامل جنبه‌های عمومی و هم جنبه‌های مختص سازوکار هستند نشان مختلط دارند.

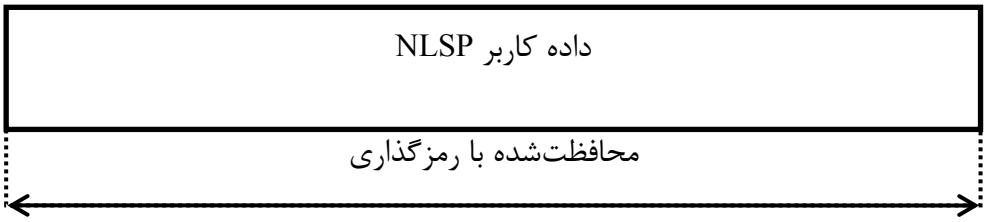
۱۳-۳-۱ ساختارهای PDU پایه (عمومی)

دو ساختار داده برای انتقال داده امن تعریف شده است. اولی برای NLSP-CL اجباری است، یکی از آن دو باید برای NLSP-CO پشتیبانی شود.
الف- PDU انتقال داده‌ی امن که به‌صورتی که در شکل ۱۳-۲ نشان داده شده است قالب‌بندی شده است.



شکل ۱۳-۲- ساختار PDU انتقال داده امن عمومی

ساختار سرآیند محافظت‌نشده در زیربند ۱۳-۳-۲ تعریف شده است. فیلد رشته‌ی هشت‌تایی در کپسول گذاشته‌شده باید شامل خروجی کارکرد کپسوله‌سازی (برای مثال، همان‌طورکه در بند ۱۱ توصیف شده است، با استفاده از ساختار تعریف شده در زیربند ۱۳-۳-۳) که بر روی Octet-String-Before-Encapsulation عمل می‌کند (که ساختار آن در زیربند ۱۳-۳-۴ توصیف شده است) باشد.
شرایط (اجباری/اختیاری و غیره) برای پشتیبانی از فیلدهایی که این PDU را تشکیل می‌دهند در زیربندهای ت-۵-۳، ت-۵- ۴(فیلدهای مختص سازوکار)، ت-۶-۴ (تنها NLSP-CO) و ت-۷-۶ (تنها NLSP-CO) تعریف شده‌اند.
ب- یک رشته بیتی بدون ساختار برای محرمانگی No_Header تنها گزینه است که در شکل ۱۳-۳ نشان داده شده است، هیچ PCI اضافه نشده است.



شکل ۱۳-۳- محرمانگی تنها با استفاده از گزینه No-Header

گزینه No-Header باید تنها زمانی که شرایط زیر برآورده شوند، استفاده شود:

الف- No_Header برابر TRUE است؛

ب- برچسب برابر FALSE است؛

پ- ICV برابر FALSE است؛

ت- ISN برابر FALSE است؛

ث- رمزگذاری برابر TRUE است؛

ج- Enc_Sync_Len=0؛

چ- Enc_Blk=1؛

ح- Pad برابر FALSE است.

۱۳-۳-۲ سرآیند محافظت‌نشده (عمومی)

قالب سرآیند محافظت‌نشده باید مانند آن‌چه در شکل ۱۳-۴ نمایش داده شده است، باشد.

SA-ID	نوع PDU	LI	شناسه پروتکل
متغیر	۱	۱	۱

شکل ۱۳-۴ سرآیند محافظت‌نشده

۱۳-۳-۲-۱ شناسه‌ي پروتکل (عمومی)

این فیلد باید محتوی شناسه‌ی پروتکل NLSP با مقدار 1011 1000 باشد.

۱۳-۳-۲-۲ LI (عمومی)

این فیلد محتوی طول فیلد PDU Type به اضافه‌ی SA-ID است.

برای NLSP-CO، فیلد SA-ID الزامی نیست. بنابراین، این فیلد باید به‌نحوی تنظیم شود که فیلد SA-ID حاضر نیست. (یعنی مقدار 00000001)

۱۳-۳-۲-۳ PDU Type (عمومی)

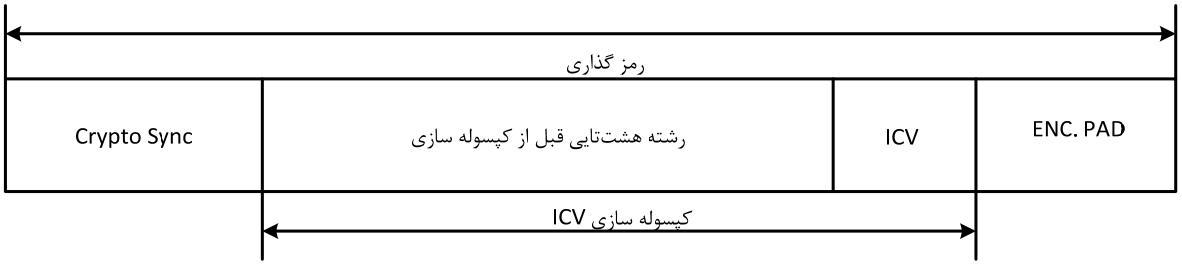
این فیلد باید محتوی مقدار نوع PDU، 01001000 باشد تا PDU انتقال داده امن را نشان دهد.

۱۳-۳-۲-۴ SA-ID (عمومی)

فیلد SA-ID باید محتوی شناسه همبستگی امنیتی هستار راه دور باشد. (صفات SA Your_SA-ID) این فیلد برای NLSP-CO الزامی نیست.

۱۳-۳-۳ Encapsulated-Octet-String (مختص سازوکار)

ساختار SDT PDU که از رویه‌های مختص سازوکار تعریف شده در بند ۱۳ استفاده می‌کند، در شکل ۱۳-۵ نشان داده شده است.



شکل ۱۳-۵ – ساختار رشته هشت‌تایی کپسوله‌سازی‌شده

۱۳-۳-۳-۱ همگام‌سازی مخفی (مختص سازوکار)

این فیلد اختیاری است و ممکن است محتوی داده‌های همگام‌سازی برای الگوریتم‌های رمزگذاری مشخص باشد. حضور، قالب و طول این فیلد به‌طور ضمنی در Enc_Alg مشخص می‌شود.

۱۳-۳-۳-۲ مقدار وارسی یکپارچگی (مختص سازوکار)

این فیلد محتوی یک مقدار وارسی یکپارچگی (ICV) است. طول این فیلد باید به‌وسیله‌ی شناسه‌ی الگوریتم ICV که در صفات همبستگی امنیتی است، تعریف شود.

۱۳-۳-۳-۳ لت رمزگذاری (مختص سازوکار)

این فیلد محتوی لت‌گذاری رمزگذاری است (End. Pad) که به‌منظور پشتیبانی از الگوریتم‌های رمزگذاری بستک برای محرمانگی استفاده می‌شود. انتخاب مقدار لت یک موضوع محلی است. تمام NLSPEها باید قادر به صرف‌نظر از این فیلد باشند. قالب این فیلد باید به‌صورت تعریف‌شده در زیربند ۱۳-۳-۵ یا به‌صورت تعریف‌شده در الگوریتم رمزگذاری، کدبندی شود. اگر یک لت دو هشت‌تایی نیاز باشد طول صفر خواهد بود و مقدار نخواهد داشت. اگر یک لت هشت‌تایی منفرد نیاز باشد، یک فیلد PAD هشت‌تایی منفرد به‌جای فیلد PAD رمزگذاری باید به‌کار رود.

استفاده از این فیلد بستگی به این دارد که آیا الگوریتم رمزگذاری نیازمند یک لت رمزگذاری مستقل است یا خیر.

۱۳-۳-۴ Octet-String-Before-Encapsulation (مختلط)

شکل ۱۳-۶ قالب رشته هشت‌تایی قبل از کپسوله‌سازی را نشان می‌دهد. این فیلد هر تعداد از فیلدهای محتوی عمومی و مختص سازوکار را شامل می‌شود.

حداقل طول محتوا و نوع داده باید وجود داشته باشند.

..	جای درج محتوی (مکانیزم ویژه)	..	جای درج محتوی	نوع داده	طول محتوی
متغیر			متغیر	۱	۲

شکل ۱۳-۶ - رشته هشت‌تایی قبل از کپسوله‌سازی

۱۳-۳-۴-۱ طول محتوا (عمومی)

این فیلد باید محتوای طول ترکیبی تمام فیلدهای محتوا و نوع داده باشد.

یادآوری– شامل ICV یا فیلدهای لت رمزگذاری نمی‌شود.

۱۳-۳-۴-۲ نوع داده (عمومی)

بیت ۸ این فیلد، پرچم «راه‌انداز به پاسخ‌دهنده» است. مقدار ۱ راه‌انداز به پاسخ‌دهنده را نشان می‌دهد. مقدار صفر پاسخ‌دهنده به راه‌انداز را نشان می‌دهد.

بیت ۷ این فیلد، پرچم «Last/Not Last» است. این بیت زمانی که SDT PDU محتوی آخرین قسمت یک دنباله باشد، مقدار صفر گرفته و در غیر این‌صورت مقدار ۱ می‌گیرد. برای NLSP-CL مقدار آن همیشه برابر صفر خواهد بود.

بیت ۱ تا ۶ این فیلد مانند زیر برای شناسایی نخستینه‌های خدمت NLSP کدبندی می‌شوند.

مقدار	نخستینه‌ی خدمت
000000	مربوط به هیچ یک از نخستینه‌های خدمت NLSP نیست (به‌عنوان مثال Test Data)
000001	NLSP-UNITDATA req/ind
000010	NLSP-CONNECT req/ind
000011	NLSP-CONNECT resp/conf
000100	NLSP-DATA req/ind
000101	NLSP-DATA-ACKNOWLEDGE req/ind
000110	NLSP-EXPEDITED DATA req/ind
000111	NLSP-DISCONNECT req/ind
001000	SA Protocol
001001-011111	ذخیره‌شده برای استفاده در آینده
100000-111111	ذخیره‌شده برای استفاده در آینده

۱۳-۳-۴-۲-۱ فیلدهای محتوا (عمومی)

کدبندی نوع فیلد محتوا به‌صورت تعریف‌شده در زیربند ۱۳-۲ است. فیلدهای محتوا مستقل از سازوکار (یعنی C0-CF) که به‌وسیله‌ی رویه‌های بندهای ۶، ۷ و ۸ به‌کار می‌روند، در ادامه آمده است.

مقدار	نوع فیلد محتوا
00-BF	ذخیره‌شده
C0	داده‌ی کاربر
C1	داده‌ی آزمایشی
C2	نشانی Calling/Source NLSP
C3	نشانی Called/Destination NLSP

C4	نشانی NLSP پاسخ‌دهنده
C5	استفاده‌نشده
C6	برچسب
C7	مرجع برچسب
C8	درخواست تأیید
C9	دلیل قطع ارتباط
CA-CF	ذخیره‌شده برای استفاده در آینده
D0-FF	ذخیره‌شده

۱۳-۳-۴-۲-۲ داده‌ی کاربر NLSP

این فیلد محتوی NLSP Userdata از نخستینه خدمت است.

۱۳-۳-۴-۲-۳ داده‌ی آزمایشی

ساختار داده‌ی آزمایشی در شکل ۱۳-۷ نمایش داده شده است.

کنترل آزمون	داده آزمون
۱	متغیر

شکل ۱۳-۷ – داده‌ی آزمایشی

کنترل آزمون محتوی یک مجموعه بیت است که به‌صورت زیر تخصیص داده می‌شوند:

الف- بیت ۱ – پرچم جهت. صفر برای اصلی، ۱ برای داده‌ی آزمایشی بازتابی.

ب- بیت ۲ تا ۴ – ذخیره‌شده برای استفاده در آینده.

پ- بیت ۵ تا ۸ – ذخیره‌شده برای استفاده خصوصی.

۱۳-۳-۴-۲-۴ نشانی NLSP مبدأ/فراخواننده

این فیلد یک نشانی لایه‌ی شبکه است که به‌صورت یکی از قالب‌های توصیف‌شده در توصیه‌نامه‌ی ISO 8348/AD2 | CCITT X.213 کدبندی می‌شود.

۱۳-۳-۴-۲-۵ نشانی NLSP مقصد/فراخوانی‌شده

این فیلد یک نشانی لایه‌ی شبکه است که به‌صورت یکی از قالب‌های توصیف‌شده در توصیه‌نامه‌ی ISO 8348/AD2 | CCITT X.213 کدبندی می‌شود.

۱۳-۳-۴-۲-۶ نشانی NLSP پاسخ‌دهنده

این فیلد یک نشانی لایه‌ی شبکه است که به‌صورت یکی از قالب‌های توصیف‌شده در توصیه‌نامه‌ی ISO 8348/AD2 | CCITT X.213 کدبندی می‌شود.

۱۳-۳-۴-۲-۷ برچسب

این فیلد برای حمل برچسب امنیتی یک PDU به‌کار می‌رود. این فیلد اگر فیلد محتوی مرجع برچسب حضور داشته باشد، حضور نخواهد داشت.

شکل ۱۳-۸ – مقدار برچسب

صادرکننده‌ی تعریف مانند محتویات یک مقدار شناسه شئ، به‌وسیله‌ی قواعد کدبندی پایه مربوط به یک شناسه شئ که در بند ۲۲ توصیه‌نامه‌ی ISO/IEC 8825 | CCITT X.209 تعریف شده است، کدبندی می‌شود.
ساختار و تفسیر محتویات برچسب به‌وسیله‌ی صادرکننده‌های تعریف مختلف، تعریف می‌شوند.

یادآوری– انتظار می‌رود که این برچسب‌ها تحت رویه‌های تعریف‌شده در ISO/IEC و ITU-T ثبت شوند. یک صادرکننده‌ی تعریف به‌عنوان یک شناسه شئ به‌وسیله‌ی رویه‌های تعریف‌شده در ISO/IEC 9834 ثبت می‌شود.

۱۳-۳-۴-۲-۸ مرجع برچسب

این فیلد یکی از مجموعه‌های برچسب‌های امنیتی تعریف‌شده در صفت Label_Set از SA را مشخص می‌کند. زمانی که این فیلد حاضر باشد همیشه باید به‌نحوی کدبندی شده باشد که قسمت مقدار فیلد دو هشت‌تایی باشد. این فیلد در مواقعی که فیلد محتوی برچسب حضور دارد، حضور نخواهد داشت.

۱۳-۳-۴-۲-۹ درخواست تأیید

در صورت حضور این فیلد نشان می‌دهد که تأیید دریافت درخواست داده شده است. این فیلد به‌صورت یک هشت‌تایی منفرد کدبندی می‌شود. (بدون طول یا مقدار)

۱۳-۳-۴-۲-۱۰ دلیل قطع اتصال

این فیلد پارامتر خدمت دلیل NLSP-DISCONNECT را حمل می‌کند و در حین حمل در شبکه‌ی اصلی کدبندی می‌شود.

یادآوری- در مواردی که شبکه‌ی اصلی یک شبکه ISO.IEC 8208 | CCITT X.25 باشد مقدار اولین هشت‌تایی دلیل است و دومین هشت‌تایی در صورت وجود کد عیب‌یابی نگاشت‌شده از دلیل NLSP-DISSCONNECT تعریف‌شده در توصیه‌نامه‌ی ISO/IEC 8878 | CCITT X.223 است.

۱۳-۳-۵ فیلدهای محتوی (مختص سازوکار)

کدبندی فیلد محتوا به‌صورت تعریف‌شده در زیربند ۱۳-۲ خواهد بود. کدبندی نوع فیلد محتوی برای فیلدهای محتوای مختص سازوکار در زیر آمده است:

مقدار	نوع فیلد محتوا
00-CF	ذخیره‌شده
D0	شماره دنباله
D1	لت هشت‌تایی منفرد
D2	لت ترافیک
D3	لت یکپارچگی
D4	لت رمزگذاری
D5-FF	ذخیره‌شده برای استفاده در آینده

۱۳-۳-۵-۱ شماره دنباله

این فیلد حاوی Your_ISN (یعنی یک شماره دنباله یکپارچگی PDU) است که باید تحت کلید جاری برای نوع داده (پیشتاز یا عادی) یکتا باشد.

یادآوری– در NLSP CO یکتا بودن بین جریان داده‌های عادی یا پیشتاز (و بنابراین محافظت از بازپخش) به‌وسیله‌ی متفاوت بودن فیلد نوع داده ارائه می‌شود. (به زیربند ۱۳-۳-۴-۲ مراجعه شود.)

۱۳-۳-۵-۲ لت هشت‌تايي منفرد

این فیلد یک فیلد نوع هشت‌تایی منفرد (بدون طول یا مقدار) برای لت‌گذاری عمومی است. (به‌عنوان مثال برای پشتیبانی یک هشت‌تایی منفرد مربوط به لت یکپارچگی) این هشت‌تایی ممکن است یک یا چند بار به‌جای یک یکپارچگی کدبندی‌شده به‌صورت TLV، رمزگذاری یا فیلد لت ترافیک برای ارائه یکپارچگی، رمزگذاری یا لت‌گذاری ترافیک، مورد استفاده قرار بگیرد. تمام NLSPEها باید این فیلد را تشخیص داده و از آن صرف‌نظر کنند.

۱۳-۳-۵-۳ لت ترافيك

این فیلد حاوی لت‌گذاری برای اهداف محرمانگی جریان ترافیک است. انتخاب مقدار لت‌گذاری یک موضوع محلی است. تمام NLSPEها باید قابلیت نادیده گرفتن این فیلد را داشته باشند. اگر یک لت دو هشت‌تایی مورد نیاز باشد، طول باید صفر باشد و هیچ مقداری نداشته باشد. اگر یک لت هشت‌تایی منفرد نیاز باشد، یک لت هشت‌تایی منفرد به‌جای یک لت ترافیک به‌کار می‌رود.

این فیلد هم‌چنین می‌تواند برای برآوردن الزامات لت رمزگذاری مورد استفاده قرار گیرد.

۱۳-۴ PDU همبستگي امنیتی

قالب PDU همبستگی امنیتی در شکل ۱۳-۹ نمایش داده شده است.

شرایط (اجباری/اختیاری و غیره) برای پیشتیبانی فیلدهایی که این PDU را شکل می‌دهند در زیربندهای ت-۵-۵ و ت-۵-۶ تعریف شده‌اند. (فیلدهای مختص سازوکار)

شناسه پرتکل	LI	نوع PDU	SA-ID	نوع SA-P	محتویات SA-PDU
۱	۱	۱	متغیر	متغیر	متغیر

شکل ۱۳-۹ – ساختار PDU همبستگی امنیتی

۱۳-۴-۱ شناسه‌ي پروتکل (PID)

این فیلد باید حاوی شناسه‌ی پروتکل NLSP با مقدار 10001011 باشد.

۱۳-۴-۲ فیلد LI

این فیلد حاوی طول فیلد نوع PDU به اضافه‌ی فیلد SA-ID است.

اگر SA-P نیاز داشته باشد که اعلام کند SA-ID همتای خود را نمی‌داند (برای مثال، در زمان برقراری یک SA جدید)، این فیلد به مقدار 00000001 تنظیم می‌شود تا نشان دهد که فیلد SA-ID ارائه نشده است.

۱۳-۴-۳ فیلد نوع PDU

این فیلد باید حاوی نوع PDU با مقدار 01001001 برای نشان‌دادن یک PDU همبستگی امنیتی باشد.

۱۳-۴-۴ فیلد SA-ID

فیلد SA-ID باید حاوی شناسه‌ی همبستگی امنیتی مربوط به هستار راه دور باشد. (یعنی صفت SA، Your_SA-ID) این فیلد هنگامی که SA-P برای برقراری یک SA جدید به‌کار می‌رود، نیاز نیست. (یعنی دریافت‌کننده هنوز SA-IDی تخصیص نداده است.)

۱۳-۴-۵ فیلد نوع SA-P

این فیلد حاوی یک شناسه شئ است که سازوکار به‌کار رفته برای ارائه پروتکل SA را نشان می‌دهد. این شناسه شئ مانند محتوی مقدار شناسه شئ با استفاده از قواعد کدبندی تعریف‌شده در بند ۲۲ از توصیه‌نامه‌ی ISO/IEC 8825 | CCITT. X.209، کدبندی می‌شود و یک شناسه طول هشت‌تایی منفرد قبل از آن می‌آید.

شناسه شئ زیر برای استفاده SA-P عمومی با رویه‌های تبادل نشانه‌ی کلید[1] تعریف‌شده در پیوست پ و الگوریتم تبادل کلید نمایی تعریف‌شده در پیوست ح، تخصیص داده می‌شود:

Join-ccitt-iso nlsp (22) sa-p-kte (1) eke (1)

استفاده از سایر الگوریتم‌ها یا پروتکل‌های SA با SA-P تعریف‌شده در پیوست پ ممکن است با شناسه‌های شئ دیگری که براساس ISO/IEC 9834-1 تخصیص داده می‌شوند، مشخص شود.

۱۳-۴-۶ محتویات SA-PDU

ساختار داخلی این فیلد بستگی به سازوکار ارائه‌دهنده پروتکل SA همان‌طورکه در زیربند ۱۳-۴-۵ مشخص شده است، دارد. پیوست پ چنین پروتکل SAای را تعریف می‌کند.

1 - Key Token

۵-۱۳ PDU کنترل امنیتی اتصال

قالب PDU کنترل امنیتی ارتباط در شکل ۱۳-۱۰ نمایش داده شده است.

شرایط (اجباری/اختیاری و غیره) برای پشتیبانی فیلدهایی که این PDU را شکل می‌دهند در زیربندهای ت-۷-۷ و ت-۸-۸ تعریف شده‌اند. (فیلدهای مختص سازوکار)

محتوی CSC-PDU	طول محتوی	SA-ID	نوع PDU	LI	شناسه پرتکل
متغیر	۱	متغیر	۱	۱	۱

شکل ۱۳-۱۰ - PDU کنترل امنیتی ارتباط

۱-۵-۱۳ شناسه‌ي پروتکل

این فیلد باید حاوی شناسه‌ی پروتکل NLSP با مقدار 10001011 باشد.

۲-۵-۱۳ فیلد LI

این فیلد باید حاوی طول فیلد نوع PDU به اضافه‌ی فیلد SA-ID باشد.

۳-۵-۱۳ فیلد نوع PDU

این فیلد حاوی نوع PDU با مقدار xx111111 برای نشان دادن یک PDU کنترل امنیت اتصال است. مقادیر بیت‌ها برای این فیلد مانند زیر هستند:

الف- بیت‌های ۱ تا ۶ حاوی نوع PDU با مقدار 111111 برای نشان دادن یک PDU کنترل امنیت اتصال هستند.

ب- بیت ۷ – پرچم UNC-UND، اگر ۱ باشد نشان می‌دهد که NLSP-CONNECT در UN-Data حمل شده است و اگر صفر باشد نشان می‌دهد که NLSP-CONNECT در UN-CONNECT حمل شده است.

پ- بیت ۸ – پرچم SA-P، نشان می‌دهد که SA-P در این اتصال به‌کار گرفته‌شده است. اگر بیت ۸، ۱ باشد، آنگاه هیچ فیلد دیگری در این PDU حضور نخواهد داشت.

۴-۵-۱۳ فیلد SA-ID

فیلد SA-ID باید حاوی شناسه‌ی همبستگی امنیتی هستار راه دور باشد. (یعنی صفت SA، Your_SA-ID) این فیلد اگر پرچم SA-P، ۱ باشد وجود نخواهد داشت.

۵-۵-۱۳ طول محتوی

این فیلد شامل طول محتوی CSC-PDU در قالب هشت‌تایی است. این فیلد اگر پرچم SA-P، ۱ باشد وجود نخواهد داشت.

۶-۵-۱۳ محتوی CSC-PDU

ساختار داخلی این فیلد به سازوکار پشتیبانی احراز هویت اتصال بستگی دارد. این فیلد اگر پرچم SA-P، ۱ باشد، وجود نخواهد داشت. فیلدهای مورد نیاز برای سازوکارهای کنترل امنیت خاص ارائه‌شده در بند ۱۰ مانند زیر هستند. (به شکل ۱۳-۱۱ مراجعه شود.)

شکل ۱۳-۱۱ – محتویات CSC-PDU

یادآوری۱- طول Enciphered-Auth-Data بستگی به الگوریتم رمزگذاری استفاده‌شده دارد و به‌وسیله‌ی صفت SA، Enc_Auth_len تعریف می‌شود.

یادآوری۲- طول اطلاعات کلید بستگی به روش توزیع کلید استفاده‌شده دارد. اگر کلید تغییر نکند شامل نخواهد شد.

۱۳-۵-۷ Auth-Data رمزگذاری شده (مختص سازوکار)

به شکل ۱۳-۱۲ مراجعه شود.

این فیلد حاوی عددی است که برای احراز هویت استفاده می‌شود و به‌عنوان یک عدد دنباله‌ی یکپارچگی (اگر انتخاب شده باشد) طول آن به‌عنوان قسمتی از صفات SA تعریف می‌شود. هنگامی که از هستار فراخواننده NLSP به هستار فراخوانی‌شده ارسال می‌شود، Your-initial-ISN صفر خواهد بود.

شکل ۱۳-۱۲ – Auth-Data رمزگذاری شده

۱۳-۵-۸ اطلاعات کلید مختص سازوکار

بسته به روش توزیع کلید انتخاب‌شده برای همبستگی امنیتی، اگر این پارامتر موجود نباشد بیانگر این خواهد بود که یک کلید موجود باید به‌کار رود یا براساس صفات SA، kdm شامل یکی از موارد زیر خواهد بود:

- Kdm_mutual - یک کلید رمزگذاری‌شده با استفاده از KEK مشترک
- Kdm_asymmetric_single - یک کلید رمزگذاری‌شده با کلید عمومی دریافت‌کننده
- Kdm_asymmetric_double - یک کلید رمزگذاری‌شده با کلید خصوصی فرستنده و کلید عمومی دریافت‌کننده
- Kdm_distributed - یک مرجع کلید
- Kdm_other - محتوی تعریف‌شده به‌صورت خصوصی

وجود این فیلد به‌طور ضمنی از مقایسه‌ی طول محتوی با صفت SA، Enc_Auth_len مشخص می‌شود.

