# Comparação TACACS+ e RADIUS

## Contents



## Introduction

Dois protocolos de segurança proeminentes usados para controlar o acesso às redes são Cisco TACACS+ e RADIUS. A especificação do RADIUS é descrita na RFC 2865 , a qual substitui a RFC 2138. A Cisco tem o compromisso de oferecer suporte a ambos os protocolos com as melhores ofertas da classe. Não é a intenção de Cisco competir com o RADIUS ou influenciar os usuários a adotarem o TACACS+. Você deve escolher a solução que melhor atenda às suas necessidades. Esse documento discute as diferenças entre TACACS+ e RADIUS, para que você possa fazer uma escolha mais informada.

A Cisco oferece suporte ao protocolo RADIUS desde o Cisco IOS® Software Release 11.1 de fevereiro de 1996. A Cisco continua a aprimorar o cliente RADIUS com novos recursos e capacidades, e oferece suporte ao RADIUS como um padrão.

A Cisco avaliou seriamente o RADIUS como um protocolo de segurança antes de desenvolver o TACACS+. Muitos recursos foram incluídos no protocolo TACACS+ para atender às necessidades do mercado de segurança em expansão constante. O protocolo foi projetado para ser dimensionado ao crescimento das redes e para se adaptar à nova tecnologia de segurança à medida que o mercado se desenvolve. A arquitetura subjacente do protocolo TACACS+

complementa a arquitetura independente de autenticação, autorização e contabilidade (AAA).

# Prerequisites

## Requirements

Não existem requisitos específicos para este documento.

## Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

## Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

# Fundamentos do RADIUS

O RADIUS é um servidor de acesso que usa o protocolo AAA. Trata-se de um sistema de segurança distribuída que protege o acesso remoto a redes e serviços de rede contra o acesso não autorizado. O RADIUS é composto por três componentes:

- Um protocolo com um formato de frame que utiliza o User Datagram Protocol (UDP) /IP.
- Um server.
- Um cliente.

O servidor é executado em um computador central, em geral no local do cliente, enquanto que os clientes residem nos servidores de acesso dial-up e podem ser distribuídos em toda a rede. A Cisco incorporou o cliente RADIUS no Cisco IOS Software Release 11.1 e posteriores e no software de outros dispositivos.

## Modelo de cliente/servidor

Um Servidor de Acesso à Rede (NAS) atua como um cliente RADIUS. O cliente é responsável por fornecer as informações de usuário para os servidores RADIUS definidos e, em seguida, processar a resposta devolvida. Os servidores RADIUS são responsáveis por receber os requisitos de conexão do usuário, autenticar o usuário e retornar todas as informações de configuração necessárias para que o cliente forneça o serviço ao usuário. Os servidores RADIUS podem funcionar como clientes proxy para outros tipos de servidores de autenticação.

## Segurança de rede

As transações entre o cliente e o servidor RADIUS são autenticadas utilizando um segredo compartilhado, que nunca é enviado na rede. Além disso, todas as senhas de usuário são enviadas criptografadas entre o cliente e o servidor RADIUS. Isso elimina a possibilidade de alguém espionando uma rede não protegida descobrir uma senha de usuário.

## Mecanismos de autenticação flexível

O servidor RADIUS oferece suporte a vários métodos de autenticação de usuários. Quando ele recebe o nome de usuário e a senha original fornecidos pelo usuário, ele pode oferecer suporte ao PPP, Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), login do UNIX e a outros mecanismos de autenticação.

### Disponibilidade do código de servidor

Há várias distribuições de código de servidor disponíveis comercial e gratuitamente. Os servidores Cisco incluem o Cisco Secure ACS for Windows, o Cisco Secure ACS para UNIX, e o Cisco Access Registrar.

## Comparar o TACACS+ e o RADIUS

Estas seções comparam os vários recursos do TACACS+ e do RADIUS.

