فصل پانزدهم

شبکه های نسل آتی (NGN[1])

۱۵-۱- مقدمه

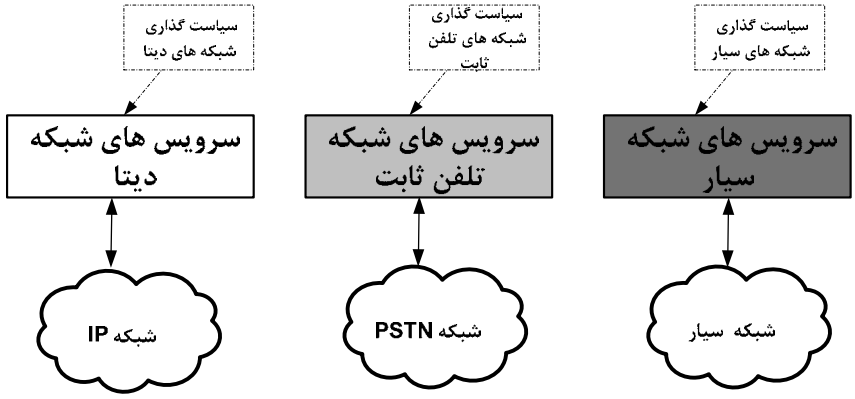
شبکه های نسل آتی ، یک ساختار شبکه ای جدید است که در آن صوت ، داده، خطوط ارتباطی با سیم و بیسیم ، در یک ساختار شبکه واحد ترکیب می شوند. درشبکه های نسل آتی، لایه سرویس و لایه های شبکه از هم جدا شده اند، بنابراین سرویس ها می توانند روی هر شبکه به صورت مستقل گسترش یابند. شبکه های نسل آتی یک تغییر چهره اساسی در ارتباطات مشتری و شبکه های کامپیوتری است .

این نوع شبکه ها، رقابت بین فراهم کنندگان سرویس در ارائه سرویس های ویدئو ، تلفن، اینترنت و غیره را به وجود می آورند. شبکه های صوت و داده در یک شبکه یکپارچه با استفاده از واسط های قدرتمند جمع می شوند. استفاده از شبکه های نسل آتی درحالتیکه شبکه های مختلف و پیچیده به صورت مجزا وجود دارند و یکپارچه نشده اند، بسیار مفیدمی باشد. شبکه حاصل با اینکه ترکیبی از شبکه های تلفن (PSTN[2])، شبکه تلفنی موبایل، شبکه ATM و شبکه های محلی سیمی و بیسیم است ، اما دارای ماهیتی کاملاً مستقل می باشد. باید توجه داشت که سرویس ها در هر محیط شبکه، هویت مستقل و کاملی دارند. بنابراین سرویس تهیه شده برای شبکه PSTN نمی تواند در شبکه های دیگر مثل موبایل یا اینترنت به سادگی استفاده شود .

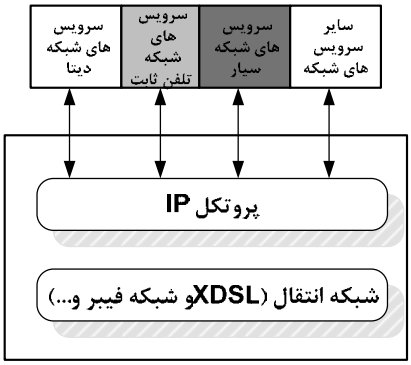
شبکه های مخابراتی کنونی ، شبکه هایی اتصال گرا هستند و شامل بلوک های یکپارچه از توابع وابسته به یکدیگر می باشند که تنها از یک نوع سرویس پشتیبانی می کنند. این شبکه ها رویکردی عمودی داشته و لایه ها کاملاً به یکدیگر وابسته هستند.

همان گونه که در شکل (۱۵-۱) مشاهده می شود، برای سرویس های مختلف با زیر ساخت های متفاوت، از لایه های متفاوتی استفاده می شود و بین لایه ها هیچ همگرایی وجود ندارد. بنابراین استفاده از سرویس های متنوع مستلزم هزینه زیادی است.

[1] Next Generatin Networks
[2] Public Switched Network



الف) شبکه های سنتی موجود
(مدل عمودی)



ب) شبکه های نسل آتی
(مدل افقی)

شکل(۱۵-۱): مقایسه مدل شبکه های سنتی موجود و شبکه های نسل آتی

نیاز دنیای امروز، شبکه ای همگراست که توانایی ارائه سرویسهای متنوع را داشته باشد. امروزه با تغییر تقاضای مشتریان، استراتژی های اپراتورها نیز تغییر کرده است. تقاضا های مشتریان شامل شخصی سازی[1] ، تسهیلات ، سرویس های آتی ، قابلیت دسترسی و فراگیر بودن است که انتظار می رود اپراتورهای ثابت و سیار پاسخگوی آنها باشند. درادامه به بررسی این نیازهای مشتریان می پردازیم:

- **شخصی سازی:** مشتری به سرویس هایی مطابق با نیازهای خود احتیاج دارد و نیز هر وسیله موجود باید یک پروفایل عمومی قابل دسترس داشته باشد ، چرا که کاربر تنها اطلاعاتی را به دست می آورد که بدان نیاز دارد.
- **تسهیلات:** داشتن دیدگاه و احساسِ یکسان نسبت به وسایل مختلف، استفاده از سرویس ها را آسان تر می کند. همچنین ساده سازی سرویس ها، پذیرش و استفاده از آنها را تسهیل می نماید. نتیجه تسهیل در استفاده، افزایش بازدهی مشترکین است.

[1] personalization

- **دسترسی و فراگیر بودن:** کاربر انتظار دارد که به هر سرویسی با هر وسیله ای و در هر مکانی و هر زمانی دسترسی داشته باشد. با این دیدگاه، کاربر یک ترمینال را بر اساس نوع سرویس، وسیله در دسترس، توانایی وسیله و اولویت، به صورت اتوماتیک انتخاب می کند.

این نیازها و نکات دیگر که درادامه بدان خواهیم پرداخت، حرکت به سوی شبکه های نسل آتی را توجیه می کند.

۱۵-۲- تعاریف مختلف شبکه های نسل آتی

شبکه های نسل آتی از دیدگاه ETSI[1] به صورت یک مفهوم فنی برای تعریف و گسترش شبکه هایی است که شامل لایه های مختلف مجزا با استفاده از رابط های باز[2] هستند و به اپراتورها و فراهم کنندگان سرویس یک خط مشی، شامل یک روش گام به گام برای گسترش و مدیریت سرویس های ابتکاری می دهند.

شبکه های نسل آتی از دیدگاه ITU-T[3] و طبق توصیه نامه Y.2001 به صورت یک شبکه مبتنی بربسته تعریف می شودکه توانایی تهیه سرویس های ارتباطی و استفاده از فنآوری پهن باند چندگانه[4] وکیفیت سرویس را دارد. همچنین شامل توابع مبتنی بر سرویس که مستقل از فنآوری های مبتنی بر انتقال در لایه های زیرین است، می باشد. شبکه های نسل آتی، یک دسترسی نامحدود برای کاربران ایجاد می کنند و از قابلیت حمل کلی برای همه کاربران در همه جا پشتیبانی می نمایند. انتقال به صورت بدون اتصال انجام می شود و معماری ماژولار در آن امکان دارا بودن لایه های مستقل از هم را فراهم می کند. ارتباط بین لایه ها از طریق رابط های باز است.

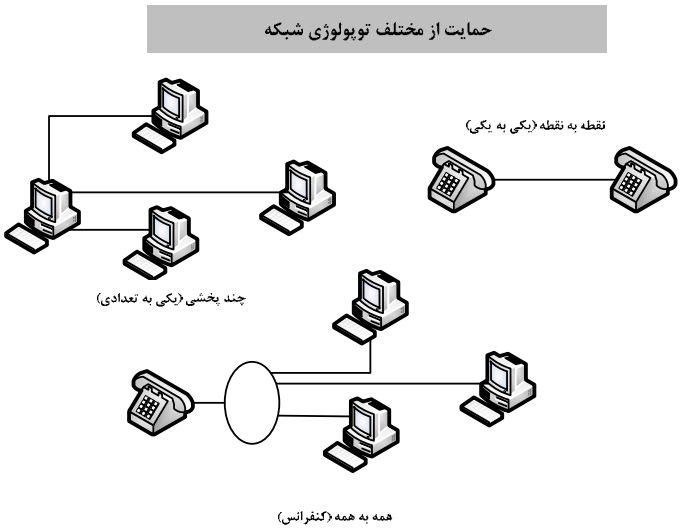
ویژگی های اصلی شبکه های نسل آتی از دیدگاه ITU-T به شرح زیر است:

- انتقال مبتنی بر بسته
- جدا سازی توابع کنترلی به صورت ظرفیت های حامل[5] و call/session و سرویس/ کاربرد[6].
- مجزا کردن فراهم سازی سرویس از شبکه حامل با استفاده از API[7] ها(JAIN[8]،Parlay)
- پشتیبانی از انواع سرویس بر اساس عناصر سازنده سرویس (سرویس های بلادرنگ/ غیر بلادرنگ/ چند رسانه ای)
- اضافه شدن ویژگی باند پهن با کیفیت سرویس انتها به انتها
- ارتباط بین شبکه ای با شبکه های موجود
- تحرک پذیری تعمیم یافته جهت تدارک همگون و فراگیر سرویس به کاربران
- سرویس همگرا بین شبکه های ثابت و سیار
- پشتیبانی از انواع فناوری های مختلف
- قابل انطباق و سازگار با تمام نیازمندی های تنظیم مقررات نظم دهنده مثل ارتباطات اضطراری ، حریم شخصی، شنود قانونی وغیره.

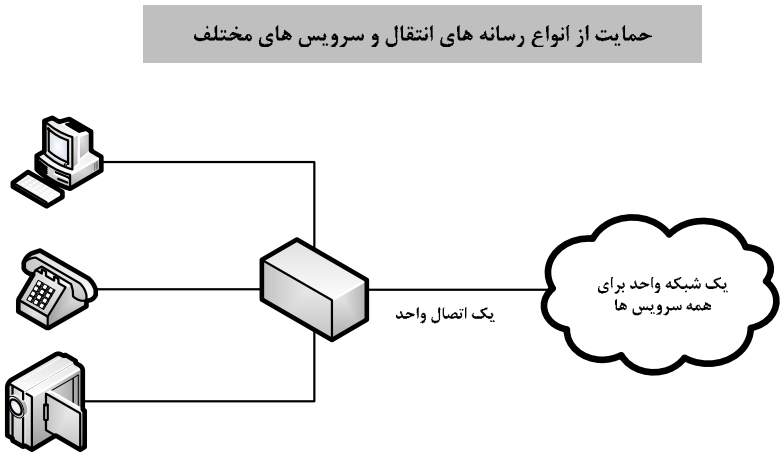
برخی از این ویژگی ها در شکل(۱۵-۲) نشان داده شده اند.

