InkBridge Networks

July 20, 2026

Evaluating TACACS+ Solutions for Multi-Vendor Networks

White Paper

By Arran Cudbard-Bell, CTO and Nick Porter, Director of Engineering

Most organisations don't discover that their TACACS+ solution has minimal policy support after they've committed to it, when deploying new network gear or policies becomes a months-long bottleneck instead of a routine configuration change.

Contents

1. Executive Summary 3
2. The multi-vendor challenge: Why TACACS+ flexibility matters 4
3. How vendor implementations differ (and why documentation won't help) 6
4. Supporting new vendors: Process and timeline 10
5. Common implementation problems 14
6. The ISE migration question 17
7. Evaluating TACACS+ solutions: A decision framework 19
8. Conclusion: Making the choice 21

1. Executive Summary

You're managing network infrastructure with Cisco routers, Juniper switches, and Arista data centre equipment. Every piece of equipment performs administrator authentication and authorisation through your TACACS+ server. But what happens when you add a piece of equipment that your TACACS+ vendor hasn't tested, or which requires a new policy?

This paper addresses the questions prospects discover too late—the ones that determine whether your TACACS+ solution enables or constrains your network strategy.

Based on deployments with major ISPs and enterprises managing heterogeneous network environments, we examine:

- Why vendor implementations differ despite standards compliance
- What actually happens when you deploy new devices
- The problems that emerge during implementation
- How to evaluate TACACS+ solutions effectively

The TACACS+ protocol is straightforward: it just carries text strings which (in theory) are well defined. The complexity comes from vendor diversity in implementation, documentation gaps that force discovery through testing, and legacy configurations that accumulated without proper documentation.

2. The multi-vendor challenge: Why TACACS+ flexibility matters

Your network isn't a monoculture, and it shouldn't be. Multi-vendor environments give you negotiating leverage, prevent single points of failure, and let you choose the best equipment for each use case. But most TACACS+ solutions work well in homogeneous environments and struggle when confronted with vendor diversity.

Starting with standards compliance

TACACS+ is defined in RFC 8907, published in September 2020. The protocol provides a framework for device administration, authenticating network administrators and authorising which commands they can run on routers, switches, and other network equipment.

Vendors claim standards compliance. From a protocol perspective, they deliver it. The challenge lies in what RFC 8907 actually specifies versus what it leaves open to interpretation. The difficulty is that vendors were shipping TACACS+ implementations for decades before RFC8907 was published. So, there is often a substantial difference between what they support, and what the RFC says should exist. That difference makes any TACACS+ system more complicated than it otherwise should be.

Where flexibility matters

Several scenarios demand TACACS+ solutions that can adapt to any vendor's implementation:

Acquisitions and mergers: When you acquire a company, you inherit their equipment choices. You might inherit decades of equipment from multiple organisations. You either have or need a TACACS+ solution that works across 5–10 different types of network equipment. And you need this to work without requiring months of development and integration.

Equipment refresh cycles: Your five-year equipment refresh doesn't align with your TACACS+ vendor's development roadmap. When you select new equipment based on features and pricing, your authentication infrastructure needs to support it.

Best-of-breed strategy: Cisco excels at certain functions, Juniper at others, Arista at still others. Selecting the best equipment for each use case means your TACACS+ server must speak to all of them.

InkBridge Networks

The bottleneck problem

If your TACACS+ solution requires a software release every time you need to support a new policy or a new vendor, you've created a bottleneck. Your network expansion waits for your TACACS+ vendor's testing schedule and development priorities.

The alternative is a TACACS+ implementation that can adapt to any policy and to any vendor's approach through configuration rather than software changes.

This paper examines what that flexibility requires and how to evaluate whether a TACACS+ solution provides it. We'll cover:

- How vendor implementations actually differ.
- The discovery and configuration process.
- The common problems that emerge.
- Cisco ISE migration specifically.
- A comprehensive evaluation framework.

3. How vendor implementations differ (and why documentation won't help)

RFC 8907 defines how to structure the conversation between network equipment and your TACACS+ server. It specifies packet formats, authentication flows, and accounting procedures. What it doesn't specify is exactly how vendors should use these mechanisms.

This section explains the variations you'll encounter and why vendor documentation typically won't prepare you for them.