### UDP e TCP

O RADIUS usa UDP, enquanto que o TACACS+ usa TCP. O TCP oferece diversas vantagens em relação ao UDP. O TCP oferece transporte orientado por conexão, enquanto o UDP a entrega pelo melhor esforço. O RADIUS requer variáveis programáveis adicionais, como tentativas de retransmissão e timeouts para compensar o empenho máximo de transporte, mas não tem o nível de suporte interno que um transporte TCP oferece:

- O uso do TCP fornece um reconhecimento separado de que um pedido foi recebido dentro de (aproximadamente) um Round-Trip Time (RTT) da rede, independentemente do quão carregado e lento o mecanismo de autenticação backend (um reconhecimento de TCP) pode estar.
- O TCP fornece indicação imediata de um servidor travado ou que não esteja em execução, por meio de uma reinicialização (RST). Você pode determinar quando um servidor trava e volta a funcionar usando conexões TCP de longa duração. O UDP não pode informar a diferença entre um servidor que está inativo, um servidor lento e um servidor inexistente.
- Utilizando manutenções de atividade de TCP, os travamentos de servidor podem ser detectados fora de banda com solicitações reais. As conexões para vários servidores podem ser mantidas simultaneamente, e você precisa apenas enviar mensagens àqueles que sabe que estão funcionando.
- O TCP é mais dimensionável e se adapta tanto a redes em crescimento quanto a redes congestionadas.

### Criptografia de Pacotes

O RADIUS criptografa somente a senha no pacote de solicitação de acesso, do cliente para o servidor. O restante do pacote não é criptografado. Outras informações, como o nome de usuário, serviços autorizados e contabilidade, podem ser capturadas por terceiros.

O TACACS+ criptografa todo o corpo do pacote, mas deixa um cabeçalho TACACS+ padrão. No cabeçalho há um campo que indica se o corpo está ou não criptografado. Para fins de depuração, é útil ter o corpo dos pacotes não criptografados. No entanto, durante a operação normal, o corpo do pacote é totalmente criptografado para proporcionar comunicações mais seguras.

## Autenticação e Autorização

O RADIUS combina autenticação e autorização. Os pacotes de aceitação acesso enviados pelo servidor RADIUS ao cliente contêm as informações de autorização. Isso dificulta a separação da autenticação da autorização.

O TACACS+ usa a arquitetura AAA, que separa AAA. Isso permite soluções de autenticação separadas que ainda podem usar o TACACS+ para autorização e relatório. Por exemplo, com o TACACS+, é possível usar a autenticação Kerberos e a autorização TACACS+ e a contabilidade. Depois que um NAS se autentica em um servidor Kerberos, ele solicita as informações de autorização de um servidor TACACS+ sem ter que autenticar novamente. O NAS informa ao servidor TACACS+ que houve êxito na autenticação em um servidor Kerberos, e o servidor então fornece as informações de autorização.

Durante uma sessão, se uma verificação de autorização adicional for necessária, o servidor de acesso verificará com um servidor TACACS+ para determinar se o usuário receberá permissão para usar um comando específico. Isso proporciona mais controle sobre os comandos que podem ser executados no servidor de acesso durante o desacoplamento do mecanismo de autenticação.

## Suporte a Vários Protocolos

O RADIUS não oferece suporte a estes protocolos:

- Protocolo AppleTalk Remote Access (ARA)
- Protocolo NetBIOS Frame Protocol Control
- Novell Asynchronous Services Interface (NASI)
- Conexão PAD X.25

O TACACS+ oferece suporte a vários protocolos.

## Gerenciamento de Roteadores

O RADIUS não permite aos usuários controlar quais comandos podem ou não ser executados em um roteador. Consequentemente, o RADIUS não é tão útil para o gerenciamento de roteadores ou tão flexível para os serviços de terminal.

O TACACS+ fornece dois métodos para controlar a autorização dos comandos do roteador por usuário ou por grupo. O primeiro método é atribuir níveis de privilégio a comandos e fazer com que o roteador verifique com o servidor TACACS+ se o usuário tem ou não autorização no nível de privilégio especificado. O segundo método é especificar explicitamente os comandos permitidos no servidor TACACS+, por grupo ou por usuário.