۱۴ انطباق

۱۴-۱ الزامات انطباق ایستا

۱۴-۱-۱ کلاس‌های انطباق

سامانه ممکن است از یک یا هر دوی کلاس‌های انطباق زیر پشتیبانی کند:

الف- حالت NLSP-CL؛

ب- حالت NLSP-CO.

پشتیبانی از این کلاس‌های انطباق توسط قابلیت‌های توصیف‌شده در زیربندهای ۱۴-۱-۲ و ۱۴-۱-۳ تعریف می‌شود.

پشتیبانی از هر یک از کلاس‌های انطباق می‌تواند به‌صورت اختیاری و با استفاده از سازوکارهای امنیتی پشتیبانی‌شده در این استاندارد ملی انجام گیرد.

استفاده از سازوکارهای امنیتی پشتیبانی‌شده در این استاندارد ملی توسط الزامات سازوکارهای امنیتی معرفی‌شده در زیربند ۱۴-۱-۵ تعریف شده است.

۱۴-۱-۲ قابلیت‌های حالت NLSP-CL

۱۴-۱-۲-۱ خدمات امنیتی

یک سامانه مطابق با حالت NLSP-CL باید از خدمات زیر پشتیبانی کند:

الف- یک یا چند مورد از خدمات زیر:

۱- محرمانگی بی‌اتصال؛

۲- یکپارچگی بی‌اتصال؛

۳- احراز هویت مبدأ داده.

ب- کنترل دسترسی، اختیاری؛

پ- محرمانگی جریان ترافیک، اختیاری.

۱۴-۱-۲-۲ محدوده‌ي محافظت

یک سامانه که ادعای انطباق با NLSP-CL را دارد باید یک یا هر دو مورد زیر را پشتیبانی کند:

الف- محافظت از تمام پارامترهای خدمت NLSP؛

ب- محافظت از داده‌ی کاربر NLSP.

یک سامانه که ادعای انطباق با NLSP-CL را دارد ممکن است به‌طور اختیاری از مورد زیر پشتیبانی کند:

پ- بدون محافظت.

۱۴-۱-۲-۳ قابلیت‌های دیگر

زمانی که حالت NLSP-CL پشتیبانی می‌شود، سامانه قابلیت ارسال و/یا دریافت یک SDT PDU را خواهد داشت.

۱۴-۱-۳ قابلیت‌های حالت NLSP-CO

۱۴-۱-۳-۱ خدمات امنیتی

یک سامانه مطابق با حالت NLSP-CO باید از خدمات امنیتی زیر پشتیبانی کند:

الف- یک یا چند خدمت زیر:

۱- محرمانگی اتصال؛

۲- یکپارچگی اتصال بدون بازیابی؛

۳- احراز هویت هستار همتا؛

ب- کنترل دسترسی، اختیاری؛

پ- محرمانگی جریان ترافیک، اختیاری.

۱۴-۱-۳-۲ محدوده‌ي محافظت

یک سامانه که ادعای انطباق با NLSP-CO را دارد باید یک یا چند مورد از موارد زیر را پشتیبانی کند:

الف- محافظت از تمام پارامترهای خدمت NLSP؛

ب- محافظت از داده‌ی کاربر NLSP شامل داده‌ی کاربر NLSP در NLSP-CONNECT و NLSP-DISCONNECT؛

پ- محافظت از داده‌ی کاربر NLSP در طی انتقال داده.

یک سامانه که ادعای انطباق با NLSP-CL را دارد می‌تواند به‌صورت اختیاری از مورد زیر پشتیبانی کند:

ت- بدون محافظت.

۱۴-۱-۳-۳ سایر قابلیت‌ها

زمانی که حالت NLSP-CO پشتیبانی می‌شود، سامانه قابلیت‌های زیر را خواهد داشت:

الف- راه‌اندازی و/یا پذیرش یک اتصال؛

ب- ارسال و دریافت یک CSC-PDU؛

پ- ارسال و/یا دریافت حداقل یکی از موارد زیر:

۱- محافظت داده با به‌کارگیری سازوکارهای کپسوله‌سازی مبتنی بر No_Headder همان‌طورکه در زیربندهای ۶-۴-۱-۲ و ۶-۴-۲-۲ تعریف شده است؛

۲- کپسوله‌سازی مبتنی بر SDT PDU همان‌طورکه در زیربندهای ۶-۴-۱-۱ و ۶-۴-۲-۱ تعریف شده است؛

ت- حداقل یکی از حالت‌های برقرارسازی اتصال NLSP تعریف‌شده در زیربند ۸-۵؛

ث- پشتیبانی تبادلات آزمایشی، اختیاری؛

ج- پشتیبانی از یک پروتکل SA درون باند، اختیاری.

۱۴-۱-۴ پشتیبانی از PDUها

جدول ۱۴-۱ نشان می‌دهد که پشتیبانی برای یک PDU مفروض برای حالت کاری داده شده، اجباری است یا اختیاری.

جدول ۱۴-۱- پشتیبانی NLSP از PDUها

PDU	شرط پشتیبانی
SDT PDU	اجباری برای CL اجباری در صورتی که CO و کپسوله‌سازی مبتنی برSDT PDU پشتیبانی شود.
SA PDU	اختیاری اگر از SA-P پشتیبانی شود.
CSC-PDU	اجباری برای NLSP-CO

۱۴-۱-۵ الزامات ایستا برای سازوکارها

یک سامانه که ادعای پشتیبانی از سازوکارهای امنیتی تعریف‌شده در این استاندارد ملی را دارد، باید الزامات زیر را با توجه به سازوکار انتخاب‌شده برآورده کند:

الف- هر سامانه که ادعای پشتیبانی خدمات امنیتی محرمانگی اتصال یا بی‌اتصال را دارد، باید این خدمات را از طریق به‌کارگیری یک سازوکار رمزگذاری ارائه کند.

ب- هر سامانه‌ای که ادعای پشتیبانی خدمات امنیتی یکپارچگی بی‌اتصال یا یکپارچگی اتصال بدون بازیابی را دارد باید این خدمات را با استفاده از مکانیزمی که از فیلد ICV تعریف‌شده در زیربند ۱۳-۳-۳-۲ یا به‌صورت اختیاری از فیلد ISN تعریف‌شده در زیربند ۱۳-۳-۵-۱ استفاده می‌کند، ارائه دهد.

پ- هر سامانه‌ای که ادعای پشتیبانی خدمت امنیتی محرمانگی جریان ترافیک را دارد، باید این خدمت را با استفاده از مکانیزمی که از فیلد لت ترافیک تعریف‌شده در زیربند ۱۳-۳-۵-۳ استفاده می‌کند، ارائه دهد.

ت- هر سامانه‌ای که ادعای پشتیبانی خدمت امنیتی احراز هویت مبدأ داده را دارد، باید این خدمت را از طریق یک سازوکار رمزگذاری یا یک سازوکار رمزنگاشتی که از فیلد ICV تعریف‌شده در زیربند ۱۳-۳-۳-۲ استفاده می‌کند، ارائه دهد.

ث- هر سامانه‌ای که ادعای پشتیبانی خدمت امنیتی احراز هویت هستار همتا را دارد، باید از فیلد رمزگذاری‌شده auth-data تعریف‌شده در زیربند ۱۳-۵-۷ پشتیبانی کند.

۱۴-۲ الزامات انطباق پویا

۱۴-۲-۱ الزامات عمومی

الف- سامانه باید بتواند به‌درستی تمامی عناصر پروتکل معتبری را تولید کند، بپذیرد و پاسخ دهد که از هر کلاس و حالت کاری که ادعای انطباق با آن شده است، پشتیبانی می‌کند.

ب- سامانه باید به‌درستی به تمام دنباله‌های نادرست عناصر پروتکل NLSP پاسخ دهد.

۱۴-۲-۲ الزامات خاص

سامانه باید برای هر کلاس انطباقی که ادعای انطباق با آن را دارد و برای هر گزینه از الزامات انطباق ایستای پیاده‌سازی‌شده، رفتار خارجی سازگار با پیاده‌سازی موارد زیر را به نمایش گذارد:

الف- کارکردهای پروتکل مشترک تعریف‌شده در بند ۶؛

ب- برای حالت NLSP-CL، کارکردهای پروتکل تعریف‌شده در بند ۷؛

پ- برای حالت NLSP-CO، کارکردهای پروتکل تعریف‌شده در بند ۸؛
ت- برای سامانه‌های NLSP-CL که از رویه‌های مختص سازوکار پشتیبانی می‌کنند، کارکردهای پروتکل در بند ۱۱؛
ث- برای سامانه‌های NLSP-CO که از رویه‌های مختص سازوکار پشتیبانی می‌کنند، کارکردهای پروتکل در بند ۱۰ برای کنترل امنیت اتصال و کارکردهای پروتکل کپسوله‌سازی در بند ۱۱ یا ۱۲.
ج- ساختار و کدبندی PDUها طبق بند ۱۳، ساختار و کدبندی PDUها.

۳-۱۴ بیانیه‌ي انطباق با پیاده‌سازی پروتکل

بیانیه‌ی انطباق با پیاده‌سازی پروتکل (PICS) داده شده در پیوست ت باید باتوجه به هر ادعای انطباق با یک پیاده‌سازی از این استاندارد ملی، تکمیل شود. PICS بر طبق پیش‌نویس PICS مربوطه تولید می‌شود.

پیوست الف

(الزامی)

نگاشت نخستینه‌های UN به توصیه‌نامه‌ي CCITT X.213 | ISO/IEC 8348

جدول الف-۱

نخستینه‌های UN	حمل شده توسط	توضیحات
UN-UNITDATA	N-UNITDATA	نگاشت ساده از نخستینه‌ی UN به نخستینه‌ی N-UNITDATA AD1 از توصیه‌نامه‌ی CCITT X.213 | ISO/IEC 8348
UN-CONNECT	N-CONNECT	پارامترها به پارامترهای معادل در توصیه‌نامه‌ی CCITT X.213 | ISO/IEC 8348 نگاشت می‌شوند، غیر از: - احراز هویت UN الحاق شده به UN Userdata که در نخستینه‌های N-CONNECT نگاشت می‌شود.
UN-DATA	N-DATA	نگاشت ساده: تمام پارامترها به پارامترهای معادل توصیه‌نامه‌ی CCITT X.213 | ISO/IEC 8348 نگاشت می‌شوند.
UN-EXPEDITED-DATA	N-EXPEDITED-DATA	نگاشت ساده
UN-DATA-ACKNOWLEDGE	N-DATA-ACKNOWLEDGE	نگاشت ساده
UN-DISCONNECT	N-DISCONNECT	نگاشت ساده

پیوست ب

(الزامی)

نگاشت نخستینه‌های UN به توصیه‌نامه‌ي ISO/IEC 8208 | CCITT X.25

در محیط OSI، به استثناء پارامتر احراز هویت UN-CONNECT UN که در «تسهیلات محافظت» DTE حمل می‌شود، نگاشت بین نخستینه‌های خدمت UN و ISO/IEC 8208 یا توصیه‌نامه‌ی CCITT پروتکل X.25 در ISO/IEC 8878 برای معادل نخستینه‌های خدمات لایه‌ی شبکه، تعریف شده است.

در جدول ب-۱، ستون وسط، بسته‌های ISO/IEC 8208 یا X.25 استفاده‌شده برای حمل نخستینه‌های UN را توصیف می‌کند. در این مورد ISO/IEC 8208 یا X.25 ممکن است به هر نحوی که این استاندارد ملی اجازه دهد استفاده شوند و به‌عنوان مثال Q-bit ممکن است به‌کار گرفته شود. ویژگی‌های خاص ISO/IEC 8208 یا X.25 بدون تغییر از NLSP عبور می‌کنند.

جدول ب-۱

نخستینه‌های UN	حمل شده به‌وسیله‌ی	توضیحات
UN-UNITDATA	N/A	
UN-CONNECT	CALL	تمام پارامترها به تسهیلات بسته معادل درتوصیه‌نامه‌ی CCITT X.213 | ISO/IEC 8348 نگاشته می‌شوند به استثناء پارامتر احراز هویت UN که در «تسهیلات محافظت» DTE حمل می‌شود.
UN-DATA	DATA	نگاشت ساده
UN-EXPEDITED-DATA	INTERRUPT	نگاشت ساده
UN-DATA-ACKNOWLEDGE	PR یا RNR	نگاشت ساده
UN-DISCONNECT	CLEAR	نگاشت ساده

پیوست پ
(الزامی)
پروتکل همبستگي امنیتی با به‌کارگیری تبادل نشانه‌ي کلید و امضای دیجیتالي

پ-۱ مرور کلی

این پیوست معرف پروتکلی برای استفاده از یک سازوکار نامتقارن جهت عملی ساختن برقرارسازی و لغو/آزادسازی SA است. این پروتکل به هستارهای در حال ارتباط NSLP امکان می‌دهد تا:

الف- اعتبار دو هستار را برای هم احراز هویت کنند؛

ب- به صفات SA از جمله کلیدها مقدار اولیه بدهند؛ و

پ- اطلاعات اولیه را برای استفاده در ارائه یکپارچگی برقرار کنند.

این پیوست یک پروتکل SA را توصیف می‌کند که به‌طور منطقی کارکردهای مجزای زیر را انجام می‌دهد:

الف- تبادل نشانه‌ی کلید (KTE) برای برقراری رمز مشترک مورد استفاده قرار می‌گیرد. این پروتکل از تبادل نشانه‌های کلید پشتیبانی می‌کند. شکل این نشانه‌ها به واسطه‌ی سازوکار مشخص می‌شود. یک نمونه از نشانه‌های کلید مشخص‌شده به‌وسیله‌ی سازوکار، که از تبادل کلیدهای نمایی پشتیبانی می‌کند و تحت نام «تبادل دیفی-هلمن»[1] از آن‌ها نام برده می‌شود، در پیوست ح به‌صورت خلاصه آورده شده است.

ب- گواهی‌نامه‌ها، امضاهای دیجیتالی و عناصر KTE برای رسیدن به احراز هویت مورد استفاده قرار می‌گیرند.

پ- تبادلات پروتکل برای مذاکره در مورد صفات SA به‌کار برده می‌شوند.

ت- تبادلات پروتکل برای اعلام آزادسازی SA به‌کار برده می‌شوند.

پیش از برقراری SA، هر کدام از هستارهای NLSP باید با استفاده از پروتکل SA، اطلاعات زیر را از قبل برقرار کنند:

الف- سازوکارهایی که مورد پشتیبانی هستند و به شکل زیر بیان می‌شوند:

۱- فهرستی از ASSRهای مورد پشتیبانی؛ و

۲- مجموعه خدمات امنیتی پشتیبانی‌شده برای هر کدام از ASSRهای مشخص‌شده در بالا.

ب- یک زوج کلید نامتقارن برای هر کدام از الگوریتم‌های نامتقارن مورد پشتیبانی که می‌تواند به‌وسیله‌ی هستار NLSP جهت امضای داده برای اهداف احراز هویت به‌کار گرفته شوند.

پ- گواهینامه‌ای از طرف یک مقام مورد اعتماد برای هر کدام از الگوریتم‌های نامتقارن مورد پشتیبانی که هویت هستار NLSP و کلید نامتقارن عمومی آن را برای اهداف احراز هویت مشخص می‌کند.

1 - Diffie Hellman Exchange

ت- کلیدهای عمومی و الگوریتم‌های نامتقارن ضمنی مربوط به هر صادرکننده‌ی گواهی‌نامه‌ی مورد اطمینانی که گواهینامه‌ها را برای هستارهای NLSPی صادر می‌کند که هستار NLSP فعلی با آن‌ها در حال ارتباط است.

پروتکل SA به‌صورت پویا اطلاعات امنیتی زیر را برقرار می‌کند. این پروتکل برای امن‌سازی ارتباطات خودش به این اطلاعات نیاز دارد.

الف- مذاکره الگوریتم رمزگذاری برای محافظت از ارتباطات پروتکل SA؛

ب- مذاکره الگوریتم نامتقارن و طرح امضای دیجیتالی مورد استفاده برای فراهم کردن احراز هویت پروتکل SA؛

پ- تولید اطلاعات کلیدسازی مورد نیاز برای الگوریتم رمزگذاری به‌منظور محافظت از ارتباطات پروتکل SA.

این پروتکل SA اطلاعات به اشتراک گذاشته‌شده زیر را بین دو هستار NLSP برقرار می‌کند:

الف- SA-IDهای محلی و راه دور؛

ب- خدمات امنیتی که میان هستارهای مرتبط با نمونه‌های ارتباط مورد استفاده قرار می‌گیرند؛

پ- سازوکارها و پارامترهای آن‌ها که به‌صورت ضمنی از طریق خدمات امنیتی انتخاب‌شده بیان می‌شوند؛

ت- کلیدهای اشتراکی اولیه برای یکپارچگی، سازوکارهای رمزگذاری و احراز هویت نمونه‌های ارتباطاتی؛

ث- مجموعه برچسب‌های امنیتی که برای کنترل دسترسی در این همبستگی مورد استفاده قرار می‌گیرند.

یک SA می‌تواند با استفاده از خدمات امنیتی انتخاب‌شده‌ی یکسان، سازوکارها و پارامترهای آن‌ها و مجموعه برچسب‌های امنیتی از SA که از پیش ایجاد شده، برقرار شود. در این مورد، فقط SA-ID و کلیدها تغییر می‌کنند و بقیه صفات یکسان باقی خواهند ماند.

هر وقت که یک SA جدید برقرار می‌شود، باید مقادیر کلید جدید نیز برقرار شوند.

در حالت NLSP بی‌اتصال، بعد از این که یک SA آزاد شد، SA-ID نباید دوباره مورد استفاده قرار گیرد. دوره‌ای که SA-ID بدون تغییر است باید از حداکثر طول عمر یک PDU در شبکه‌ی اصلی بیشتر باشد.

صفت SA، Adr-Served با ابزاری خارج از این پروتکل برقرار می‌شود.

راه‌انداز صفت SA برای راه‌انداز تبادل پروتکل SA به حالت true و برای پاسخ‌دهنده به حالت false تنظیم می‌شود.

پ-۲ تبادل نشانه‌ی کلید (KTE)

هستارهای NLSP پروتکل SA خود را با یک KTE شروع می‌کنند تا یک رمز به اشتراک گذاشته (یعنی یک رشته بیتی) بین هستارها را تولید کنند. هستارهای NLSP سپس از یک زیرمجموعه از این رشته بیتی مخفی به همراه یک الگوریتم کلید خصوصی استفاده می‌کنند تا باقیمانده ارتباطات مابین خود را رمزگذاری کنند، و به این ترتیب قابلیت محرمانگی را برای باقیمانده تبادلات پروتکل SA فراهم می‌کنند.

KTE شامل تبادل دو مقدار Key-Token-1 و Key-Token-2 است که از پارامترهای مختص سازوکار و اعداد تولیدشده‌ی محلی با استفاده از الگوریتم‌های مختص سازوکار نظیر الگوریتم‌های پیوست ح محاسبه

می‌شوند. مقادیر مبادله‌شده بعدها توسط دو هستار در حال ارتباط برای تولید رشته بیتی مخفی به اشتراک گذاشته‌شده به‌کار برده می‌شوند.

زیرمجموعه‌ای از این رشته بیتی در کنار یک الگوریتم کلید خصوصی مورد استفاده قرار می‌گیرد تا باقیمانده تبادل پروتکل SA را رمزگذاری و از احراز هویت پروتکل SA و مذاکره صفت SA پشتیبانی کند. به‌علاوه، زیرمجموعه‌ای از این رشته بیتی نیز مورد ارجاع قرار می‌گیرد تا به‌عنوان کلید و صفات ISN مربوط به همبستگی در حال برقرار شدن مورد استفاده قرار گیرد. این رشته بیتی به یکی از دو روش زیر مورد ارجاع قرار داده می‌شود:

۱- با تبادل اطلاعات موقعیت در مذاکره صفت SA؛ یا

۲- از طریق دانش پیشین.

پ-۳ احراز هویت پروتکل SA

برای اینکه یک هستار NLSP بتواند اصالت هستار دیگری را طی برقرارسازی SA تأیید کند، به یک گواهی احراز هویت و یک زوج کلید عمومی نیاز دارد.

هستارهای NLSP برای درستی‌سنجی هویت یکدیگر گواهی‌نامه و امضاهای دیجیتالی (مانند مواردی که در استاندارد ISO 9594-8 تعریف‌شده است) را مبادله می‌کنند. یک گواهی‌نامه حداقل حاوی برخی اطلاعات شناسایی برای یک NLSPE به علاوه‌ی کلید عمومی هستار است.

گواهی‌نامه به‌وسیله‌ی یک مقام مورد اعتماد تأیید و با استفاده از رویه‌ای خارج از حیطه‌ی پروتکل NLSP، برای NLSP ارائه می‌شود. گواهی‌نامه شامل امضای احراز هویت مقام مورد اعتماد است. یک هستار NLSP که در این پروتکل SA شرکت می‌کند باید کلید عمومی مقام مورد اعتماد صادرکننده‌ی گواهی‌نامه را داشته باشد. روش به‌کار رفته برای به‌دست آوردن کلید عمومی مقام مورد اعتماد خارج از حیطه‌ی این استاندارد ملی است. برای این که یک هستار NLSP نشان دهد که یک گواهی‌نامه خاص را دارا است، باید اثبات کند که کلید مخفی متناظر با کلید عمومی گواهی‌نامه را دارد.

اثبات مناسب بودن عملیات و جلوگیری از حملات بازپخش به‌وسیله‌ی داده‌های علامت‌گذاری‌شده‌ی مختص عملیات این پروتکل که حاوی اعداد مشخص تعیین‌شده به‌صورت مشترک هستند، انجام می‌گیرد. این امر همانند روند زیر برای دو هستار در ارتباط A (راه‌انداز SA) و B (پاسخ‌دهنده) انجام می‌گیرد:

الف- محتویات SA ساخته می‌شوند، این محتویات شامل گواهی A و Key-Token-3 (که به‌وسیله‌ی الگوریتمی همانند الگوریتمی که در پیوست ح توصیف شده است، محاسبه می‌شود) هستند و سپس امضاء می‌شوند. (به‌عنوان مثال به‌وسیله‌ی امضای احراز هویت تعریف‌شده در استاندارد ISO 9594-8) این امضا تبادل ID و طول محتوا را در بر نمی‌گیرد. سپس محتویات SA که حاوی امضاء و طول محتوا است اما تبادل ID را شامل نمی‌شود، رمزگذاری می‌شوند. کلید رمزگذاری، n بیت اول رشته بیتی تولیدشده به‌وسیله‌ی تبادل KTE است که n تعداد بیت‌های مورد نیاز الگوریتم به‌کار رفته است.

ب- محتویات SA ساخته شده، مذاکرات صفات SA (به بند پ-۴ مراجعه شود) یا دلیل آزادسازی/لغو (به بند پ-۵ مراجعه شود) را حمل می‌کند. محتویات SA به‌وسیله‌ی اطلاعات معادل مرتبط با B و Key-Token-4 به جای Key-Token-3 امضا و رمزگذاری می‌شوند.

هر هستار درستی امضای احراز هویت هستار همتا را ابتدا به‌وسیله‌ی رمزگشایی تبادل دریافتی و سپس درستی‌سنجی امضاء و وارسی نشانه‌ی کلید برای مقابله در برابر حمله بازپخش ارزیابی می‌کند. ارزیابی درستی به به‌کارگیری کلید عمومی هستار همتا و پردازش توافق‌شده برای درستی‌سنجی امضاء[1]، نیاز دارد.

پ-۴ مذاکره صفت SA

پ-۴-۱ انتخاب خدمت امنیتی

به‌عنوان یک تصمیم محلی، هستار NLSP راه‌انداز یک یا چند مجموعه از انتخاب‌های خدمت امنیتی مورد پذیرش را صادر می‌کند. هر عنصر در مجموعه حاوی موارد زیر است:

الف- ASSR_ID که معناشناسی خدمات امنیتی انتخاب‌شده (که در زیر فهرست شده است) را برای این عنصر در مجموعه تعریف می‌کند؛ و

ب- مقادیر انتخاب خدمت (معناشناسی آن توسط ASSR_ID تعریف می‌شود) برای محرمانگی، احراز هویت، کنترل دسترسی، یکپارچگی و محرمانگی جریان ترافیک.

هستار NLSP دریافت‌کننده براساس خط‌مشی امنیتی محلی خود، PCI زیر را به صادرکننده‌ی پیام برمی‌گرداند:

الف- اگر یکی از مجموعه خدمات پیشنهادشده مورد قبول باشد، دریافت‌کننده یک عنصر خدمت انتخاب شده‌ی منفرد را برمی‌گرداند.

ب- اگر هیچ یک از مجموعه خدمات پیشنهادشده مورد قبول نباشد، دریافت‌کننده، SA را رد می‌کند و وضعیت نشان‌دهنده‌ی دلیل رد شدن SA را برمی‌گرداند.

یادآوری– این مذاکره به هر دو هستار NLSP این امکان را می‌دهد که خدمات امنیتی که با خط‌مشی امنیتی محلی آن‌ها سازگار است را انتخاب کنند.

پ-۴-۲ مذاکره مجموعه برچسب[2]

براساس خط‌مشی امنیتی محلی، هستار NLSP راه‌انداز یک مجموعه از برچسب‌های امنیتی و مراجعی که نیاز دارد تحت محافظت این SA انتقال داده شود را صادر می‌کند. هر عنصر در مجموعه حاوی موارد زیر است:

الف- یک مرجع که می‌تواند به جای برچسب در طی طول عمر SA به دلایل کارایی حمل شود؛ و

ب- معناشناسی کامل برچسب.

1 - Verifying the signature
2 - Label Set Negotiation

براساس خط‌مشی امنیتی محلی، هستار NLSP دریافت‌کننده تعیین می‌کند که کدام مجموعه پیشنهادی از برچسب‌ها را می‌خواهد تحت محافظت این SA انتقال بدهد. هستار NLSP دریافت‌کننده PCI زیر را به صادرکننده‌ی پیام برمی‌گرداند:

الف- اگر یک یا چند برچسب در مجموعه‌ی پیشنهادی قابل قبول باشد، دریافت‌کننده یک زیرمجموعه از مجموعه مراجع پیشنهادی را برمی‌گرداند.

