# RADIUS의 작동 방식 검토

## 목차



## 소개

이 문서에서는 RADIUS 서버의 정의 및 작동 방식에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

## 배경 정보

RADIUS(Remote Authentication Dial-In User Service) 프로토콜은 Livingston Enterprises, Inc.에서 액세스 서버 인증 및 계정 관리 프로토콜로 개발한 것입니다. RADIUS 사양 RFC 2865로 RFC 2138이 더 이상 사용되지 않습니다. RADIUS 계정 관리 표준 RFC 2866으로 RFC 2139가 더 이상 사용되지 않습니다.

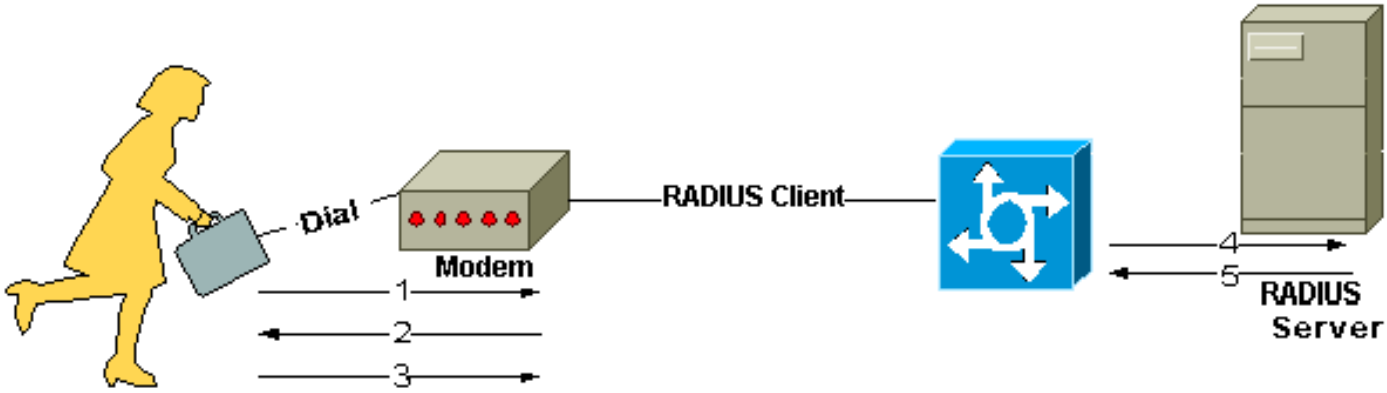
NAS(Network Access Server)와 RADIUS 서버 간의 통신은 UDP(User Datagram Protocol)를 기반

으로 합니다. 일반적으로 RADIUS 프로토콜은 연결 없는 서비스로 간주됩니다. 서버 가용성, 재전송 및 시간 초과와 관련된 문제는 전송 프로토콜이 아닌 RADIUS 활성화 디바이스에서 처리됩니다.

### RADIUS는 클라이언트/서버 프로토콜입니다

RADIUS 클라이언트는 일반적으로 NAS이며 RADIUS 서버는 일반적으로 UNIX 또는 Windows NT 시스템에서 실행되는 데몬 프로세스입니다. 클라이언트는 사용자 정보를 지정된 RADIUS 서버에 전달하고 반환된 응답에 대해 작동합니다. RADIUS 서버는 사용자 연결 요청을 수신하고, 사용자를 인증한 다음 클라이언트가 사용자에게 서비스를 제공하는 데 필요한 설정 정보를 반환합니다. RADIUS 서버는 다른 RADIUS 서버 또는 다른 종류의 인증 서버에 대한 프록시 클라이언트 역할을 할 수 있습니다.

이 그림은 다이얼인 사용자와 RADIUS 클라이언트 및 서버 간의 상호 작용을 보여줍니다.




*전화 접속 사용자와 RADIUS 클라이언트 및 서버 간의 상호 작용*

1. 사용자가 NAS에 대한 PPP 인증을 시작합니다.
2. NAS에서 사용자 이름 및 비밀번호(PAP(Password Authentication Protocol)) 또는 챌린지(CHAP(Challenge Handshake Authentication Protocol))를 묻는 프롬프트를 표시합니다.
3. 사용자 응답.
4. RADIUS 클라이언트는 사용자 이름 및 암호화된 비밀번호를 RADIUS 서버로 전송합니다.
5. RADIUS 서버가 Accept(수락), Reject(거부) 또는 Challenge(챌린지)로 응답합니다.
6. RADIUS 클라이언트는 Accept(수락) 또는 Reject(거부)와 함께 번들로 제공되는 서비스 및 서비스 파라미터에 따라 작동합니다.