The three authorisation models

Vendors implement TACACS+ authorisation in a few different ways. All three approaches comply with RFC 8907. All three require different configuration on your TACACS+ server.

Command-by-command authorisation

Every time an administrator types a command, the equipment sends an authorisation request to your TACACS+ server: "Should I let them do this?" Your server responds with "yes" or "no" for each individual command.

This provides granular control. An administrator might be authorised to run "show" commands for viewing configuration but not "set" commands for making changes. The equipment validates each command with the TACACS+ server before executing it.

The trade-off is protocol traffic volume. In an active session, the equipment can send dozens or hundreds of authorisation requests during one administrator session. This large volume becomes a problem when automated systems log in to each piece of equipment to perform status checks. For a large network, this traffic can quickly turn into hundreds of thousands of authorisation queries every few minutes.

Authorisation with privilege levels

The equipment sends a single authorisation request immediately after login. Your TACACS+ server responds with a privilege level: "assign them to privilege level 2". The list of commands that are allowed at each privilege level is statically configured on the equipment. Once set, the equipment doesn't send additional authorisation requests during the session.

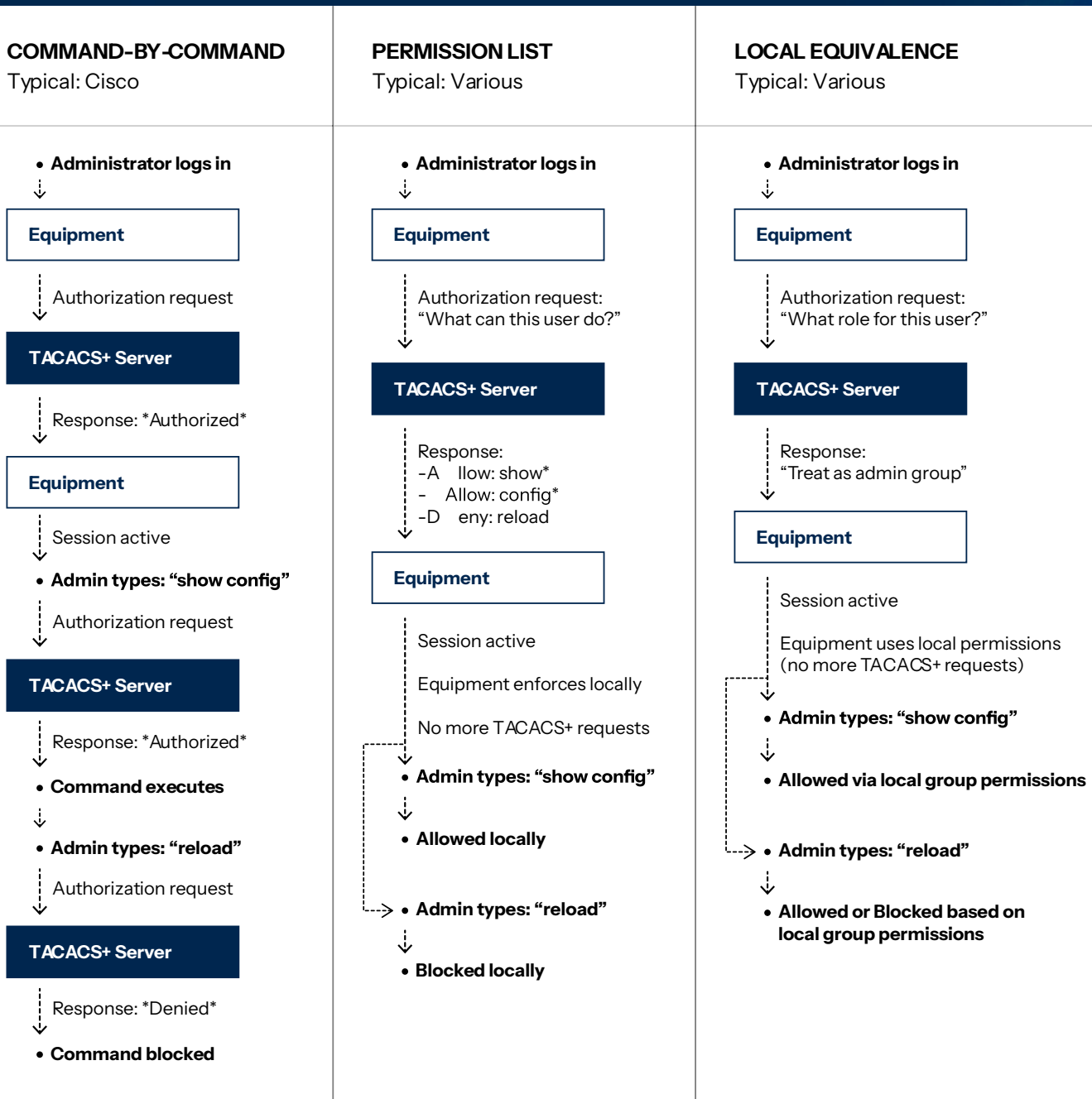
The administrator's permissions are determined at login based on the list your server provides. The equipment enforces those permissions locally without further TACACS+ interaction.