ب- اگر هیچ برچسبی در مجموعه‌ی پیشنهادی قابل قبول نباشد، دریافت‌کننده SA را رد کرده و یک وضعیت نشان‌دهنده دلیل رد شدن SA را برمی‌گرداند.

یادآوری– این مذاکره به هستار TLSP اجازه می‌دهد یک مجموعه برچسب که با خط مشی امنیتی محلی آن سازگار است را انتخاب کند.

پ-۴-۳ انتخاب ISN و کلید

به‌عنوان یک تصمیم محلی، هستار NLSP راه‌انداز، قسمتی از رشته بیتی حاصل از KTP را برای استفاده به‌عنوان کلیدها و/ یا ISNها در طی ارتباطات (یعنی ارتباطات NLSP نه ارتباطات پروتکل SA) با هستار دریافت‌کننده انتخاب می‌کند. کلید/ISN با تبادل موقعیت بیت آغازین در رشته بیتی حاصل از KTE مشخص می‌شود. طول کلید/ISN با استفاده از پارامترهای مرتبط با خدمت انتخابی مشخص می‌شود. یک مجموعه اشاره‌گر برای موارد زیر به هستار NLSP دریافت‌کننده ارسال می‌شود:

الف- کلید رمزگذاری داده‌ی عادی؛

ب- کلید رمزگذاری داده‌ی پیشتاز؛

پ- کلید تولید وارسی یکپارچگی داده‌ی عادی؛

ت- کلید تولید وارسی یکپارچگی داده‌ی پیشتاز؛

ث- My ISN برای داده‌ی عادی؛

ج- My ISN برای داده‌ی پیشتاز؛ و

ح- کلید تولید احراز هویت.

به‌طور مشابه، هستار NLSP دریافت‌کننده به‌صورت محلی مشخص می‌کند کدام یک از قسمت‌های رشته بیتی حاصل از KTE را برای کلیدها/ISNها استفاده خواهد کرد. هستار NLSP دریافت‌کننده PCI زیر را به صادرکننده‌ی پیام برمی‌گرداند:

الف- اگر دریافت‌کننده همان موقعیت بیت پیشنهادشده به‌وسیله‌ی هستار NLS راه‌انداز را انتخاب کند هیچ PCI صریحی برگشت داده نمی‌شود؛

ب- اگر دریافت‌کننده SA را به‌دلیل سایر شکست‌های مذاکره رد کند، هیچ PCI صریحی برگشت داده نمی‌شود؛

پ- اگر دریافت‌کننده موقعیت‌های بیتی متفاوتی را برای کلیدها/ISNهای خود انتخاب کند، یک مجموعه اشاره‌گر برگشت خواهد داد.

یادآوری ۱- یک مقدار کلید یکسان می‌تواند برای اهداف متعدد با فراهم کردن اشاره‌گر یکسان جهت بیش از یک کلید/ISN به‌کار رود.

یادآوری ۲- این رویه در صورتی که موقعیت انتخاب کلیدها و ISNها از قبل مشخص باشد، نیاز نیست انجام شود.

ب-۴-۴ مذاکره صفات گوناگون SA

به‌عنوان یک تصمیم محلی، هستار NLSP راه‌انداز مقدار صفات SA زیر را برای SA در حال برقرارسازی مشخص می‌کند:

الف- حفظ این صفات SA در هنگام قطع اتصال (فقط NLSP-CO)؛

ب- محافظت از پارامترهای CO (فقط NLSP-CO)؛

پ- گزینه No-Header باید استفاده شود (فقط NLSP-CO).

هستار NLSP راه‌انداز این مجموعه صفات SA پیشنهادی را در قالب فیلد پرچم‌های مختلف به هستار NLSP دریافت‌کننده ارسال می‌کند.

هستار دریافت‌کننده‌ی NLSP براساس تصمیم‌گیری محلی، PCI زیر را به صادرکننده‌ی پیام برمی‌گرداند:

الف- اگر دریافت‌کننده تمام صفات SA پیشنهادی را بپذیرد، هیچ PCI صریحی برگشت داده نمی‌شود. اگر دریافت‌کننده SA را رد نکند، دلالت بر این دارد که صفات SA برای هستار NLSP دریافت‌کننده قابل قبول هستند.

ب- اگر هیچ کدام از صفات قابل قبول نباشند، دریافت‌کننده SA را رد کرده و صفاتی که باعث رد شدن شده را برمی‌گرداند.

پ-۴-۵ کلیددهی مجدد

اگر یک SA برای کلیددهی مجدد به SA قدیمی برقرار شود آنگاه فقط کلید و انتخاب ISN انجام می‌شود. به‌جای تنظیم خدمت، مجموعه‌ی برچسب و مذاکره صفات گوناگون SA، مرجعی به SA قدیمی که این صفات از آن به ارث رسیده‌اند در Old_Your_SA-ID قرار داده می‌شوند.

پ-۵ لغو/آزادسازی SA

یک هستار می‌تواند از طریق مبادله‌ی دو طرفه‌ی SA PDUها با یک کد دلیل امضاء و رمزگذاری‌شده توسط رویه‌های تعریف‌شده در بند پ-۳، نشان دهد که دیگر از یک همبستگی امنیتی استفاده نمی‌کند.

پ-۶ نگاشت کارکردهای پروتکل SA به تبادلات پروتکل

این پروتکل SA سه کارکرد توصیف‌شده در بالا را در طول سه تبادل پروتکل متفاوت اجرا می‌کند:

الف- اولین تبادل شامل EKE و تبادل گواهی‌نامه است و هیچ رمزگذاری در آن استفاده نمی‌شود.

ب- دومین تبادل شامل یک مذاکره امنیتی محافظت‌شده برای ارائه احراز هویت توصیف‌شده در بند پ-۳ است.

پ- وقتی که دیگر نیاز نیست SA شامل کد دلیل[1] محافظت‌شده باشد، (برای فراهم‌سازی احراز هویت به صورتی که در بند پ-۳ توصیف شده) یک تبادل مجزا آغاز می‌شود.

پ-۶-۱ (اولین) تبادل KTE

پ-۶-۱-۱ درخواست برای آغاز پروتکل SA

هستار NLSP یا مدیریت امنیتی محلی پروتکل SA را راه‌اندازی می‌کنند.
هستار NLSP راه‌انداز کارکردهای زیر را انجام می‌دهد و اطلاعات زیر را به دریافت‌کننده ارسال می‌کند:
الف- یک SA-ID موجود انتخاب و به‌عنوان My_SA-ID صادرکننده‌ی پیام قرار داده می‌شود.
ب- KTE آغاز شده و نشانه‌ی کلید ۱ فرستاده می‌شود.
پ- فهرستی از سازوکارهای محرمانگی پیشنهادی که می‌تواند برای محافظت از دومین تبادل پروتکل SA استفاده شود. این فهرست به‌صورت مجموعه‌ای از یک یا چند عنصر که شامل ASSR_ID و خدمات امنیتی محرمانگی انتخاب‌شده است، بیان می‌شود. اگر سازوکار از قبل توافق شده باشد، نیاز نیست که این فهرست ارسال شود.
ت- فهرستی از سازوکارهای یکپارچگی پیشنهادی که یکی از آن‌ها برای امضای دیجیتالی دومین تبادل پروتکل SA به‌کار می‌رود. این فهرست به‌صورت مجموعه‌ای از یک یا چند عنصر شامل ASSR_ID و خدمات امنیتی یکپارچگی انتخاب‌شده بیان می‌شود. اگر سازوکار از قبل توافق شده باشد، نیاز نیست که این فهرست ارسال شود.

یادآوری ۱- خدمات امنیتی محرمانگی انتخاب‌شده باید تنها یک الگوریتم رمزگذاری متقارن و حالت‌های کاری آن را شناسایی کنند. خدمات امنیتی یکپارچگی انتخاب‌شده باید تنها یک الگوریتم نامتقارن و طرح امضاهای دیجیتالی مربوط به آن را شناسایی کنند.

یادآوری ۲- موارد پ و ت ممکن است از قبل شناخته شده باشند.

در مورد CO، اگر پس از اتمام مهلت زمانی هیچ PDU برای اولین تبادل بازنگردد، SA برقرار نمی‌شود و هیچ تلاش دیگری صورت نمی‌پذیرد.
در مورد CL، اگر پس از اتمام مهلت زمانی هیچ PDU برای اولین تبادل بازنگردد، هستار NLSP راه‌انداز PDU اولین تبادل خود را دوباره ارسال می‌کند. تعداد ارسال‌های مجدد به تعداد متناهی تعریف شده به‌صورت محلی محدود شده است.

پ-۶-۱-۲ دریافت اولین SA PDU توسط دریافت‌کننده

در هنگام دریافت اولین SA PDU، هستار NLSP دریافت‌کننده کارکردهای زیر را انجام می‌دهد و اطلاعات زیر را به راه‌انداز می‌فرستد:

1 - Reason code

الف- My_SAID دریافتی در فیلد Your-SAID مربوط به سرآیند عمومی توصیف‌شده در زیربند ۱۳-۴ قرار داده می‌شود.
ب- یک SAID موجود انتخاب شده و به‌عنوان My_SAID صادرکننده‌ی پیام ارسال می‌شود.
پ- هستار NLSP دریافت‌کننده براساس خط‌مشی امنیتی محلی، PCI توصیف‌شده در زیر را به صادرکننده‌ی پیام برمی‌گرداند:
۱- اگر دریافت‌کننده یکی از سازوکارهای یکپارچگی پیشنهادی را بپذیرد، سازوکار انتخاب‌شده را برمی‌گرداند. اگر راه‌انداز یک سازوکار منفرد را پیشنهاد داده باشد، هیچ PCI صریحی برگشت داده نمی‌شود.
۲- اگر هیچ کدام از سازوکارهای محرمانگی قابل قبول نباشد، دریافت‌کننده SA را رد کرده و دلیل رد شدن را برمی‌گرداند.
ت- اگر هم سازوکار محرمانگی و هم یکپارچگی انتخاب شده باشند، محاسبه‌ی KTE آغاز و Key-Token-2 ارسال می‌شود.
در مورد CO، اگر PDUای از دومین تبادل پس از مهلت زمانی بازنگردد، SA برقرار نشده و هیچ تلاش دیگری صورت نمی‌پذیرد.
در مورد CL، اگر PDUای از دومین تبادل پس از اتمام مهلت زمانی بازنگردد، هستار NLSP راه‌انداز دوباره PDU اولین تبادل خود را ارسال می‌کند. تعداد ارسال‌های مجدد به تعداد متناهی تعریف شده به‌صورت محلی محدود شده است.
در مورد CL، اگر PDU مربوط به اولین تبادل دوباره دریافت شود، PUD بازگشتی از نو ارسال می‌شود.

پ-۶-۲ (دومین) تبادل احراز هویت مذاکره‌ی امنیتی و احراز هویت

پ-۶-۲-۱ دریافت اولین SA PDU به‌وسیله‌ی راه‌انداز

در هنگام دریافت اولین SA PDU، هستار NLSP راه‌انداز کارکردهای زیر را انجام می‌دهد:
الف- MY_SAID دریافتی در فیلد Your_SAID مربوط به سرآیند عمومی همان‌طورکه در زیربند ۱۳-۴ توصیف شده است، قرار می‌گیرد.
ب- گواهی‌نامه‌ی راه‌انداز مربوط به سازوکار یکپارچگی انتخاب‌شده در گواهی فیلد محتوا قرار داده می‌شود.
پ- راه‌انداز Key-Token-3; را تولید می‌کند.
ت- فهرستی از خدمات امنیتی پیشنهادی که برای محافظت ارتباطات NLSP به‌کار می‌روند در Content Field Service Selection قرار داده می‌شود.
ث- یک مجموعه از برچسب‌های پیشنهادی که می‌توانند به‌وسیله‌ی SA در طی ارتباط NLSP محافظت شوند در Label_Def قرار داده می‌شوند.
ج- یک مجموعه از انتخاب‌های کلید/ISN در Key Selection قرار داده می‌شود.
چ- صفات SA مختلفی که برای این SA لازم هستند در پرچم‌های SA قرار داده می‌شوند.

ح- اگر برقرارسازی SA یک SA قدیمی را کلیددهی مجدد می‌کند آنگاه Old Your SA-ID به SA-ID مربوط به SA قدیمی تنظیم می‌شود. اگر این روند انجام پذیرد موارد ت، ث و ج نباید اجرا شوند.
خ- محافظت از محتویات SA همان طور که در بند پ-۳ توصیف شد.
در مورد CO، اگر یک PDU از دومین تبادل پس از اتمام مهلت زمانی بازنگردد، SA برقرار نشده و هیچ تلاش دیگری صورت نمی‌پذیرد.
در مورد CL، اگر یک PDU از دومین تبادل پس از اتمام مهلت زمانی بازنگردد، هستار NLSP راه‌انداز دوباره PDU دومین تبادل خود را ارسال می‌کند. تعداد ارسال‌های مجدد به تعداد متناهی تعریف شده به‌صورت محلی محدود شده است.
در مورد CL، اگر PDU از اولین تبادل دوباره دریافت شود، PUD دومین تبادل دوباره ارسال می‌شود.

پ-۶-۲-۲ دریافت PDU دومین تبادل به‌وسیله‌ی دریافت‌کننده

به محض دریافت PDU دومین تبادل، هستار NLSP دریافت‌کننده کارکردهای زیر را انجام داده و اطلاعات زیر را به راه‌انداز می‌فرستد:
الف- MY_SAID دریافتی، در فیلد Your_SAID سرآیند عمومی همان‌طورکه در زیربند ۱۳-۴ توصیف شده است، قرار می‌گیرد.
ب- موارد زیر وارسی می‌شوند. اگر وارسی هر موردی با شکست مواجه شود، آنگاه SA رد شده و دلیل رد شدن SA برگردانده می‌شود:
۱ - وارسی می‌شود که امضای دیجیتالی دریافتی معتبر باشد.
۲ - وارسی می‌شود که Key-Token-3 دریافتی معتبر باشد.
۳ – وارسی می‌شود که کدام یک از خدمات مجموعه خدمات امنیتی پیشنهادی مورد قبول هستند. تنها یکی از خدمات امنیتی پیشنهادی می‌تواند انتخاب شود.
۴ - مجموعه برچسب‌های پیشنهادی وارسی می‌شوند تا مشخص شود آیا مورد قابل قبولی وجود دارد.
۵ – صفات گوناگون SA وارسی می‌شوند تا مشخص شود که همگی مورد قبول باشند.
پ- اگر Old Your SA-ID در PDU دریافتی باشد، آنگاه SA مناسب از SA-ID مورد ارجاع رونوشت می‌شود. در این مورد فیلدهایی که در قسمت‌های پ و ث در زیر توصیف شده‌اند نمی‌توانند ارسال شوند.
در صورتی که تمام وارسی‌ها موفقیت‌آمیز باشند، موارد زیر ارسال می‌شوند:
الف- گواهی‌نامه راه‌انداز مربوط به سازوکار یکپارچگی انتخابی ارسال می‌شود.
ب- خدمات امنیتی انتخابی که مورد استفاده برای محافظت از ارتباطات NLSP هستند، ارسال می‌شوند. اگر مجموعه خدمات پیشنهادی محتوی یک عنصر باشند هیچ PCIی برگشت داده نمی‌شود.
پ- دریافت‌کننده Key-Token-4 را تولید می‌کند.
ت- زیرمجموعه انتخابی از برچسب‌های پیشنهادی که با استفاده از این SA می‌توانند در طی ارتباط NLSP محافظت شوند، ارسال می‌شود.

ث- یک مجموعه از اشاره‌گرهای کلید/ISN ارسال می‌شود. اگر کلیدهای پیشنهادی راه‌انداز برای استفاده‌ی پاسخ‌دهنده مورد قبول باشند، هیچ مقدار جدیدی ارسال نمی‌شود.
ج – محافظت از محتویات SA همان‌طورکه در بند پ-۳ توصیف شده است.
در مورد CL، اگر PDU دومین تبادل دوباره دریافت شود ، دریافت‌کننده، PDU دومین تبادل خود را از نو ارسال می‌کند.

پ-۶-۳ تبادل آزادسازی/لغو SA

پ-۶-۳-۱ درخواست برای آغاز آزادسازی/لغو SA

هستار NLSP یا مدیریت امنیتی محلی، آزادسازی/لغو SA را راه‌اندازی می‌کنند. نیازی نیست که راه‌انداز یک آزادسازی/لغو SA همان راه‌انداز برقرارسازی SA باشد.
الف- اگر هستار محلی راه‌انداز برقرارسازی SA باشد، آنگاه Key-Token-3 تولید می‌شود در غیر این‌صورت Key-Token-4 تولید می‌شود. در هر دو حالت نشانه‌ی تولیدشده در محتویات SA قرار داده می‌شود.
ب- کد دلیل مناسب در فیلد محتوی Abort/Release Reason،SA قرار داده می‌شود.
پ – محافظت از محتوی SA همان‌طورکه در بند پ-۳ توصیف شده است.
در مورد CO، اگر یک PDU تأیید درخواست آزادسازی/لغو پس از اتمام مهلت زمانی بازنگردد، SA برقرار نشده و هیچ تلاش دیگری صورت نمی‌گیرد.
در مورد CL، اگر یک PDU از یک تبادل آزادسازی/لغو پس از اتمام مهلت زمانی بازنگردد، هستار NLSP راه‌انداز، PDU درخواست آزادسازی/لغو SA را دوباره ارسال می‌کند. ارسال‌های مجدد به یک تعداد متناهی تعریف شده به‌صورت محلی، محدود شده‌اند.

پ-۶-۳-۲ دریافت درخواست آزادسازی/لغو SA

به‌محض دریافت PDU تأیید آزادسازی/لغو SA، هستار NLSP دریافت‌کننده کارکردهای زیر را انجام می‌دهد و اطلاعات زیر را به راه‌انداز ارسال می‌کند:
الف- اگر هستار محلی، راه‌انداز برقرارسازی SA باشد، آنگاه Key-Token-3 تولید می‌شود در غیر این‌صورت Key-Token-4 تولید می‌شود. در هر دو حالت نشانه‌ی تولیدشده در محتویات SA قرار داده می‌شود.
ب- کد دلیل مناسب در فیلد دلیل آزادسازی/لغو محتوی SA قرار داده می‌شود.
پ – محافظت از محتویات SA همان‌طورکه در بند پ-۳ توصیف شده است.
در مورد CL، اگر PDU از درخواست آزادسازی/لغو دوباره دریافت شود، دریافت‌کننده PDU دومین تبادل خود را تا حداکثر تعداد محدود داده شده، دوباره ارسال می‌کند.

پ-۷ SA PDU – محتویات SA

برای این پروتکل SA خاص، قالب فیلد محتویات SA مربوط به SA PDU که در زیربند ۱۳-۴ تعریف شده، در شکل پ-۱ نمایش داده شده است.

شکل پ-۱ – محتویات SA

پ-۷-۱ ID تبادل

اگر PDU مربوط به اولین تبادل نشانه‌ی کلید (KTE) باشد این فیلد مقدار 00000000 را خواهد داشت و اگر PDU مربوط به دومین تبادل مذاکره/احراز هویت باشد، مقدار 00000001 را خواهد داشت. اگر PDU مربوط به درخواست آزادسازی/لغو SA باشد مقدار 10000000 و اگر PDU مربوط به تأیید آزادسازی/لغو SA باشد، مقدار 10000001 را خواهد داشت.

پ-۷-۲ طول محتوا

طول هشت‌تایی‌های تمام فیلدهای محتوا به جز فیلد طول محتوا.

پ-۷-۳ فیلدهای محتوا

کدبندی نوع فیلد محتوا در زیربند ۱۳-۲ تعریف شده است. فیلدهای محتوای SA-P (یعنی A0-BF) که به‌وسیله‌ی رویه‌های این پیوست استفاده می‌شوند، در زیر آمده‌اند:

مقدار	نوع فیلد محتوا
A0	MY SA-ID
A1	Old Your SA-ID
A2	Key Token 1
A3	Key Token 2
A4	احراز هویت امضای دیجیتالی
A5	احراز هویت گواهی‌نامه
A6	Service Selection
A7	SA Rejection Reason
A8	SA Abort/Release Reason
A9	Label-Def
AA	SA Flags
AB	انتخاب کلید
AC	ASSR
AD	Key Token 3
AE	Key Token 4
AF-BF	ذخیره‌شده برای استفاده در آینده

یادآوری– کدهای دیگر برای استفاده خصوصی در زیربند ۱۳-۲ از متن اصلی این استاندارد ملی، ذخیره شده‌اند.

فیلدهای The Service Selection و SA Rejection Reason و Label-Def و SA Flags و Key Selection در این تعریف محتوای پروتکل SA، اختیاری هستند.

پ-۷-۳-۱ My SA-ID

این فیلد اجباری تنها در اولین مبادله مورد استفاده قرار می‌گیرد. این پارامتر شناسه‌ی محلی برای یک همبستگی امنیتی است.

پ-۷-۳-۲ Old Your SA-ID

این فیلد اگر صفات (غیر از کلیدها)، از SA قدیمی ارث برده[1] شوند، در دومین تبادل مورد استفاده قرار می‌گیرد.

پ-۷-۳-۳ Key-Token-1، Key-Token-2، Key-Token-3 و Key-Token-4

این فیلدهای اجباری همان‌طورکه پیش‌تر در این پیوست توصیف شد، برای پشتیبانی KTE و احراز هویت مورد استفاده قرار می‌گیرند.

پ-۷-۳-۴ احراز هویت امضای دیجیتالی – گواهی‌نامه

این فیلدهای اجباری همان طور که پیش‌تر در این پیوست توصیف شد، برای پشتیبانی احراز هویت مورد استفاده قرار می‌گیرند.

پ-۷-۳-۵ انتخاب خدمت

این فیلد اختیاری در اولین و دومین تبادل مورد استفاده قرار می‌گیرد:
الف- اگر در طی اولین تبادل مورد استفاده قرار گیرد، سازوکارهای محرمانگی و/یا یکپارچگی پیشنهادی که در طول دومین تبادل پروتکل SA به‌کار می‌رود را شناسایی می‌کند. در این مورد، تنها دو هشت‌تایی اول ارائه می‌شوند.
ب- اگر در طی دومین تبادل مورد استفاده قرار گیرد، برای پیشنهاد تمام سازوکارهای مورد استفاده در طی ارتباطات NLSP که به‌وسیله‌ی SA در حال برقرارسازی محافظت می‌شوند، به‌کار می‌رود.
این فیلد پس از وقوع پارامتر ASSR می‌آید و ممکن است یک یا چند بار در تبادلات اول یا دوم PDU برای تشکیل یک مجموعه پیشنهادی از خدمات امنیتی جهت مذاکره، حضور داشته باشد. هر پارامتر به پارامتر ASSR پیشین بلافصل مربوط است.
این پارامتر حاوی یک دنباله از هشت‌تایی‌ها است که سطوح مورد نیاز خدمات امنیتی انتخاب‌شده را مشخص می‌کنند. معناشناسی سطوح به‌عنوان قسمتی از خط‌مشی امنیتی تعریف شده است. هشت‌تایی‌ها برای هر یک از خدمات امنیتی به ترتیب مشخص‌شده در زیر، ظاهر می‌شوند. دنباله هشت‌تایی‌ها می‌تواند کوتاه شود

1 - Inherited

اگر هشت‌تایی‌های کوتاه‌شده همگی مربوط به خدماتی باشند که مقدار آن‌ها صفر است. یک هشت‌تایی با مقدار ۲۵۵ نشان می‌دهد که خدمات امنیتی انتخابی از قبل برقرار شده‌اند.

هشت‌تایی	*معنی*
۱	محرمانگی بی‌اتصال/ محرمانگی اتصال
۲	یکپارچگی بی‌اتصال/ یکپارچگی اتصال بدون بازیابی
۳	احراز هویت مبدأ داده/ احراز هویت هستار همتا
۴	کنترل دسترسی
۵	محرمانگی جریان ترافیک

پ-۷-۳-۶ دلیل رد شدن SA

این فیلد اختیاری ممکن است در اولین یا دومین تبادل PDU حاضر باشد. این فیلد برای نشان دادن رد شدن یک SA در طی برقرارسازی آن، ارائه می‌شود. این فیلد حاوی دلیل رد شدن به‌صورت زیر است:

مقدار	*معنی*
۱	سازوکار محرمانگی پشتیبانی نمی‌شود.
۲	سازوکار یکپارچگی پشتیبانی نمی‌شود.
۳	سازوکار کنترل دسترسی پشتیبانی نمی‌شود.
۴	سازوکار احراز هویت پشتیبانی نمی‌شود.
۵	محرمانگی جریان ترافیک پشتیبانی نمی‌شود.
۶	سازوکار محرمانگی رد شده است.
۷	سازوکار یکپارچگی رد شده است.
۸	سازوکار کنترل دسترسی رد شده است.
۹	سازوکار احراز هویت رد شده است.
۱۰	محرمانگی جریان ترافیک رد شده است.
۱۱	امضای احراز هویت نامعتبر است.
۱۲	گواهی‌نامه نامعتبر است.
۱۳	مجموعه برچسب پیشنهادی رد شده است.
۱۴	Retain_on_Disconnect رد شده است.
۱۵	Param_Prot رد شده است.
۱۶	No_Header رد شده است.

پ-۷-۳-۷ دلیل آزادسازی/لغو SA

این فیلد اجباری در نشان و درخواست آزادسازی/لغو SA ارائه شده است. این فیلد برای مشخص کردن دلیل آزادسازی/لغو SA استفاده می‌شود.

برای لغو به صفر و برای آزادسازی عادی به ۱ تنظیم می‌شود. مقادیر ۲ تا ۱۲۷ برای استفاده در آینده ذخیره شده‌اند. مقادیر دیگر برای استفاده در کدهای دلیل تعریف‌شده‌ی خصوصی به‌کار می‌روند.