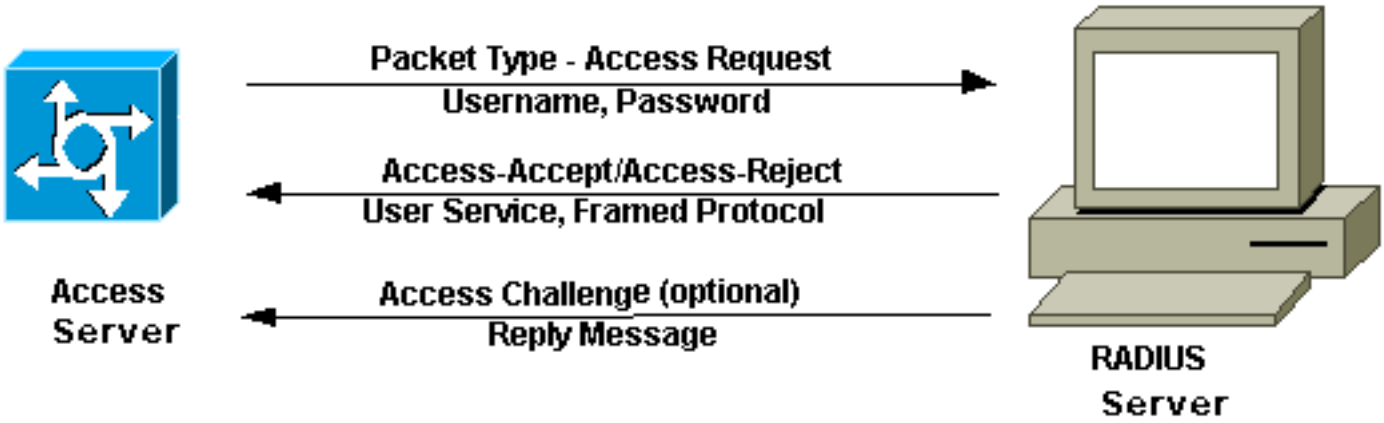
## 인증 및 권한 부여

RADIUS 서버는 다양한 방법으로 사용자를 인증할 수 있습니다. 사용자가 제공한 사용자 이름 및 원래 비밀번호가 제공된 경우 PPP, PAP 또는 CHAP, UNIX 로그인 및 기타 인증 메커니즘을 지원할 수 있습니다.

일반적으로 사용자 로그인은 NAS에서 RADIUS 서버로의 쿼리(Access-Request) 및 서버의 해당 응답(Access-Accept 또는 Access-Reject)으로 구성됩니다. Access-Request 패킷에는 사용자 이름, 암호화된 비밀번호, NAS IP 주소 및 포트가 포함됩니다. RADIUS의 초기 구축은 UDP 포트 번호 1645로 수행되었으며, 이는 "데이터 메트릭" 서비스와 충돌합니다. 이 충돌로 인해 RFC 2865는 RADIUS에 대해 공식적으로 포트 번호 1812를 할당했습니다. 대부분의 시스코 디바이스 및 애플리케이션은 포트 번호 집합 중 하나를 지원합니다. 요청의 형식은 사용자가 시작하려는 세션 유형에 대한 정보도 제공합니다. 예를 들어 쿼리가 문자 모드에서 제공되는 경우 추론은 "Service-Type = Exec-User"이지만 요청이 PPP 패킷 모드에서 제공되는 경우 추론은 "Service Type = Framed User" 및 "Framed Type = PPP"입니다.

RADIUS 서버가 NAS에서 Access-Request를 수신하면 데이터베이스에서 나열된 사용자 이름을 검색합니다. 사용자 이름이 데이터베이스에 없으면 기본 프로필이 로드되거나 RADIUS 서버가 즉시 Access-Reject 메시지를 보냅니다. 이 액세스 거부 메시지는 거부 이유를 나타내는 텍스트 메시지와 함께 할 수 있습니다.

RADIUS에서는 인증과 권한 부여가 함께 결합됩니다. 사용자 이름이 발견되고 암호가 올바르면 RADIUS 서버는 이 세션에 사용할 매개변수를 설명하는 특성-값 쌍의 목록이 포함된 Access-Accept 응답을 반환합니다. 일반적인 매개변수에는 서비스 유형(셸 또는 프레임), 프로토콜 유형, 사용자를 할당할 IP 주소(정적 또는 동적), 적용할 액세스 목록 또는 NAS 라우팅 테이블에 설치할 고정 경로가 포함됩니다. RADIUS 서버의 컨피그레이션 정보는 NAS에 설치할 수 있는 항목을 정의합니다. 다음 그림에는 RADIUS 인증 및 권한 부여 시퀀스가 나와 있습니다.




*RADIUS 인증 및 권한 부여 시퀀스*

# 어카운팅

RADIUS 프로토콜의 계정 관리 기능은 RADIUS 인증 또는 권한 부여와 상관없이 사용할 수 있습니다. RADIUS 어카운팅 기능을 사용하면 세션 시작 및 종료 시 데이터를 전송할 수 있습니다. 이는 세션 동안 사용된 리소스(예: 시간, 패킷, 바이트 등)의 양을 나타냅니다. 인터넷 서비스 공급자(ISP)는 RADIUS 액세스 제어 및 계정 관리 소프트웨어를 사용하여 특수한 보안 및 청구 요구 사항을 충족할 수 있습니다. 대부분의 시스코 디바이스에 대한 RADIUS의 계정 관리 포트는 1646이지만 1813일 수도 있습니다(RFC 2139에 지정된 대로 포트 변경으로 인함).

클라이언트와 RADIUS 서버 간의 트랜잭션은 네트워크를 통해 전송되지 않는 공유 암호를 사용하여 인증됩니다. 또한 사용자 비밀번호는 클라이언트와 RADIUS 서버 간에 암호화되어 전송되므로, 안전하지 않은 네트워크에서 스누핑하는 누군가가 사용자 비밀번호를 결정할 가능성을 배제할 수 있습니다.

# 관련 정보

- 인증 프로토콜
- RFC(설명 요청)
- Technical Support - Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.