InkBridge Networks

Local equivalence authorisation

After login, the equipment sends an authorisation request. Your TACACS+ server responds: “Treat this person as if they’re a member of this local group” or “Treat them as this local user”. The equipment then uses its own local permission system without further TACACS+ interaction.

This approach works well when the equipment has a well-defined local permission structure. You map your administrators to existing local roles rather than defining permissions through TACACS+.



InkBridge Networks

Attribute format variations

Unlike RADIUS, DNS, or DHCP, TACACS+ is string-based protocol. That is, TACACS+ attributes are text-based name-value pairs. Vendors use different attribute names and expect different value formats for the same logical function. In fact, it is perfectly valid for a TACACS+ system to send a string such as "hello=today", or even "purple=cold"!

This flexibility allows vendors to easily extend TACACS+ with their own definitions. The downside is that unless the vendor documents the attributes and values that they use, you're stuck. There is no way to know what those attributes are, what they mean, or what values they expect!

While our TACACS+ server can accept every possible attribute, with any possible value, it is still hard to create meaningful policies when you don't know what those things mean. The result is that any TACACS+ project has to include time provisions for figuring out exactly what is going on. These provisions can be a source of risk in any project.

Timestamp format: RFC 8907 specifies that timestamps should include time zone information. One vendor we encountered was sending timestamps without the time zone, making it impossible to determine whether the timestamp represented UTC or local time. This creates ambiguity in audit logs and requires additional logic to interpret timestamps correctly.

Username restrictions: One customer discovered that their equipment didn't support the @ symbol in usernames. This wasn't a TACACS+ protocol limitation; rather, it was a vendor implementation decision. Administrators using email addresses as usernames (a common organisational pattern) couldn't authenticate to that equipment.

Privilege level representation: Different vendors use different attribute names and different numeric ranges to represent privilege levels. Some use 0-15, others use 0-7, still others use text strings rather than numbers.

These variations aren't documented comprehensively. In many cases, you can only discover them during deployment. This limitation makes deployments complex and frustrating.

As the TACACS+ experts, we often get questions from customers about what kind of TACACS+ functionality is supported by their networking equipment. Unfortunately, in most cases, only the equipment vendor can answer that question. There are dozens of vendors of networking equipment, each of whom may have dozens or hundreds of products. While we have significant experience with TACACS+, there is always the possibility that we will run into surprises or unknowns. Customers should be aware of these protocol limitations and plan accordingly.

In the end, the only way to determine what a product does is to check the vendor documentation.

InkBridge Networks

The documentation gap

Vendor documentation for TACACS+ configuration typically provides about three pages of instructions:

1. Enter your TACACS+ server IP address.
2. Enter your shared secret.
3. Enable TACACS+ authentication.

What's consistently missing:

- Which authorisation model does this vendor use?
- What attributes does the equipment expect in authorisation responses?
- What format should those attributes take?
- What does the request-response flow look like?

We've worked with major ISPs managing millions of users who couldn't answer these questions about their own deployed equipment. In one deployment, a customer team had ten people reviewing their TACACS+ implementation, and none of them knew what their system was actually doing. The knowledge had been lost during a corporate acquisition.

Equipment vendors all too often assume you already understand their specific TACACS+ implementation. The documentation tells you where to configure it, not how it actually works.

Authentication method variations

Most equipment supports PAP (Password Authentication Protocol), straightforward username and password submission. Some equipment also supports ASCII authentication, which uses a challenge-response flow where the TACACS+ server sends prompts that display on the administrator's screen.