پ-۷-۳-۸ Label-Def

این فیلد اختیاری تنها برای استفاده در دومین تبادل PDU به‌کار می‌رود. فیلد Label-Def ممکن است یک یا چند بار استفاده شود:

الف- اگر به‌وسیله‌ی ارسال‌کننده‌ی پیام مورد استفاده قرار گیرد برای پیشنهاد یک مجموعه برچسب امنیتی به کار می رود. ارسال‌کننده باید همیشه از هر دو زیرفیلد استفاده کند.

ب- اگر به‌وسیله‌ی دریافت‌کننده پیام مورد استفاده قرار گیرد برای انتخاب یک زیرمجموعه از مجموعه برچسب پیشنهادی به‌کار می‌رود. دریافت‌کننده تنها باید از زیرفیلد Label-Def استفاده کند.

فیلد Label-Def به دو زیرفیلد تقسیم می‌شود:

الف- یک زیرفیلد Label-Def دو هشت‌تایی (مقدار FF FF در مبنای ۱۶ نباید استفاده شود زیرا این مقدار برای رجوع به برچسب خالی ذخیره شده است.)

ب- یک زیرفیلد برچسب که محتویات آن در زیربند ۱۳-۳-۴-۳-۷ تعریف شده است.

Label_Def یک عدد مربوط به برچسب امنیتی تعریف‌شده در زیرفیلد برچسب است. Label_Def در سایر PDUها به‌عنوان جایگزینی برای حمل برچسب امنیتی مربوطه به‌کار می‌رود.

پ-۷-۳-۹ انتخاب کلید

این فیلد اختیاری تنها برای اســتفاده در دومین تبادل PDU است. این فیلد ممکن است در SCI-Contents به هر تعدادی رخ دهد.

این فیلد به سه زیرفیلد تقسیم می‌شود:

الف- پرچم‌های کاربرد (دو هشت‌تایی)؛

ب- اطلاعات انتخاب کلید (دو هشت‌تایی)؛ و

پ- مرجع کلید (متغیر).

پ-۷-۳-۹-۱ پرچم‌های کاربرد

این زیرفیلد حاوی پرچم‌هایی است که اهداف امنیتی را نشان می‌دهد که قرار است برای آن‌ها کلید تعریف شده در زیرفیلد قبلی استفاده شود. بیت‌ها به‌نحوی کدبندی شده‌اند که مقدار صفر به معنی FALSE و مقدار ۱ به معنی TRUE است. کلید می‌تواند برای ترکیبی از هر یک از اهداف زیر استفاده شود. ترکیب‌های مجاز بستگی به خط‌مشی امنیتی محلی دارند.

شماره بیت / هشت‌تایی ۱	خدمت	داده	مبدأ داده
۱	محرمانگی	عادی	راه‌انداز SA
۲	محرمانگی	عادی	پاسخ‌دهنده SA
۳	محرمانگی	پیشتاز	راه‌انداز SA
۴	محرمانگی	پیشتاز	پاسخ‌دهنده SA
۵	تولید ICV	عادی	راه‌انداز SA
۶	تولید ICV	عادی	پاسخ‌دهنده SA
۷	تولید ICV	پیشتاز	راه‌انداز SA
۸	تولید ICV	پیشتاز	پاسخ‌دهنده SA

شماره بیت/ هشت‌تایی ۲	خدمت	داده	مبدا داده
۱	احراز هویت		راه‌انداز SA
۲	احراز هویت		پاسخ‌دهنده SA
۳	ISN	عادی	راه‌انداز SA
۴	ISN	عادی	پاسخ‌دهنده SA
۵	ISN	پیشتاز	راه‌انداز SA
۶	ISN	پیشتاز	پاسخ‌دهنده SA

پاسخ‌دهنده می‌تواند انتخاب‌ها را برای استفاده خود بازنویسی کند.

پ-۷-۳-۹-۲ اطلاعات انتخاب کلید

این فیلد، مکانی در رشته بیتی حاصل از KTE را مشخص می‌کند که کلید انتخاب‌شده، از آن مقدار می‌گیرد. طول کلید از طریق خدمات امنیتی انتخاب‌شده‌ی مرتبطی که الگوریتم مربوطه را مشخص می‌کند، تعیین می‌شود. چندین کلید ممکن است از موقعیت بیت یکسان (یعنی کلید یکسان) استفاده کنند. ترکیب‌های مجاز بستگی به خط‌مشی امنیتی محلی دارند.

پ-۷-۳-۹-۳ مرجع کلید

این زیرفیلد اختیاری برای فعال‌سازی مرجع بعدی به کلید استفاده می‌شود. این امر به‌عنوان مثال می‌تواند برای اهداف ممیزی یا انتخاب یک کلید جدید برای یک اتصال (با به‌کارگیری PDU کنترل امنیت اتصال)، استفاده شود. مقدار این مرجع باید برای همبستگی امنیتی یکتا باشد.

پ-۷-۳-۱۰ پرچم‌های SA

این فیلد اختیاری تنها برای استفاده در دومین تبادل PDU است. مکان‌های بیتی زیر برای اعلام صفات SA شناسایی شده به‌کار می‌روند. مقدار صفر به معنی false و مقدار ۱ به معنی true است.

بیت	*صفت SA*
۱	Retain-on-Disconnect
۲	Param_Prot
۳	No_Header
۸-۴	ذخیره‌شده برای استفاده در آینده

بیت‌های ۴ تا ۸ در زمان انتقال به صفر تنظیم می‌شوند و در هنگام دریافت از آن‌ها صرف‌نظر می‌شود.

پ-۷-۳-۱۱ ASSR

این فیلد در صورتی که فیلد انتخاب خدمت ارائه شود، باید حضور داشته باشد. این فیلد شناسه‌ی شئ است (همان‌طورکه در استاندارد ISO/IEC 9834 تعریف شده است) که مجموعه قواعد امنیتی (تعریف‌کننده‌ی سازوکارهایی که باید برای کیفیت محافظت خدمت انتخاب‌شده اعمال شوند) را مشخص می‌کند.
این فیلد ممکن است بیش از یک بار حضور داشته باشد که در این‌صورت پارامترهای انتخاب خدمت که در ادامه هر رویداد می‌آیند به پارامتر ASSR پیشین بلافصل مربوط می‌شوند.

پیوست ت
(الزامی)
پیش‌نویس NLSP PICS[1]

ت-۱ مقدمه

متصدی پیاده‌سازی پروتکل که ادعای انطباق با این استاندارد ملی را دارد، باید پیش‌نویس بیانیه‌ی انطباق با پیاده‌سازی پروتکل (PICS)[2] زیر را تکمیل کند.

یک پیش‌نویس PICS تکمیل‌شده، PICS برای پیاده‌سازی مورد نظر است. PICS بیانیه‌ای از قابلیت‌ها و گزینه‌های یک پروتکل پیاده‌سازی شده است. PICS می‌تواند کارکردهای مختلفی داشته باشد از جمله:

- به‌وسیله‌ی پیاده‌ساز پروتکل به‌عنوان یک فهرست وارسی برای کاهش خطر شکست در انطباق با استاندارد به خاطر خطاهای سهوی استفاده شود.
- به‌وسیله‌ی متصدی و دریافت‌کننده‌ی پروتکل – یا دریافت‌کننده‌ی بالقوه - پیاده‌سازی که مرتبط با اساس مشترک از درک ارائه شده توسط پیش‌نویس استاندارد PICS هستند، استفاده شود.
- به‌وسیله‌ی کاربر – یا کاربر بالقوه‌ی - پیاده‌سازی، به‌عنوان اساس وارسی اولیه‌ی امکانات تعامل کاری با یک پیاده‌سازی دیگر استفاده شود. (توجه داشته باشید که اگرچه تعامل کاری هرگز نمی‌تواند تضمین شود، شکست تعامل کاری اغلب می‌تواند از روی PICSهای ناقص پیش‌بینی شود.)
- به‌وسیله‌ی یک آزماینده‌ی پروتکل به‌عنوان اساس انتخاب آزمایش‌های مناسب برای وارسی ادعای انطباق پیاده‌سازی استفاده شود.

ت- ۲ اختصارات و نمادهای خاص

ت-۲-۱ نمادهای وضعیت

ت-۲-۱-۱

M اجباری

ت-۲-۱-۲

O اختیاری

---

۱ - آزادسازی حقوق مؤلف برای پیش‌نویس PICS : کاربران این استاندارد ملی می‌توانند آزادانه پیش‌نویس PICS موجود در این پیوست را بازتولید کنند ، بنابراین می‌توان از این پیش‌نویس برای اهداف مورد نظر و انتشار PICS تکمیل‌شده استفاده کرد.

2- Protocol Implementation Conformance Statement

ت-۲-۱-۳

O.<n> اختیاری، اما پشتیبانی از حداقل یکی از گروه اختیارات برچسب‌زده شده به‌وسیله‌ی عدد یکسان <n> نیاز است.

ت-۲-۱-۴

X ممنوع شده

ت-۲-۱-۵

<item> نماد مورد مشروط[1]، وابسته به پشتیبانی مشخص‌شده برای <item> (به زیربند ت-۳-۴ مراجعه شود.)

ت-۲-۲ کوته‌نوشت‌های عمومی

ت-۲-۲-۱

N/A غیر کاربردی

ت-۲-۲-۲

PICS بیانیه‌ی انطباق با پیاده‌سازی پروتکل

N/A غیر کاربردی

PICS بیانیه‌ی انطباق با پیاده‌سازی پروتکل

ت-۳ دستورالعمل کامل کردن پیش‌نویس PICS

ت-۳-۱ ساختار عمومی پیش‌نویس PICS

قسمت اول پیش‌نویس PICS – شناسایی و خلاصه‌ی پروتکل – همان‌طورکه نشان داده شد باید با اطلاعات ضروری برای شناسایی کامل متصدی و پیاده‌سازی، تکمیل شود.

قسمت اصلی پیش‌نویس PICS یک پرسشنامه با قالب ثابت است که به سه زیربند اصلی تقسیم شده است. این سه زیربند ویژگی‌های عمومی NLSP-CL و NLSP-Co را پوشش می‌دهند. و به دنبال آن‌ها بندهایی مختص هر یک از این دو حالت عملیات آورده شده است. این بندها به زیربندهای بیشتری که هر کدام شامل گروهی از موارد مجزا است تقسیم شده‌اند. سؤالات این پرسشنامه در ستون سمت راست با علامت زدن یک پاسخ در مواردی که انتخاب محدود است (به‌طور معمول «بله» یا «خیر») یا با وارد کردن یک مقدار یا یک

1 - Conditional item

مجموعه یا محدوده‌ای از مقادیر، پاسخ داده می‌شوند. توجه شود که در بعضی موارد می‌توان دو یا چند انتخاب از میان پاسخ‌های موجود را انتخاب کرد. بنابراین تمام انتخاب‌های مرتبط باید علامت زده شوند.
هر مورد با مرجع آن در ستون اول مشخص می‌شود؛ ستون دوم حاوی سوالی است که پاسخ‌دهی می‌شود و ستون سوم حاوی مرجع یا مراجع مشخص‌کننده‌ی مورد، در بدنه‌ی اصلی این استاندارد ملی است. ستون‌های باقیمانده وضعیت یک مورد را ثبت کرده– چه پشتیبانی اجباری، اختیاری، ممنوع یا مشروط باشد- و فضا را برای پاسخ ارائه می‌کند. (به زیربند ت-۳-۴ مراجعه شود.)
یک متصدی هم‌چنین مجاز است که خود (یا از وی درخواست شود) اطلاعات بیشتری (که به‌عنوان اطلاعات اضافی یا اطلاعات استثناء گروه‌بندی می‌شوند) را ارائه کند. هر نوعی از اطلاعات بیشتر باید در زیربندی از موارد برچسب خورده‌ی A<i> یا X<i> به ترتیب برای ارجاع متقابل اهداف ارائه شود که در آن i هر شناسایی غیرمبهم مورد است. (به‌عنوان مثال به‌صورت یک عدد ساده) محدودیت دیگری برای قالب و نمایش آن وجود ندارد.
یک پیش‌نویس PICS تکمیل‌شده، شامل هر نوع اطلاعات اضافی و استثناء، یک بیانیه‌ی انطباق با پیاده‌سازی پروتکل برای پیاده‌سازی مورد نظر است.

یادآوری– در جایی که یک پیاده‌سازی قابلیت پیکربندی به چند روش را دارد (برای مثال موارد موجود در زیربند ت-۵-۱)، یک PICS منفرد ممکن است بتواند تمامی این پیکربندی‌ها را توصیف کند. با این وجود، به‌منظور اینکه ارائه اطلاعات آسان‌تر و شفاف‌تر شود، متصدی این انتخاب را دارد که چندین PICS را ارائه دهد که هر کدام زیرمجموعه‌ای از قابلیت‌های پیکربندی پیاده‌سازی را پوشش می‌دهند.

ت-۳-۲ اطلاعات افزونه

موارد اطلاعات اضافی به متصدی اجازه می‌دهد که اطلاعات بیشتری به قصد کمک به تفسیر PICS ارائه کند. انتظار نمی‌رود که حجم زیادی از اطلاعات ارائه شود و PICS بدون چنین اطلاعاتی نیز می‌تواند کامل در نظر گرفته شود. به‌عنوان مثال می‌توان طرح کلی راه‌هایی که یک پیاده‌سازی (تک) می‌تواند در محیط‌ها و پیکربندی‌های مختلف برقرار شده و عمل کند ؛ یا یک توجیه مختصر – براساس الزامات کاربردی خاص – برای شامل نشدن ویژگی‌هایی که با وجود اختیاری بودن در پیاده‌سازی‌های پروتکل امنیتی لایه‌ی شبکه ارائه می‌شوند را نشان داد.
ارجاع به هر یک از موارد اطلاعات اضافی ممکن است در کنار هر پاسخ در پرسشنامه وارد شود یا در موارد اطلاعات استثناء آورده شوند.

ت-۳-۳ اطلاعات استثناء

بعضی از اوقات ممکن است که متصدی بخواهد به یک مورد با حالت‌های اجباری یا ممنوع‌شده به‌نحوی پاسخ دهد (بعد از اینکه هر یک از شرایط اعمال شد) که با الزامات مشخص‌شده در تعارض باشد. هیچ پاسخ از پیش چاپ‌شده‌ای برای این مورد در ستون پشتیبانی وجود ندارد، در عوض متصدی باید این پاسخ را با یک مرجع X<i> به اطلاعات استثناء در ستون پشتیبانی بنویسد و یک توجیه مناسب در خود مورد استثناء ارائه کند.

پیاده‌سازی که برای آن یک مورد استثناء الزامی باشد مطابق با این استاندارد ملی نیست.

یادآوری - یک علت محتمل برای موقعیت توصیف‌شده در بالا زمانی است که نقصی در این استاندارد ملی گزارش شده است، و انتظار می‌رود که اصلاحیه‌ای الزامات رعایت نشده توسط پیاده‌سازی را تغییر دهد.

ت-۳-۴ وضعیت مشروط

پیش‌نویس PICS حاوی تعدادی مورد مشروط است. این‌ها مواردی هستند که برای آن‌ها، هم کاربردپذیری خود مورد و هم وضعیت آن در صورت کاربرد – به‌صورت اجباری، اختیاری یا ممنوع‌شده – وابسته به آن است که سایر موارد معین پشتیبانی شده‌اند یا خیر.

موارد مشروط مجزا به‌وسیله‌ی یک نماد مشروط در قالب <item>:<s> در ستون وضعیت نشان داده می‌شوند که در آن <item> مرجع موردِ ظاهرشده در ستون اول جدول برای موارد دیگر است و <s> یکی از نمادهای وضعیت M، O، O.n یا X است.

اگر موردی که توسط نماد مشروط به آن ارجاع داده شده است، مورد مشروط قابل اعمال باشد وضعیت آن با <s> مشخص شده و ستون پشتیبانی به‌طور معمول تکمیل می‌شود. در غیر این‌صورت مورد مشروط مرتبط نیست و باید پاسخ غیر کاربردی (N/A) علامت زده شود.

هر موردی که مرجع آن در نمادهای مشروط استفاده شده باشد در ستون موارد با ستاره مشخص می‌شود.

ت-۴ شناسایی

ت-۴-۱ شناسایی پیاده‌سازی

متصدی	
نقطه تماس برای پرسمان‌های مرتبط با این PICS	
نام(ها) و نسخه(های) پیاده‌سازی	
اطلاعات ضروری دیگر برای شناسایی کامل (به‌عنوان مثال نام‌ها و نسخه(ها) برای ماشین‌ها و سامانه عامل‌ها، نام(های) سامانه	
یادآوری ۱- تنها سه مورد اول برای هر پیاده‌سازی ضروری هستند. سایر اطلاعات ممکن است برای رعایت الزامات در جهت شناسایی کامل، تکمیل شوند. **یادآوری ۲**- اصطلاحات «نام» و «نسخه» باید متناسب با واژه‌گزینی متصدی به‌طور مناسب تفسیر شوند. (به‌عنوان مثال، نوع، سری و مدل)	

ت-۴-۲ خلاصه‌ی پروتکل

شناسایی مشخصات پروتکل	توصیه‌نامه‌ی ISO/IEC 11577| CCITT X.273 (1994)
شناسایی اصلاحات و غلط‌های این پیش‌نویس PICS که به عنوان قسمتی از این PICS تکمیل شده است.	توصیه‌نامه‌ی ISO/IEC 11577| CCITT X.273 (1994) الحاقیه: اصلاحیه: الحاقیه: اصلاحیه: الحاقیه: اصلاحیه: الحاقیه: اصلاحیه:
آیا هیچ مورد استثنایی مورد نیاز است؟ (به زیربند ت-۳-۳ مراجعه شود.) **یادآوری**– پاسخ بله به معنی این است که پیاده‌سازی با این استاندارد ملی انطباق ندارد.	بله □ خیر □

تاریخ اظهارنامه	

ت-۵ ویژگی‌های مشترک بین NLSP-CO و NLSP-CL

ت-۵-۱ قابلیت‌های اصلی (مشترک)

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی
CO*	آیا مد اتصال پشتیبانی می‌شود؟	۵-۱	O.1	بله □ خیر □
CL*	آیا مد بی‌اتصال پشتیبانی می‌شود؟	۵-۱	O.1	بله □ خیر □
AC	آیا کنترل دسترسی پشتیبانی می‌شود؟	۵-۲	O	بله □ خیر □
TFC*	آیا محرمانگی جریان ترافیک پشتیبانی می‌شود؟	۵-۲	O	بله □ خیر □
ParamProt*	آیا محافظت از تمام پارامترهای خدمت NLSP پشتیبانی می‌شود؟	۵-۵-۱- الف	O.2	بله □ خیر □
UserDatProt	آیا محافظت از داده‌ی کاربر NLSP پشتیبانی می‌شود؟	۵-۵-۱- ب	O.2	بله □ خیر □
NoProt*	آیا بدون محافظت پشتیبانی می‌شود؟	۵-۵-۱-پ	O	بله □ خیر □
SdtBase*	آیا کارکرد کپسوله‌سازی مبتنی بر SDT PDU پشتیبانی می‌شود؟	۵-۵-۳	CO:O.3 CL:M ParamProt: M	بله □ خیر □
NoHead	آیا کارکرد کپسوله‌سازی No Header پشتیبانی می‌شود؟	۵-۵-۳	CO:O.3 CL:X ParamProt:X	بله □ خیر □ N/A □
SA-P*	آیا SA-P درون باند پشتیبانی می‌شود؟	۵-۴-۱	O	بله □ خیر □
LabMech*	آیا سازوکار برچسب پشتیبانی می‌شود؟	۶-۲- چ ۶-۴-۱- ث ۶-۴-۲- ج	SdtBase:O	بله □ خیر □ N/A □
SDTMech*	آیا کارکرد کپسوله‌سازی مبتنی بر SDT PDU استانداردشده پشتیبانی می‌شود؟	۱۱	SdtBase:O	بله □ خیر □ N/A □
NoHeadMech	آیا کارکرد کپسوله‌سازی No Header استانداردشده پشتیبانی می‌شود؟	۱۲	NoHead:O	بله □ خیر □ N/A □

ت-۵-۲ PDUها (مشترک)

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی در ارسال	پشتیبانی در دریافت
SDT*	آیا PDU انتقال داده امن در ارسال/دریافت پشتیبانی می‌شود؟	۱-۱-۴-۶ ۳-۱۳	SdtBase:M	بله □ N/A □	بله □ N/A □
SA*	آیا PDU همبستگی امنیتی در ارسال/دریافت پشتیبانی می‌شود؟	۱-۴-۵ ۴-۱۳	SA-P:O	بله □ N/A □	بله □ N/A □

ت-۵-۳ فیلدهای مشترک SDT PDU بین CO و CL و عمومی برای سازوکار

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی در ارسال	پشتیبانی در دریافت
SdtPID	مقدار فیلد PID در هر SDT PDU 10001011	۱-۲-۳-۱۳	SDT:M	بله □ N/A □	بله □ N/A □
SdtLI	فیلد نشان‌گر طول در هر SDT PDU	۲-۲-۳-۱۳	SDT:M	بله □ N/A □	بله □ N/A □
SdtPDUType	مقدار فیلد نوع PDU در هر 01001000 SDT PDU	۳-۲-۳-۱۳	SDT:M	بله □ N/A □	بله □ N/A □
SdtContLen	طول محتوا در هر SDT PDU	۱-۴-۳-۱۳	SDT:M	بله □ N/A □	بله □ N/A □
DataType	فیلد نوع داده در هر SDT PDU	۲-۴-۳-۱۳	SDT:M	بله □ N/A □	بله □ N/A □
UserData	فیلد محتوی نوع Co-Userdata	۳-۴-۳-۱۳	SDT:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
CSAddr	فیلد محتوی نوع نشانی C2 - Calling/Source NLSP	۳-۴-۳-۱۳	ParamProt:M	بله □ N/A □	بله □ N/A □
CDAddr	فیلد محتوی نوع نشانی C3 NLSP - Calling/Destination پ	۳-۴-۳-۱۳	ParamProt:M	بله □ N/A □	بله □ N/A □
برچسب	فیلد محتوی نوع c6-Label	۳-۴-۳-۱۳	LabMech:O.4	بله □ خیر □ N/A □	بله □ خیر □ N/A □
LabRef	فیلد محتوی نوع C7 - Label Reference	۳-۴-۳-۱۳	LabMech:O.4	بله □ خیر □ N/A □	بله □ خیر □ N/A □
LabelExe	آیا عدم‌شمول متقابل برچسب و مرجع برچسب در هر SDT PDU اجباری است؟	۳-۴-۳-۱۳	LabMech:M	بله □ N/A □	بله □ N/A □

ت-۵-۴ فیلدهای مشترک SDT PDU بین CO و CL با سازوکار کپسوله سازی مبتنی بر SDT خاص

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت (یادآوری)	پشتیبانی در ارسال	پشتیبانی در دریافت
Synch	همگام‌سازی Crypto	۱۱-۳، ۱۳-۳-۳-۱	O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
ICV	فیلد ICV	۱۱-۳، ۱۳-۳-۳-۲	COInteg:M CLInteg:M	بله □ N/A □	بله □ N/A □
EncPad	لت برای رمزگذاری	۱۱-۳، ۱۳-۳-۳-۳	COConf:O CLConf:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
SeqNo	فیلد محتوی شماره دنباله	۱۱-۳، ۱۳-۳-۵-۱	COInteg:O CLInteg:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
SinglePad	فیلد لت عمومی هشت‌تایی منفرد	۱۱-۳، ۱۳-۳-۵-۲	O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
TFCPad	لت ترافیک	۱۱-۳، ۱۳-۳-۵-۳	TFC:M	بله □ N/A □	بله □ N/A □
یادآوری– تمام فیلدهای بالا مشروط به انتخاب SDTMech هستند.					

