The Remote Authentication Dial-In User Service (RADIUS)

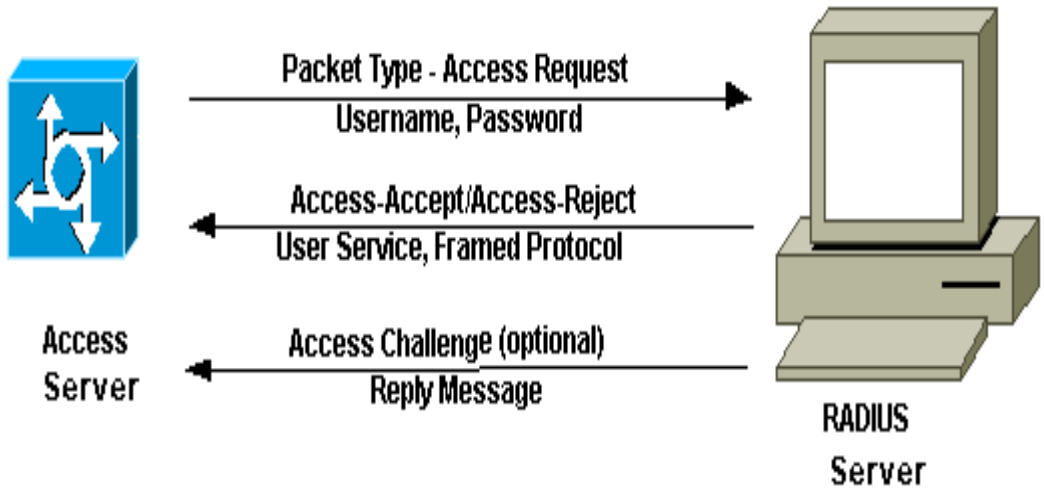
RADIUSمخفف کلمه (Remote Authentication Dial-In User Service) است استاندارد قدیمی RADIUSسرور بر روی پورت 1645فعالیت دارد که به دلیل تداخل با Data Metrics در استاندارد RFC2865به پورت 1812 برای Authentication و Authorization تغییر کرد .و از شماره پورت های 1646 و 1813 برای Accounting استفاده می کند.

RADIUS سرورتوانایی استفاده از متدهای مختلف برای احراز هویت و مجوز دسترسی دادن به یک RADIUS Clientرا دارا می باشد.(..... PPP-PAP-CHAP-UNIX Login)

اصولا مجوز دسترسی به شبکه توسط یک Userشامل ارسال Queryاز سمت NAS (Network Access server)به سمت سرورمیباشد(Access-Request) که شاملUsername،Encrypted passwordو پورت میباشد.

پاسخ سرور به این درخواست(Access-Accept or Access-Reject) میباشد.(مطابق شکل زیر)

RADIUS سرور بعد از دریافت درخواست، Access-Request را بررسی میکند درصورت تایید رمز عبور،اگر Username ارسال شده در لیست Users data base سرور موجود باشد،پیغام Access-Acceptبه سمت clientارسال میشود که شامل لیستی از صفت ها که مشخص کننده پارامتر های مورد استفاده هستند را شامل میشود، همچنین نوع سرویس (shell or framed)، نوع پروتکل،IP برای فراهم کردن دسترسی user به Access-List ویا اضافه کردن static Route در جدول مسیریابی NAS می باشد. configuration information در RADIUSسرور،تعین کننده انچه در NAS قرار میگیرد است.



	RADIUS	TACACS+
Protocol and Port(s) Used	UDP: 1812 and 1813 -or- UDP: 1645 and 1646	TCP: 49
Encryption	Encrypts only the Password field	Encrypts the entire payload
Authentication and Authorization	Combines authentication and authorization	Separates authentication and authorization
Primary Use	Network access	Device administration

این پروتکل در سیستم عامل های مختلفی که در دنیا وجود دارد با انواع و اقسام روش ها و با استفاده از نرم افزارهای مختلف قابل پیاده سازی می باشد.RADIUS به سروری گفته می شود که می تواند عملیات های AAAیا همان سه عملیاتی که اشاره شد را انجام دهد ، در ویندوزها سرور شرکت مایکروسافت نیز با عنوان NPS یا Network Policy Servicesشناخته می شود. این سرویس را می توانید در ویندوز های سرور 2008 به بالا مشاهده کنید.

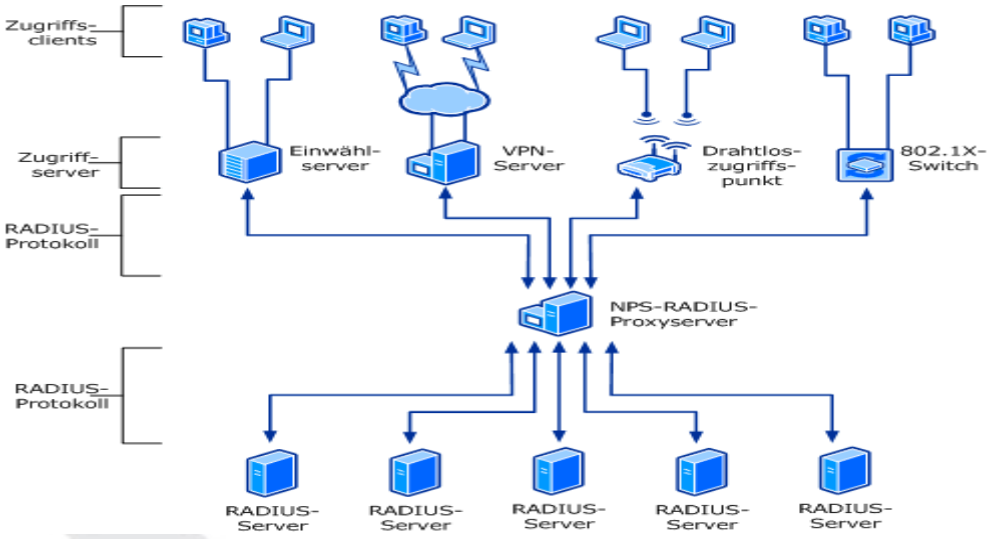
در ویندوز های سرور موارد زیر را میتوانیم به عنوان یک RADIUS Server client داشته باشیم.

Dial-Up Server

Wireless Access Point

VPN Server

802.1X Switch



Cisco Identity Services Engine (ISE)

نسل جدید سیستم شناسایی و کنترل دسترسی است (جایگزین ACS)که شبکه را قادر می سازد سرویس دهی را ساده تر انجام دهد و وضعیت امنیت زیرساخت را بهبود ببخشد. معماری منحصر به فرد Cisco ISE این امکان را می دهد که به صورت Real time اطلاعات شبکه ، کاربران و دستگاه ها را جمع آوری کند. سپس مدیر می تواند با استفاده از این اطلاعات برای شناسایی دسترسی به عناصر مختلف شبکه مانند سوئیچ ها ، WLAN، VPNو ... اقدام کند .

Cisco ISEمحصولی جدید است که راه حل ها و سرویس های مختلف امنیتی را در یک محصول به صورت یکجا برای ما فراهم می کند. این محصول کنترل دسترسی و راه حل های امنیتی را برای ارتباطات کابلی ، وایرلس و VPN را به صورت ساده و خودکار فراهم می کند .