ASCII authentication matters for multi-factor authentication deployments. Several MFA methods require the ability to send challenge prompts and receive responses.

We've encountered network equipment that didn't implement ASCII authentication correctly. Some equipment initially didn't support displaying challenge information, which prevented customers from deploying one-time password systems. The customer raised a feature request with the vendor, who eventually added proper support, but the initial deployment plan required revision.

If MFA is in your requirements, you need to verify ASCII authentication support before finalising your design. This limitation isn't always documented in vendor materials.

Why this matters for evaluation

When evaluating TACACS+ solutions, asking "Do you support Cisco?" or "Do you support Juniper? takes too narrow a focus. The critical question is: "How do you handle vendors whose implementation details aren't fully documented?"

The answer reveals whether the solution architecture allows adaptation through configuration or requires software releases for each new vendor variation.

InkBridge Networks

4. Supporting new vendors: Process and timeline

When you introduce new network equipment to your TACACS+ infrastructure, you need to validate that authentication and authorisation work correctly with that vendor's implementation. This section explains the discovery process and what determines the timeline.

What requires validation

Authentication method support: Does the equipment support the authentication methods you need? If your security requirements include multi-factor authentication, the equipment must support ASCII authentication (challenge-response). Equipment that only supports PAP won't work with most MFA implementations.

Attribute format compliance: Does the equipment send attributes in the format specified by RFC 8907? Format issues typically surface during testing. They require troubleshooting because they're not documented in vendor materials.

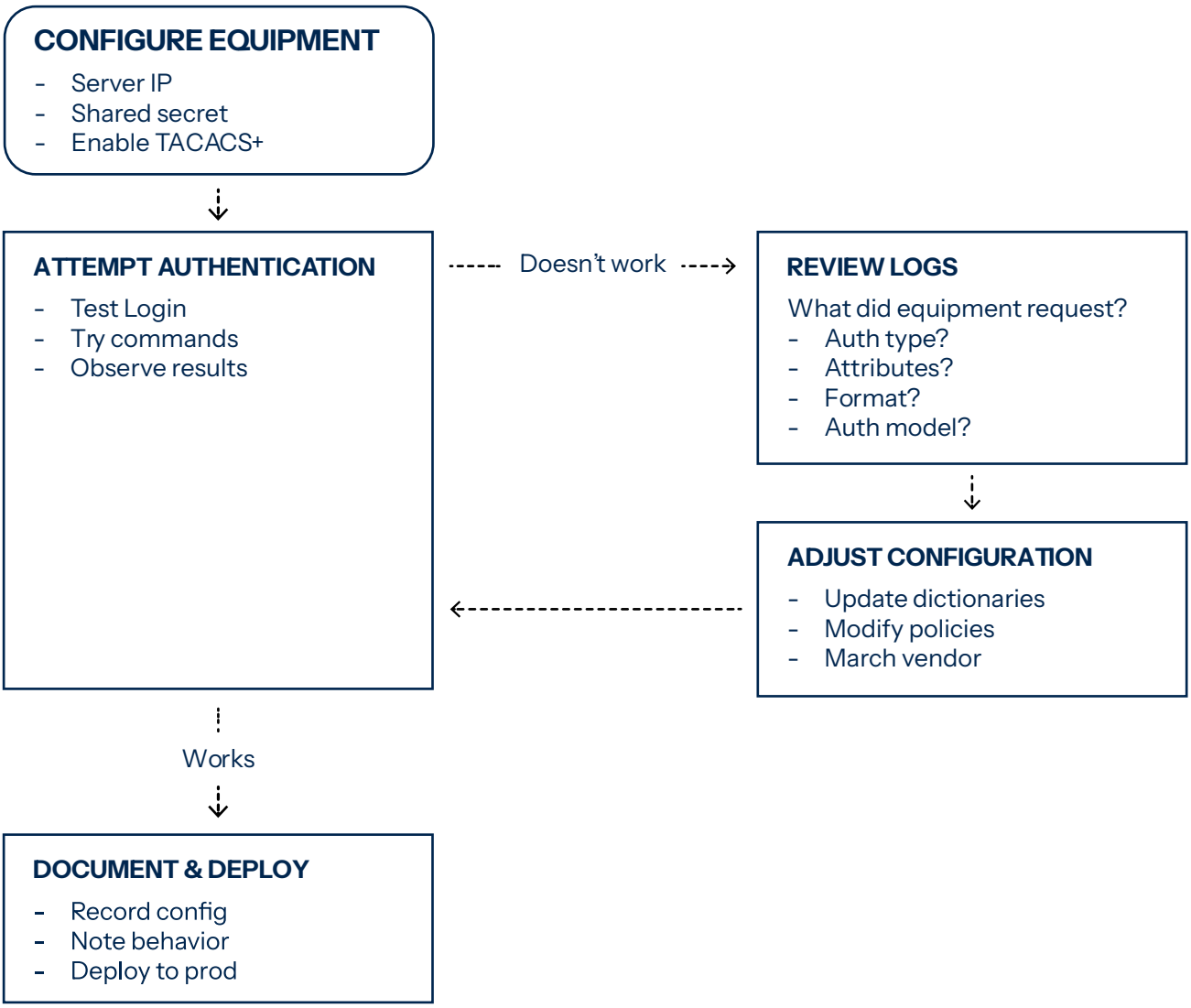
Authorisation behaviour: How does this vendor use TACACS+ for authorisation? Does it authorise every command individually? Does it request authorisation once at login and expect a permission list? Does it expect local user equivalence? Understanding this determines how you configure server policies.