ت-۵-۵ فیلدهای SA PDU عمومی برای SA-P

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی در ارسال	پشتیبانی در دریافت
SaPID	مقدار فیلد PID در هر SA PDU 10001011	۱۳-۴-۱	SA:M	بله □ N/A □	بله □ N/A □
SaLI	آیا فیلد نشان‌گر طول در هر SA PDU ارسال می‌شود؟	۱۳-۴-۲	SA:M	بله □ N/A □	بله □ N/A □
SaPDUType	فیلد نوع PDU با مقدار 01001001 در هر SA PDU	۱۳-۴-۳	SA:M	بله □ N/A □	بله □ N/A □
SaSA-ID	فیلد SA-ID	۱۳-۴-۴	SA:M	بله □ N/A □	بله □ N/A □
SA-PType	فیلد نوع SA-P	۱۳-۴-۵	SA:M	بله □ N/A □	بله □ N/A □
SAKTE*	آیا پروتکل SA که از تبادل نشانه‌ی کلید استفاده می‌کند پشتیبانی می‌شود؟	پیوست پ	SA:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □

ت-۵-۶ فیلدهای محتوی SA PDU مختص تبادل نشانه‌ی کلید SA-P

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی در ارسال	پشتیبانی در دریافت
SAExchId	ID تبادل	پ-۷-۱	SAKTE:M	بله □ N/A □	بله □ N/A □
ContLen	آیا فیلد نشان‌گر طول در هر SA PDU ارسال می‌شود؟	پ-۷-۲	SAKTE:M	بله □ N/A □	بله □ N/A □
MySA-ID	فیلد محتوی My SA-ID	پ-۷-۳-۱	SAKTE:M	بله □ N/A □	بله □ N/A □
OldYrSA-ID	فیلد محتوی Old Your SA –ID	پ-۷-۳-۲	SAKTE:M	بله □ N/A □	بله □ N/A □
KeyTokens	فیلدهای محتوی Key-Token-1، Key Token-2، Key Token-3 و Key Token-4	پ-۷-۳-۳	SAKTE:M	بله □ N/A □	بله □ N/A □
AuthFields	امضای دیجیتالی احراز هویت و فیلدهای محتوی گواهی‌نامه احراز هویت	پ-۷-۳-۴	SAKTE:M	بله □ N/A □	بله □ N/A □
ServSel*	فیلد محتوی انتخاب خدمت	پ-۷-۳-۵	SAKTE:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
SARejReas	فیلد محتوی دلیل رد کردن SA	پ-۷-۳-۶	SAKTE:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
SAAbReas	فیلد محتوی دلیل آزادسازی/لغو SA	پ-۷-۳-۷	SAKTE:M	بله □ خیر □ N/A □	بله □ خیر □ N/A □
LabDef	فیلد محتوی تعریف برچسب	پ-۷-۳-۸	SAKTE:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
KeySel*	فیلد محتوی انتخاب کلید	پ-۷-۳-۹	SAKTE:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
KeyUse	زیرفیلد پرچم‌های کاربرد	پ-۷-۳-۹-۱	KeySel:M	بله □ N/A □	بله □ N/A □
KeySelInfo	زیرفیلد اطلاعات انتخاب کلید	پ-۷-۳-۹-۲	KeySel:M	بله □ N/A □	بله □ N/A □
KeyRefx	زیرفیلد مرجع کلید	پ-۷-۳-۹-۳	KeySel:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
SAFlags	فیلد محتوی پرچم‌های SA	پ-۷-۳-۱۰	SAKTE:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
ASSR	فیلد محتوی ASSR	پ-۷-۳-۱۱	ServSel:M	بله □	بله □

				□ N/A	□ N/A

پ-۵-۷ الگوریتم‌های پشتیبانی‌شده

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی
RegKTE	فهرست الگوریتم‌های تبادل نشانه‌ی کلید پشتیبانی‌شده ثبت شده	-	O	نام‌ها: نشان‌گر شئ:
UnRegKTE	فهرست الگوریتم‌های تبادل کلید نمایی پشتیبانی‌شده ثبت نشده	-	O	نام‌ها:
RegICV	فهرست اسامی الگوریتم‌های ICV پشتیبانی‌شده ثبت شده	-	O	نام‌ها: نشان‌گر شئ:
UnRegICV	فهرست الگوریتم‌های ICV پشتیبانی‌شده ثبت نشده	-	O	نام‌ها:
RegConf	فهرست اسامی الگوریتم‌های محرمانگی پشتیبانی‌شده ثبت شده	-	O	نام‌ها: نشان‌گر شئ:
UnRegConf	فهرست الگوریتم‌های محرمانگی پشتیبانی‌شده ثبت نشده	-	O	نام‌ها:

ت-۶ ویژگی‌های مختص NLSP-CL

ت-۶-۱ قابلیت‌های عمده (NLSP-CL)

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی
*CLConf	آیا محرمانگی بی‌اتصال پشتیبانی می‌شود؟	۵-۲	CL:O.5	بله □ خیر □ N/A □
*CLInteg	آیا یکپارچگی بی‌اتصال پشتیبانی می‌شود؟	۵-۲	CL:O.5	بله □ خیر □ N/A □
DOA	آیا احراز هویت مبدأ داده پشتیبانی می‌شود؟	۵-۲	CL:O.5	بله □ خیر □ N/A □

ت-۶-۲ راه‌انداز/پاسخ‌دهنده (مد بی‌اتصال)

مورد	سؤال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی
CLXmtProt	آیا پیاده‌سازی قابلیت ارسال واحدهای داده‌ی بی‌اتصال محافظت‌شده را دارد؟	۶-۷	CL:O.6	بله □ خیر □ N/A □
CLRcvProt	آیا پیاده‌سازی قابلیت پذیرش واحدهای داده بی‌اتصال محافظت‌شده‌ی ورودی را دارد؟	۷-۷	CL:O.6	بله □ خیر □ N/A □
CLXmt	آیا پیاده‌سازی قابلیت ارسال واحدهای داده بی‌اتصال محافظت‌نشده را دارد؟	۱-۶-۷	NoProt:M	بله □ N/A □
CLRcv	آیا پیاده‌سازی قابلیت پذیرش واحدهای داده بی‌اتصال محافظت‌نشده ورودی را دارد؟	۱-۷-۷	NoProt:M	بله □ N/A □

ت-۶-۳ محیط (مد بی‌اتصال)

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی
CL1	آیا اجزای اجباری IS 8348 AD1 پشتیبانی می‌شوند؟	۲-۵	CL:M	بله □ N/A □

ت-۶-۴ فیلدهای SDT PDU (مد بی‌اتصال)

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی
SdtSA-ID	آیا فیلد SA-ID در هر SDT PDU ارسال می‌شود؟	۴-۲-۳-۱۳	CL:M	بله □ N/A □

ت-۷ ویژگی‌های مختص NLSP-CO

ت-۷-۱ قابلیت‌های عمده (NLSP-CO)

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی
SNAcP	آیا پروتکل به‌طور مستقیم به توصیه‌نامه‌ی SIO/IEC 8208| CCITT X.25 نگاشت می‌شود؟	۵-۳، پیوست ب	CO:O.7	بله □ خیر □
SNISP*	آیا پروتکل به توصیه‌نامه‌ی ISO/IEC 8348 |CCITT X.213 نگاشت می‌شود؟	۵-۳، پیوست الف	CO:O.7	بله □ خیر □
COConf*	آیا محرمانگی اتصال پشتیبانی می‌شود؟	۵-۲	CO:O.8	بله □ خیر □ N/A □
COInteg*	آیا یکپارچگی اتصال بدون بازیابی پشتیبانی می‌شود؟	۵-۲	CO:O.8	بله □ خیر □ N/A □
PEA	آیا احراز هویت هستار همتا پشتیبانی می‌شود؟	۵-۲	CO:O.8	بله □ خیر □ N/A □

*ExCSC	آیا رویه‌های CSC-PDU نمونه‌ی تعریف شده در NLSP پشتیبانی می‌شوند؟	۱۰	CO:O	بله □ خیر □ N/A □

ت-۷-۲ PDUها (مد اتصال)

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی در ارسال	پشتیبانی در دریافت
*CSC	کنترل امنیت اتصال PDU	۸-۵، ۱۳-۵	CO:M	بله □ N/A □	بله □ N/A □

ت-۷-۳ حالت‌های آزادسازی/برقرارسازی اتصال

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی به عنوان هستار فراخوانی‌کننده	پشتیبانی به عنوان هستار فراخوانی‌شده
UNConn	NLSP-CONNECT در UN-CONNECT	۸-۵-۱-۲	CO:O.9	بله □ خیر □ □ N/A □	بله □ خیر □ N/A □
UNConnSAP	NLSP-CONNECT در UN-CONNECT با SA-P	۸-۵-۱-۲	CO:O.9	بله □ خیر □ N/A □	بله □ خیر □ N/A □
UNData	NLSP-CONNECT در UN-DATA	۸-۵-۱-۲	CO:O.9	بله □ خیر □ N/A	بله □ خیر □ N/A □
UNDataSAP	NLSP-CONNECT در UN-DATA با SA-P	۸-۵-۱-۲	CO:O.9	بله □ خیر □ N/A □	بله □ خیر □ N/A □
DUNDisc	NLSP-DISCONNECT در UN-DISCONNECT	۸-۱۰	CO:O.10	بله □ خیر □ N/A □	بله □ خیر □ N/A □
DUNData	NLSP-DISCONNECT در UN-DATA	۸-۱۰	CO:O.10	بله □ خیر □ N/A □	بله □ خیر □ N/A □

ت-۷-۴ محیط (مد اتصال)

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی
CO1	آیا عناصر اجباری IS 8384 پشتیبانی می‌شوند؟	۵-۳	SNISP:M	بله □ N/A □
ConOpt1	آیا پیاده‌سازی داده‌ی پیشتاز را ارائه می‌دهد؟	۸-۷	CO:O	بله □ خیر □ N/A □
ConOpt3	آیا پیاده‌سازی تأیید دریافت را ارائه می‌دهد؟	۸-۹	CO:O	بله □ خیر □

				□ N/A

ت-۷-۵ زمان‌سنج‌ها و پارامترها (مد اتصال)

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی
T1	آیا زمان‌سنج بین ارسال NLSP-DISCONNECT و صادر شدن UN-DISCONNECT پشتیبانی می‌شود؟	۱۰-۸	CO:O	بله □ خیر □ N/A □

ت-۷-۶ فیلدهای SDT PDU (مد اتصال)

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت (یادآوری)	پشتیبانی در ارسال	پشتیبانی در دریافت
TestData	فیلد محتوی نوع C1 – داده‌ی آزمایشی	۳-۴-۳-۱۳	O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
RAddr	فیلد محتوی نوع C4 – نشانی NLSP پاسخ‌دهنده	۳-۴-۳-۱۳	ParamProt:M	بله □ N/A	بله □ N/A
ConfReq	فیلد محتوی نوع C8 – درخواست تأیید	۳-۴-۳-۱۳	ParamProt:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
Reason	فیلد محتوی نوع C9 – دلیل قطع اتصال	۳-۴-۳-۱۳	ParamProt:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □
یادآوری– تمام موارد در زیربند ت-۷-۶ مشروط به این هستند که SDT پشتیبانی شود.					

ت-۷-۷ فیلدهای CSC-PDU – عمومی (مد اتصال)

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی در ارسال	پشتیبانی در دریافت
CscPID	مقدار فیلد PID در هر CSC-PDU 10001011	۱-۵-۱۳	CSC:M	بله □ N/A □	بله □ N/A □
CscLI	فیلد نشان‌گر طول در هر CSC-PDU	۲-۵-۱۳	CSC:M	بله □ N/A □	بله □ N/A □
CscPTyp	فیلد نوع PDU با مقدار xx111111 در هر CSC-PDU	۳-۵-۱۳	CSC:M	بله □ N/A □	بله □ N/A □
UNC-UNDFlg	آیا پرچم SA-P در فیلد نوع PDU در هر CSC-PDU ارسال می‌شود؟	۳-۵-۱۳	CSC:M	بله □ N/A □	بله □ N/A □
SA-PFlg	آیا پرچم SA-P در فیلد نوع PDU در هر CSC-PDU ارسال می‌شود؟	۳-۵-۱۳ پ	CSC:M	بله □ N/A □	بله □ N/A □
CscSA-ID	فیلد SA-ID	۴-۵-۱۳	CSC:O	بله □ خیر □ N/A □	بله □ خیر □ N/A □

ContLen	فیلد طول محتوی در هر CSC-PDU	۱۳-۵-۵	CSC:M	بله □ N/A □	بله □ N/A □

ت-۷-۸ نمونه محتوی CSC-PDU (مد اتصال)

مورد	سوال‌ها/ویژگی‌ها	مرجع (زیربند)	وضعیت	پشتیبانی
CscInit	آیا پیاده‌سازی قابلیت آغاز تبادل CSC-PDU را دارد؟	۳-۱۰	ExCSC:O.1.1	بله □ خیر □ N/A □
CscResp	آیا پیاده‌سازی قابلیت پاسخ‌دهی به یک همتای راه‌انداز تبادل CSC-PDU را دارد؟	۳-۱۰	ExCSC:O.1.1	بله □ خیر □ N/A □
EncAuth	فیلد AUTH-DATA رمزگذاری‌شده	۱۳-۵-۷	ExCSC:M	بله □ N/A □
KeyInfox	فیلد اطلاعات کلید	۱۳-۵-۸	ExCSC:O	بله □ خیر □ N/A □

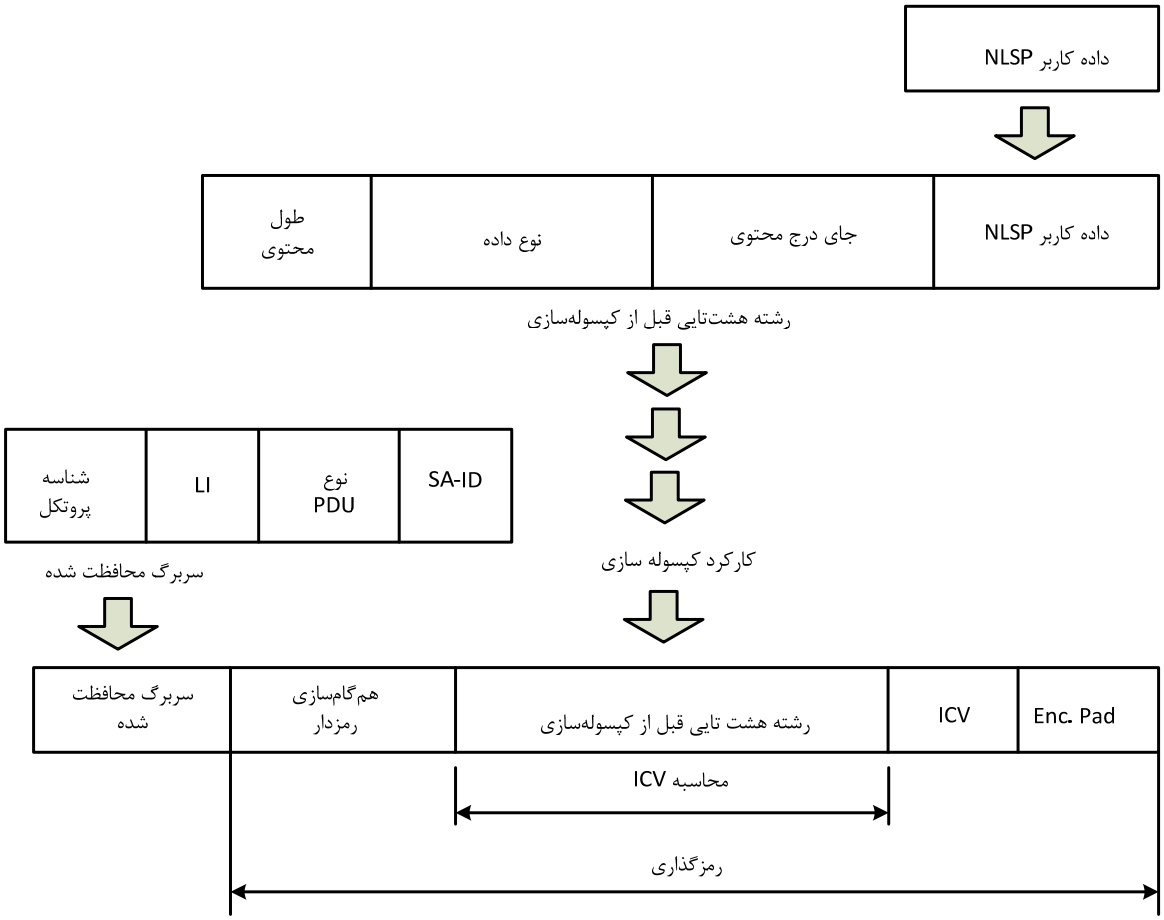
پیوست ث
(اطلاعاتی)
آموزش برخی از مفاهیم پایه‌ای NLSP

ث-۱ مبانی محافظت

اساس محافظت داده‌های کاربر در NLSP، PDU انتقال داده امن (SDT PDU) یا محافظت No_Header است. SDT PDU به‌وسیله‌ی یک کارکرد کپسوله‌سازی که یک مقدار وارسی یکپارچگی (ICV) را می‌افزاید و سپس آن‌را برای محرمانگی رمزگذاری می‌کند، از داده‌ها محافظت می‌کند. فیلدهای لت می‌توانند برای پشتیبانی از محرمانگی جریان ترافیک و سازوکارهای ICV بستک به همراه داده‌ی محافظت‌شده قرار داده شوند. یک فیلد لت جداگانه برای سازوکارهای رمزگذاری بستک می‌تواند بعد از ICV قرار گیرد.

اطلاعات کنترل امنیت اضافی (مثل برچسب، شماره دنباله)، قبل از اینکه در یک SDT PDU محافظت شود، می‌توانند در کنار داده‌ی کاربر قرار گیرند تا یک Octet-String-Before-Encapsulation تولید کنند. سپس همان‌طورکه در بالا توصیف شد، Octet-String-Before-Encapsulation، به‌وسیله‌ی یک کارکرد کپسوله‌سازی محافظت می‌شود. یک سرآیند واضح در ابتدای PDU قرار می‌گیرد تا نوع PDU و مجموعه «صفات امنیتی» (کلیدها و غیره – به بند ۵ مراجعه شود) به‌کار رفته برای محافظت واحد داده را شناسایی کند. نحوه‌ی ساخت یک SDT PDU در شکل ث-۱ نمایش داده شده است.

NLSP-CO از یک رویکرد دوم اختیاری به نام No_Header نیز برای محافظت NLSP Userdata پشتیبانی می‌کند. در این رویکرد داده‌ی NLSP، بدون افزودن اطلاعات کنترل امنیت یا سرآیند واضح، به‌طور مستقیم رمزگذاری می‌شود.



شکل ث-۱– ساختن یک PDU انتقال داده امن

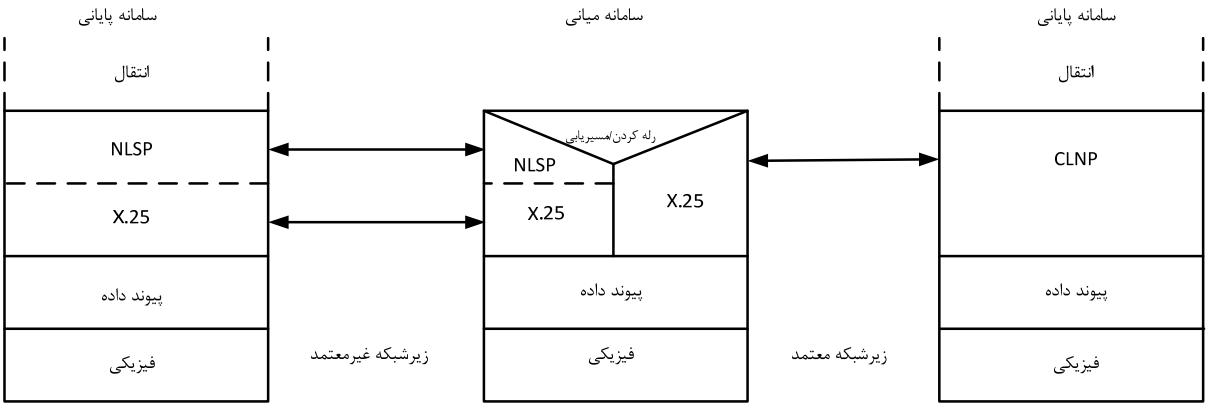
ث-۲ خدمت زیرساخت در برابر NLSP

NLSP دو واسط خدمت ادراکی دارد. اولین واسط که خدمت NLSP نامیده می‌شود، واسطی است که برای پروتکل‌های بالای NLSP ارائه شده است. (پروتکل‌هایی که از ارتباطات محافظت‌شده استفاده می‌کنند.) واسط دیگر که خدمت UN (شبکه‌ی اصلی) نامیده می‌شود، به‌وسیله‌ی NLSP برای به‌کارگیری پروتکل‌های ارتباطی اصلی استفاده می‌شود. NLSP ممکن است به‌طور ناپیدا بدون تأثیر بر عملیات پروتکل‌های بالا یا پایین خود، اضافه شود. واسط NLSP خدمات مورد انتظار به‌وسیله‌ی پروتکل‌های بالا را منعکس می‌کند و خدمت UN به قالب خدمات پروتکل‌های اصلی نگاشت می‌شود.

داده‌های کاربر در واسط خدمت NLSP، قبل از اینکه به سمت واسط خدمت UN اصلی فرستاده شوند، محافظت‌شده‌اند. (به‌عنوان مثال با کپسوله‌سازی در یک SDT PDU)

واسط‌های خدمت NLSP و UN هر دو (به‌جز در یک جنبه‌ی اصلی) شبیه به خدمات شبکه OSI هستند. هستاری که به‌وسیله‌ی NLSP خدمت‌دهی می‌شود، همیشه یک هستار انتقال نیست و خدمت UN هرگز به‌طور مستقیم برای یک هستار انتقال واسطه نمی‌شود. همان‌طورکه پس از این توصیف خواهد شد، در بعضی موارد (به شکل ث-۲ مراجعه شود) خدمت NLSP ممکن است برای یک رله و کارکرد مسیریابی در یک سامانه‌ی میانی یا حتی هستاری که از پروتکل لایه‌ی شبکه پشتیبانی می‌کند، واسطه شود. (به شکل‌ها

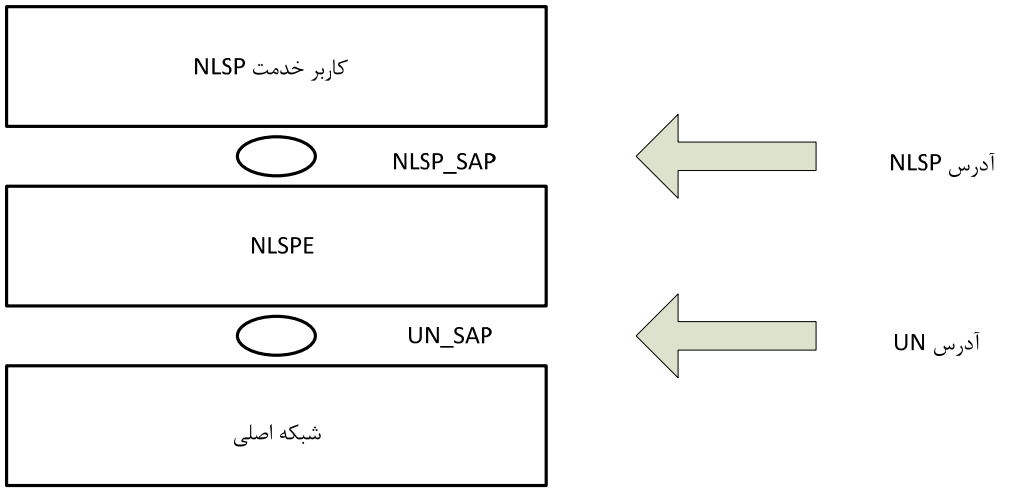
مراجعه شود.) همراه با خدمت UN، واسط خدمت از دید پروتکل‌های اصلی ممکن است مانند خدمت شبکه به نظر برسد اما از دید یک پشته(زیرنویس) کامل OSI، واسطی برای هستار NLSP در لایه‌ی شبکه است و بنابراین یک خدمت شبکه OSI خالص نیست.



شکل ث-۲– نمایش NLSP-CO به همراه یک سامانه میانی

ث-۳ نشانی‌دهی NLSP

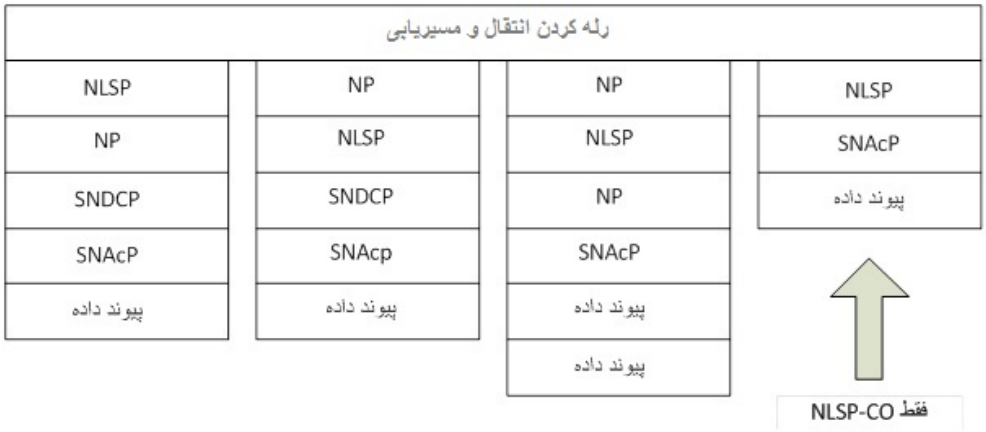
هستار NLSP (NLSPE) در بین کاربر خدمت NLSP و شبکه‌ی اصلی، جاسازی شده است. نقاط دسترسی خدمت متناظر NLSP_SAP و UN_SAP هستند. در پیکربندی‌هایی که در حال حاضر توسط NLSP پشتیبانی می‌شوند (به شکل ث-۳-۱ و یادآوری مراجعه شود) نشانی، هستار متصل‌شده به NLSP_SAP را شناسایی می‌کند، به‌عنوان مثال کاربر خدمت NLSP، نشانی NLSP است. نشانی، هستار متصل‌شده به UN_SAP را شناسایی می‌کند، به‌عنوان مثال NLSPE نشانی UN است. NLSPEهای همتا، یک زیرلایه در لایه‌ی شبکه را شکل می‌دهند. مرزهای بالایی و پایینی نقاط برهم‌کنشی هستند که در آن‌جا نشانی‌ها مبادله می‌شوند. شکل زیر نقاط دسترسی خدمت و نشانی‌های متناظر را نشان می‌دهد.