## Interoperabilidade

Devido às várias interpretações das Request For Comments (RFCs) do RADIUS, a conformidade com as RFCs do RADIUS não garante a interoperabilidade. Mesmo que diversos fornecedores implementem clientes RADIUS, isso não significa que eles sejam interoperáveis. A Cisco implementa a maioria dos atributos RADIUS e adiciona consistentemente mais. Se os clientes usam somente os atributos RADIUS padrão em seus servidores, eles poderão trabalhar com diversos fornecedores, desde que esses fornecedores implementem os mesmos atributos. No entanto, muitos fornecedores implementam extensões que são atributos proprietários. Se um

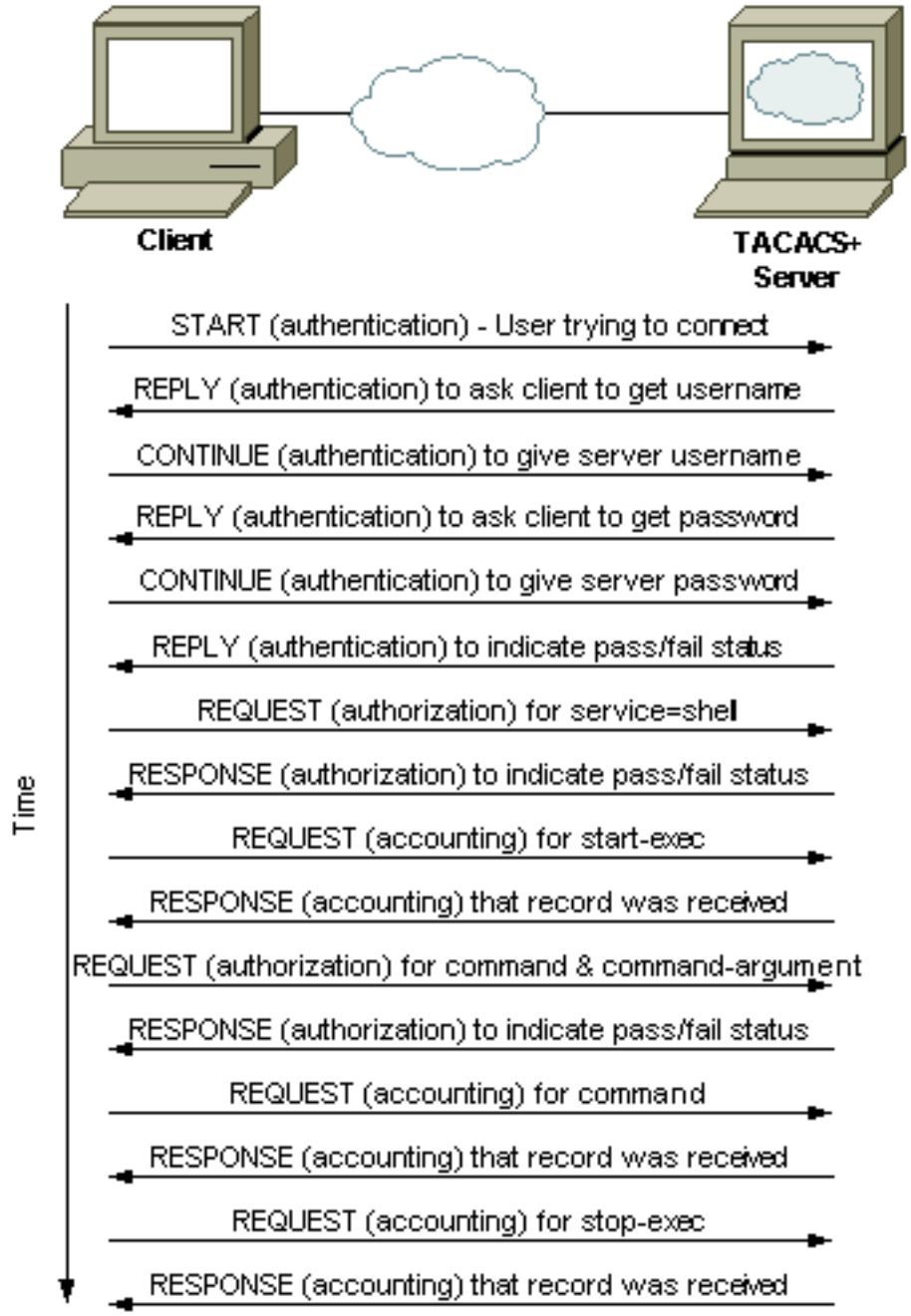
cliente usa um desses atributos estendidos específicos do fornecedor, a interoperabilidade não é possível.

