استاندارد ملی ایران

۱۳۲۸۵-۸-۱۳

چاپ اول

اسفند ۱۳۹۲

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization

INSO

13285-8-13

1st. Edition

Feb.2013

فن‌آوری اطلاعات – معماری افزاره UPnP– قسمت ۸-۱۳: پروتکل کنترلی افزاره درگاه اینترنتی – شعاع خدمت برای سرویس گیرنده

Information technology - UPnP Device Architecture – Part 8-13: Internet Gateway Device Control Protocol – Radius Client Service

ICS:35.200

به‌نام 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 پیشرفت‌های 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 صدور گواهی 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

" فن‌آوری اطلاعات- معماری افزاره UPnP – قسمت ۸-۱۳: پروتکل کنترلی افزاره درگاه اینترنتی –شعاع خدمت برای سرویس گیرنده"

رئیس:	**سمت و/یا نمایندگی**
بدلی افشرد، بابک (فوق لیسانس مهندسی کامپیوتر)	اداره کل استاندارد آذربایجان‌شرقی

دبیر:

خاکپور، علی (لیسانس مهندسی کامپیوتر)	شرکت ایران دیتا

اعضاء: (اسامی به ترتیب حروف الفبا)

اصل‌زاد، محمدعلی (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکاپژوه
اکبری سروری, شبنم (لیسانس مهندسی کامپیوتر)	شرکت پگاسوس
بدلی افشرد، محمدرضا (فوق لیسانس مهندسی برق)	نیروگاه حرارتی تبریز
تفسیری, حامد (لیسانس مهندسی کامپیوتر)	شرکت پگاسوس
خوشقدم، سهیلا (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکاپژوه
عظیمی حسینی، سارا (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکاپژوه
علی‌وند شاهگلی، فاطمه (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکاپژوه

فهرست مندرجات

پیش‌گفتار

استاندارد " فن‌آوری اطلاعات- معماری افزاره UPnP- قسمت ۸-۱۳: پروتکل کنترلی افزاره درگاه اینترنتی- شعاع خدمت برای سرویس گیرنده" که پیش‌نویس آن در کمیسیون‌های مربوط توسط شرکت ریزفناوران آرکا پژوه تهیه و تدوین شده و در دویست و هفتاد و هفتمین اجلاس کمیته ملی استاندارد رایانه تاریخ ۹۱/۱۲/۲۴ مورد تصویب قرارگرفته‌است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوّب بهمن‌ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحوّلات و پیشرفت‌های ملی و جهانی در زمینه صنایع ، علوم و خدمات، استاندارد های ملی ایران در موقع لزوم تجدید نظر خواهد شد و هرگونه پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه‌شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

منبع و مأخذی که برای تهیهٔ این استاندارد مورد استفاده قرارگرفته به شرح زیر است :

ISO/IEC 29341-8-13:2008, Information technology– UPnP Device Architecture – Part 8-13: Internet Gateway Device Control Protocol – Radius Client Service.

فن‌آوری اطلاعات- معماری افزاره UPnP- قسمت ۸-۱۳: پروتکل کنترلی افزاره درگاه اینترنتی – شعاع خدمت[1] برای سرویس گیرنده

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعریف خدمتی است که کنترل و پیکربندی مولفه شعاع نقاط دسترسی بی‌سیم IEEE 802.11 را برای فضای شبکه مدیریت نشده به نام شبکه‌های محلی دفتری کوچک و مستقر، فعال می‌سازد.

این تعریف خدمت مطابق با معماری افزاره UPnP نسخه ۱/۰ می‌باشد.

هدف این خدمت این است که نصب و راه‌اندازی شبکه‌های بی‌سیم را ساده‌تر نموده و چارچوبی برای تشخیص و پایش بر مشکلات را در شبکه‌های بی‌سیم فراهم نماید.

این نوع خدمت تنظیمات و پیکربندی پارامترهای وابسته شعاعی از یک نقطه دسترسی بی‌سیم را از راه دور ممکن می‌سازد.