InkBridge Networks

Discovery in greenfield deployments

For new equipment in a test environment, the process is iterative:

1. Configure the equipment to use your TACACS+ server.
2. Attempt authentication and authorisation.
3. Review TACACS+ server logs to see what the equipment requested.
4. Adjust server configuration to provide what the equipment expects.
5. Test again.
6. Repeat until behaviour matches requirements.



The timeline depends on several factors:

Vendor documentation quality: Typically poor. Most vendors provide minimal TACACS+ documentation.

Similarity to known vendors: Cisco variants often behave similarly to each other. Equipment from vendors you haven't encountered may require more discovery work.

Authorisation complexity: Command-by-command authorisation requires more policy definition than simple privilege level assignment.

For straightforward implementations with reasonable vendor documentation: adding a new vendor could take hours to a few days. For equipment with poor documentation or complex authorisation requirements, that timeline could extend to weeks.

Discovery in brownfield migrations

When migrating from an existing TACACS+ infrastructure, you can capture current traffic to understand expected behaviour. Use packet capture tools (Wireshark filters on TCP port 49) to observe the request-response patterns between your equipment and your current TACACS+ server.

This approach reveals what's actually happening versus what documentation claims should happen. We've worked with customers who needed to analyse old TACACS+ server source code because no documentation existed for their legacy implementation. In one case, a spin-off organisation had no one who understood what their inherited TACACS+ system was doing. The knowledge had remained with the parent company.

Packet analysis shows:

- Which authentication methods the equipment uses
- What attributes it sends in authorisation requests
- What attributes it expects in authorisation responses
- The sequence and timing of the protocol exchange

You can then build new TACACS+ policies to replicate the existing behaviour.

Configuration approaches

Software release dependency: Some TACACS+ solutions require software updates to support new vendor attributes. Each vendor variation needs to be coded into the product. You then need to wait for your TACACS+ vendor's development schedule to align with your deployment needs.

Dictionary-based configuration: Flexible implementations use dictionaries, i.e. text configuration files that define vendor-specific attributes. Adding support for a new vendor's attribute format means updating the dictionary file. This is a configuration change, not a software change. It requires no programming and can happen in hours rather than months.

At the protocol level, TACACS+ attributes are text-based name-value pairs. The protocol itself doesn't limit vendor support. The limitations come from how TACACS+ solutions are architected.

InkBridge Networks

When software upgrades are required

Software upgrades become necessary when the TACACS+ standard itself changes. RFC 8907 was published in 2020. The previous TACACS+ documentation dates to the 1990s. Protocol-level changes are infrequent and measured in decades, not years.

New protocol extensions (such as draft standards for SSH keys with TACACS+) require software changes. However, these are strategic additions that expand capabilities, not routine updates for vendor support.

The past 20 years of TACACS+ deployment haven't required protocol-level software changes to support different vendor equipment.