## Tráfego

Devido às diferenças previamente mencionadas entre o TACACS+ e o RADIUS, a quantidade de tráfego gerada entre o cliente e o servidor varia. Estes exemplos ilustram o tráfego entre o cliente e o servidor para TACACS+ e RADIUS quando utilizados para gerenciamento de roteador com autenticação, autorização de execução, autorização de comando (que o RADIUS não pode fazer), contabilização de execução e de comando (que o RADIUS não pode fazer).

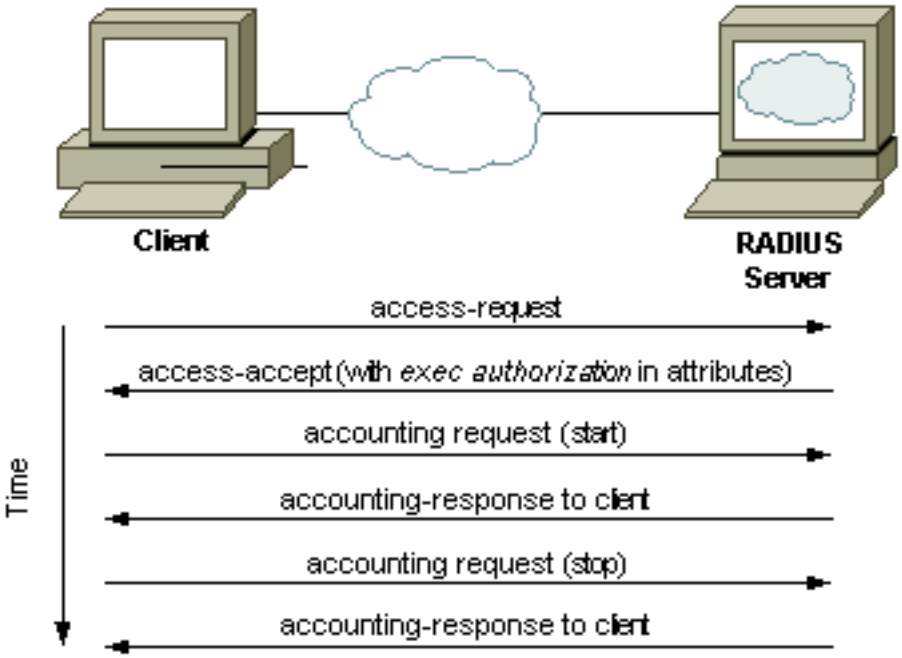
### Exemplo de Tráfego TACACS+

Este exemplo presume que a autenticação de login, a autorização de execução, a autorização de comandos, a contabilidade de execução de início-parada e a contabilidade de comandos são implementadas com o TACACS+ quando um usuário se conecta a um roteador via Telnet, executa um comando e sai do roteador:




## Exemplo de Tráfego RADIUS

Esse exemplo presume que a autenticação de logon, a autorização de execução e o relatório de execução de início-parada são implementados com RADIUS quando um usuário se liga pela Telnet a um roteador, executa um comando e sai do roteador (outros serviços de gerenciamento não estão disponíveis):