۲ تعاریف مدل‌سازی خدمات

۲-۱ نوع خدمت

این خدمت همان‌طور که در زیر مشخص شده، اختیاری است:

urn:schemas-upnp-org:device:*WLANAccessPointDevice:1*

نوع خدمت زیر خدمتی را که مطابق با این الگوست مشخص می‌نماید.

urn:schemas-upnp-org:service:*RadiusClient:1*

این خدمت عمل پرس و جوی متغیر حالت را پشتیبانی نمی‌کند.

۲-۲ متغیرهای حالت

جدول ۱ تمام متغیرهای حالت خدمت شعاعی سرویس گیرنده را نشان می‌دهد.

جدول ۱- متغیرهای حالت

نام متغیر	مورد نیاز یا اختیاری [a]	نوع داده	مقدار اجازه داده شده	مقدار اولیه [b]	واحد Eng.
NumberOfAuthServerEntries	R	ui2	بزرگتر یا مساوی	0	N/A
AuthServerIPAddress	R	رشته	آدرس IP، تعداد کاراکتر کمتر یا مساوی	بدون حروف	N/A
AuthServerPortNumber	R	Ui2	شامل اعداد بین ۱ تا ۶۵۵۳۵	0	N/A
AuthServerSharedSecret	R	رشته	رمز اشتراکی	بدون حروف	N/A
متغیرهای حالت غیراستاندارد پیاده‌سازی شده توسط ارائه دهنده افزاره UPnP	X	TBD	TBD	TBD	TB [c]

1- Service

ادامه جدول ۱

[a] R: مورد نیاز، O: اختیاری، X: غیراستاندارد
[b] مقادیر فهرست شده در در این ستون مورد نیاز است. برای مشخص کردن مقادیر استاندارد اختیاری یا برای محول کردن انتساب مقادیر به ارائه دهنده، باید به نمونه خاصی از جدول مناسب زیر مراجعه نمائید.
[c] باید تعریف شود (To Be Defined)

۲-۲-۱ متغیر NumberOfAuthServerEntries

این متغیر تعداد ورودی‌های سرویس دهنده احراز هویت (تعداد عناصر موجود در آرایه) را نشان می‌دهد که برای این نقطه دسترسی پیکربندی شده است. نقطه دسترسی تلاش خواهد کرد تا با سرویس‌دهندگان احراز هویت مذکور در آرایه مرتب شده تائید هویت نماید. این متغیر قابل خواندن/نوشتن و رویدادی است.

۲-۲-۲ متغیر AuthServerIPAddress

این متغیر آدرس IP نسخه یا نسخه ۶ سرویس دهنده احراز هویت می‌باشد، مانند یک شعاع سرویس‌دهنده برای 802.1x مبتنی بر تائید هویت می‌باشد.

۲-۲-۳ متغیر AuthServerPortNumber

این متغیر یک شماره پورت (مانند ۱۶۴۵ یا ۱۸۱۲ برای شعاع) از سرویس دهنده احراز هویت می‌باشد، مانند یک شعاع سرویس دهنده برای تایید هویت مبتنی بر EAP. این متغیر قابل خواندن/نوشتن است.

۲-۲-۴ متغیر AuthServerSharedSecret

این متغیر یک رشته است که نشان‌دهنده رمز عبور در متن ساده برای نقطه دسترسی به تایید هویت در سرویس دهنده احراز هویت می‌باشد، مانند شعاع سرویس دهنده ، برای تایید هویت مبتنی بر EAP می‌باشد. این متغیر قابل خواندن/نوشتن می‌باشد

۲-۳ رویداد و مدیریت

جدول ۲- مدیریت رویداد

نام متغیر	رویداد	رویداد مدیریت شده	بیشینه نرخ رویداد [a]	ترکیب منطقی	کمینه Delta در هر رویداد [b]
NumberOfAuthServerEntries	بلی	خیر	N/A	N/A	N/A
متغیرهای حالت غیراستاندارد پیاده‌سازی شده توسط ارائه دهنده افزاره UPnP	TBD	TBD	TBD	TBD	TBD
[a] با **N** مشخص شده، نرخ =(رخداد) $\frac{Event}{(N\ secs)}$					
[b] *(allowedValueRange Step) * (N)*					

۲-۳-۱ مدل رویداد

فقط یک متغیر حالت از خدمت *RadiusClient* رویدادی است:

رویداد NumberOfAuthServerEntries: رویداد متغیر حالت کمک می‌کند تا فهرست سرویس‌دهنده احراز هویت سرویس گیرنده را با فهرست سرویس دهنده احراز هویت نگهداری شده در افزاره نقطه دسترسی[1] (AP)، همگام‌سازی نماید.