شکل ث-۳-۱– SAPهای بالا و پایین و نشانی‌ها

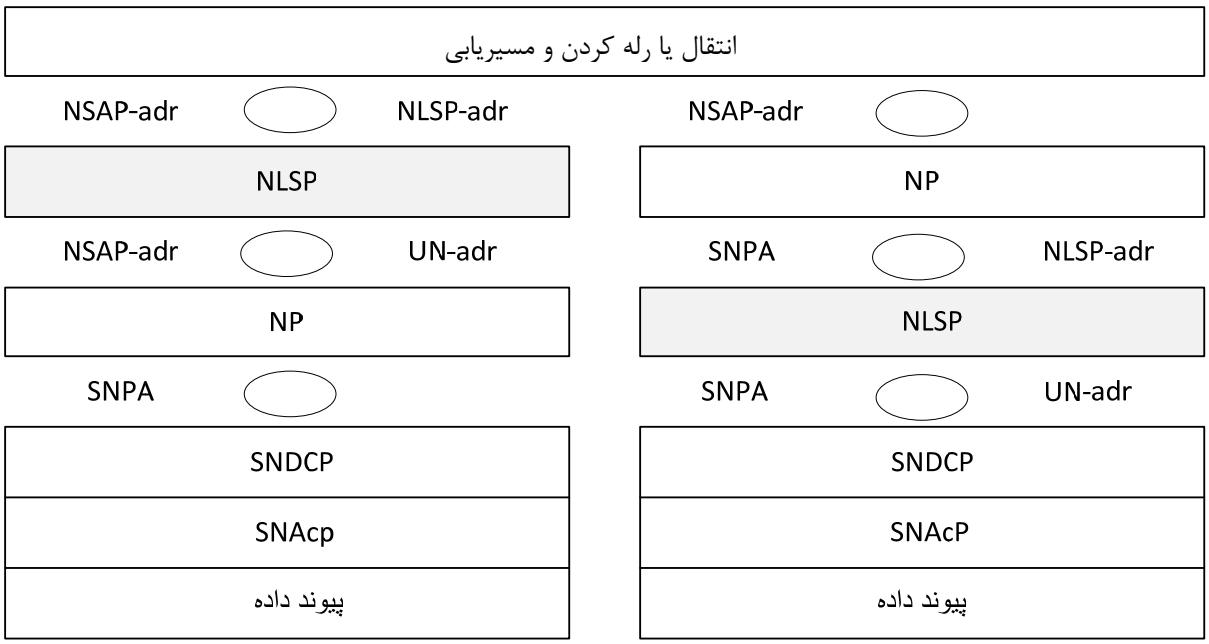
یادآوری– در پیکربندی‌های منعکس‌کننده‌ی CO-mode N-services، نشانی NLSP ممکن است یک نشانی NLSP در سامانه‌ی پایانی را به‌جای NLSP_SAP در سامانه میانی، شناسایی کند. (به بندهای ث-۴ و ث-۵ مراجعه شود.)

NLSP در داخل لایه‌ی شبکه قرار می‌گیرد و می‌تواند در مرز پایین، مرز بالا یا جایی مابین آن‌ها قرار گیرد. NLSP و مرز خدمت UN اصلی آن، بسته به این محل جای‌گذاری در نقش‌های مختلفی عمل می‌کنند. به‌طور مشابه نشانی‌های استفاده‌شده، معناشناسی متفاوتی بستگی به این جای‌گذاری دارند. شکل ث-۳-۲ جایگاه‌های محتمل NLSPE در لایه‌ی شبکه را نشان می‌دهد:

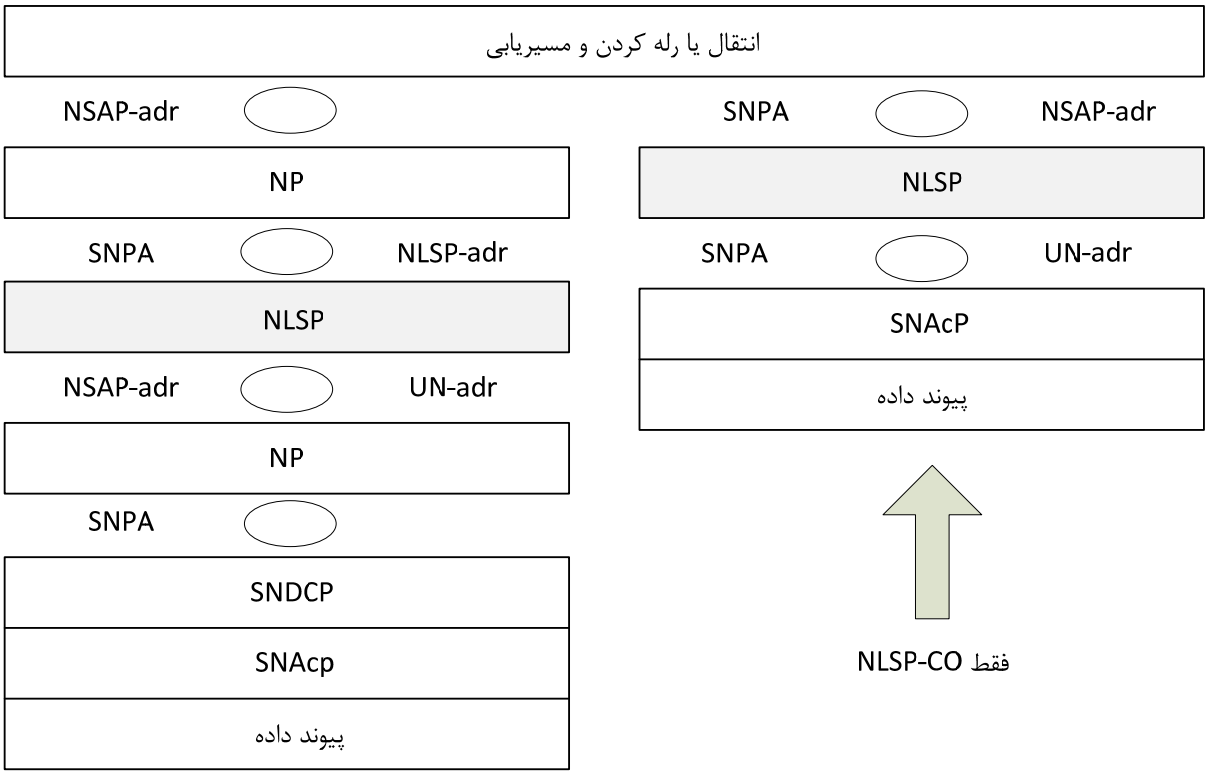


شکل ث-۳-۲ – جایگاه NLSP در لایه‌ی شبکه

شکل‌های ث-۳-۳ و ث-۳-۴ قالب نشانی‌های استفاده‌شده در لایه‌ی شبکه محتوی یک زیرلایه‌ی NLSP در جایگاه‌های مختلف را معین می‌کنند.



شکل ث-۳-۳ – نشانی‌ها در یک لایه‌ی شبکه محتوی یک زیرلایه‌ی NLSP با یک پروتکل شبکه (NP) در بالا و NLSP در پایین



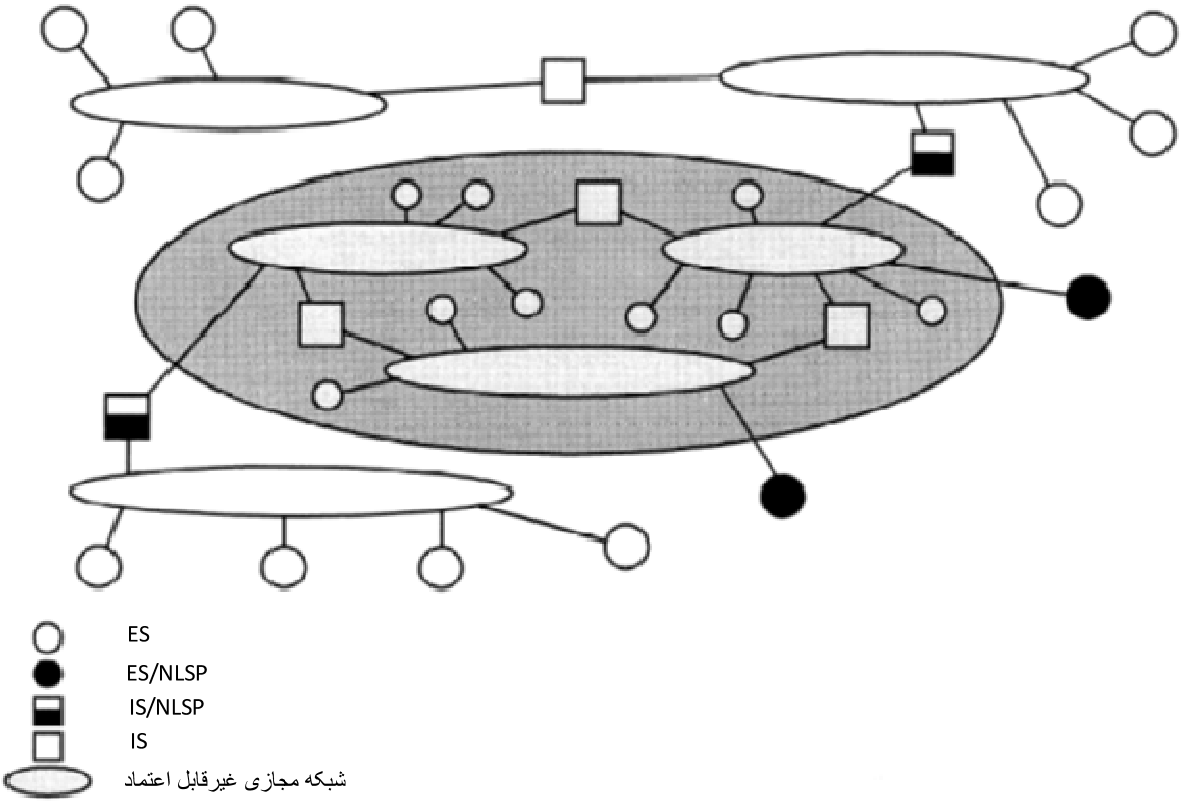
شکل ث-۳-۴ – نشانی‌ها در یک لایه‌ی شبکه محتوی یک زیرلایه‌ی NLSP با پروتکل شبکه (NP) در بالا و NLSP در پایین - بدون پروتکل شبکه

از NSAP'-adr (UN-adr) توسط NLSP برای نشانی‌دهی در یک شبکه‌ی اصلی در مواردی که یک پروتکل شبکه (مد اتصال یا بی‌اتصال) در زیر زیرلایه‌ی NLSP قرار می‌گیرد، استفاده می‌شود. نشانی‌های 'NSAP، یک دامنه‌ی نشانی‌دهی کپسوله‌شده را شکل می‌دهند که توسط زیرلایه‌ی NLSP پیوست شده‌اند. نشانی‌های 'NSAP نحوی یکسان با نشانی‌های NSAP دارند و به‌وسیله‌ی رویه‌های ثبت‌نام نشانی NSAP، ثبت می‌شوند. نشانی‌های NSAP شکل‌دهنده یک دامنه‌ی شبکه مورد اعتماد تنها در یک دامنه محافظت‌شده به‌وسیله‌ی زیرلایه‌های NLSP مورد استفاده قرار می‌گیرند.

'SNPA ممکن است با SNPA تعیین‌شده به‌وسیله‌ی هستار NP بالا، همسان باشد. با این وجود، نشانی 'SNPA ممکن است براساس محل NLSPE همتا، متفاوت باشد.

دامنه‌ی نشانی‌دهی کپسوله‌شده ممکن است به‌عنوان یک زیرشبکه‌ی مجازی در یک OSIE در نظر گرفته شود؛ این دامنه به‌وسیله‌ی یک گروه از هستارهای NLSP در ES یا IS که هر کدام یک پشته N لایه یکسان در بالای پروتکل‌های زیرشبکه وابسته به فناوری (SNAcP، پروتکل همگرایی وابسته به شبکه زیرشبکه) داشته باشند، محدود شود. بنابراین تمام این NLSPEها یک جایگاه یکسان در لایه‌ی شبکه خواهند داشت.

شکل ث-۳-۵ یک سناریوی محتمل از یک OSIE حاوی یک UN مجازی پیوست‌شده به‌وسیله‌ی هستارهای NLSP در ESها و ISها را نشان می‌دهد.



شکل ث-۳-۵ – UN مجازی در یک OSIE

پشته‌های پروتکل لایه‌ی شبکه و جای‌گذاری هستارهای NLSP بستگی به پروتکل‌های استفاده‌شده در زیرشبکه‌ها و پیکربندی آن‌ها دارد. فرآیند انتخاب به‌وسیله‌ی مقامی که پیکربندی ایستای مربوط به یک ترکیب از شبکه‌های معتمد و غیرمعتمد را تعریف می‌کند، انجام می‌گیرد. این فرآیند نیازمند مدیریت امنیت و کارکردهای مسیریابی اضافی است که خارج از حیطه‌ی این استاندارد ملی است.

بسته به محل جای‌گذاری NLSPE در لایه‌ی شبکه، نشانی NLSP و نشانی UN معناشناسی متفاوتی دارند. به‌طور مفهومی دو جای‌گذاری متمایز هستند. (به شکل ث-۳-۶ مراجعه شود.)

-جای‌گذاری[1] A – NLSP_SAP متناظر با OSI NSAP است. کاربر خدمت NLSP یک هستار انتقال است. نشانی شناسایی هستار انتقال مانند نشانی NSAP تعریف می‌شود و مشابه نشانی NLSP است.

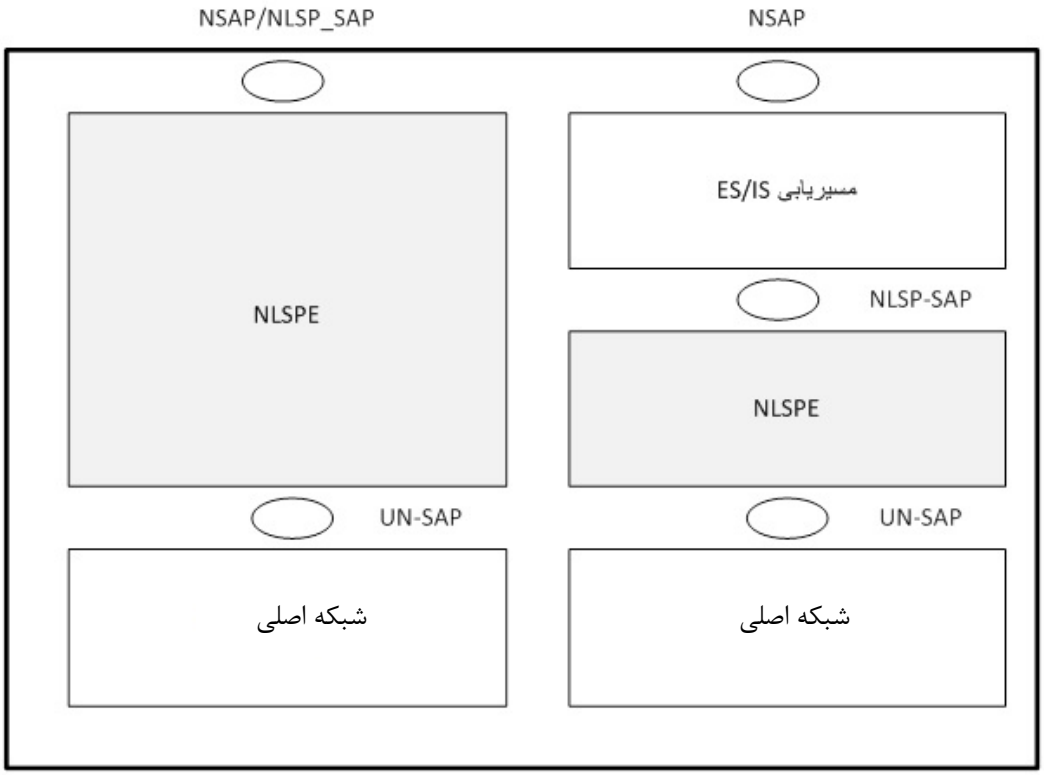
شبکه‌ی اصلی به‌عنوان یک دامنه شبکه محافظت‌نشده در نظر گرفته می‌شود که در واقع شبکه OSI است. بنابراین نشانی شناسایی NLSPE متناظر با نشانی OSI NSAP خواهد بود. با این وجود، اگر پارامترهای خدمت NLSP محافظت‌شده باشند (Param_Prot، صحیح است)، پارامترهای منتقل‌شده در نخستینه‌های خدمت از طریق مرزهای NLSP_SAP و UN_SAP می‌توانند متفاوت باشند.

-جای‌گذاری B – NLSP بین دو زیرلایه‌ی شبکه قرار می‌گیرد. زیرلایه بالا یک دامنه شبکه محافظت‌شده را مشخص می‌کند، در صورتی که زیرشبکه‌ی اصلی یک دامنه شبکه محافظت‌نشده را نشان می‌دهد.

1 - Placement

در یک سامانه‌ی پایانی، نشانی NSAP کاربران خدمت شبکه مختلفی که در سامانه‌ی پایانی کنار هم قرار گرفته‌اند را مشخص می‌کند. نشانی NLSP هستار مسیریابی سامانه‌ی پایانی را مشخص می‌کند که مسئول کارکردهای مسیریابی ES است.

در یک سامانه‌ی میانی، نشانی NSAP حاوی اطلاعات مسیریابی برای رله کردن NPDUها در دامنه شبکه محافظت‌شده است. نشانی NLSP هستار مسیریابی ES/IS در یک IS را مشخص می‌کند. نشانی UN، NLSPE پیوست‌شده به UN را مشخص می‌کند.



شکل ث-۳-۶ – جای‌گذاری NLSPE در لایه‌ی شبکه

نشانی(های) NLSP که به‌وسیله‌ی NLSPE راه دور خدمت‌رسانی می‌شوند، در صفت «SA، Adr_Served» نگهداری می‌شود. نشانی UN مربوط به یک NLSPE راه دور در صفت «SA، Peer_Adr» نگهداری می‌شود.

- اگر Param_Prot برابر FALSE باشد:

کارکردهای NLSP محدود به نگاشت نخستینه‌های خدمت از NLSP_SAP به UN_SAP می‌شوند. نشانی NSAP به‌طور مستقیم به نشانی UN نگاشت می‌شود. صفت NLSP SA، Adr_Served و صفت SA، Peer_Adr مقدار یکسانی را نگه می‌دارند.

- اگر Param_Prot، برابر TRUE باشد:

حالت محافظت‌شده – نگاشت‌های نشانی بستگی به محل NLSPE دارد و با استفاده از صفات Adr_Served و Peer_Adr ارائه می‌شود.

جدول ث-۱ حاوی کارکردهای نگاشت نشانی NLSPE بسته به جای‌گیری‌های مختلف آن‌ها و تناظر بین صفات Peer_Adr و Adr_Served است. جدول ث-۱ تنها نشانی‌های مقصد را پوشش می‌دهد.

ث-۴ NLSP مد اتصال

ث-۴-۱ عملیات پایه

پیچیدگی عمده‌ی NLSP مربوط به مدیریت برقراری اتصال برای ارتباطات مد اتصال است.

جدول ث-۱

جایگاه	Param_Prot	NLSP address	UN address	NLSP vs UN address
A	FALSE	نشانی NSAP	نشانی NSAP	یکسان
A	TRUE	نشانی NSAP	نشانی UN همتا	متفاوت
B: سامانه‌ی پایانی	FALSE	نشانی NLSP (یادآوری)	نشانی UN همتا	یکسان
B: سامانه‌ی پایانی	TRUE	نشانی NLSP (یادآوری)	نشانی UN همتا	متفاوت
B: سامانه میانی	FALSE	نشانی NLSP (یادآوری)	نشانی UN همتا	یکسان
B: سامانه میانی	TRUE	نشانی NLSP (یادآوری)	نشانی UN همتا	متفاوت
یادآوری– نگاشت از نشانی NLSP به یا از نشانی NSAP چیزی است که کارکردهای مسیریابی مربوط به پروتکل بالای NLSP با آن سر و کار دارند.				

دو حالت پایه برای برقراری یک اتصال NLSP پشتیبانی می‌شوند. در یکی از آن‌ها پارامترهای NLSP-CONNECT در نخستینه‌های خدمت UN-CONNECT حمل می‌شوند. در دیگری پارامترهای NLSP-CONNECT بعد از کپسوله‌سازی در یک SDT PDU و در UN-DATA پس از برقراری اتصال UN، حمل می‌شوند. هر دو حالت برقراری اتصال NLSP انواع مختلفی دارند. یکی با SA-P درون باند استفاده می‌شود و دیگری با یک SA که برون باند برقرارشده است، به‌کار می‌رود.

PDU «کنترل امنیت اتصال» (CSC) برای اعلام حالت برقراری اتصال به‌کار می‌رود و اگر SA-P درون باند در اتصال UN حمل نشود، تبادل CSC-PDUها برای موارد زیر نیز استفاده می‌شود:

الف- برقراری صفات امنیتی مختص سازوکار برای محافظت از اتصال (به‌عنوان مثال، کلیدها، شماره‌های دنباله یکپارچگی)؛

ب- انجام احراز هویت هستار همتا.

در مواردی که NLSP-CONNECT در UN-CONNECT با SA-P درون باند حمل می‌شود، یک اتصال UN برای حمل SA-P برقرار می‌شود و سپس قبل از مبادله‌ی UN-CONNECTای که پارامترهای NLSP-CONNECT را حمل می‌کند، آزاد می‌شود. CSC-PDUها در دومین تبادل UN-CONNECT برای احراز هویت مجدد هستارهای NLSP همتا به‌کار می‌روند.

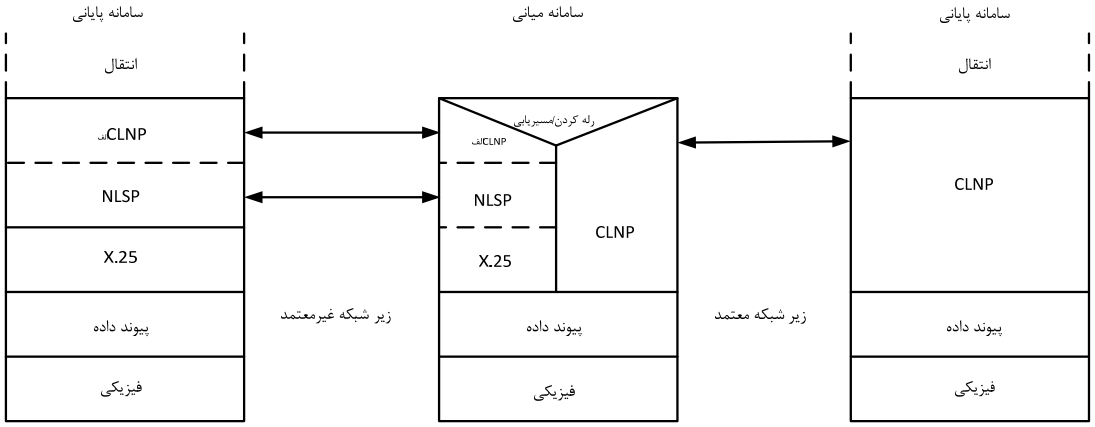
برقراری SA به‌وسیله‌ی تبادل SA PDUها یا SDT PDUهایی که اطلاعات لازم جهت راه‌اندازی صفات SA را حمل می‌کنند، انجام می‌شود. پیوست پ یک پروتکل SA را برای این منظور تعریف می‌کند.

اگر پارامترهای NLSP-CONNECT نیاز به محافظت داشته باشند، می‌توانند در یک SDT PDU کپسوله‌سازی شوند یا قبل از انتقال رمزگذاری (No_Header انتخاب شده است) شوند.

زمانی که یک اتصال برقرار شد، داده‌های کاربر به‌وسیله‌ی کپسوله‌سازی در یک SDT PDU و در صورت انتخاب حالت No_Header با رمزنگاری داده‌ی کاربر NLSP، محافظت می‌شوند.

ث-۴-۲ جای‌گذاری

NLSP مد اتصال می‌تواند در جاهای مختلف در لایه‌ی شبکه جای‌گذاری شود. این امر برای کاربر NLSP یا یک واسط خدمت شبکه OSI (در این مورد کاربر متناظر با یک هستار انتقال است) را ارائه می‌کند یا در صورتی که کاربر یک هستار پروتکل شبکه اضافی باشد (به‌عنوان مثال CLNP در توصیه‌نامه‌ی X.233 ITU-T| ISO/IEC 8473-1)، خدمت مربوط به واسط زیرشبکه را ارائه می‌کند. واسط زیر NLSP به‌طور مجازی مشابه خدمت شبکه OSI است به جز این‌که کاربر خدمت NLSP جایگزین خدمت انتقال است و خدمت می‌تواند در یک سامانه میانی یا سامانه‌ی پایانی عمل کند. پروتکلی که زیر NLSP عمل می‌کند مانند این است که بین دو سامانه‌ی پایانی ارائه خدمت شبکه OSI عمل می‌کند، اگر چه به ظاهر تنها با یک سامانه‌ی میانی برهم‌کنش دارد و به‌طور مستقیم برای خدمت انتقال واسطه نمی‌شود. عملیات NLSP-CO با یک سامانه‌ی میانی و انتها به انتها در شکل‌های ث-۴-۱، ث-۴-۲، ث-۴-۳ و ث-۴-۴ نشان داده شده است. جای‌گذاری‌های دیگر NLSP نیز امکان‌پذیر هستند.



[الف] این مورد شامل کارکرد همگرایی برای حالت بااتصال می‌شود.

شکل ث-۴-۱ – نمایش NLSP در یک محیط چند شبکه

ث-۴-۳ نگاشت واسط خدمت NLSP/UN

در یک سامانه‌ی پایانی، واسط خدمت NLSP به‌طور مستقیم به خدمت شبکه OSI نگاشت می‌شود.
از دو نوع نگاشت خدمت UN پشتیبانی می‌شود. در یکی، واسط خدمت UN، به یک معادل خدمت شبکه OSI با CSC-PDU حمل شده در فیلد داده‌ی کاربر UN Connect نگاشت می‌شود. دیگری به‌طور مستقیم به توصیه‌نامه‌ی X.25 همان طور که در توصیه‌نامه‌ی CCITT، X.223 ISO/IEC 8878 | تعریف شده است، نگاشت می‌شود (به جز در حالتی که CSC-PDU در فیلد تسهیلات محافظت X.25 حمل شود).

ث-۴-۴ نشانی‌دهی

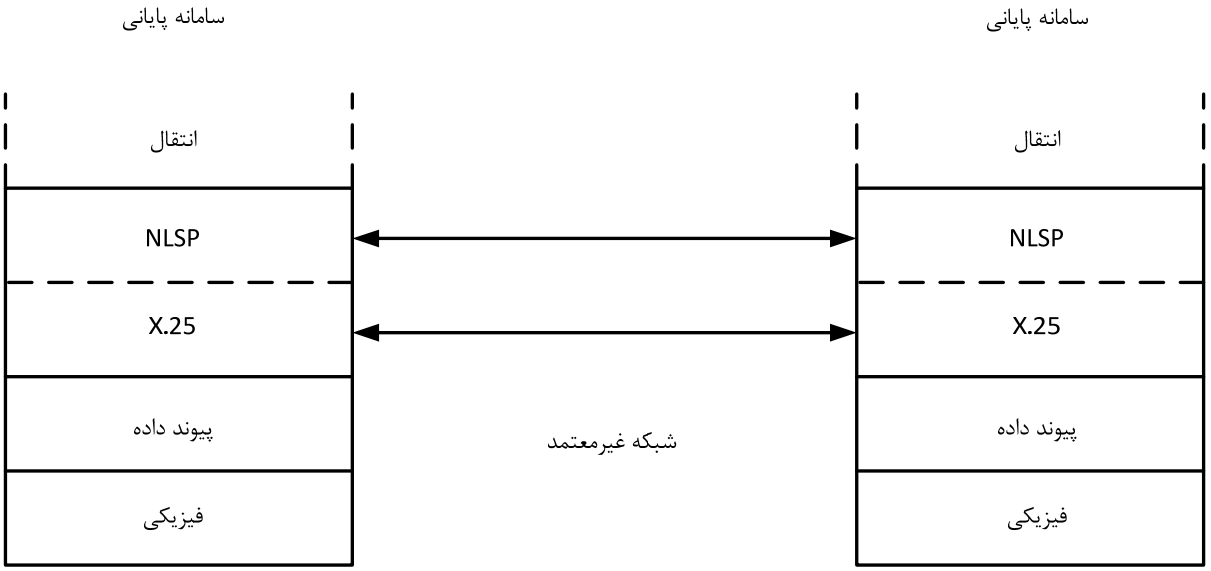
اگر NLSP در بالای لایه‌ی شبکه عمل کند، نشانی‌های به‌کار رفته در واسط خدمت NLSP ، نشانی‌های NSAP خدمت شبکه OSI بوده یا اگر زیر پروتکل لایه‌ی شبکه‌ی دیگر مثل CLNP عمل کنند، نشانی‌های SNPA هستند. اگر پنهان‌سازی نشانی فعال باشد (Param_Prot برابر FALSE باشد)، آنگاه نشانی‌های واسط خدمت UN مانند نشانی‌های واسط خدمت NLSP خواهند بود.
اگر پنهان کردن نشانی‌ها ارائه شود (Param_Prot، برابر TRUE باشد) نشانی‌های استفاده‌شده در واسط خدمت UN (نشانی‌های UN) در همان قالب نشانی‌های NLSP هستند (به‌عنوان مثال در موردی که نشانی NLSP یک نشانی NSAP با ساختار توصیه‌نامه‌ی CCITT X.213 | ISO/IEC 8348 باشد)، با این وجود، این نشانی‌ها برای شناسایی هستارهای NLSP که در یک سامانه میانی یا سامانه‌ی پایانی قرار می‌گیرند، به‌کار می‌روند. این نشانی‌های UN مانند نشانی‌های NSAP مدیریت می‌شوند. طرح‌های ثبت‌نام[1] یکسان برای تخصیص نشانی‌ها و پروتکل‌های مسیریابی یکسان برای مدیریت مسیریابی می‌تواند به‌کار رود. با این حال، آن‌ها در دامنه‌های مسیریابی جداگانه هستند. نگاشت از نشانی NSAP به نشانی UN به‌وسیله‌ی NLSP با به‌کارگیری صفت همبستگی امنیتی Adr-served مدیریت می‌شود تا نشانی NSAPای که به‌وسیله‌ی نشانی‌های UN نگه‌داشته‌شده در صفت همبستگی امنیتی Peer_Adr خدمت‌رسانی می‌شوند را شناسایی کند.

ث-۵ مد بی‌اتصال NLSP

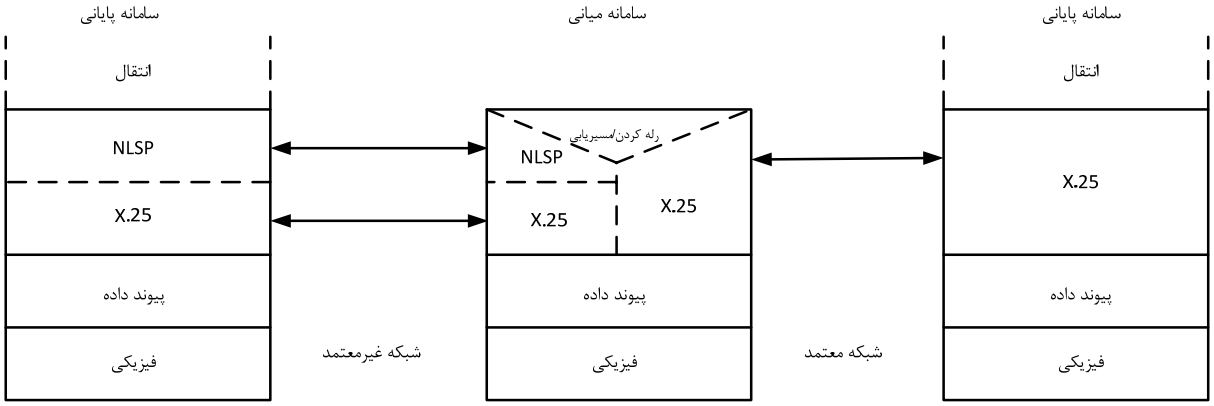
ث-۵-۱ عملیات پایه

محافظت از NLSP-CL به سادگی با کپسوله‌سازی داده‌ی کاربر در یک SDT PDU ارائه می‌شود.

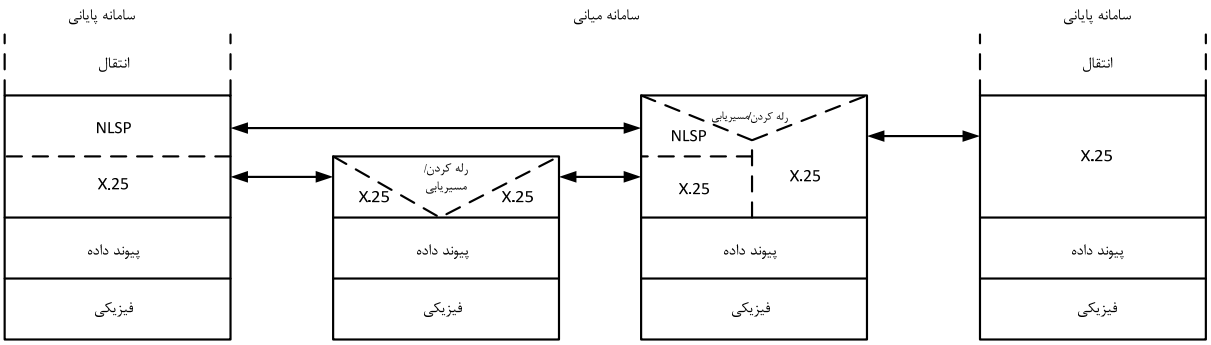
1 - Registration schemes



شکل ث-۴-۲ – نمایش NLSP-CO بین سامانه‌های پایانی



شکل ث-۴-۳ – NLSP-CO با یک شبکه غیرمعتمد



شکل ث-۴-۴ – نمایش NLSP-CO با سامانه‌ی رله غیرمعتمد

ث-۵-۲ جای‌گذاری

NLSP در مد بی‌اتصال می‌تواند به یکی از اشکال زیر عمل کند:

الف- در بالای لایه‌ی شبکه، قبل از اداره کردن به‌وسیله‌ی پروتکل شبکه‌ی بی‌اتصال (توصیه‌نامه‌ی X.233 ITU-T | ISO/IEC 8473-1) (به شکل ث-۵-۱ مراجعه شود) NSDUها را در یک SDT PDU کپسوله‌سازی می‌کند. این پشته تنها بین دو سامانه‌ی پایانی به‌کار می‌رود، یا

ب- زیر پروتکل شبکه‌ی بی‌اتصال، PDUهای پروتکل بی‌اتصال را قبل از نگاشت به زیرشبکه اصلی، کپسوله‌سازی می‌کنند (به شکل ث-۵-۲ مراجعه شود.). این پشته برای استفاده به همراه سامانه‌های میانی رله «مورد اعتماد» یا حالت انتها به انتها است که هیچ رله شبکه‌ای بین دو سامانه در حال ارتباط وجود ندارد، است یا

پ- می‌تواند زیر یک لایه پروتکل توصیه‌نامه‌ی ITU-T X.233 | ISO/IEC 8473-1 (CLNP) برای دامنه «مورد اعتماد»/«قرمز» و نگاشت به یک لایه پروتکل CLNP دیگر برای دامنه «غیرمعتمد»/«سیاه»، عمل کند. این پشته انعطاف‌پذیرترین پشته است و می‌تواند در هر محیطی کار کند. سامانه‌های میانی «مورد اعتماد» پروتکل CLNP بالایی را پس از حذف کردن محافظت امنیت ارائه‌شده به‌وسیله‌ی NLSP، رله می‌کنند. سامانه‌های رله «غیرمعتمدِ» دیگر، بر روی پروتکل CLNP پایینی رله کرده و داده‌ی محافظت‌شده NLSP را به‌طور شفاف ارسال می‌کنند. (به شکل ث-۵-۳ مراجعه شود.)

یادآوری ۱– بازنمود دو لایه‌ی توصیه‌نامه‌ی ITU-T X.233 | ISO/IEC 8473-1 و یک لایه‌ی NLSP صورت لزوم دلالت بر ماشین‌های پروتکل جداگانه ندارند. این امر به خط‌مشی پیاده‌سازی محلی بستگی دارد.

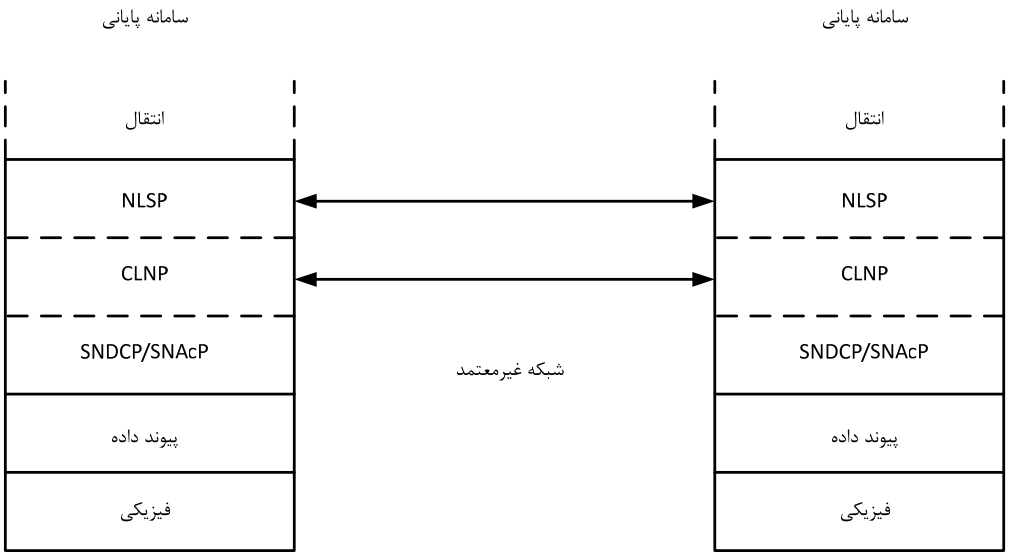
یادآوری ۲– وجود دو لایه‌ی پروتکل CLNP در صورت لزوم وجود پیاده‌سازی‌های جداگانه را متضمن نمی‌شود.

ث-۵-۳ نگاشت واسط خدمت NLSP/UN

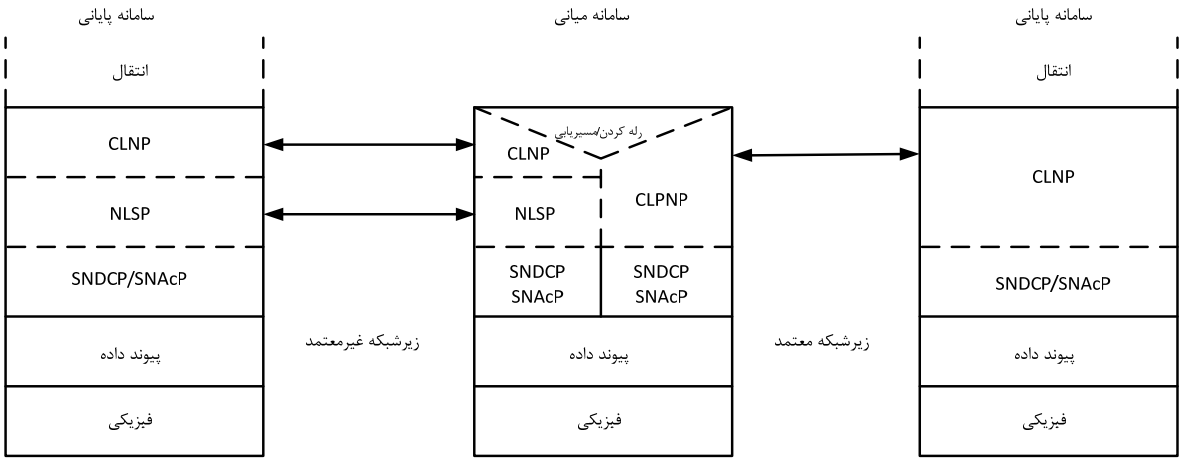
در مواردی که NLSP در بالای لایه‌ی شبکه عمل می‌کند، واسط خدمت NLSP مشابه خدمت شبکه‌ی OSI است و واسط خدمت UN نیز به جز این‌که برای یک هستار NLSP به‌جای خدمت شبکه واسطه می‌شود، شبیه به لایه‌ی شبکه OSI است.

در دومین حالت که NLSP زیر CLNP عمل می‌کند، واسط خدمت NLSP معادل خدمت ارائه‌شده به‌وسیله‌ی زیرشبکه‌ای است که زیر CLNP عمل می‌کند و خدمت UN مانند خدمت زیرشبکه است.

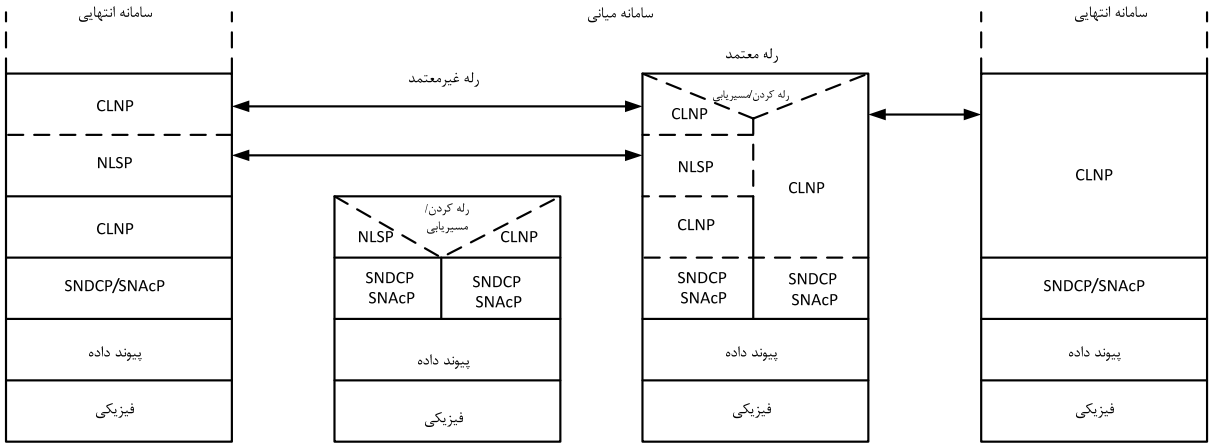
در حالت آخر، واسط بالای NLSP، پروتکل CLNP بالایی را مانند یک زیرشبکه در نظر می‌گیرد. واسط UN برای پروتکل CLNP اصلی مانند یک خدمت شبکه OSI به نظر می‌رسد.



شکل ث-۵-۱ – تشریح NLSP-CL بین سامانه‌های پایانی



شکل ث-۵-۲ – تشریح NLSP-CL با زیرشبکه غیرمعتمد



شکل ث-۵-۳ – نمایش NLSP-CL با سامانه‌ی رله غیرمعتمد

ث-۵-۴ نشانی‌دهی

در مواردی که NLSP در بالای لایه‌ی شبکه عمل می‌کند، نشانی استفاده‌شده به‌وسیله‌ی NLSP یک نشانی NSAP شبکه OSI است. در موردی که NLSP تحت توصیه‌نامه‌ی ITU-T X.233 | ISO/IEC 8473-1 (CLNP) عمل می‌کند، قبل از این‌که به زیرشبکه‌ی اصلی نگاشت شود، نشانی استفاده‌شده در واسط بالا و پایین NLSP یک نشانی زیرشبکه است. (به عنوان مثال نشانی MAC شبکه محلی) اگر NLSP بین دو لایه CLNP عمل کند، نشانیی که به هستار NLSP فرستاده می‌شود یک نشانی زیرشبکه است.

اگر پنهان‌سازی نشانی فعال باشد (Param_Prot، برابر FALSE باشد)، آنگاه نشانی‌های واسط خدمت UN مانند نشانی‌های واسط خدمت NLSP خواهند بود.

اگر پنهان‌سازی نشانی‌ها ارائه شده باشد (Param_Prot، برابر TRUE باشد) نشانی‌های به‌کار رفته در واسط خدمت UN (نشانی‌های UN) مانند نشانی‌های NLSP خواهند بود، با این وجود، این نشانی‌ها برای شناسایی هستارهای NLSP که در بین سامانه میانی یا پایانی قرار گرفته‌اند، به‌کار می‌روند. این نشانی‌های UN می‌توانند مانند نشانی‌های NSAP مدیریت شوند. طرح‌های ثبت‌نام یکسان برای تخصیص نشانی‌ها و پروتکل‌های مسیریابی یکسان برای مدیریت مسیریابی می‌تواند به‌کار رود. با این حال، این نشانی‌ها در دامنه‌های مسیریابی تفکیک‌شده قرار دارند. نگاشت از نشانی NSAP به نشانی UN به‌وسیله‌ی NLSP با به‌کارگیری صفت همبستگی امنیتی Adr-served انجام می‌گیرد تا نشانی NSAP که به‌وسیله‌ی نشانی‌های UN نگه‌داشته‌شده در صفت همبستگی امنیتی Peer_Adr خدمت‌رسانی می‌شود را شناسایی کند.

ث-۵-۵ قطعه‌بندی

قطعه‌بندی و سرهم‌بندی توسط توصیه‌نامه‌ی ITU-T X.233 | ISO/IEC 8473-1 (CLNP) انجام می‌شوند. قطعه‌بندی بسته به زیرشبکه‌های اصلی که PDU از آن‌ها عبور کرده است، می‌تواند قبل یا بعد از پردازش NLSP انجام پذیرد. اگر قطعه‌بندی قبل از NLSP انجام شود، آنگاه هر قطعه کپسوله‌شده در NLSP است که به دستگاه واکپسوله‌سازی NLSP فرستاده می‌شود و سپس از کپسول خارج شده و دوباره به‌وسیله‌ی CLNP سرهم‌بندی می‌شود. اگر قطعه‌بندی بعد از NLSP صورت پذیرد، CLNP ابتدا قطعات را سرهم‌بندی می‌کند. کل PDU به‌وسیله‌ی NLSP از کپسول خارج می‌شود. سپس CLNP، PDU از کپسول خارج‌شده را به نشانی مقصد (که توسط پروتکل‌های اتصال عادی مشخص می‌شود) تحویل می‌دهد.

ث-۶ صفات و همبستگی‌های امنیتی

NLSP-CO و NLSP-CL به یک مجموعه صفات مرتبط به اسم صفات همبستگی امنیتی برای انجام ارتباطات امن نیاز دارند. این صفات شامل موارد زیر می‌شوند:

الف- اطلاعات مربوط به «خط‌مشی» پایه که عملیات NLSP را تعریف یا محدود می‌کنند، به‌عنوان مثال الگوریتم رمزگذاری، اندازه‌ی بستک رمزگذاری، طول شماره دنباله یکپارچگی و صادرکننده‌ی تعریف برچسب؛

ب- مقادیر اولیه‌ی مورد نیاز برای کنترل عملیات NLSP، به‌عنوان مثال کلیدهای اصلی و شماره‌های دنباله یکپارچگی اولیه؛
پ- مقادیر جاری مورد نیاز برای کنترل کارکرد NLSP: کلیدهای کاری برای اتصال خاص، شماره دنباله یکپارچگی جاری.
وجود مجموعه‌ای از صفات مرتبط، همبستگی امنیتی نامیده می‌شود. مجموعه صفات به‌کار رفته برای محافظت یک PDU بی‌اتصال یا یک اتصال به‌وسیله‌ی یک شناسه‌ی همبستگی امنیتی مورد ارجاع قرار می‌گیرند.
اولین مجموعه از اطلاعات مربوط به «خط‌مشی»، «مجموعه توافق‌شده از قواعد امنیتی» (ASSR) نامیده می‌شود. پیشنهاد می‌شود که این مورد از طریق ثبت‌نام برقرار شود.
مجموعه دوم از اطلاعات کنترل اولیه نیز می‌تواند برون باند با به‌کارگیری یک واسط مدیریت محلی یا مدیریت OSI برقرار شود، یا درون باند با به‌کارگیری پروتکلی که توأم با NLSP کار می‌کند (که «پروتکل برقراری همبستگی امنیتی» نامیده می‌شود)، برقرار شود.
مجموعه سوم از اطلاعات به‌عنوان قسمتی از عملیات پروتکل NLSP پایه، به‌روزرسانی می‌شود. برای مثال، کلیدهای فعلی می‌توانند از طریق تبادل PDUهای کنترل امنیت اتصال در NLSP-CO برقرار شوند. شماره‌های دنباله یکپارچگی جاری در هر PDU انتقال داده امن به‌روزرسانی می‌شوند.

ث-۷ رابطه کارکردی پویا بین NLSP و CLNP

ث-۷-۱ مقدمه

زیربند ث-۵-۲ رابطه بین NLSP و CLNP برای یک نمونه از ارتباط را توصیف می‌کند. هدف از این بند نشان‌دادن انعطاف‌پذیری NLSP به‌کارگرفته شده با CLNP برای پشتیبانی اتصالات محافظت‌شده و محافظت‌نشده مستقل از معماری ارتباطات است.
شکل ث-۷-۱ جریان داده در داخل و خارج این پروتکل‌های ترکیبی را نشان می‌دهد. متن زیر این جریان داده و پارامترهای ارتباط مورد نیاز برای آن را توصیف می‌کند.

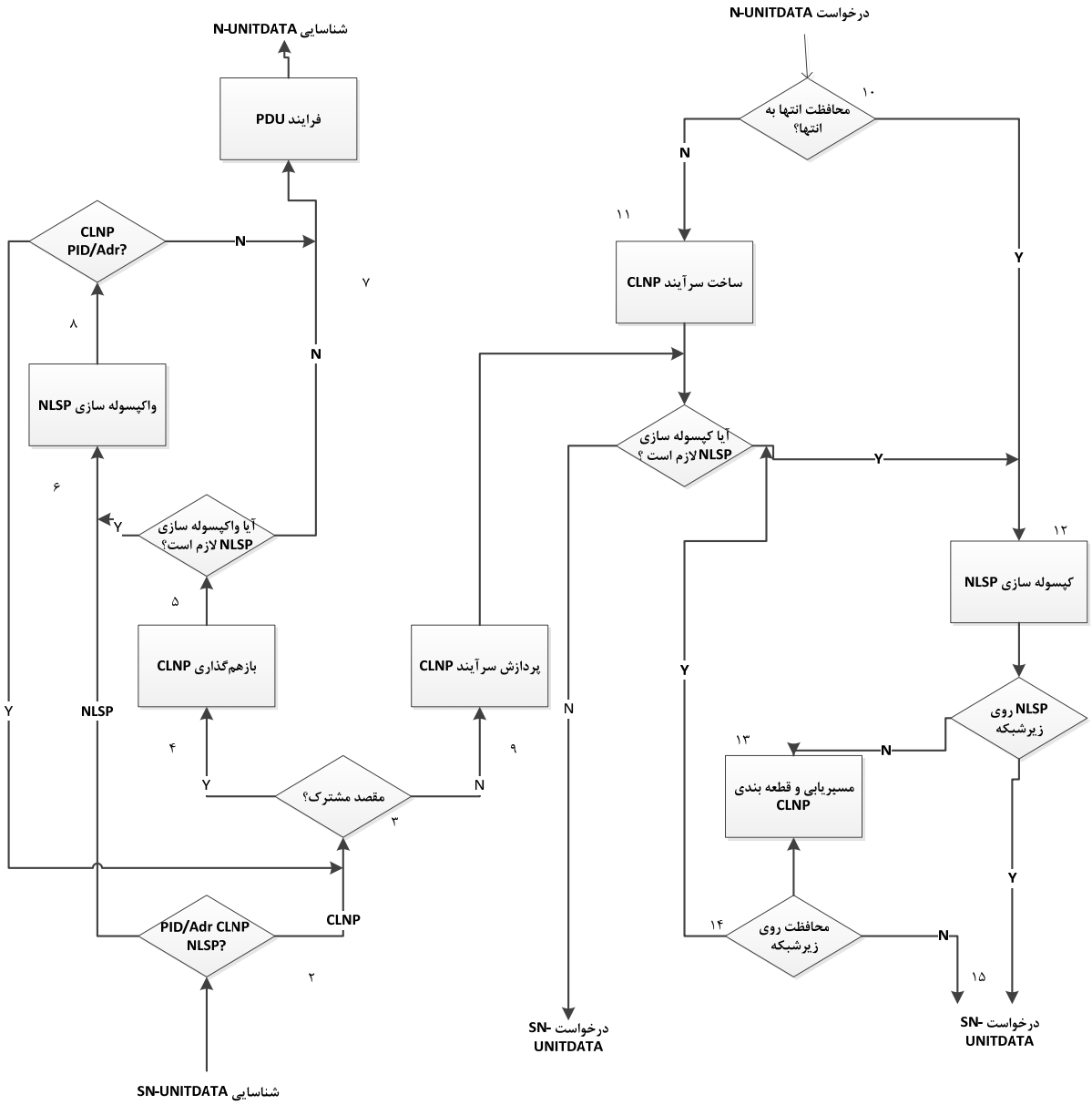
ث-۷-۲ نشان SN-UNITDATA

الف- در نشان SN-UNITDATA (۱) [توصیه‌نامه‌ی ITU-T X.233 | ISO/IEC 8473-1 (CLNP) (به زیربند ۵-۵ مراجعه شود)] شناسه‌ی پروتکل (PID) در اولین هشت‌تایی (یا اگر نشانی‌دهی استفاده شده باشد برای شناسایی پروتکل نشانی) برای تشخیص این‌که آیا اولین قسمت از PDU محتوی سرآیند یک CLNP یا NLSP است وارسی می‌شود (۲).
ب- اگر اولین سرآیند CLNP را شناسایی کند، آنگاه یک تصمیم برمبنای نشانی مقصد در سرآیند CLNP گرفته می‌شود (۳). اگر نشانی مقصد به‌عنوان یکی از نشانی‌های سامانه‌ی پایانی تشخیص داده شود، آنگاه CLNP PDU به فرآیند سرهم‌بندی فرستاده می‌شود (۴) [CLNP (به زیربند ۶-۸ مراجعه شود)]. اگر

نشانی، نشانی یکی از سامانه‌های پایانی نباشد، آنگاه سرآیند CLNP برای ارسال پردازش می‌شود (۸) همان‌طورکه در زیربند ث-۶-۴ تشریح شده است.