The experience factor

TACACS+ vendors with substantial multi-vendor deployment experience have typically encountered most implementation variations. They've worked through the Cisco authorisation model, the Juniper approach, and the ways various other vendors interpret the standard.

This experience means faster discovery and fewer surprises. When you describe your equipment mix, experienced vendors can often predict the challenges you'll encounter and the configuration approach that will work.

5. Common implementation problems

These problems emerge from deployments with major ISPs and enterprise customers. They typically surface during implementation or shortly after go-live.

Problem 1: MFA authentication method incompatibility

Multi-factor authentication requires challenge-response authentication (ASCII authentication in TACACS+ terminology). The TACACS+ server sends a challenge that displays on the administrator's screen. The administrator enters additional information (such as a one-time password). The server validates it.

Some network equipment vendors don't implement ASCII authentication correctly. The equipment may only support PAP, or it may implement ASCII authentication but not display challenge information properly.

Some equipment initially didn't support displaying challenge information to the user. Customers couldn't deploy one-time password systems because the OTP prompt never appeared on the administrator's screen. The customer raised a feature request with the vendor. The vendor eventually added proper ASCII authentication support, but the customer's initial MFA deployment plan required revision.

Impact: If MFA is in your requirements and your equipment doesn't support ASCII authentication correctly, you either need to change vendors, wait for vendor support, or revise your security approach.

What to check: Test ASCII authentication with your specific equipment before finalising the design. Verify that challenges display as intended and responses are processed properly.

Problem 2: Legacy configuration accumulation

TACACS+ configurations grow over 15–20 years in brownfield environments. Organisations add rules and permissions but rarely remove them. The original implementers leave. Documentation doesn't exist or hasn't been updated.

One organisation inherited TACACS+ configuration from two others, and they had "morphed over the years into a bit of a mess," in one engineer's words. Understanding what should actually be happening required substantial reverse-engineering effort.

Impact: Cleaning up legacy configuration is often the largest effort in TACACS+ migration projects. This is an organisational challenge, not a technical one. You need to define current organisational structure, determine who needs access to which devices, establish appropriate permission levels, and map existing users to the new structure.

InkBridge Networks

This takes longer than the technical migration work.

What to plan for: Treat configuration cleanup as a separate project with dedicated time. Use the migration as an opportunity to establish proper documentation and change management processes.

Problem 3: Inadequate vendor documentation

Equipment manuals provide minimal TACACS+ configuration guidance, typically a few pages explaining where to enter the server IP address and shared secret. They don't explain which authorisation model the vendor uses, what attributes the equipment expects, or what format those attributes should take.

Discovery happens through trial and error. You configure authentication, attempt to log in, review logs to see what failed, adjust configuration, and try again.

Impact: Discovery time for poorly-documented equipment can extend from days to weeks. The effort happens during deployment when timeline pressure is highest.

What to look for: TACACS+ vendors with substantial multi-vendor deployment experience have likely already solved these problems. Ask for specific examples of how they've handled vendor implementation variations.

Problem 4: Vendor-specific authorisation models

RFC 8907 provides a framework for TACACS+ but leaves significant interpretation room around authorisation. Some equipment sends an authorisation request for every command. Other vendors send a single request at login. Still others use local equivalence.

Your server policies must adapt to each vendor's model. "One size fits all" configuration doesn't work.

InkBridge Networks

Impact: Solutions with declarative configuration and fixed options struggle with vendor diversity. You need flexibility in policy language to handle different authorisation models.

What to evaluate: Ask vendors how they handle different authorisation models. Look for procedural or scripting approaches that allow policies matching each vendor's implementation.