هیچ یک از رویدادها قابل مدیریت نمی‌باشد.

۴-۲ عملیات

جدول ۳ عملیات مورد نیاز و اختیاری را برای افزاره UPnP AP فهرست نموده است. این موارد توسط اطلاعات دقیق در مورد این عملیات، شامل شرح کوتاهی از عملیات، تاثیرات این عملیات روی متغیرهای حالت و کدهای خطای تعریف شده توسط عملیات دنبال می‌شود.

امنیت عملیات UPnP در این خدمت اختیاری است اما به شدت توصیه می‌شود، برای این منظور از پروتکل امنیت UPnP که به عنوان گروه کاری امنیت UPnP تعریف شده است، استفاده شود. اگر AP امنیت را برای عملیات UPnP پیاده‌سازی نماید، جدول ۳ عملیاتی که باید امن شوند را نشان می‌دهد. بقیه ممکن است به‌صورت امن یا باز پیاده‌سازی شود. عملیات امن باید هر دو مورد محرمانه بودن و یکپارچگی را پشتیبانی کند.

مجوز دسترسی از افزاره محتوی به ارث برده خواهد شد (به‌عنوان مثال افزاره نقطه دسترسی WLAN).

جدول ۳- عملیات

نام	امن یا باز*	مورد نیاز یا اختیاری
GetGenericAuthServerEntry	S	R
GetSpecificAuthServerEntry	S	R
AddAuthServerEntry	S	R
DeleteAuthServerEntry	S	R
FactoryDefaultReset	S	R
ResetAuthentication	S	R
* R = مورد نیاز، O = اختیاری، X = غیر استاندارد این ستون به این امر اشاره می‌کند خدمت امنیت افزاره در افزاره شامل شونده حاضر است یا خیر.		

۱-۴-۲ GetGenericAuthServerEntry

این عمل ورودی‌های سرویس دهنده احراز هویت را به‌صورت یک ورودی در یک زمان بازیابی می‌کند. نقاط کنترل می‌تواند این عمل را با یک اندیس آرایه افزایشی تا زمانی فراخوانی کند که هیچ ورودی روی دروازه یافت نشود. اگر NumberOfAuthServerEntries در طول فراخوانی به‌روز رسانی شود، فرایند ممکن است مجبور شود دوباره شروع کند. ورودی‌های آرایه به هم پیوسته است. به محض اینکه که ورودی‌ها حذف شدند، آرایه فشرده می‌شود و متغیر رخدادی NumberOfAuthServerEntries کاهش داده می‌شود. ورودی‌های سرویس دهنده احراز هویت به‌طور منطقی به‌صورت آرایه‌ای در AP ذخیره شده‌اند و با استفاده از اندیس آرایه بین محدوده صفر تا NumberOfAuthServerEntries - 1 بازیابی می‌شود.

1- Access Point

۲-۴-۱-۱ آرگومان‌ها

جدول ۴: آرگومان‌های GetGenericAuthServerEntry

آرگومان	جهت	متغیر حالت وابسته
NewAuthServerIndex	ورودی	NumberOfAuthServerEntries
NewAuthServerIPAddress	خروجی	AuthServerIPAddress
NewAuthServerPortNumber	خروجی	AuthServerPortNumber
NewAuthServerSharedSecret	خروجی	AuthServerSharedSecret

۲-۴-۱-۲ وابستگی در حالت (اگر وجود دارد)

۲-۴-۱-۳ تاثیر در حالت (اگر وجود دارد)

۲-۴-۱-۴ خطاها

کد خطا	توصیف کد	توضیحات
۴۰۲	آرگومان نامعتبر	قسمت معماری افزاره UPnP در کنترل مشاهده گردد.
۷۱۳	اندیس نامعتبر	اندیس آرایه مشخص شده خارج از محدوده می‌باشد.