پ- اگر اولین سرآیند NLSP را شناسایی کند، آنگاه پارامترهای خدمت زیرشبکه و داده‌های کاربر به‌وسیله‌ی NLSP مانند UN-UNITDATA پردازش می‌شوند. سپس وارسی می‌شود که آیا نشان کاربر NLSP-UNITDATA حاصله اولین هشت‌تایی یک CLNP PID است (۸). اگر چنین باشد، NLSP-UNITDATA همان‌طورکه در قسمت ب گفته شد پردازش می‌شود (۳)، در غیر این‌صورت نشان NLSP-UNITDATA به نشان N-UNITDATA نگاشت خواهد شد (۷).

ت- پس از سرهم‌بندی مجدد CLNP (در صورت نیاز) (۴) یک تصمیم دیگر مورد نیاز است. (۵) اگر CLNP PDU حاوی یک NLSP PDU باشد (اولین هشت‌تایی حاوی NLSP PID باشد)، آنگاه پارامترهای خدمت CLNP و داده‌های کاربر به‌وسیله‌ی NLSP مانند نشان UN-UNITDATA پردازش می‌شوند (۶)، در غیر این‌صورت به‌طور مستقیم به نشان N-UNITDATA نگاشت می‌شوند (۷). سپس وارسی می‌شود که آیا اولین هشت‌تایی نشان کاربر NLSP-UNITDATA حاصله، یک CLNP PID است یا خیر(۸) (یا اگر نشانی‌دهی برای شناسایی پروتکل به‌کار رفته باشد، نشانی را وارسی می‌کند.) اگر چنین باشد، NLSP-UNITDATA همان‌طورکه در قسمت ب گفته شد پردازش می‌شود (۳)، در غیر این‌صورت نشان NLSP-UNITDATA به نشان N-UNITDATA نگاشت خواهد شد (۷).



شکل ث-۷-۱ – نمودار جریان NLSP با CLNP

ث-۷-۳ درخواست N-UNITDATA

الف- در هنگام درخواست یک N-UNITDATA (۱۰)، بسته به پارامترهای خدمت (به‌عنوان مثال نشانی مبدأ یا مقصد) و خط‌مشی امنیتی محلی، درخواست یا به‌طور مستقیم به CLNP نگاشت می‌شود (به زیربند ۴-۵ مراجعه شود) (۱۱) یا به یک درخواست NLSP-UNITDATA نگاشت شده و براساس آن پردازش می‌شود. (۱۲)

ب- اگر N-UNITDATA به‌وسیله‌ی CLNP پردازش شود (۱۱)، CLNP PDU حاصله یا به‌طور مستقیم به یک درخواست SN-UNITDATA نگاشت می‌شود (۱۵) یا به یک درخواست NLSP-UNITDATA برای پردازش به‌وسیله‌ی NLSP نگاشت می‌شود. (۱۰)

پ- اگر N-UNITDATA یا یک CLNP PDU به‌وسیله‌ی NLSP پردازش شود (۱۲)، درخواست UN-UNITDATA حاصله یا به‌طور مستقیم به یک درخواست SN-UNITDATA نگاشت می‌شود (۱۵) یا به یک CLNP مانند یک N-UNITDATA (۱۳) برای پردازش نگاشت می‌شود. این امر به پارامترهای خدمت و خط‌مشی امنیتی محلی بستگی دارد. در ادامه‌ی پردازش CLNP، اگر محافظت اضافی بر روی زیرشبکه نیاز باشد (۱۴)، محافظت بیشتر از NLSP ممکن است ارائه شود ، در غیر این‌صورت CLNP PDU به SN-UNITDATA نگاشت می‌شود.

ث-۷-۴ ارسال CLNP PDU

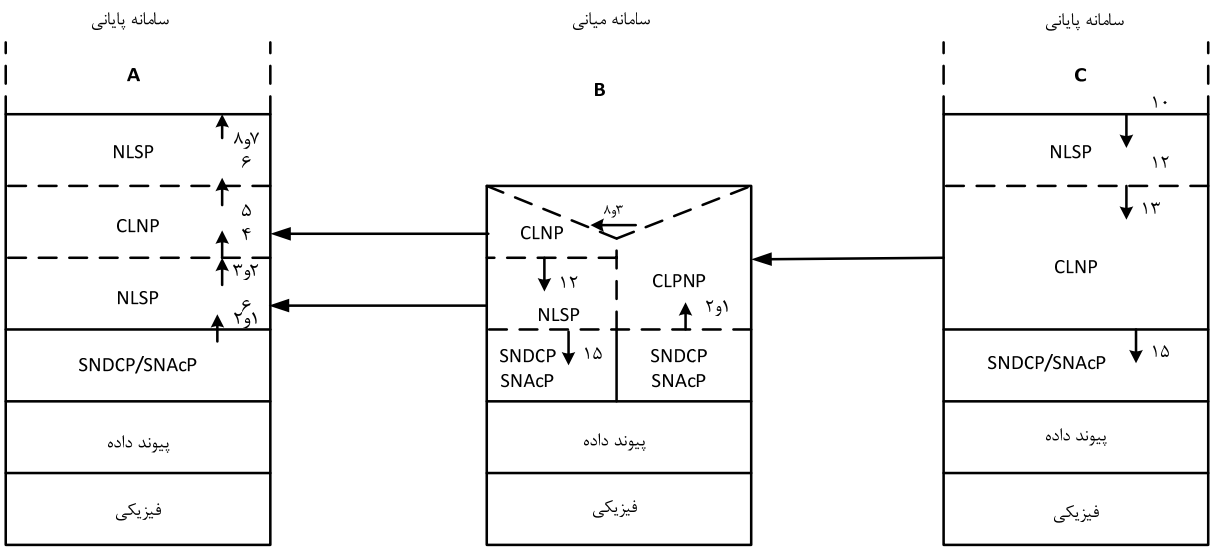
تصمیم‌گیری برای محافظت یک CLNP PDU ارسال‌شده براساس اطلاعات درون سرآیند CLNP PDU، داده‌های کاربر و خط‌مشی امنیتی محلی صورت می‌گیرد. اگر محافظت نیاز باشد، CLNP PDU به یک درخواست NLSP-UNITDATA برای پردازش به‌وسیله‌ی NLSP نگاشت می‌شود. (۱۲) بسته به پارامترهای خدمت و الزامات خط‌مشی امنیتی محلی، UN-UNITDATA محافظت‌شده حاصله یا به‌طور مستقیم به یک درخواست SN-UNITDATA نگاشت می‌شود [CLNP (به زیربند ۶-۵ مراجعه شود)] (۱۵) یا به یک CLNP برای پردازش مانند N-UNITDATA نگاشت می‌شود. (۱۳) این امر به پارامترهای خدمت و الزامات خط‌مشی امنیتی محلی بستگی دارد.

ث-۷-۵ تکرار واسط CLNP NLSP-CL

زیربندهای قبلی رابطه کارکردی بین NLSP-CL و CLNP را نشان می‌دهند. به دلیل سادگی، عملیات این پروتکل‌ها به‌وسیله‌ی واسط‌های خدمت به‌صورت مجزا نشان داده می‌شود. عملیات دو پروتکل ممکن است به‌صورت یک پروتکل لایه ۳ منفرد که عملیات ماشین‌های پروتکل CLNP و NLSP را ترکیب می‌کند، پیاده‌سازی شود.

ث-۸ کارکرد پویای مربوط به مدل لایه‌ای

رویکرد لایه‌ای برای توصیف NLSP می‌تواند به توصیف نمودار جریان پیکربندی نمونه‌ی داده شده در شکل ث-۷-۲ مرتبط شود، مانند زیر:



شکل ث-۷-۲ – مدل لایه‌ای مرتبط به نمودار جریان

عمل	مرجع نمودار جریان
در سامانه‌ی پایانی A	
نشان‌دهنده SN-UNITDATA در سامانه‌ی پایانی C	۱
وارسی CLNP یا NLSP	۲
وارسی محلی بودن مقصد	۳
سرهم‌بندی مجدد CLNP	۴
وارسی NLSP	۵
نگاشت به UN-UNITDATA و واکپسوله‌سازی NLSP	۶
نگاشت به نشان N-UNITDATA	۷
وارسی CLNP	۸
در سامانه میانی B	
نشان SN-UNITDATA در سامانه میانی B	۱
وارسی CLNP یا NLSP	۲
وارسی محلی بودن مقصد	۳
پردازش CLNP برای ارسال	۸
نگاشت به NLSP-UNITDATA و کپسوله‌سازی NLSP	۱۲
نگاشت UN-UNITDATA به درخواست SN-UNITDATA	۱۵
در سامانه‌ی پایانی C	
درخواست N-UNITDATA در سامانه‌ی پایانی A	۱۰
نگاشت به NLSP-UNITDATA و کپسوله‌سازی NLSP	۱۲
نگاشت UN-UNITDATA به CLNP برای پردازش مانند N-UNITDATA	۱۳
نگاشت CLNP PDU به درخواست SN-UNITDATA	۱۵

پیوست ج
(الزامی)
مثالی از یک مجموعه توافق شده از قواعد امنیتی

یک مجموعه توافق‌شده از قواعد امنیتی (ASSR) سازوکارهای امنیتی را برای استفاده برقرار می‌کند. این مجموعه شامل تمام پارامترهای مورد نیاز برای تعریف کارکرد سازوکار مربوط به خدمات امنیتی انتخابی مفروض می‌شود. این پیوست مثالی از چگونگی نوشته شدن مقادیر صفات SA (که ممکن است توسط یک ASSR برقرار شوند) را در یک پیش‌نویس ارائه می‌کند.

ASSR-ID **XYZ (شناسه شئ)** -- مرجع شئ به‌کار رفته در SA-P را می‌دهد.

SA-ID_Length **4**

پودمان تعریف خدمات امنیتی انتخاب‌شده -- خدمات امنیتی را که می‌توانند تحت قواعد امنیتی پشتیبانی شوند مشخص می‌کند و به سطوح محافظتی که به‌وسیله‌ی الگوریتم‌های مختلف، طول‌های کلید و غیره پشتیبانی می‌شوند، نامی را اختصاص می‌دهد.

PE Auth:	هیچکدام	پایین	بالا
AC:	هیچکدام	پایین	بالا
Confid:	هیچکدام	پایین	بالا
Integ:	هیچکدام	پایین	بالا

نگاشت برچسب امنیتی -- برچسب امنیتی را به انتخاب‌های خدمت امنیتی نگاشت می‌کند.

XYZ Label_Def_Auth
Label-> Sensitivity = Unclass
دلالت دارد بر:
PE Auth none, AC none, Confid none, Integ none
Label-Sensitivity = Confidential
دلالت دارد بر:
PE Auth low, AC low, Confid low, Integ none
Label-Sensitivity = Secret
دلالت دارد بر:
PE Auth high, AC high, Confid high, Integ high

Param_Prot **TRUE** -- انتخاب می‌کند که کدام یک از سطوح محافظت نیاز به محافظت از تمام پارامترهای خدمت دارند.

برای خدمات امنیتی انتخاب شده: Integ = high یا Conf = high

پودمان سازوکار – برچسب‌های امنیتی برای کنترل دسترسی

برای خدمات امنیتی انتخاب شده: AC = high یا Conf = high

-- نشان می‌دهد که کدام انتخاب خدمت امنیتی نیاز به برچسب‌های امنیتی دارد.

Label_Def_Auth XYZ

(توجه شود که باید مانند Auth برای محافظت برچسب‌های QOS باشد.)

نشان صریح بله

پودمان سازوکار – مقدار وارسی یکپارچگی

برای خدمات امنیتی انتخاب شده: Integ > none یا PE Auth = High یا برچسب‌های امنیتی سازوکار

ICV_Alg	XYZ
کلیددهی مجدد پس از	10000 PDUs
سازوکار توزیع کلید	نامتقارن

پودمان سازوکار – شماره دنباله یکپارچگی

برای خدمات امنیتی انتخاب شده: Integ = high یا Auth = High

ISN_Len ۸ هشت‌تایی در مجموع

شماره دنباله ۴ هشت‌تایی

یکی افزایش می‌یابد

Timestamp ۴ هشت‌تایی

میلی‌ثانیه از نقطه همگام‌سازی

پنجره ISN دریافت دنباله قبلی را دور می‌ریزد #.

Timestamp باید در تأخیر شبکه مابین maximum×2 تغییر کند. اگر خارج از پنجره باشد آنگاه یک حمله بازپخش خواهد بود.

پودمان سازوکار – رمزگذاری

برای خدمات امنیتی انتخاب شده: Conf > low

Enc_Alg_ID	XYZ
حالت	زنجیری
Enc_Blk	۸ هشت‌تایی
اطلاعات تبادل کلید	(Prime p, Generator a)
کلیددهی مجدد پس از	1000 PDUs
سازوکار توزیع کلید	نامتقارن

پودمان سازوکار – No Header

برای خدمات امنیتی انتخاب شده: Conf = low و Integ = none و سازوکار بدون برچسب

پودمان سازوکار – احراز هویت اتصال

برای خدمات امنیتی انتخاب شده: AC > Low یا PE Auth >Low

XYZ Enc_Alg_ID

پودمان سازوکار – توزیع کلید نامتقارن

برای رمزگذاری سازوکار یا مقدار وارسی یکپارچگی

RSA Enc_Alg

پیوست چ
(اطلاعاتی)
صفات و همبستگي‌های امنیتی

برای محافظت از یک نمونه ارتباطی (یک SDU بی‌اتصال یا یک اتصال) یک مجموعه از اطلاعات (کلیدها و سایر صفاتی که برای کنترل عملیات امنیتی نیاز هستند) باید بین هستارهای در حال ارتباط، برقرار گردد. از این مجموعه اطلاعات به‌عنوان همبستگی امنیتی (SA) یاد می‌شود.

اطلاعاتی که یک SA را شکل می‌دهند یا اطلاعات ایستا هستند که می‌توانند وقتی که SA برقرار شد «سفارشی‌سازی[1]» شوند و سپس در طی همبستگی ثابت بمانند یا اطلاعات پویایی هستند که می‌توانند در طی طول عمر همبستگی امنیتی به‌روزرسانی شوند.

یک SA ممکن است به‌صورت برون باند یا به‌صورت درون باند توسط تبادل SA PDUها برای NLSP-CO برقرار شود. زمانی که روش درون باند به‌کار می‌رود، سازوکارهای خاص تشخیص SA-P ممکن است مانند این استاندارد ملی تعریف شوند یا ممکن است از سازوکارهای خصوصی استفاده شود.

قبل از برقراری یک SA هر هستار NLSP باید قبلاً برقرار شده باشد:

الف- یک مجموعه مشترک از قواعد امنیتی با داشتن خدمات امنیتی انتخاب‌شده، سازوکارهای امنیتی، شامل تمام پارامترهای مورد نیاز برای تعریف کارکرد سازوکارها (به‌عنوان مثال الگوریتم، طول کلید، طول عمر کلید) که باید استفاده شوند را مشخص می‌کنند. این قواعد امنیتی به‌صورت مشترک به توافق رسیده‌اند و به‌وسیله‌ی هستارهای در حال ارتباط به‌صورت یکتا مشخص می‌شوند. قواعد امنیتی و شناسه‌های آن‌ها ممکن است به‌وسیله‌ی شخص ثالث‌ها ثبت شوند. برای مشاهده یک نمونه از مجموعه قواعد امنیتی به پیوست ج مراجعه شود.

ب- خدمات امنیتی و بنابراین سازوکارهای امنیتی که ممکن است استفاده شوند.

اگر روش درون باند برقراری یک SA استفاده شود ، موارد زیر باید از پیش برقرار شوند:

پ- خدمات امنیتی انتخاب‌شده‌ی اولیه و بنابراین سازوکارهای امنیتی که در برقراری یک SA اعمال می‌شوند.

ت- اطلاعات کلیددهی پایه مورد نیاز برای برقراری یک SA.

در برقراری SA، یک هستار NLSP، اطلاعات زیر که با همتای راه دور خود به اشتراک گذاشته است را برقرار می‌سازد:

ث- SA-IDهای محلی و راه دور.

---

1 - Customise

ج- خدمات امنیتی که بین هستارهای مرتبط به یک نمونه ارتباطی استفاده می‌شوند.
چ- سازوکارها و پارامترهای آن‌ها که به‌طور ضمنی در خدمات امنیتی انتخاب‌شده مشخص شده‌اند.
ح- کلیدهای مشترک اولیه برای یکپارچگی، سازوکارهای رمزگذاری و احراز هویت یک نمونه ارتباطی.
خ- مجموعه برچسب‌های امنیتی و نشانی‌هایی که برای کنترل دسترسی در این همبستگی ممکن است به‌کار روند.

مراجع SA و کلیدهای مشترک [موارد ث و ح بالا] باید برای هر همبستگی برقرار شوند. اطلاعات دیگر ممکن است از قبل برقرار شوند و برای چندین همبستگی مشترک باشند. به‌علاوه، به‌عنوان قسمتی از برقرارسازی یک SA شخصی‌سازی شده، هویت همتای راه دور باید محرز شود. پیوست پ سازوکاری که برای توزیع کلید و احراز هویت می‌تواند استفاده شود را تعریف می‌کند.

اطلاعات زیر می‌توانند به‌صورت پویا برای یک نمونه ارتباطی به‌روزرسانی شوند:

د- شماره(های) دنباله یکپارچگی که برای داده‌ی عادی و پیشتاز در هر جهت نیاز هستند.
ذ- یک برچسب امنیتی.
ر- اطلاعات کلیددهی مجدد برای سازوکارهای رمزگذاری/یکپارچگی.

برای نیل به احراز هویت، سازوکارهای احراز هویت باید به هر نمونه‌ی ارتباطی اعمال شوند.

صفات SA متفاوت که ممکن است در مراحل مختلف یک همبستگی امنیتی برقرار شوند در شکل چ-۱ نشان داده شده‌اند.

از پیش برقرار شده	ایستا	پویا
محدوده‌ی خدمات امنیتی انتخاب‌شده خدمات امنیتی انتخاب‌شده‌ی اولیه اطلاعات کلید پایه مجموعه توافق‌شده قواعد امنیتی	کلیدهای اولیه SA-ID احراز هویت برچسب امنیتی	ISN احراز هویت SA-ID اطلاعات کلیددهی مجدد
خدمات امنیتی انتخاب‌شده سازوکارهای انتخاب‌شده مجموعه برچسب امنیتی/ مجموعه نشانی‌ها		

شکل چ-۱ – نمایش ۳ سطح از همبستگی امنیتی

پیوست ح
(اطلاعاتی)
نمونه تبادل نشانه‌ي کلید- الگوریتم EKE

در ادامه یک مثال از الگوریتم تبادل نشانه‌ی کلید که می‌تواند با پروتکل همبستگی امنیتی تعریف‌شده در پیوست پ به‌کار رود، آمده است.

دو پارامتر برای EKE نیاز است: اولی یک عدد اول p بزرگ است (به‌نحوی که p-1 یک فاکتور اول بزرگ دارد) و دومی یک عدد «a» که در محدوده‌ی 1<a<p-1 قرار دارد.

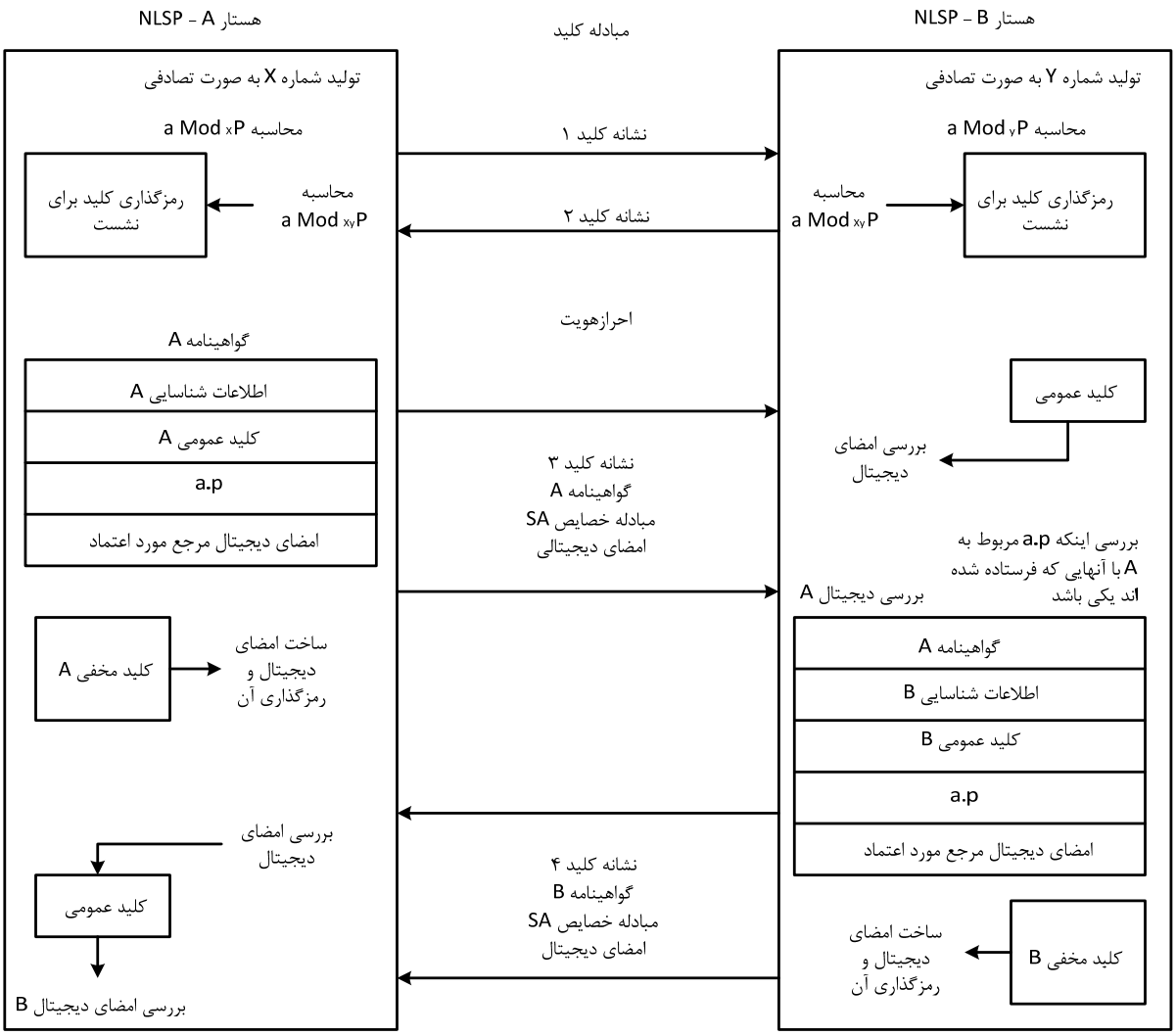
A و B دو طرف یک اتصال فرض می‌شوند (به شکل ح-۱ مراجعه شود). EKE با انتخاب یک عدد تصادفی بزرگ X به‌وسیله‌ی A و انتخاب یک عدد تصادفی بزرگ به‌وسیله‌ی B آغاز می‌شود. A مقدار (a**X mod p) را محاسبه کرده و a، p و (a**X mod p) را برای B ارسال می‌کند، B مقدار (a**XY mod p) را محاسبه کرده و آن را به A ارسال می‌کند. A و B هر دو مقدار (a**XY mod p) را محاسبه می‌کنند. یک شنودگر[1] تنها می‌تواند مقادیر (a**X mod p) و (a**Y mod p) را ببیند و نمی‌تواند مقادیر X و Y را تشخیص دهد، بنابراین نمی‌تواند (a**XY mod p) را محاسبه کند.

پس از آن، A و B می‌توانند زیرمجموعه‌ای از بیت‌ها در (a**XY mod p) را به‌عنوان کلید و به‌عنوان اطلاعاتی برای مقابله با حملات بازپخش در دومین تبادل، استفاده کنند.

مقادیر توصیف‌شده در پروتکل SA تعریف‌شده در پیوست پ عبارتند از:

- رشته بیتی EKE مشترک برابر (a**XY mod p) است.
- Key Token 1 a، p، (a**X mod p) است که در آن «a»، «p» و (a**X mod p) در قالب یک رشته هشت‌تایی الحاق‌شده کدبندی می‌شوند.
- Key Token 2 برابر با (a**Y mod p) است.
- Key Token 3 اطلاعات مشتق‌شده از رشته بیتی KTE مشترک (a**XY mod p) برای مقابله با حملات بازپخش است.
- Key Token 4 اطلاعات مشتق‌شده از رشته بیتی KTE مشترک (a**XY mod p) برای مقابله با حملات بازپخش است.

1 - Eavesdropper



شکل ح-۱ – نمایش اشتقاق کلید بر- خط و اشتقاق با استفاده از EKE