---

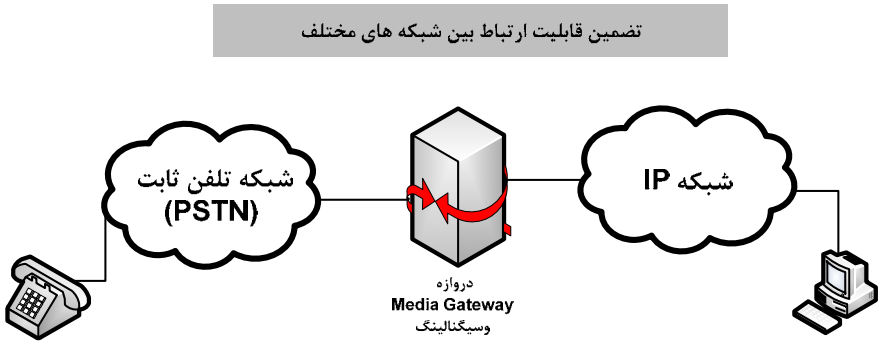
[1] European Telecommunications Standards Institute
[2] open interface
[3] International Telecommunication Union-Telecommunication
[4] multiple broadband
[5] Bearer capabilities
[6] application/service
[7] Application Program Interface
[8] Java APIs for Integrated Networks



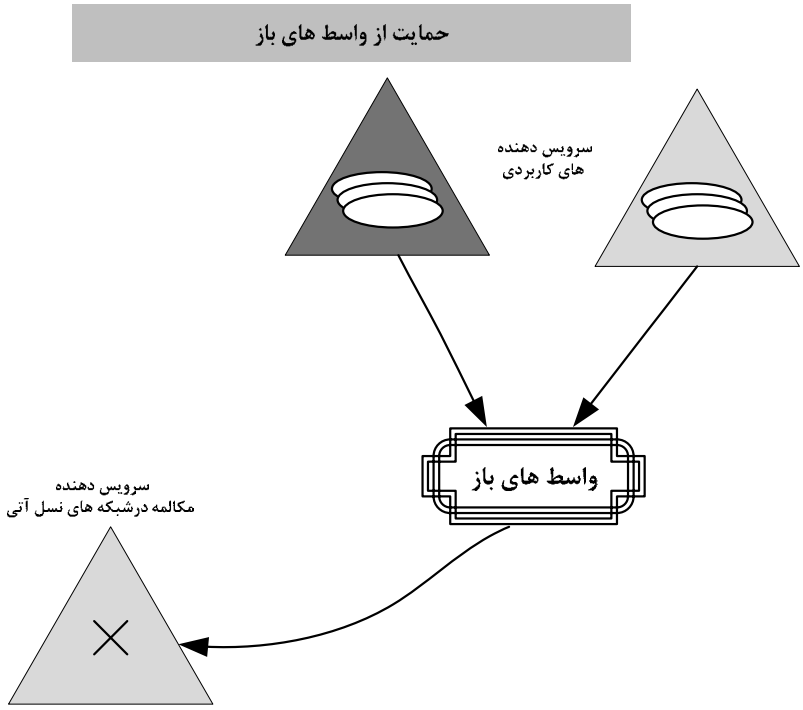
(الف) حمایت از انواع اتصالات



(ب) حمایت از سرویس های مختلف



(الف) حمایت از قابلیت ارتباط بین شبکه ای



(ج) حمایت از واسط های باز

شکل(۱۵-۲): برخی ویژگی های شبکه های نسل آتی

۱۵-۳- معماری کلی شبکه های نسل آتی

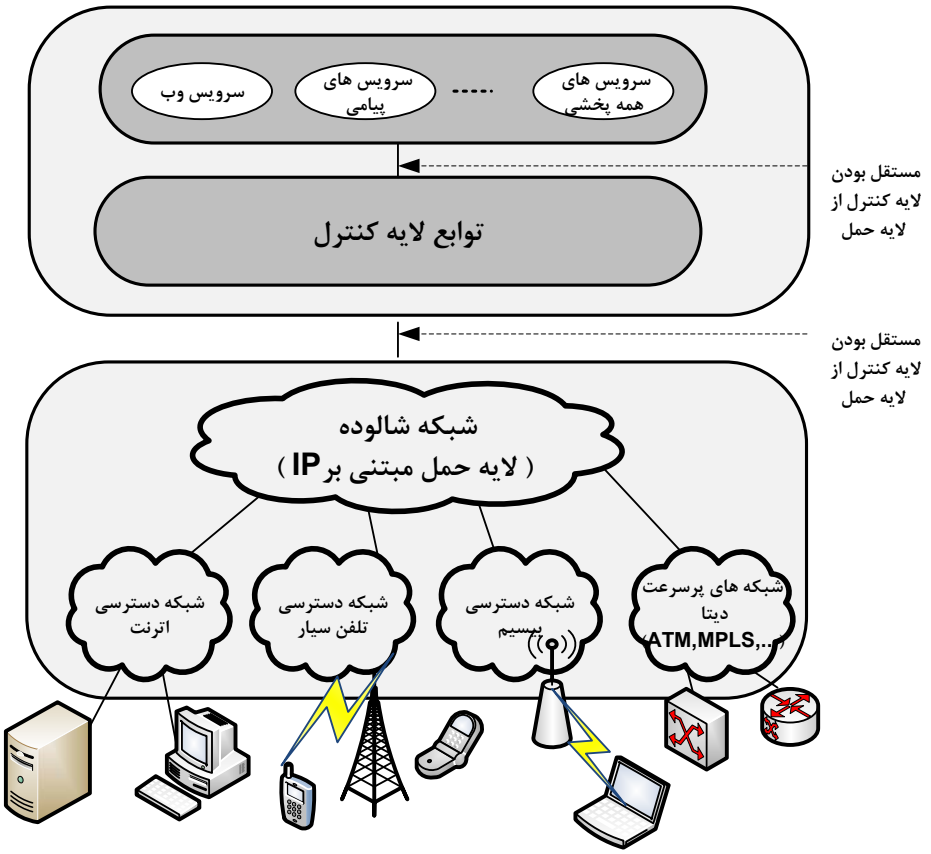
در معماری شبکه های نسل آتی، سعی بر آن است تا از در گیر شدن با فنآوری خاص ، معماری خاص و توپولوژی خاص پرهیز شود. بر این اساس یک معماری کلی لایه بندی شده در شبکه های نسل آتی وجود دارد که مطابق آن، چهار لایه ی دسترسی، حمل، مدیریت و سرویس های شبکه[1] وجود دارند. این لایه بندی ، در شکل(۱۵-۳) نشان داده شده است.

شکل(۱۵-۳): معماری لایه بندی شده شبکه های نسل آتی

[1] Access ، Transport ، Management ،Network sevices

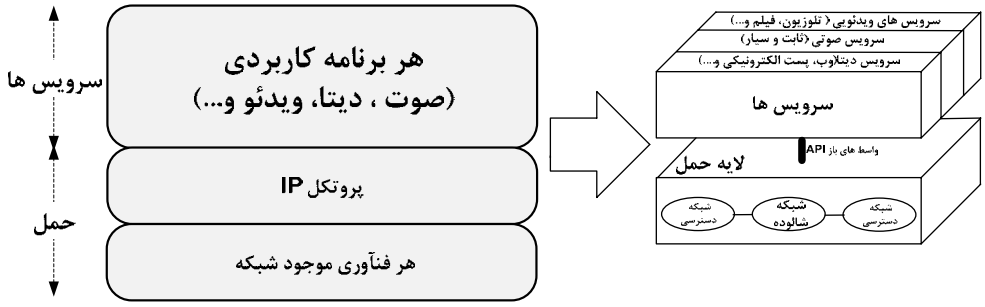
گرچه ظاهر این لایه بندی با معماری ارائه شده در زیر متفاوت است اما عناصر آنها کاملاً با هم مطابق هستند. بنابراین توضیحات بیشتر در قسمت بعد داده می شود.

یک دیدگاه دیگر در لایه بندی شبکه های نسل آتی، لایه بندی به صورت لایه حمل و لایه سرویس با یک زیرساخت ارتباطی یکسان است. در این لایه بندی عناصر ارتباطی و بسترهای انتقال در لایه حمل قرار می گیرند . برخلاف شبکه های ارتباطی گذشته، همه این بسترها با حفظ استقلال و سازگاری در کنار یکدیگر و در یک لایه قرار می گیرند. در لایه سرویس، سرویس های شبکه های ارتباطیِ قدیمی به همراه سرویس های آتی که درشبکه های نسل آتی به صورت منحصر به فرد به وجود آمده است، ارائه می شود. این معماری در شکل (۱۵-۴) نشان داده شده است.



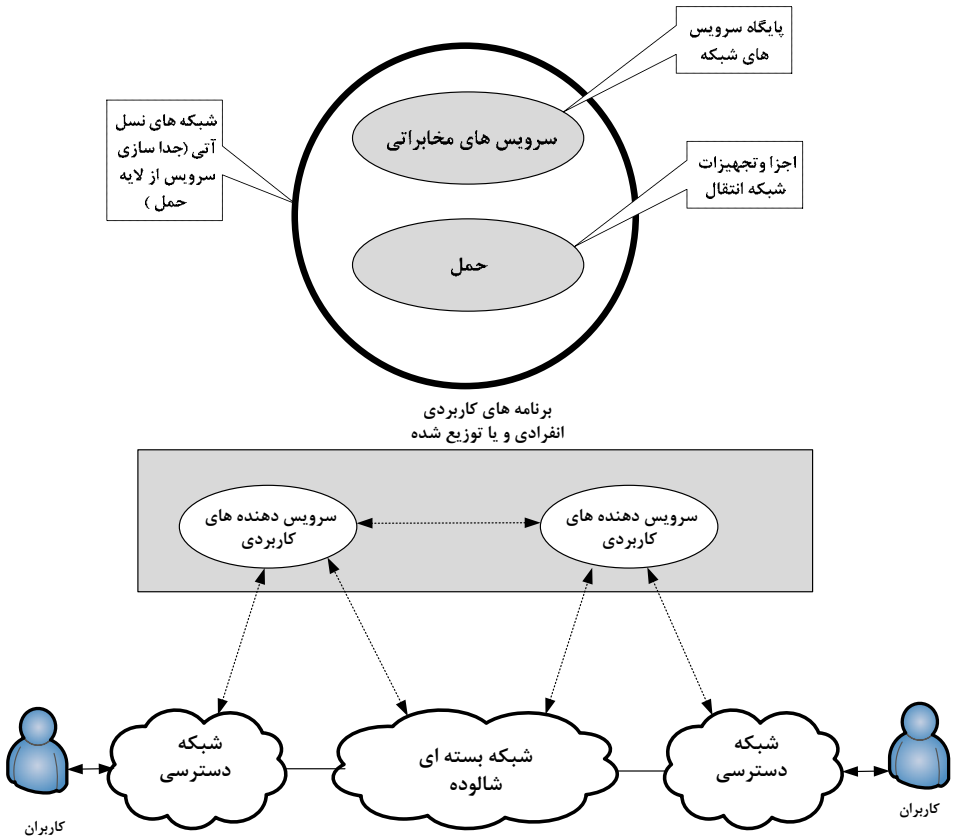
شکل(۱۵-۴): معماری ETSI منطبق با جداسازی لایه

دراین معماری پلات فرم اصلیِ اغلب سرویس ها ، پروتکل IP است . اکثر شبکه ها از انتقال بسته های IP پشتیبانی می کنند و IP نقش اساسی را در جدا سازی سرویس ها از شبکه حامل اعمال می کند. به عبارت دیگر : همه چیز بر روی IP و IP بر روی همه چیز. نمایش این ایده در شکل(۱۵-۵) نشان داده شده است.



شکل(۱۵-۵): معماری شبکه های نسل آتی طبق توصیه نامه Y.2011 منطبق بر اصل جداسازی لایه ها

در معماری شبکه های نسل آتی ،لایه سرویس از لایه حمل کاملاً مجزا است و ارتباط بین آنها از طریق API ها برقرار می شود . جزئیات این جداسازی در شکل (۱۵-۶) نشان داده شده است.



شکل (۱۵-۶): جدا سازی لایه سرویس و حمل با استفاده از پلات فرم ارتباطی

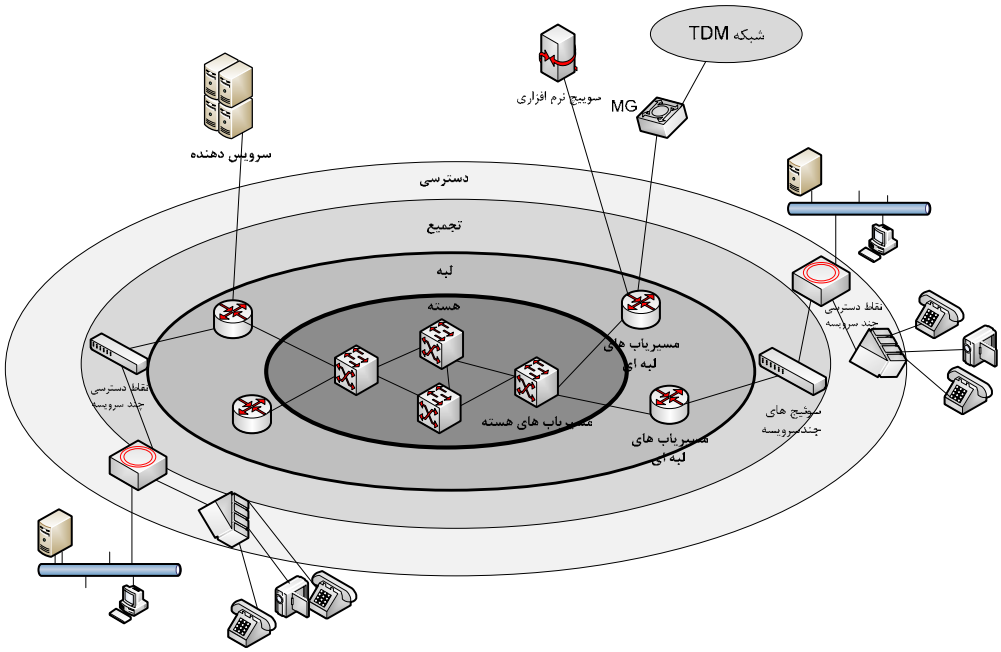
۱۵-۴- معماری لایه حمل از دیدگاه ITU-T

مطابق معماری ITU-T که منطبق بر اصل جداسازی لایه ها است ،لایه حمل شامل لایه(شبکه) هسته و لایه (شبکه) دسترسی[1] است . این معماری که در شکل(۱۵-۵) نشان داده شد به تفصیل در ذیل ارائه می شود.

۱۵-۴-۱- لایه هسته در شبکه های نسل آتی

لایه هسته شبکه های نسل آتی، یک شبکه همگرا و چند سرویسه مبتنی بر IP/MPLS[2] است که بر روی شبکه انتقال موجود قرارمی گیرد و از قابلیت اطمینان در سطح حامل ، امکان مهندسی ترافیک[3] ، کنترل و تضمین کیفیت سرویس ، گسترش پذیری ، ایمنی و مدیریت برخوردار است.

در شکل (۱۵-۷) جایگاه لایه هسته در پیاده سازی شبکه های نسل آتی نشان داده شده است . همان گونه که مشاهده می شود، لایه هسته مبتنی بر IP است و از عناصری چون مسیریاب های لبه ای و مسیریاب های هسته تشکیل شده است . نقطه مرکزی ارتباطات در شبکه های نسل آتی ، لایه هسته می باشد.



شکل(۱۵-۷): جایگاه لایه هسته در معماری شبکه های نسل آتی

۱۵-۴-۱-۱- سرویس های لایه هسته

لایه هسته درشبکه های نسل آتی باید سرویس های زیر را ارائه دهد:

- سرویسIP (بهترین تلاش)
- سرویس حمل صوت بر روی IP (VoIP[1])

[1] Core network , access network
[2] Multiprotocol label switching
[3] Teraffic Engineering (TE)

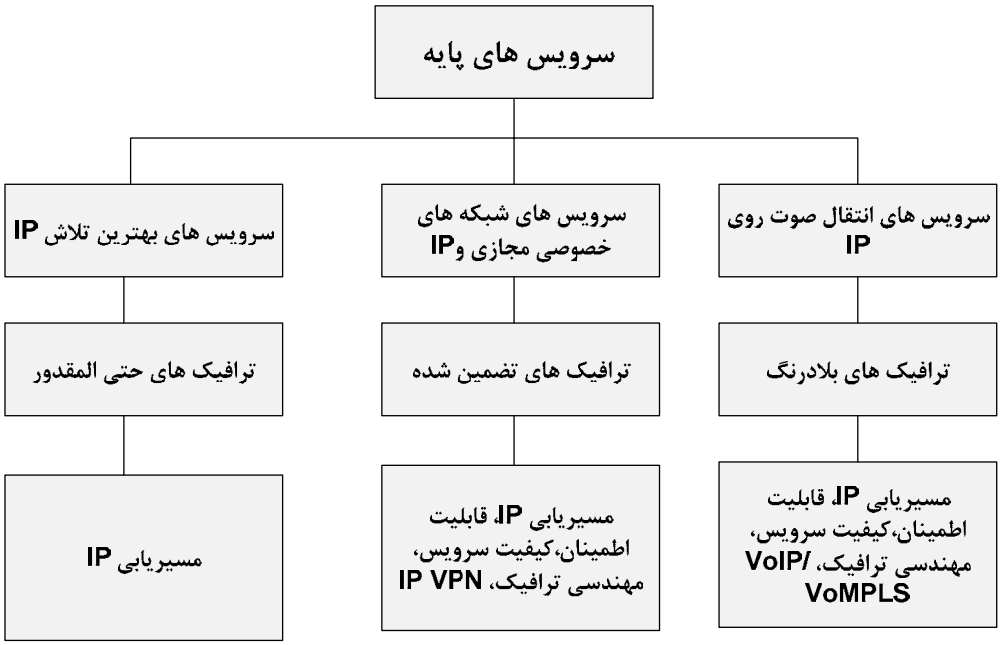
- سرویس های[2] VPN مبتنی بر IP شامل:
  - مبتنی بر MPLS لایه ۲و۳ (VPN MPLS)
  - سرویس شبکه محلی مجازی VPLS[3]
  - سرویس ارتباط امن مبتنی بر IPsec[4] و L2TP[5]
  - سرویس VPN ترکیبی
  - سرویس نمونه سازی مداری[6]
  - سرویس شبکه خصوصی مجازی صوتی[7] مبتنی بر IP
  - سرویس همه پخشی و چند پخشی IP
  - سرویس شبکه خصوصی مجازی با قابلیت چند پخشی

۱۵-۴-۱- ۲- تاثیر سرویس پایه در مشخصات فنی لایه هسته

ارائه سرویس پایه، مستلزم رعایت برخی نکات در مشخصات فنیِ لایه هسته است. شکل (۱۵-۸) این مشخصات و نیازمندی های آنها را نشان می دهد.

- ارائه سرویس IP بهترین تلاش، نیازمند کاهش ترافیک است و این نیز با پشتیبانی از مسیریابی IP فراهم می شود.
- ارائه سرویس های VPN وIP تضمین شده در لایه هسته به ترافیک ضمانت شده احتیاج دارند که خود مستلزم پشتیبانی از مسیریابی IP ، کیفیت سرویس، مهندسی ترافیک و IP VPN است.
- ارائه سرویس VoIP نیازمند ترافیک بلادرنگ است و ترافیک بلادرنگ نیز نیازمند پشتیبانی از مسیریابی IP ، قابلیت اطمینان، کیفیت سرویس ،مهندسی ترافیک و VoIP/VoMPLS[8] است.

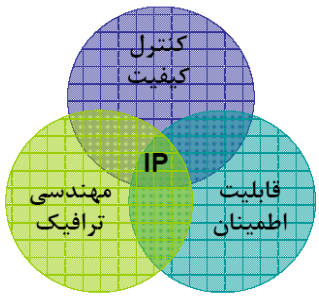
[1] Voice over IP
[2] Virtual Private Network
[3] Virtual private LAN service
[4] IP Security
[5] Layer 2 Transport Protocol
[6] Circuit Emulation
[7] voice VPN
[8] Voice over MPLS



شکل (۱۵-۸): تاثیر سرویس پایه در مشخصات فنی لایه ی هسته

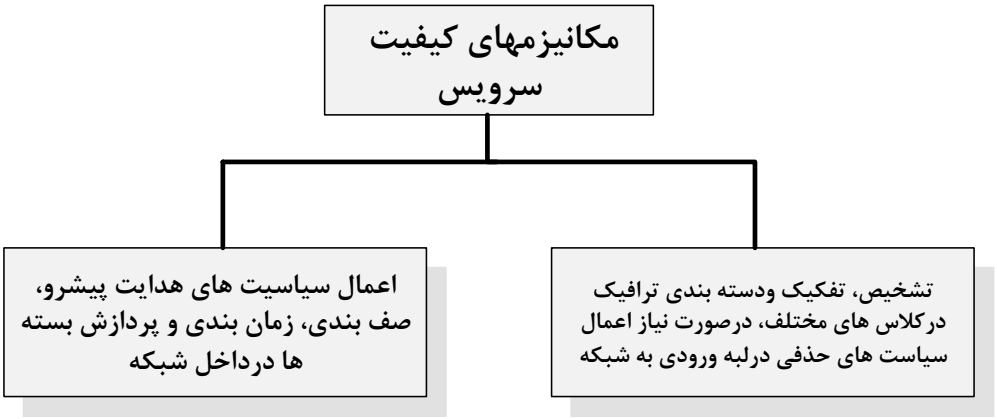
۱۵-۴-۱-۳- مشخصات فنی لایه هسته

سه مشخصه نشان داده شده در شکل (۱۵-۹) در راس مشخصات فنی لایه هسته شبکه های نسل آتی وجود دارد. این مشخصه به شرح زیر می باشند:



شکل(۱۵-۹): سه ویژگی مهم در هسته شبکه های نسل آتی

کیفیت سرویس در لایه هسته : تعریف عمومی کیفیت سرویس مطابق استاندارد E.800 ITU ،عبارت است از کارایی کلی سرویس به حدی که رضایت استفاده کننده را جلب نماید. موضوع کیفیت سرویس و حفظ آن در شبکه های IP که به عنوان بستر شبکه های نسل آتی به کار گرفته می شوند، ازاهمیت خاصی برخوردار است چرا که شبکه های IP در ذات خود فاقد مکانیزم های کنترل و حفظ کیفیت سرویس می باشند. بنابراین راه حل عمومی ، تجهیز این شبکه به مجموعه ای ازمکانیزم ها است که به حفظ پارامترهای کیفیت سرویس منطبق با نیازهای هر سرویس اقدام می کند. فلوچارت این مکانیزم ها درشکل(۱۵-۱۰) نشان داده شده است.



شکل (۱۵-۱۰): مکانیزم های کیفیت سرویس

برای ایجاد کیفیت سرویس در هسته شبکه های نسل آتی، تاکنون ازفن آوری هایی نظیر MPLS ، ATM ، Diff-serv [1]، RPR[2]، RSVP [3] استفاده شده است.

قابلیت اطمینان در لایه هسته: قابلیت اطمینان در لایه هسته شبکه های نسل آتی در حدی که مورد نظر یک حامل باشد، مستلزم دستیابی به نرخ دسترسی برابر با ۹۹۹,۹۹٪ است که به کمک تکنیک ها و روش های متعدد و بعضاً مکمل ارائه می گردد که در تمامی سطوح و لایه های شبکه به کار گرفته می شوند.

مهندسی ترافیک در لایه هسته: توانایی نگاشت موثر جریان های ترافیکی بر روی توپولوژی شبکه موجود، به منظور استفاده بهینه از منابع شبکه، مهندسی ترافیک نامیده می شود. همانطور ه درفصل قبل نیز اشاره گردید، مهندسی ترافیک دارای مزایای زیر است:

- افزایش کارایی شبکه
- کاهش ازدحام
- بکارگیری بهتر منابع و حداکثر بهره وری اقتصادی

یکی از روش های مهندسی ترافیک، مسیریابی مبتنی برقید می باشد که درآن مسیری که بهترین تطابق را با نیازمندی های ترافیکی کاربر دارد، تخصیص داده می شود.

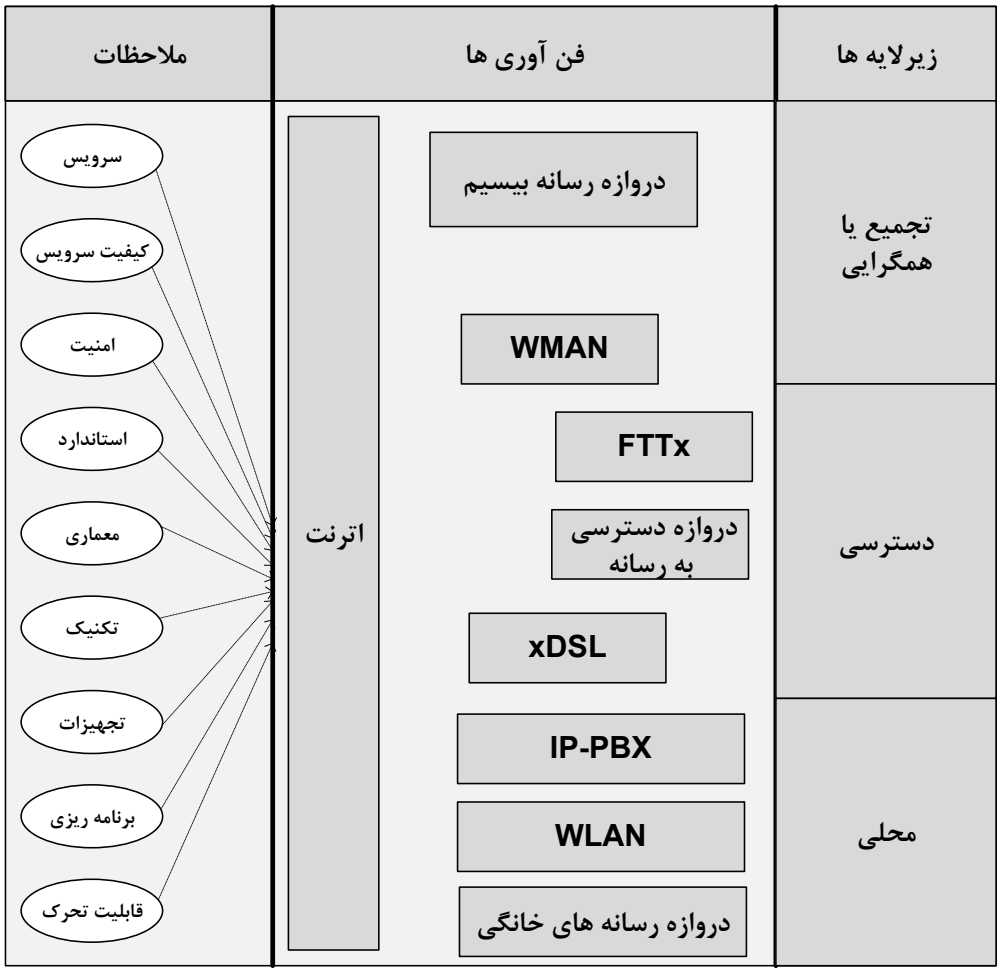
۱۵-۴-۲- لایه دسترسی در شبکه های نسل آتی

لایه دسترسی درشبکه های نسل آتی، شامل رسانه دسترسی و تجهیزات مورد نیاز جهت انتقال ترافیک مشترکین از محل آنها تا نقاط پایانی حلقه دسترسی[4](LX) می باشد. شبکه دسترسی در حقیقت نقطه اتصال کاربران در شبکه است و وسیع ترین و پر هزینه ترین بخش شبکه را در بر می گیرد. این بخش، امکان تبدیل فرمت داده (صوت، دورنگار یا داده) و تبدیل پروتکل های

[1] differentiated services
[2] Resilient Packet Ring
[3] Resource ReSerVation Protocol
[4] Local eXchang

لازم برای اتصال به شبکه را فراهم می آورد. این بخش در شبکه سوئیچ نرم افزاری، MG[1] نامیده می شود. بخش فوق شامل سه زیر لایه: تجمیع یا همگرایی[2] ، زیر لایه دسترسی[3] و زیر لایه محلی[4] است. این لایه بندی و ترتیب قرار گرفتن آنها در شکل(۱۵-۱۱) نشان داده شده است.

در زیر لایه تجمیع از فنآوری های[5] WMG , TMG و در زیر لایه دسترسی از فنآوری های[6] FTTX ،[7] AMG ،[8] WMAN ، xDSL و در زیر لایه ی محلی از فنآوری هایی نظیر[9] H/RMG ، [10]WLAN ،[11] IP-PBX و نیز در تمامی لایه دسترسی از فنآوری اترنت استفاده می شود.



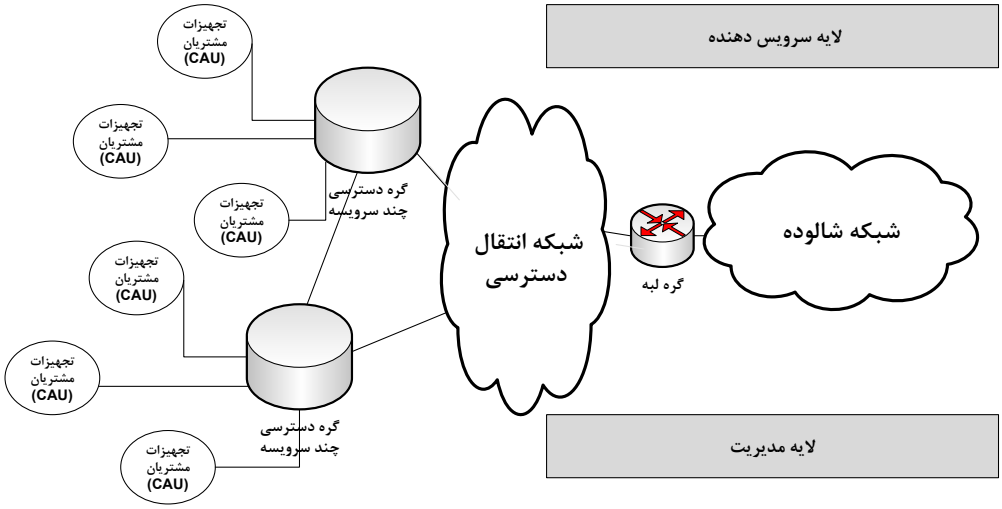
شکل (۱۵-۱۱): زیر لایه های شبکه دسترسی، فنآوری ها

[1] Media Gateway
[2] Aggregation or Cnovergence sub layer
[3] Access sub layer
[4] Local sub layer
[5] Wireless MediaGateway ,Trunking Media Gateway
[6] Commonly used term to reference both FTTH and FTTP (fiber-to-the premises)
[7] Access MediaGateway
[8] Wireless Metropolitan Area Network
[9] Home /Residential MediaGateway
[10] Wireless Local Area Network
[11] IP-Private Branch Exchange

در لایه دسترسی به مواردی نظیر سرویس ،کیفیت سرویس ، امنیت ، استاندارد ، معماری، تکنیک ، تجهیزات ، سازماندهی سلولی و تحرک پذیری[1] باید توجه داشت.

۱۵-۴-۲- ۱-گره ها و عناصر شبکه دسترسی در شبکه های نسل آتی

اجزاء اصلی شبکه دسترسی که در شکل (۱۵-۱۲) نشان داده شده را می توان به بخش های تجهیزات مشتریان([2] CAU) ، گره دسترسی چند سرویسه، شبکه اتصال و انتقال دسترسی ، گره لبه و لایه مدیریت دسترسی تقسیم کرد.



شکل (۱۵-۱۲): اجزا و گره های شبکه دسترسی

تجهیزات مشتری در محل استقرار مشترک خانگی یا تجاری قرار می گیرند و امکان دسترسی به انواع سرویس ها (داده ، صوت و ویدئو) را فراهم می کنند. این واحد، می تواند ترکیبی از واحد های فرعی مانند NT[3]، STB[4] و تجهیزات متصل به LAN باشد. این واحد همچنین می تواند وسیله ای باشد که توسط چندین کاربر به صورت اشتراکی مورد استفاده قرار گیرد (مثلاً یک هاب مستقر در زیرزمین یک مجتمع). به طور کلی می توان گفت که CAU نقطه پایان دهی شبکه عمومی است.

تجهیزات مشتریان به انواع ذیل تقسیم بندی می شوند:

- **کاربران خانگی** : در بخش کاربران خانگی ، وسایل الکترونیکی به واحد های دیجیتال تبدیل می شوندکه می توانند در داخل خانه به منظور پایش یا کنترل و یا سرویس امنیتی با هم ارتباط داشته باشند(برای مثال دوربین های دیجیتال با کامپیوترهای خانگی و STB ها به تبادل اطلاعات خواهند پرداخت). به همین ترتیب از اینترنت برای بازیابی اطلاعات استفاده خواهد شد (اطلاعات به داخل STB یا نمایشگرها دانلود می شود). از روش های مختلفی نظیر شبکه های مخابراتی و شبکه تلویزیون کابلی می توان برای دسترسی به خانه ها استفاده کرد.CAUها از طریق شبکه های خانگی باسیم یا بیسیم، دسترسی در داخل خانه و دسترسی عمومی را پشتیبانی می کنند. این تجهیزات همچنین

[1] Mobility
[2] Customer Access Unit
[3] Network Termination
[4] Set Top Box

Bluetooth و سایر روش های رادیویی محلی را پشتیبانی خواهند کرد. در ابتدا ترکیبی از DSL[1] و PSTN/ISDN[2] به عنوان واسط شبکه دسترسی استفاده می شود. بعدها DSL به تنهایی می تواند سرویس های مختلف را تامین کند. سرویس تلفنی یا به صورت in band (VoDSL[3]) و یا توسط پایانه های موبایل (به کمک hand over مناسب از شبکه موبایل به شبکه خانگی یا تجاری) در دسترس خواهد بود. در دراز مدت و هنگامی که قیمت پایان دهنده های شبکه کاهش یابد، دسترسی فیبر وارد میدان خواهد شد.

- **شرکت های کوچک و متوسط (SME[4])** : این شرکت ها به این نتیجه رسیده اند که ارائه سرویس هایی نظیر تجارت الکترونیکی و شبکه های خاص بین مراکز تجاری برای بقای آنها ضروری است. امروزه تقریبا تمام شرکت های کوچک و متوسط از ترکیبی از ISDN،PSTN استفاده می کنند، اما با استفاده روز افزون از سرویس های داده، این روش ها دیگر جوابگو نیستند. بنابراین اپراتورها سعی در جایگزینی PSTN و خطوط داده با خطوط پر سرعتی دارند که بتوانند سرویس های داده و صوت را پشتیبانی نمایند (VoDSL یا PBX با استفاده از VoIP یا VoTDM[5])
- **شرکت های بزرگ** : در شرکت های بزرگ ، CAU به وسیله ای تبدیل خواهد شد که بتواند تمام سرویس هایی(PBXها و اترنت و LAN و خطوط اجاره ای) را که برای انتقال در شبکه بر روی یک جریان ATM یا IP مالتی پلکس شده اند، پشتیبانی کند. به کمک رشد سریع شبکه های حلقوی SDH[6] برای کاربردهای تجاری و مناطق شهری، اغلب شرکت های بزرگ، دسترسی فیبر اختصاصی خواهند داشت. DSL می تواند تا زمان نیاز به پهنای باند بیشتر به عنوان روش دسترسی عمده به کار گرفته شود.

با توجه به مطالب فوق، CAU به وسیله ای تبدیل خواهد شد که بتواند تمام سرویس هایی که در حال حاضر به وسیله DSL،ISDN،PSTN و اترنت ارائه می شوند را پشتیبانی کند. از آنجایی که تقریبا تمام شرکت های کوچک و متوسط دارای اتصال سیم های مسی هستند ، DSL نخستین روش دسترسی خواهد بود.

گره دسترسی چند سرویسه

به عنوان بخشی از زیر ساخت دسترسی که واسط هایی را برای انواع مختلف CAU تامین می کند. این گره، ترافیک ورودی را مالتی پلکس یا متمرکز کرده و می تواند عملیات تبدیل را برای انواع مختلف ترافیک انجام دهد. درشبکه های نسل آتی، گره دسترسی به یک گره دسترسی چند سرویسه متحول خواهد شد که می تواند موارد زیر را پشتیبانی کند :

- راه حل های مقرون به صرفه و خود اتکا برای PSTN، ISDN، xDSL .
- راه حل های دسترسی مجتمع برای پوشش سرویس های باند پهن و باند باریک برای خانه ها و مراکز تجاری.

گره دسترسی که دسترسی CAU ها به شبکه را ممکن می سازد، می تواند در یک ساختار حلقه ای یا نقطه به نقطه قرار داشته باشد. واسط های کاربر انتهایی آن شامل DSL (متقارن، نامتقارن و بسیارپرسرعت) ISDN، PSTN و دسترسی مستقیم فیبر است. گره دسترسی، معماری های توزیع شده را نیز پشتیبانی می کند. به علاوه این گره می تواند برای دسترسی به مناطقی که توسط دسترسی ثابت پوشش داده نشده اند با سیم های LMDS[7] و سایر فناوری های رادیویی در یک محل قرارگیرد. این گره همچنین می تواند برای تامین زیر ساخت هایی مانند خطوط اجاره ای ، شبکه خصوصی مجازی VPN و

[1] Digital Subscriber Line
[2] Integrated Services Digital Network
[3] Voice over DSL
[4] Small and Medium Enterprises
[5] Voice over TDM
[6] Synchronous Digital Hierarchy
[7] Local Multipoint Distribution Service

سیستم مخابراتی موبایل جهانی[1] UMTS مورداستفاده قرار گیرد. همچنین گره دسترسی می تواند در محیط چند اپراتوری سرویس دهد به این معنی که اپراتورها می توانند سرویس های انتقال را به سایر اپراتورهای دسترسی ارائه دهند.
گره دسترسی می تواند به صورت داخلی قاب های[2] STM و ATM را مالتی پلکس و سوئیچ کند. در موقعیت های خاص مانند کاربردهای تجاری یا حلقه شهری ، می تواند ترافیک IP را نیز مسیریابی نماید. گره دسترسی برای ارتباط با مرکز سوئیچ محلی در PSTN یا شبکه لبه، می تواند قالب های مختلف صوت را به هم تبدیل نماید (مثلا از VoDSL به V5.2). با افزایش حجم ترافیک داده، بعضی از وظایف گره لبه احتمالا به گره دسترسی منتقل خواهد شد. شبکه اتصال و انتقال دسترسی، بخشی از زیر ساخت دسترسی است که امکان اتصال و دسترسی به سطوح بالاتر شبکه مخابراتی را به وجود می آورد.
از آنجاییکه فیبر نوری پهنای باند بیشتری را پشتیبانی می کند و قابلیت اطمینان و کیفیت سرویس بهتری ارائه می دهد، ازآن به صورت وسیعی برای انتقال به کار گرفته خواهد شد (به خصوص برای اتصال گره های دسترسی چند سرویسه به هسته شبکه).

۱۵-۵- اجزای شبکه های نسل آتی

اجزای کلیدی شبکه های نسل آتی عبارتند از:
توابع کنترلی نشست تماس(CSCF[3]) : CSCF، توابعِ PSTN ، نوع منطق تماس و توابع کنترلی تماس را فراهم می کند و همچنین با MGC و سوئیچ نرم افزاری و CS در ارتباط است .
Media Server : یکی از تجهیزات شبکه های نسل آتی است که برای تهیه اعلان ها و رمز نگاری صوت استفاده می شود. یک Media Server اثر متقابل با کانال حامل یا واسط تماس دارد.
OSS[4] : نمای شبکه، طرح شبکه، ساخت شبکه، مدیریت شبکه ، فعال سازی و تامین ذخیره سرویس در شبکه به عهده OSS است.
BSS[5] **:** نمای مشتری،[6] CCBS ، بازاریابی، فروش، مذاکره سرویس[7] و نظم بخشیدن به ثبت ورود به عهده BSS است.
مودم xDSL :کاربران انتهایی در صورت استفاده از سرویس IP پهن باند ، در محل خود مودم xDSL خواهند داشت.
DSLAM و دروازه دسترسی: در کنار نقاط پایانی حلقه دسترسی و در محل MDF[8] قرار می گیرند. این تجهیزات نقش رابط بین دو شبکه دسترسی و تجمیع را به عهده دارند.
سرویس دهنده دسترسی پهن باند(BRAS[9]) : عملیات مربوط به احراز هویت، اعتبار سنجی ، حسابرسی(AAA[10]) ترافیک IP کاربران را انجام داده و آنها را از یک یا چند DSLAM جمع آوری می کند. BRAS می تواند در محل DSLAM یا در مکان دیگری (راه دور) قرارگیرد.
MG/MGW یا GW[11]: نام عمومی واحدی است که عمل ترجمه بین شبکه هایی با استانداردهای مختلف را بر عهده دارد. MG ها بسته به محل استفاده در شبکه اسامی مختلفی دارند. MG یک وسیله برای تبادل کد بین کانالهای حامل

[1] Universal Mobile Telecommunication System
[2] Synchronous Transport Module
[3] Call Session Control Function
[4] Operations support system
[5] Basic Service Set
[6] Completion of Calls to Busy Subscriber
[7] service negotiation
[8] Main Distribution Frame
[9] Broadband Access Server
[10] Authentication , Authorization ,Accounting
[11] GateWay

PSTN(TDM)[1] کدشده G.711 و VoIP و کانال حامل کدشده G.7xx است که در شبکه های نسل آتی استفاده می شود. خاتمه تماس صوت در بدنه سوئیچ داخلیPSTN ، فشرده سازی و بسته بندی داده صوت و تحویل بسته های صوتی فشرده شده به شبکه IP توسط MG انجام می شود. MG برای یک شروع کننده تماس صوتی در شبکه IP ، این توابع را به صورت معکوس اجرا می کند. یک MG ، محیط فراهم شده توسط یک نوع از شبکه را به فرمتی که شبکه ای از نوع دیگر نیاز دارد تبدیل می کند. با توجه به این خصوصیت تبدیل فرمت رسانه های مختلف مانند صوت و ویدئو را انجام داده و انتقال اطلاعات بین شبکه های مختلف را مدیریت می کند.

MGC: کنترلری است که بخشی از مراحل تماس را که متعلق به کنترل ارتباط برای کانال های انتقال در داخل یک MG است را کنترل می کند.MGC ثبت و مدیریت منابع را در MG و تبادل پیام بین[2] ISUP و سوئیچ های اداره مرکزی را از طریق یک [3] SG انجام می دهد.MGC بعضی وقت ها سوئیچ نرم افزاری نامیده می شود. ارتباط سیگنالینگ MGC با شبکه هایی مثل PSTN و[4]PLMN به صورت مستقیم و با PBX ها از طریق RMG،AMG است.

سرویس دهنده کاربردی ([5] AS): واحدی است که پشتیبانی اجرای سرویس و غیره را برای سرویس دهنده های تماس و کنترل و منابع خاص شبکه های نسل آتی (سرویس دهنده رسانه و سرویس دهنده پیام) به عهده دارد.

سوئیچ نرم افزاری: سوییچ نرم افزاری فناوریی است که امکان ارایه سرویس مکالمه، سرویس باند وسیع و حتی سرویس بیسیم را بر روی بستر شبکه IP فراهم می کند. با گسترش شبکه های IP، هزینه ارتباطات داده مبتنی بر شبکه‌های IP بسیار کاهش یافته است. این مساله و همچنین مساله همگرایی شبکه های داده و شبکه های تلفنی ، نگاه‌ها را به سمت امکان ارایه سرویس مکالمه مبتنی برشبکه IP معطوف داشته است. سوئیچ نرم افزاری ابتدا در مخابرات راه دور و بین الملل مطرح شد زیرا مقایسه هزینه بالای این نوع مکالمه با روش‌های قبلی، امکان ورود راه حل‌های آتی را فراهم می آورد. استفاده از فناوریVoIP هزینه مکالمات بین المللی را ده‌ها برابر کاهش داده است. فناوری VoIP در طول تکوین خود، راه حل‌های مختلفی را آزموده است و فناوری سوییچ نرم افزاری الگوی کاملی از یک سامانه کامل VoIP است که تمامی سرویس موجود در شبکه های تلفنی موجود (سوییچ مداری) را فراهم می آورد و امکان ایجاد یک شبکه تلفنی کامل را بر مبنای VoIP فراهم می‌کند. فناوری سوییچ نرم افزاری بعنوان یک جایگزین برای سوئیچ‌های TDM کلاس۵,۴ مطرح است و امکان کنترل مکالمه و ارائه سرویس را بر روی شبکه IP فراهم می آورد. سوئیچ نرم افزاری، امکان کنترل مکالمه را چه بصورت نقطه به نقطه و از طریق پروتکل هایی مثل SIP و H.323 و یا از طریق MG فراهم می آورد. بخش سوئیچینگ معمولاعناصر MGCP[6] ، SG ، سرویس دهنده رسانه (MS[7]) و سرویس دهنده کاربرد (AS) را در برمی گیرد.

سوئیچ نرم افزاری بر روی نرم افزار کاری تماسCall Agent یا MGC نوشته می شود. سوئیچ نرم افزاری، کنترل تحویل سرویس در داخل شبکه را به عهده دارد. همچنین مسئول کنترل تماس و کنترل دستی MG از طریق پروتکل H.248 است. در حقیقت بخش اصلی سامانه است که کنترل مکالمه و سرویس را انجام می دهد.

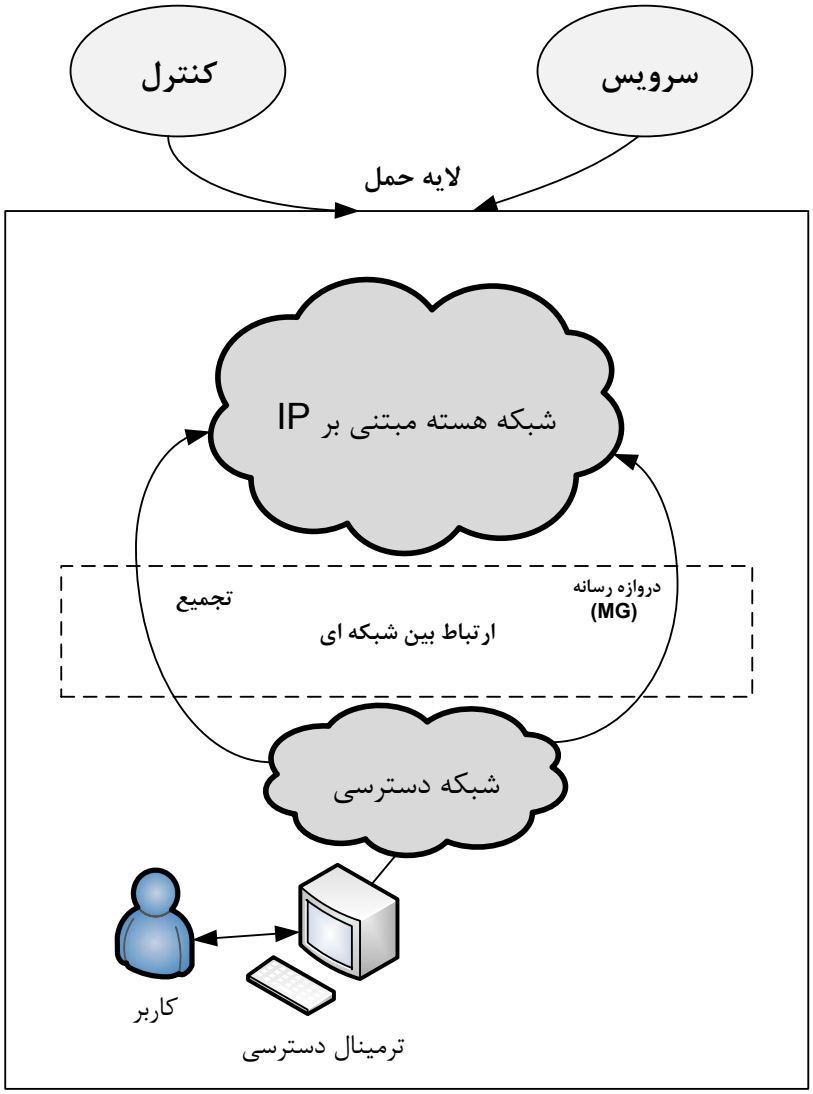
[1] Time division multiplexing
[2] ISDN User Part
[3] Signaling Gateway
[4] Public Land Mobile Network
[5] Application Server
[6] Media Gateway Control Protocol
[7] Media Server

۱۵-۵-۱- دامنه های مختلف در لایه حمل

دسترسی در لایه حمل با دامنه های مختلفی تعریف شده است که عبارتند از: سطح ملی ، سطح استانی و سطح خصوصی . دامنه ملی در هسته IP و دامنه استانی در شبکه تجمیع و در نقاط دسترسی به شبکه و دامنه خصوصی برای فراهم کنندگان سرویس تهیه شده است.

۱۵-۵-۲- ارتباط بین شبکه ای در لایه حمل

مطابق با شکل(۱۵-۱۳)، ارتباط بین شبکه ای در شبکه های نسل آتی به معنی برقراری ارتباط با شبکه های موجود(PSTN ،GSM[1]) از طریق SG و MG ها با شبکه هسته IP مبتنی بر بسته می باشد.



شکل(۱۵-۱۳): دامنه های مختلف در لایه حمل

[1] Global System for Mobile communication

از آنجایی که همگرایی در شبکه های نسل آتی و بهره گیری از شبکه های موجود از اهداف بسیار مهم و حیاتی شبکه های نسل آتی می باشد، تضمین ارتباط بین شبکه ای بحث مهم و کلیدی است. در ارتباط بین شبکه ای برای ارتباط با انواع مختلف شبکه ها از MG متناسب با آن شبکه استفاده می شود به همین دلیل MG های متنوعی تعریف شده است که در زیر معرفی می شوند:

- **WMG** : واسط کاربر بین شبکه PLMN و شبکه هسته IP مبتنی بر بسته.
- **TMG**: واسط کاربر شبکه PSTN و شبکه هسته IP مبتنی بر بسته. TMG اجازه ارتباط بین شبکه ای بین شبکه تلفنی TDM کلاسیک و شبکه های نسل آتی مبتنی بر بسته را می دهد. برای محیط دفتر مرکزی طراحی شده است. چنین GW هایی معمولا تعداد زیادی از مدارات مجازی دیجیتال و مدارات حامل TDM با سیگنالینگ حمل شده بر روی یک مسیر جداگانه (از طریق یک SG[1]) را مدیریت می کنند. تبدیل جریان 64kbps مدار یا خط ارتباطی[2] TDM به بسته های دیتا و معکوس آن نیز توسط TMG انجام می شود.
- **AMG**: واسط شبکه تلفنی و R/HMG[3] با شبکه هسته IP مبتنی بر بسته است. AMG ها امکان تبدیل ترافیک جریان دسترسی آنالوگ POTS[4] یا وسایل دسترسی 2Mb/s را به بسته فراهم می کنند. همچنین امکان دسترسی مشترک به سرویس ها و شبکه های نسل آتی را به وجود می آورد. AMG به صورت واسط بین سیگنالینگ و مدیای مبتنی بر IP در شبکه های نسل آتی و مدارات دسترسی کاربران انتهایی در شبکه موجود PSTN(TDM) عمل می کند و واسط های شبکه کاربر(مانند ISDN یا سرویس های آنالوگ سنتی) را به یک شبکه VoIP یا VoTDM متصل می کند. این وسیله معمولاً سیگنالینگ برخوانی TDM را پایان دهی کرده و این اطلاعات را برای تصمیم گیری های کنترل برخوانی به یک MGC یا سوئیچ نرم افزاری تحویل می دهد.

RMG : یک RMG واسط LAN وPBX با شبکه هسته IP مبتنی بر بسته است که در یک دفتر کوچک یا دفتر خانگی قرار می گیرد و ممکن است چند درگاه صوتی آنالوگ و درگاه اترنت داشته باشد. واسط سمت شبکه، معمولا xDSL است . به کمک LAN چندین کامپیوتر می توانند به طور همزمان به اینترنت دسترسی داشته باشند ویایک VPN تشکیل دهند. این واحد ارتباط میان شبکه ای بین صوت سوئیچ مداری و VoATM یا VoIP را در طرف شبکه برقرار می کند.

- **SG** : یک SG ، ارتباط بین شبکه ای شفافی از سیگنالینگ بین سوئیچ مداری و شبکه IP فراهم می کند. SG خاتمه دهنده سیگنالینگ است و نیزمبدل سیگنالینگ بین شبکه های نسل آتی و دیگر شبکه ها مثل STP[5] وSS7 ، با استفاده از پروتکل های سیگنالینگ مبتنی برIP است. به خاطر قوانین حساس در شبکه های صوتی یکپارچه، اغلب SG ها برای اطمینان از دسترسی بالا در گروه های دو یا بیشتر گسترش یافته اند.
- **NAS** : یک شکل خاص از AGW[6] است که برای پایان دهی برخوانی های مودم یا اتصالات HDLC[7] طراحی شده و دسترسی به شبکه IP را فراهم می کند.

---

[1] Signaling GateWay
[2] TDM circuit/trunk
[3] Residential/ Home Media Gateway
[4] Plain Old Telephon Service
[5] Signalling Transfer Point
[6] Access GateWay
[7] High Level Data Link Control

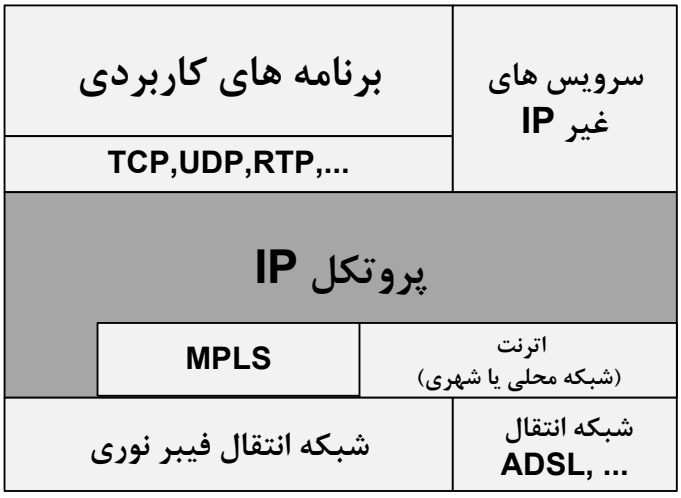
۱۵-۶- معماری پروتکل ها و معماری تابعی در شبکه های نسل آتی

در این بخش، به بررسی معماری پروتکل ها در شبکه های نسل آتی می پردازیم. معماری پروتکل ها با توجه به ویژگی شبکه های نسل آتی که در آن سازگاری کامل بین قسمت های مختلف برقراراست، ارائه می شود. در رابطه با پروتکل های به کار رفته در ساختار شبکه های نسل آتی نیز لیستی از پروتکل های کلیدی با توجه به استانداردهای اصلی درشبکه های نسل آتی ارائه می شود. همچنین معماری دیگری تحت عنوان معماری تابعی در شبکه های نسل آتی توصیف می شود. واحدهای این معماری از توابع تشکیل شده اند و این توابع نقش بسیار مهمی در ساختار شبکه های نسل آتی دارند که به بیان این توابع، تعریف و کاربرد آنها در شبکه های نسل آتی می پردازیم .

۱۵-۶-۱- معماری پروتکل ها در شبکه های نسل آتی

در معماری های قبلی پروتکل ها، نحوه روی هم قرار گرفتن پروتکل ها مهم بود، چون تنها گروه های خاصی از آنها با یکدیگر سازگار بودند، بنابراین آگاهی از پروتکل های لایه های بالایی و پایینی از اهمیت زیادی برخوردار بود. در شبکه های نسل آتی نحوه خاصی برای زنجیره پروتکل تجویز نشده است . به عبارت دیگر هر لایه X بر روی هر لایه Y قرار می گیرد.

در این معماری، IP نقش کلیدی را بازی می کند به طوری که، در بین لایه های موجود حضور IP اجباری است. IP همگرایی بین لایه های مختلف را تضمین می کند و به عنوان یک پروتکل ابتدایی و فراگیر مطرح است. یک مدل ساده شده از معماری پروتکل ها در شکل (۱۵-۱۴) نشان داده شده است. معماری نمایش داده شده، گرچه کامل نیست و ترکیب های دیگری نیز از آن ممکن است، اما گرایش معماری بر مبنای همگراییِ مبتنی برIP می باشد.



شکل (۱۵-۱۴): معماری پروتکل ساده شده شبکه های نسل آتی

شبکه های نسل آتی نیازمند پروتکل هایی برای پشتیبانی از موارد زیر می باشد:

- انواع سرویس ها به صورت یکپارچه
- سرویس های آتی
- مهاجرت کامل به سمت شبکه های نسل آتی

- قابلیت اطمینان
- توسعه پذیری و غیره

در شبکه های نسل آتی، نهادهای استاندارد گذاری مثل IETF، ITU-T ، ETSI[1] واسط ها و پروتکل ها را تعریف می کنند.

۱۵-۶-۱-۱- پروتکل های IETF

پروتکل های ارائه شده توسط IETF درارتباط با شبکه های نسل آتی به شرح زیر می باشند:

- SIP پروتکلی است که نحوه آغاز مکالمه ، تغییرات احتمالی شرایط مکالمه و پایان مکالمه را معین می کند. این مکالمه می تواند یک ارتباط دو طرفه، چند طرفه و چند رسانه ای باشد. برخی دیگرازپروتکلها که حسن عملکرد ارتباطات مبتنی بر SIP را تضمین می کنند عبارتند از:
- RSVP: برای رزرو منابع شبکه
- RTP: برای انتقال بهنگام اطلاعات و ارائه بازخورد از وضعیت کیفیت سرویس
- RTSP[2]: برای کنترل تحویل صحیح و بهنگام صوت و تصویر
- SAP[3]: برای ارسال پیامهای چند رسانه ای چندپخشی
- SDP [4]: برای توصیف ارتباطات چند رسانه ای
- MIME[5]: استاندارد غیر رسمی برای توصیف محتوا در اینترنت
- HTTP [6] : پروتکل استاندارد برای ارسال صفحات وب
- COPS [7] : برای پشتیبانی از سیاست ها

۱۵-۶-۱-۲- پروتکل های ITU-T

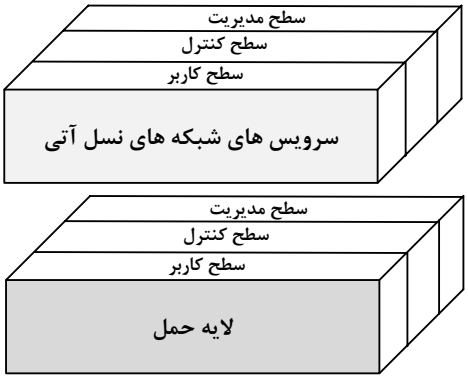
پروتکل های ارائه شده توسط ITU-T درارتباط با شبکه های نسل آتی به شرح زیر می باشند:

- H.323: استانداردیست که پروتکل ها، اجزا و روشهای لازم برای ساماندهی سرویس های چند رسانه ای بهنگام از قبیل صوت و تصویر بر روی شبکه های بسته ای از قبیل شبکه های IP را ارائه می دهد. این پروتکل بخشی از پروتکلهای خانواده H.32x و سرویسهای چند رسانه ای را روی شبکه گسترده ای از سرویسها پشتیبانی می نماید.

۱۵-۶-۲- معماری تابعی ITU-T

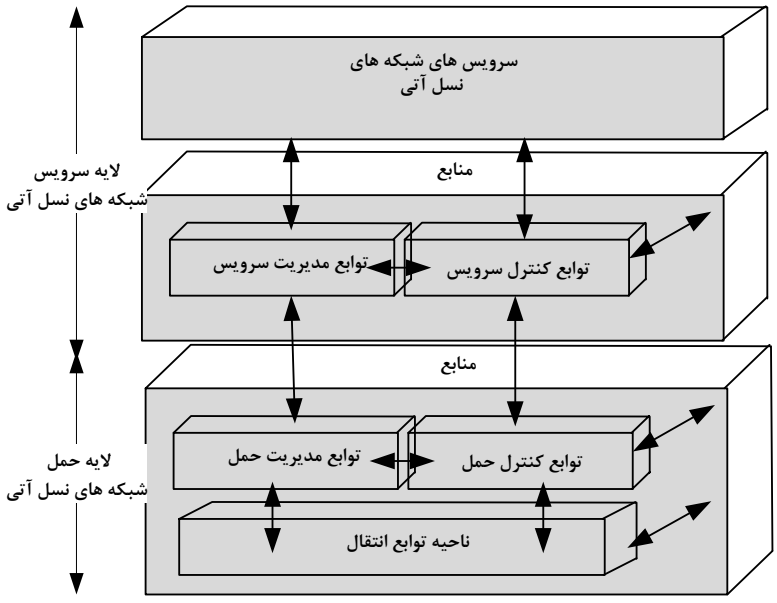
همان گونه که قبلاً نیز اشاره شد، در راستای ویژگی مهم شبکه های نسل آتی، معماری پیشنهادی ITU-T ، دو لایه کاملاً مجزا از هم است که در آن لایه سرویس از لایه حمل جدا می شود و هر لایه خود دارای سه سطح کاربر، کنترل و مدیریت است. این معماری پایه، در شکل (۱۵-۱۵) نشان داده شده است.

[1] European Telecommunications Standards Institute
[2] Real Time Stream Protocol
[3] Service Advertising Protocol
[4] Service delivery platform
[5] Community Oriented Policing Services
[6] HyperText Transfer Protocol
[7] Community Oriented Policing Services



شکل(۱۵-۱۵): معماری تابعی پایه

در لایه حمل، توابع کنترل و مدیریت انتقال به صورت افقی و ناحیه توابع ارسال به صورت عمودی از طریق واسط ها با یکدیگر در ارتباط اند. هر کدام از سطوح توابع کنترل و ارسال به صورت جداگانه با منابع شبکه اتصال دارند. مطابق شکل (۱۵-۱۶)، در لایه سرویس شبکه های نسل آتی نیز توابع کنترل و مدیریت سرویس به صورت افقی با یکدیگر و با سرویس ها (کاربردها، سرویس های میان افزار وBaseware) به صورت عمودی مرتبط می شوند. در ارتباط بین لایه سرویس و حمل، توابع مدیریتی دو لایه با هم و توابع کنترلی نیز با هم ارتباط دارند. توابع کنترل سرویس نیز با هم در ارتباط اند. توابع کنترل سرویس نیز با منابع شبکه اتصال دارند.



شکل (۱۵-۱۶): ملاحظات معماری تابعی پایه Recommendation Y.2011

۱۵-۶-۲-۱- توابع پایه در معماری ITU-T

لایه سرویس شامل توابع کاربرد، سرویس، کنترل و دیتا بیس مشتری است و لایه انتقال شامل توابع ورود به شبکه، توابع لایه دسترسیِ لایه حمل، توابع هسته لایه حمل، توابع GW ، توابع اداره رسانه و توابع سازگار در لایه حمل است. برخی از این توابع برای کنترل و برخی دیگر به عنوان واسط عمل می کنند. به عبارت دیگر ارتباط برخی کنترلی و برخی واسطه ای است. توابع ورود به شبکه، توابع دسترسیِ لایه حمل ، هسته لایه حمل، GW و اداره واسط ها و توابع مشتری از نوع واسط هستند. سایر توابع اعم از توابع کاربرد ، کنترل ، سرویس، دیتا بیس مشتری و سازگاری لایه حمل، توابع کنترلی می باشند. توابع شارژ و صورت حساب و توابع مدیریت در هر دو لایه سرویس و انتقال به کاربرده می شوند.

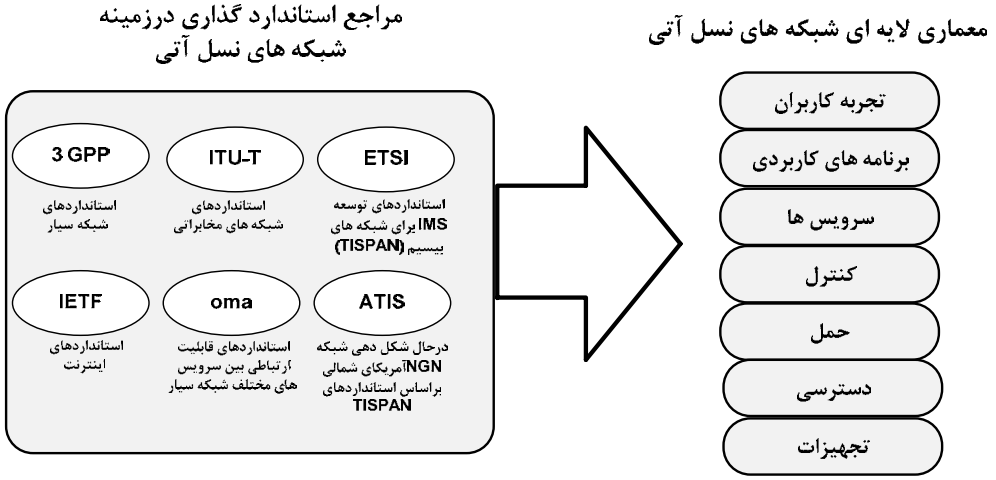
۱۵-۷- معماری داده و معماری کاربردها درشبکه های نسل آتی

در این بخش به معماری داده در شبکه های نسل آتی پرداخته و ساختار آن، لایه بندی و جریان داده در شبکه های نسل آتی را بررسی می کنیم. معماری داده در شبکه های نسل آتی با توجه به جریان داده در بین لایه ها در شبکه های نسل آتی توصیف می شود.

۱۵-۷-۱ شبکه های نسل آتی و لایه بندی معماری داده

شبکه های نسل آتی، لایه بندی توابع را در معماری به سطح کنترل کاربر[1] می آورد. در نتیجه معماری داده، باز می شود. این تغییر معماری به کنترل در فاز اجرای سرویس و فاز مدیریت سرویس نیاز دارد. با توجه به این تغییر، پیاده سازی استانداردها و واسط های مدیریت نیز قابل توجیه است.

استانداردها و عملگرهای پیاده سازی شده، با مفهوم معماری لایه بندی در شبکه های نسل آتی سازگارند. نهادهای استاندارد گذاری مثل ITU-T, 3GPP 3GPP2[2]،... در حال همگرایی به یک طرح عمومی شبکه های نسل آتی و لایه بندی با یک راه انداز قوی هستند. همچنین تعداد زیادی از اپراتورهای مخابراتی در حال راه اندازی یا ارزیابی شبکه لایه بندی شده شبکه های نسل آتی هستند. معماری داده شبکه های نسل آتی با توجه به بدنه استانداردها به صورت شکل (۱۵-۱۷) است.



شکل(۱۵-۱۷): معماری داده در شبکه های نسل آتی

[1] User Control Plane
[2] 3rd Generation Partnership Project

مفهوم لایه بندی مبتنی بر کارایی(درامد) و بهینه سازی (هزینه راه اندزی)، به اشتراک گذاشتن زیر بنای ساختار عمومی سرویس برای باز کردن محیط کاربردی و نیز ادغام منابع است و امکان سرمایه گذاری بهینه و افزایش کارایی را فراهم می کند. در شبکه های نسل آتی، سطوح کنترلی از افقی به عمودی تبدیل می شوند و در نتیجه پیام ها بیشتر و پیچیده تر می گردند. نتیجه لایه بندی درمعماری داده ، توزیع داده در بین لایه هاست. جریان داده درون همان لایه متمرکز می شود و اثر متقابل داده از درون نودهای لایه متناظر در اجرای سرویس، کنترل می شود.

۱۵-۷-۲- پیاده سازی معماری داده

در طراحی معماری داده لایه بندی شده، باید به نیازمندی های سرویس، در فاز اجرا و مدیریت رسیدگی شود. در فاز مدیریت سرویس[1] تمرکز بر عملکرد و تقاضای کاربر نهایی است. در فاز اجرای سرویس[2] تمرکز بر آزمایش اجرای داده و تقاضای پایانی برای رسیدگی به تجربه کاربر نهایی است.

مدیریت سرویس در معماری داده: باید ویژگی های[3] ACID معماری داده و دسترسی on line از منظر سرویس را تامین کند.

اجرای سرویس در معماری داده : اجرای معماری داده مبتنی بر روند اجرای سرویس و ترکیب/ادغامِ مورد نیاز سرویس های مختلف، پروفایل ها و مجتمع سازی آنها در همه جا است. اجرای سرویس به تجهیزات درلایه های مختلف نیاز دارد. این تجهیزات عبارتند از AAA و[4]HSS ودیتا بیس کاربر. هرکدام از این تجهیزات به پروفایل های Gold ، Silver ، Bronze مشتری های تجاری و ... دسترسی دارند.

۱۵-۸- امنیت در شبکه های نسل آتی

امنیت، یک کاراکتر مهم در همه سرویس ها است و برای حفظ منافع کاربران و فراهم کنندگان سرویس ها ضروری است. از آنجا که مباحث امنیتی، مباحثی کاملا مهم و حیاتی در هر شبکه ای است، نیاز به تعریف این ویژگی در ساختار شبکه های نسل آتی کاملاً محسوس و اجباری است. بنابراین دراین بخش به بیان ساختارهای امنیتی لایه بندی شده در شبکه های نسل آتی می پردازیم. در این بخش ابتدا ضرورت پیاده سازی امنیت در شبکه های نسل آتی مورد بررسی قرار می گیرد و سپس به تعریف امنیت در ساختار شبکه های نسل آتی پرداخته و لایه های امنیتی و همچنین سطوح امنیتی در شبکه های نسل آتی را مورد مطالعه قرار می دهیم.

امنیت، یک کاراکتر مهم در همه سرویس ها است و برای منافع فراهم کنندگان سرویس ها ضروری است. اولین چالشی که فراهم کنندگان سرویس ها با آن مواجه هستند ، اطمینان از کارایی پیش بینی پذیری سرویس در یک ترافیک بد است که از نقاط پایانی چندگانه توزیع شده در مرزهای شبکه سرچشمه می گیرد. امروزه این نوع رفتارها، با رفتارهایی مثل حمله های[5] DDoSوکرم های توربو وspam های نامه های الکترونیکی وphishing و ویروس ها شناسایی شده اند. بخشی از ترافیک تولید شده به خاطر اثرات و وقایع بعدی است که می توانند عملیات عادی شبکه را قطع کنند و ریسک را برای پشتیبانی از

[1] service Management
[2] service Execution
[3] Atomicity, Consistency, Isolation, and Durability
[4] Home Subscriber Server
[5] Distributed Denial of Service

وسایلی که مسئول مسیریابی پایه و سوئیچینگ بسته ها هستند بالا می برد. برای اطمینان از کارایی بالای امنیت شبکه، باید از وضعیت سنتی به یک وضعیت توسعه به منظورکاهش اثرات حمله ها حرکت نمود. گر چه به صورت مختصر می توان گفت، منابع مورد نیاز در این زمینه، تخصص ها و سیستم های امنیتی به هم وابسته که دیدگاه های فراگیر از شبکه های کامل ارایه می دهند، هستند، اما نباید از بهبود عملکردهای امنیتی نیز غافل شد. به دلیل دسترسی آسان وافزایش ابزارهای حمله پیچیده و روند فزاینده محرک های بد و متنوع ، امروزه دراینترنت ترافیک بد شایع شده است. بنابراین فراهم کنندگان سرویس ها باید به دنبال تعریف موضوعاتی در زمینه محافظت سرویس ها و شبکه باشند.

امروزه مشتریان از فراهم کنندگان سرویس درباره پیاده سازی پیشگیری های امنیتی برای شرایط ترافیک بد سوال می کنند. مشتری به محافظت اتوماتیک و انتها به انتها نیاز دارد. در این مسیر، راه حل هایی که به CPE[1] های خاص با توسعه زیاد و باز نویسی های کلان در توپولوژی های شبکه نیاز دارد، مقرون به صرفه نیستند. در حالی که در اینترنت از قابلیت اعتماد ضمنی به سمت بی اعتمادی فراگیر در حرکت هستیم ، امنیت قلب شبکه های آینده خواهد بود. امنیت در تجهیزات بحرانی قرار داده می شود تا از مواردی مثل آنچه در زیر آمده حمایت کند :

- قابلیت دسترسی و اطمینان سرویس
- استمرار تجاری
- SLA[2] های توافقات سطح سرویس
- اعتماد مشتری

۱۵-۸-۱ شرایط لازم امنیتی

پارامترهایی که در رسیدن به امنیت باید رعایت شوند عبارتند از:

- شناسایی ترمینال وکاربر: بررسی درستی شناسه کاربران و ترمینال ها و بررسی مجوز کار برای استفاده از منابع
- امنیت و مجوزها : تصدیق درستی ارتباط با دیگر شبکه ها و با فراهم کنندگان کاربردها و با کاربران.
- سرویس ها و کاربردها :
- شروط امنیتی شامل :

قابلیت اعتماد[3] : ممانعت از نفوذ اطلاعات غیر مجاز یا دسترسی غیر مجاز

جامعیت داده[4] : منع تغییر داده غیر مجاز

عدم رد[5] : اعمال انجام شده نمی توانند رد شوند.

دسترسی : قابلیت دسترسی به سرویس و داده

خصوصی سازی : منع دسترسی به پروفایل به صورت غیر مجاز و افشاسازی و تغییر و تبدیل

- خصوصی سازی شبکه :به اپراتورها در شبکه امکان می دهدتا دید را نسبت به توپولوژی شبکه محدود کنند.
- CLIR / CLIP[6] : امکان شناسایی شروع کننده تماس نشست را فراهم می کند.

[1] Customer Premise Equipment
[2] Service Level Agreement
[3] Confidentiality
[4] Integrity
[5] Non Repudiation
[6] Calling Line Identification Restriction/ Calling Line Identification Presentation

۱۵-۸-۲- تهدیدهای وابسته به شبکه های نسل آتی

سه کلاس از تهدیدهادرشبکه های نسل آتی عبارتند از: تهدید وابسته به پیام، تهدید وابسته به کاربرو تهدید وابسته به سیستم. صفات امنیتی سیستم که بر تهدیدهای سیستم اثر می گذارند شامل قابلیت اعتماد، ایمنی داده ، تصدیق و قابلیت دسترسی می باشند. برخی تهدید هایی که سیستم با آنها مواجه است این ویژگی ها را به خطر می اندازد. مطابق با این اثر ، ITU-T ۵ مدل از تهدیدهای ممکن ارائه کرده است که عبارتند از:

۱-تخریب[1] (حمله به قابلیت دسترسی): با تخریب اطلاعات و یا منابع شبکه ، قابلیت دسترسی به خطر می افتد.

۲-خطای ناشی از اختلال[2] (حمله به ایمنی داده): ورود بدون مجوز ایمنی داده را به خطر می اندازد.

۳-حذف[3] (حمله به قابلیت دسترسی): سرقت ،حذف و یا گم کردن اطلاعات ویا منابع، به قابلیت دسترسی لطمه می زند.

۴-افشا[4] (حمله به قابلیت اعتماد): دسترسی بدون مجوز برای رسیدن به چیز با ارزش ، اعتماد به سیستم را تهدید می کند.

۵-قطع کردن[5] (حمله به قابلیت دسترسی): با قطع سرویس ها ، شبکه خارج از دسترس یا غیر قابل استفاده می شود.

۱۵-۸-۳- دامنه های امنیتی شبکه

شکل (۱۵-۱۸) دامنه های امنیتی مختلف با توجه به آسیب پذیری شبکه را نشان می دهد. این دامنه ها مبتنی براستانداردITU-T X.805 و به شرح ذیل اند:

- کنترل دسترسی : محدودیت و کنترل دسترسی به عناصر شبکه ، سرویس ها وکاربردها مثل رمز عبور، ACL[6]، دیوارآتش.
- تصدیق درستی : تهیه و تدارک شناسایی مثل رمز مشترک ، PKI[7] ، امضای دیجیتالی، سند دیجیتالی
- عدم رد :عملی را که در شبکه در حال اجراست نمی شود رد کرد مثل عملیات سیستم که ضبط شده یا امضای دیجیتالی.
- قابلیت اعتماد داده : اطمینان از قابلیت اعتماد داده مثل رمزنگاری.
- امنیت ارتباط : اطمینان از اینکه اطلاعات تنها از مبدا به مقصد در جریان اند مثل VPN, MPLS , L2TP.
- ایمنی داده : اطمینان ازدریافت داده ای که ارسال شده یا بازیابی داده ای که ذخیره شده مثل MD5[8] ، امضای دیجیتالی، نرم افزار آنتی ویروس.
- قابلیت دسترسی : اطمینان از دسترسی به عناصر شبکه، سرویس ها و کاربردها برای کاربران قانونی مثل IDS/IPS[9]. بررسی کدهای دریافتی برای تشخیص خطای شبکه و BC/DR[10].
- خصوصی سازی : اطمینان از شناسایی و استفاده از شبکه ای که خصوصی نگه داشته شده مثل NAT[11] و رمزگذاری .

[1] Destruction
[2] Corruption
[3] Removal
[4] Disclosure
[5] Interruption
[6] Applied Colored Label
[7] public key infrastructure
[8] Message-Digest algorithm 5
[9] Intrusion Detection System/ Intrusion Prevention System
[10] Business Continuity/Disaster Recovery
[11] Network Address Translation

شکل(۱۵-۱۸): دامنه های امنیتی مبتنی بر ITU-T X.805

در هر کدام از دامنه های امنیتی برخی از تهدیدهای امنیتی ذکر شده در مدل ITU-T وجود دارد.

۱۵-۸-۴- لایه های امنیتی

مفهوم لایه های امنیتی، همگرایی مرتبه ای را در امنیت برای شبکه بیان می کند. نگاشت نیازهای شبکه و امکان گروه بندی برای لایه های امنیتی می تواند در تعریف اینکه چطور عناصر شبکه در لایه های بالایی به حفاظت توسط لایه های پایینی تکیه می کنند، سودمند باشد.

سه لایه امنیتی به صورت لایه امنیتی پایه، لایه امنیتی کاربردها و لایه امنیتی سرویس ها تعریف شده اند. هر لایه، تهدیدها و آسیب پذیری خاص خود را دارد. امنیت در لایه۱، امنیت درلایه ۲و امنیت در لایه ۲، امنیت در لایه ۳ را فراهم می کند.

۱۵-۸-۴-۱- تعریف لایه های امنیتی

- **لایه امنیتی پایه :** این لایه، بلوک های ساختمانی پایه از شبکه ها ،سرویس ها و کاربردهاست. مثل مسیریاب های منحصر به فرد، سوئیچ ها، سرویس دهنده ها ،لینک های WAN[1] نقطه به نقطه و لینک های اترنت.
- **لایه امنیتی کاربردها :** شامل کاربردهای مبتنی بر شبکه است. کاربران انتهایی به آن دسترسی دارند. مثل جستجوگر وب ، پست الکترونیکی، تجارت الکترونیکی و فهرست کمکی .
- **لایه امنیتی سرویس ها :** شامل سرویس هایی است که برای کاربران انتهایی فراهم می شوند مثلIP, ATM ,Wi-Fi[2] ، IM[3], QoS , VoIPو سرویس های محلی، سرویس های تماس رایگان .

[1] Wide Area Network
[2] Wireless Fidelity
[3] Instant Message

۱۵-۸-۴-۲- کاربرد لایه های امنیتی در شبکه های IP

لایه امنیتی پایه : شامل مسیریاب های منحصر به فرد و سرویس دهنده ها.

لایه امنیتی سرویس ها: شامل لایه حمل IP ، سرویس های پشتیبانی IP مثلDHCP ,DNS, AAA ، سرویس های ارزش افزوده مثل QoS , VoIP , VPN .

لایه امنیتی کاربردها : شامل کاربردهای پایه مثل[1] FTP و دسترسی وب ، کاربردهای ساختاری مثل پست الکترونیکی، کاربردهای پایانی سطح بالا مثل تجارت الکترونیکی و آموزش الکترونیکی.

۱۵-۸-۵- سطوح امنیتی

مفهوم سطوح امنیتی، برای اطمینان از اینکه فعالیت های شبکه بنیادی به صورت مستقل انجام می شود، مفید است. (مثل توافق امنیتی در سطح امنیتی کاربران انتهایی که اثری بر روی توابع وابسته به سطح امنیتی مدیریت ندارد). در جایی که فعالیت های شبکه به اندازه گیری های امنیتی برای محافظت از شبکه وابسته است، سطوح امنیتی اجازه شناساییِ پتانسیل آسیب پذیری شبکه را می دهد.

۱۵-۸-۵-۱- تعریف سطوح امنیتی

سطوح امنیتی، نوعی از عملیات را که در شبکه اتفاق می افتد، نمایش می دهند. هر سطح امنیتی برای هرلایه امنیتی به کار می رود در نتیجه ۹ جنبه امنیتی به صورت سه بعدی ۳×۳ داریم. هر جنبه امنیتی، آسیب پذیری ها و تهدید های منحصر به فرد خود را دارد.

- **سطح امنیتی کاربر انتهایی :** در این سطح، دسترسی و استفاده از شبکه به وسیله مشتری با اهداف مختلف انجام می شود، مثل حمل و اتصال پایه، دسترسی به سرویس های ارزش افزوده(VoIP , VPN) ، دسترسی به کاربردهای پایه شبکه مثل پست الکترونیکی.
- **سطح امنیتی سیگنالینگ/کنترل :** در این سطح، فعالیت هایی انجام می شود که می توانند توابع شبکه را کارا کنند و ارتباطات ماشین به ماشین را برقرار نمایند.
- **سطح امنیتی مدیریت :** در این سطح، مدیریت و تامین ذخیره عناصر شبکه و پشتیبانی از توابع[2] FCAPS انجام می شود.

پرسش های فصل

۱. دلیل گرایش به سمت شبکه های نسل آتی را تشریح نمایید.
۲. تفاوت مدل لایه ای شبکه های نسل آتی را با شبکه های معمولی توضیح دهید.
۳. نیازمندی های جدید مشتریان که باعث حرکت به سمت شبکه های نسل آتی می شودرا بنویسید.
۴. تعریف شبکه های نسل آتی را ازدیدگاه ITU-T نوشته و مدل لایه ای آن را رسم کنید.
۵. تفاوت معماری پیشنهادی ITU-T و ETSI را برای شبکه های نسل آتی بنویسید.
۶. مفهوم جدا بودن لایه سرویس از لایه حمل را درشبکه های نسل آتی توضیح دهید.
۷. نیازمندی های ارائه سرویس های جدید درلایه هسته شبکه های نسل آتی را توضیح دهید.

[1] File Transfer Protocol
[2] Fault, Configuration, Accounting, Performance, and Security

۸. وظیفه اصلی لایه دسترسی درشبکه ها ی نسل آتی را نوشته و چند مورد از فنآوری های این لایه را بنویسید.
۹. مفهوم و وظیفه اصلی سوئیچ نرم افزاری را درشبکه های نسل آتی تشریح نمایید.
۱۰. نقش IP را درمعماری پروتکل ها درشبکه های نسل آتی توضیح دهید.
۱۱. به نظر شما مهاجرت ازشبکه های سنتی فعلی به سمت شبکه های نسل آتی، مستلزم اجرای چه مراحلی است؟
۱۲. با مراجعه به اینترنت ، لیستی از شرکت ها به همراه محصولات آنها را درزمینه شبکه های نسل آتی بدست آورید.
۱۳. با مراجعه به اینترنت ، لیستی از سرویس های نسل آتی را بنویسید.
۱۴. لزوم ارائه امنیت درشبکه های نسل آتی را تشریح نمایید.
۱۵. مهمترین تهدید های امنیتی شبکه های نسل آتی را توضیح دهید.