## Suporte a Dispositivos

Esta tabela lista o suporte ao recurso de AAA do TACACS+ e RADIUS por tipo de dispositivo para as plataformas selecionadas. Isso inclui a versão de software na qual o suporte foi adicionado. Verifique as Release Notes do Produto para obter mais informações se o seu produto não estiver na lista.

| Dispositivo Cisco | Autenticação TACACS+ | Autorização TACACS+ | Contabilidade TACACS+ | Autenticação RADIUS | Autorização RADIUS | Contabilidade RADIUS |
|---|---|---|---|---|---|---|
| Cisco Aironet [1] | 12.2(4)JA | 12.2(4)JA | 12.2(4)JA | todos os access points | todos os access points | todos os access points |
| Software Cisco IOS [2] | 10,33 | 10,33 | 10.333 | 11.1.1 | 11.1.14 | 11.1.15 |
| Cisco Cache Engine | — | — | — | 1,5 | 1.56 | — |
| Cisco Catalyst Switches | 2,2 | 5.4.1 | 5.4.1 | 5.1 | 5.4.14 | 5.4.15 |
| Cisco CSS 11000 | 5,03 | 5,03 | 5,03 | 5,0 | 5.04 | — |

| | | | | | | |
|---|---|---|---|---|---|---|
| Content Services Switch | | | | | | |
| Cisco CSS 11500 Content Services Switch | 5,20 | 5,20 | 5,20 | 5,20 | 5.204 | — |
| Cisco PIX Firewall | 4,0 | 4.07 | 4.28,5 | 4,0 | 5.27 | 4.28,5 |
| Cisco Catalyst 1900/2820 Switches | 8.x enterprise[9] | — | — | — | — | — |
| Cisco Catalyst 2900XL/3500XL Switches | 11.2.(8)SA610 | 11.2.(8)SA610 | 11.2.(8)SA610 | 12.0(5)WC511 | 12.0(5)WC5[11, 4] | 12.0(5)WC5[1, 5] |
| Concentrador Cisco VPN 3000 [6] | 3.0 | 3.0 | — | 2.012 | 2.0 | 2.012 |
| Cisco VPN 5000 Concentrator | — | — | — | 5.2X12 | 5.2X12 | 5.2X12 |

notas da tabela

1. Terminação somente de clientes wireless, e não do tráfego de gerenciamento em versões diferentes do Cisco IOS Software Release 12.2(4)JA ou posterior. No Cisco IOS Software Release 12.2.(4)JA ou posterior, a autenticação para a terminação dos clientes wireless e do tráfego de gerenciamento é possível.
2. Consulte o Feature Navigator (agora substituído pelo Software Advisor (somente clientes registrados)) para obter informações sobre o suporte a plataformas no Cisco IOS Software.
3. A contabilidade de comandos não foi implementada até o Cisco IOS Software Release 11.1.6.3.

4. Sem autorização de comandos.
5. Sem contabilidade do comandos.
6. Bloqueio de URL somente, e não de tráfego administrativo.
7. Autorização para o tráfego não-VPN via PIX.**Nota:** Versão 5.2 - Suporte de lista de acesso para Access Control List (ACL) RADIUS Vendor-Specific Attribute (VSA) ou autorização TACACS+ para tráfego VPN terminando no PIX Versão 6.1 - suporte para autorização de atributo 11 RADIUS da ACL para tráfego VPN terminando no PIX Versão 6.2.2 - suporte para ACLs descarregáveis com autorização RADIUS para tráfego VPN na terminação PIX Versão 6.2 - suporte para autorização para tráfego de gerenciamento de PIX através do TACACS+.
8. Contabilidade de tráfego não-VPN via PIX somente, e não de tráfego de gerenciamento.**Observação:** Versão 5.2 - Suporte para contabilização de pacotes TCP do cliente VPN através do PIX.
9. Somente software Enterprise.
10. Necessita de Flash de 8 M para a imagem.
11. Somente terminação VPN.

## Informações Relacionadas

- Página de suporte RADIUS
- TACACS+ na Documentação do IOS
- Página de Suporte do TACACS/TACACS+
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems