Esaminare il funzionamento di RADIUS

Sommario

Introduzione

In questo documento viene descritto cos'è un server RADIUS e come funziona.

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

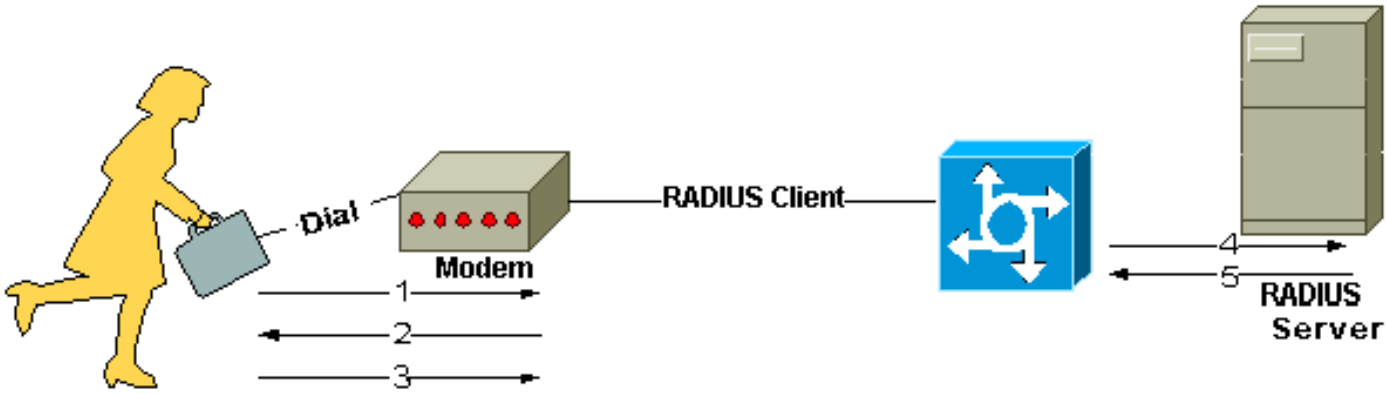
Il protocollo RADIUS (Remote Authentication Dial-In User Service) è stato sviluppato da Livingston Enterprises, Inc. come protocollo di autenticazione e accounting del server di accesso. La specifica RADIUS RFC 2865 ha reso la specifica RFC 2138 obsoleta. La specifica RADIUS per l'accounting RFC 2866 ha reso obsoleta la specifica RFC 2139.

La comunicazione tra un server di accesso alla rete (NAS) e un server RADIUS è basata sul protocollo UDP (User Datagram Protocol). In genere, il protocollo RADIUS è considerato un servizio senza connessione. I problemi relativi alla disponibilità, alla ritrasmissione e ai timeout del server vengono gestiti dai dispositivi abilitati per RADIUS anziché dal protocollo di trasmissione.

RADIUS è un protocollo client/server

Il client RADIUS è in genere un server NAS e il server RADIUS è in genere un processo daemon eseguito su un computer UNIX o Windows NT. Il client passa le informazioni utente ai server RADIUS designati e interviene sulla risposta restituita. I server RADIUS ricevono le richieste di connessione degli utenti, autenticano l'utente e quindi restituiscono le informazioni di configurazione necessarie al client per fornire il servizio all'utente. Un server RADIUS può fungere da client proxy per altri server RADIUS o altri tipi di server di autenticazione.

Nella figura viene illustrata l'interazione tra un utente connesso e il client e il server RADIUS.



Interazione tra l'utente della connessione remota e il client e il server RADIUS

1. L'utente avvia l'autenticazione PPP sul server NAS.
2. Il server NAS richiede il nome utente e la password (se Password Authentication Protocol [PAP]) o la richiesta (se Challenge Handshake Authentication Protocol [CHAP]).
3. L'utente risponde.
4. Il client RADIUS invia nome utente e password crittografata al server RADIUS.
5. Il server RADIUS risponde con Accept, Reject o Challenge.
6. Il client RADIUS agisce sui servizi e i parametri dei servizi forniti con Accept o Reject.

Autenticazione e autorizzazione

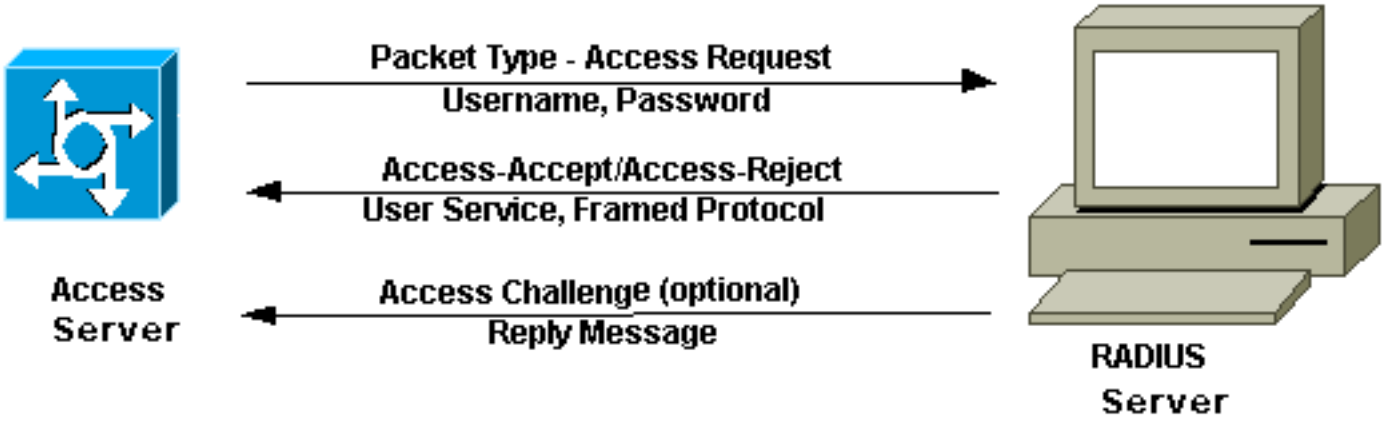
Il server RADIUS può supportare diversi metodi per autenticare un utente. Quando viene fornito con il nome utente e la password originale forniti dall'utente, può supportare i meccanismi di autenticazione PPP, PAP o CHAP, UNIX e altri.

In genere, un accesso utente è costituito da una query (Access-Request) dal server NAS al server RADIUS e da una risposta corrispondente (Access-Accept o Access-Reject) dal server. Il pacchetto Access-Request contiene il nome utente, la password crittografata, l'indirizzo IP NAS e la porta. La distribuzione iniziale di RADIUS è stata eseguita con la porta UDP numero 1645, in conflitto con il servizio "Data Metrics". A causa di questo conflitto, la RFC 2865 ha assegnato ufficialmente il numero di porta 1812 per RADIUS. La maggior parte dei dispositivi e delle applicazioni Cisco supporta entrambi i tipi di numeri di porta. Il formato della richiesta fornisce inoltre informazioni sul tipo di sessione che l'utente desidera avviare. Se ad esempio la query viene presentata in modalità carattere, l'inferenza sarà "Service-Type = Exec-User", ma se la

richiesta viene presentata in modalità pacchetto PPP, l'inferenza sarà "Service Type = Framed User" e "Framed Type = PPP".

Quando il server RADIUS riceve la richiesta di accesso dal server NAS, cerca in un database il nome utente elencato. Se il nome utente non esiste nel database, viene caricato un profilo predefinito oppure il server RADIUS invia immediatamente un messaggio di rifiuto di accesso. Questo messaggio di accesso/rifiuto può essere accompagnato da un messaggio di testo che indica il motivo del rifiuto.

In RADIUS, autenticazione e autorizzazione sono associate. Se viene trovato il nome utente e la password è corretta, il server RADIUS restituisce una risposta di accettazione dell'accesso, che include un elenco di coppie attributo-valore che descrivono i parametri da utilizzare per questa sessione. I parametri tipici includono il tipo di servizio (shell o framed), il tipo di protocollo, l'indirizzo IP da assegnare all'utente (statico o dinamico), l'elenco degli accessi da applicare o una route statica da installare nella tabella di routing NAS. Le informazioni di configurazione nel server RADIUS definiscono ciò che può essere installato sul NAS. Nella figura seguente viene illustrata la sequenza di autenticazione e autorizzazione RADIUS.



Sequenza di autenticazione e autorizzazione RADIUS

Contabilità

Le funzionalità di accounting del protocollo RADIUS possono essere utilizzate indipendentemente dall'autenticazione o dall'autorizzazione RADIUS. Le funzioni di accounting RADIUS consentono l'invio di dati all'inizio e alla fine delle sessioni, ovvero la quantità di risorse (ad esempio tempo, pacchetti, byte e così via) utilizzate durante la sessione. Un provider di servizi Internet (ISP, Internet Service Provider) può utilizzare il software di contabilità e controllo degli accessi RADIUS per soddisfare esigenze specifiche di sicurezza e fatturazione. La porta di accounting per RADIUS per la maggior parte dei dispositivi Cisco è 1646, ma può anche essere 1813 (a causa della modifica delle porte specificata nella RFC 2139).

Le transazioni tra il client e il server RADIUS vengono autenticate tramite l'utilizzo di un segreto condiviso che non viene mai inviato in rete. Inoltre, le password utente vengono inviate in modo crittografato tra il client e il server RADIUS per evitare che un utente che utilizza lo snooping su una rete non protetta possa determinare una password utente.

Informazioni correlate

- Protocolli di autenticazione
- RFC (Requests for Comments)

- Supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).