۲-۴-۲ عمل GetSpecificAuthServerEntry

این عمل ورودی‌های سرویس دهنده احراز هویت را برای ترکیب خاص {آدرس، پورت} بازیابی می‌کند.

۲-۴-۲-۱ آرگومان‌ها

جدول ۵- آرگومان‌های GetSpecificAuthServerEntry

آرگومان	جهت	متغیر حالت وابسته
NewAuthServerIPAddress	ورودی	AuthServerIPAddress
NewAuthServerPortNumber	ورودی	AuthServerPortNumber
NewAuthServerSharedSecret	خروجی	AuthServerSharedSecret

۲-۴-۲-۲ وابستگی در حالت (اگر وجود دارد)

۲-۴-۲-۳ تاثیر در حالت (اگر وجود دارد)

۲-۴-۲-۴ خطاها

کد خطا	توصیف کد	توضیحات
۴۰۲	آرگومان نا معتبر	قسمت معماری افزاره UPnP در کنترل مشاهده گردد.
۷۱۴	چنین ورودی در آرایه وجود ندارد.	مقدار مشخص شده ترکیب AuthServerIPAddress و AuthServerPortNumber در آرایه وجود ندارد.

۲-۴-۳ AddAuthServerEntry

این عمل یک ورودی جدید سرویس دهنده احراز هویت در فهرست سرویس دهنده احراز هویت ایجاد می کند.

۲-۴-۳-۱ آرگومان‌ها

جدول ۶- آرگومان‌های AddAuthServerEntry

آرگومان	جهت	متغیر حالت وابسته
NewAuthServerIP	ورودی	AuthServerIPAddress
NewAuthServerPortNumber	ورودی	AuthServerPortNumber
NewAuthServerSharedSecret	ورودی	AuthServerSharedSecret

۲-۴-۳-۲ وابستگی در حالت (اگر وجود دارد)

۲-۴-۳-۳ تاثیر در حالت (اگر وجود دارد)

۲-۴-۳-۴ خطاها

کد خطا	توصیف کد	توضیحات
۴۰۲	آرگومان نامعتبر	قسمت معماری افزاره UPnP در کنترل مشاهده گردد.
۷۰۱	قبلا ورودی سرویس دهنده احراز هویت داشت	ورودی سرویس دهنده مشخص شده قبلا در ورودی سرویس دهنده احراز هویت موجود بوده است. این موقعی اتفاق می‌افتد که IP و پورت یکسان باشد، ولی رمز اشتراکی متفاوتی داشته باشند.

۲-۴-۴ عمل DeleteAuthServerEntry

این عمل ورودی موجود سرویس دهنده احراز هویت را از فهرست سرویس دهنده احراز هویت حذف می‌کند. ورودی سرویس دهنده احراز هویت با استفاده از آدرس IP و شماره پورت سرویس دهنده احراز هویت مشخص می‌شود.

۲-۴-۴-۱ آرگومان‌ها

جدول ۷- آرگومان‌ها برای DeleteAuthServerEntry

آرگومان	جهت	متغیر حالت وابسته
NewAuthServerIPAddress	ورودی	AuthServerIPAddress
NewAuthServerPortNumber	ورودی	AuthServerPortNumber

۲-۴-۴-۲ وابستگی در حالت (اگر وجود دارد)

۲-۴-۴-۳ تاثیر در حالت (اگر وجود دارد)

۲-۴-۴-۴ خطاها

کد خطا	توصیف کد	توضیحات
۴۰۲	آرگومان نا معتبر	قسمت معماری دستگاه UPnP در کنترل مشاهده گردد.
۷۱۴	چنین ورودی در آرایه وجود ندارد	مقدار مشخص شده ترکیب AuthServerIPAddress و AuthServerPortNumber در آرایه وجود ندارد

۲-۴-۵ FactoryDefaultReset

این عمل همه متغیرهای حالت مربوط به خدمت RadiusClient را به تنظیمات پیش فرض کارخانه آن‌ها باز نشانی[1] می‌کند. این عمل همه ورودی‌های شعاع سرویس دهنده را از بین می‌برد. این عمل همچنین همه نشست‌های[2] بی‌سیم را که با استفاده از شعاع سرویس دهنده احراز هویت شده بودند بازنشانی می‌کند.

اگر نقطه کنترل عمل FactoryDefaultReset از امینت افزاره را فراخوانی کند (یا خدمت پیکربندی WLAN اگر این خدمت در افزاره AP مقیم باشد)، این عمل باید به‌طور داخلی فراخوانی شود، در حالیکه برعکس آن درست نیست به‌عنوان مثال، بازنشانی این خدمت بازنشانی امنیت افزاره (یا بازنشانی پیکربندی WLAN) را فراخوانی نخواهد کرد.

۲-۴-۵-۱ آرگومان‌ها

آرگومانی ندارد.

۲-۴-۵-۲ وابستگی در حالت (اگر وجود دارد)

۲-۴-۵-۳ تاثیر در حالت (اگر وجود دارد)

۲-۴-۵-۴ خطاها

کد خطا	توصیف کد	توضیحات
۴۰۲	آرگومان نامعتبر	قسمت معماری افزاره UPnP در کنترل مشاهده گردد.

۲-۴-۶ ResetAuthentication

این عمل همه ایستگاه‌های بی‌سیم را که از طریق شعاع سرویس دهنده احراز هویت شده بودند بازنشانی می کند.

اگر نقطه کنترل عمل ResetAuthentication از خدمت پیکربندی WLAN را فراخوانی کند این عمل باید به‌طور داخلی فراخوانی شود البته اگر خدمت RadiusClient در افزاره AP مقیم باشد، در حالیکه برعکس آن درست نیست.

۲-۴-۶-۱ آرگومان‌ها

هیچ آرگومانی ندارد.

۲-۴-۶-۲ وابستگی در حالت (در صورت وجود)

۲-۴-۶-۳ تاثیر در حالت (در صورت وجود)

۲-۴-۶-۴ خطاها

کد خطا	توصیف کد	توضیحات
۴۰۲	آرگومان نامعتبر	قسمت معماری افزاره UPnP در کنترل مشاهده گردد.

1- reset
2- sessions

۲-۴-۷ عملیات غیر استاندارد پیاده‌سازی شده توسط ارائه دهنده افزاره UPnP

به‌منظور تسهیل در صدور گواهینامه، عملیات غیراستاندارد پیاده‌سازی شده توسط ارائه دهندگان افزاره UPnP باید در قالب این خدمت گنجانده شود. معماری افزاره UPnP اسامی مورد نیاز برای عملیات غیراستاندارد را فهرست نموده است (بخش توصیف را مشاهده نمایید).

۲-۴-۸- کدهای خطای متداول

جدول پیش‌رو کدهای خطای متداول در عملیات برای این نوع خدمت را فهرست نموده است.

جدول ۸- کدهای خطای متداول

کد خطا	توصیف کد	توضیحات
۴۰۱	عمل نامعتبر	قسمت معماری افزاره UPnP در کنترل مشاهده گردد.
۴۰۲	آرگومان نامعتبر	قسمت معماری افزاره UPnP در کنترل مشاهده گردد.
۴۰۴	متغیر نامعتبر	قسمت معماری افزاره UPnP در کنترل مشاهده گردد.
۵۰۱	خرابی عمل	قسمت معماری افزاره UPnP در کنترل مشاهده گردد.
۶۰۰- ۶۹۹	TBD	خطاهای عمل متداول. تعریف شده توسط کمیته کار انجمن UPnP
۷۰۱- ۷۹۹		خطاهای عمل متداول. تعریف شده توسط کمیته کار انجمن UPnP
۸۰۰- ۸۹۹	TBD	(مشخص شده توسط ارائه دهنده افزاره UPnP)

۲-۵ تئوری عملیات

۲-۵-۱ عملیات مشتری RADIUS

یک AP که توسط فن‌آوری UPnP فعال شود ممکن است فهرستی از شعاع سرویس دهنده‌های احراز هویت راه دور برای تایید هویت EAP نگهداری کنند. این فهرست می‌تواند توسط نقاط کنترل به‌روزرسانی شوند. افزاره AP همچنین ممکن است توانایی اجرای سرویس دهنده احراز هویت را به‌طور محلی داشته باشد. افزاره AP یک سرویس دهنده احراز هویت از فهرست سرویس دهنده احراز هویت به ترتیبی که به فهرست اضافه شده‌اند، انتخاب می‌کند.

۳ توصیف خدمت XML

```
<?xml version="1.0"?>
<scpd xmlns="urn:schemas-upnp-org:service-1-0">
     <specVersion>
         <major>1</major>
         <minor>0</minor>
     </specVersion>
     <actionList>
         <action>
            <name>GetGenericAuthServerEntry</name>
            <argumentList>
                <argument>
                    <name>NewAuthServerIndex</name>
                    <direction>in</direction>
```

```
<relatedStateVariable>NumberOfAuthServerEntries</relatedStateVariable>
              </argument>
              <argument>
                  <name>NewAuthServerIPAddress</name>
                  <direction>out</direction>
<relatedStateVariable>AuthServerIPAddress</relatedStateVariable>
              </argument>
              <argument>
                  <name>NewAuthServerPortNumber</name>
                  <direction>out</direction>
 <relatedStateVariable>AuthServerPortNumber</relatedStateVariable>
                  </argument>
                  <argument>
                      <name>NewAuthServerSharedSecret</name>
                      <direction>out</direction>
 <relatedStateVariable>AuthServerSharedSecret</relatedStateVariable>
                  </argument>
                  </argumentList>
             </action>
             <action>
                <name>GetSpecificAuthServerEntry</name>
                <argumentList>
                   <argument>
                         <name>NewAuthServerIPAddress</name>
                         <direction>in</direction>
<relatedStateVariable>AuthServerIPAddress</relatedStateVariable>
                 </argument>
                 <argument>
                      <name>NewAuthServerPortNumber</name>
                      <direction>in</direction>

<relatedStateVariable>AuthServerPortNumber</relatedStateVariable>
                  </argument>
                  <argument>
                       <name>NewAuthServerSharedSecret</name>
                       <direction>out</direction>
<relatedStateVariable>AuthServerSharedSecret</relatedStateVariable>
                  </argument>
               </argumentList>
              </action>
              <action>
                  <name>AddAuthServerEntry</name>
                  <argumentList>
                      <argument>
                          <name>NewAuthServerIPAddress</name>
                          <direction>in</direction>
<relatedStateVariable>AuthServerIPAddress</relatedStateVariable>
                      </argument>
                      <argument>
                          <name>NewAuthServerPortNumber</name>
                          <direction>in</direction>
<relatedStateVariable>AuthServerPortNumber</relatedStateVariable>
               </argument>
               <argument>
```

```
                    <name>NewAuthServerSharedSecret</name>
                    <direction>in</direction>
<relatedStateVariable>AuthServerSharedSecret</relatedStateVariable>
                </argument>
                </argumentList>
        </action>
        <action>
            <name>DeleteAuthServerEntry</name>
            <argumentList>
               <argument>
                    <name>NewAuthServerIPAddress</name>
                    <direction>in</direction>
<relatedStateVariable>AuthServerIPAddress</relatedStateVariable>
              </argument>
              <argument>
                   <name>NewAuthServerPortNumber</name>
                   <direction>in</direction>
<relatedStateVariable>AuthServerPortNumber</relatedStateVariable>
              </argument>
        </argumentList>
        </action>
        <action>
             <name>FactoryDefaultReset</name>
        </action>
        <action>
            <name>ResetAuthentication</name>
        </action>
        </actionList>
        <serviceStateTable>
            <stateVariable sendEvents="yes">
                <name>NumberOfAuthServerEntries</name>
                <dataType>ui2</dataType>
           </stateVariable>
           <stateVariable sendEvents="no">
                <name>AuthServerIPAddress</name>
                <dataType>string</dataType>
           </stateVariable>
           <stateVariable sendEvents="no">
               <name>AuthServerPortNumber</name>
               <dataType>ui2</dataType>
          </stateVariable>
          <stateVariable sendEvents="no">
               <name>AuthServerSharedSecret</name>
               <dataType>string</dataType>
          </stateVariable>
     </serviceStateTable>
</scpd>
```