Problem 5: Security for internet-connected devices

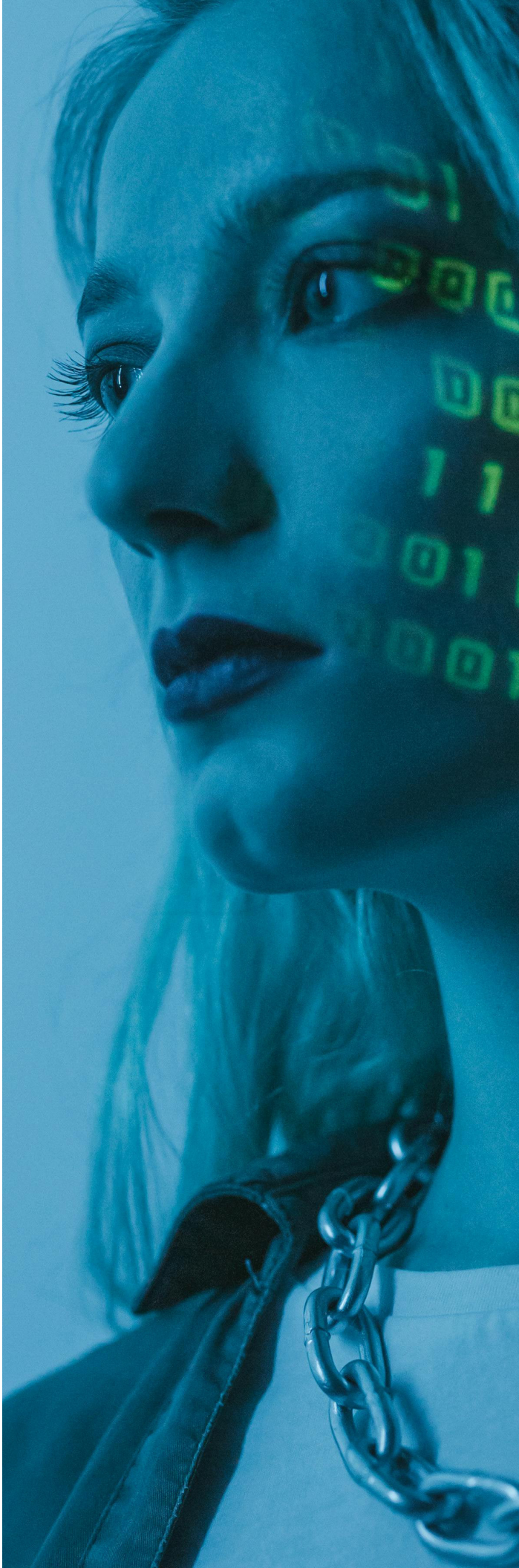
TACACS+ uses obfuscation from the 1990s. While this obfuscation hasn't been broken in ways that enable practical attacks, it doesn't meet modern cryptographic standards. This matters when TACACS+ traffic crosses the public internet.

TACACS+ is commonly used for command logging—every command an administrator runs gets sent to the server for audit purposes. This audit trail contains sensitive information. If an administrator sets a password, you don't want that value in your logs.

There is no finalised standard for TACACS+ over TLS yet, though draft standards are in progress.

Impact: For devices that communicate over the public internet, TACACS+ obfuscation alone isn't sufficient.

What to implement: Wrap TACACS+ traffic with IPSec or another secure transport mechanism for internet-facing deployments. Verify that command logging properly elides passwords and secrets.



6. The ISE migration question

Organisations considering migration from Cisco ISE often hear: “We don’t offer a 1-1 mapping from Cisco ISE configuration, but generally it’s not much work.” This section explains what that statement means.

Architectural differences

Cisco ISE and FreeRADIUS-based TACACS+ implementations take fundamentally different approaches:

Declarative vs procedural configuration: ISE presents configuration through a graphical interface of checkboxes, dropdown menus, and form fields. You declare what you want and ISE implements it in its predetermined way.

FreeRADIUS uses a policy language where you write procedures describing how to make authorisation decisions. You have conditional logic, variables, database queries, and external system integrations available.

Standalone vs integrated: ISE is designed to be a complete solution with its own user interface, configuration database, and management system. The easier deployment path is to manage everything through ISE.

FreeRADIUS-based solutions integrate with existing infrastructure. User information comes from existing LDAP or Active Directory. Authorisation policies query existing databases. Configuration integrates with existing automation tools.

What translates from ISE

The TACACS+ capabilities translate directly:

- Groups of TACACS+ client devices
- Groups of users with different permission levels
- Command authorisation rules
- Service authorisation settings
- Accounting and audit logging

If ISE can do it for TACACS+, a flexible FreeRADIUS implementation can do it.

InkBridge Networks

What changes

The configuration method changes. You're not clicking through GUI screens. You're writing policy logic that defines authorisation decisions.

This is similar to moving from Excel formulas to Python scripts. The capabilities are greater (you can do things that weren't possible in the GUI) but the approach is different.

Migration effort

Technical translation: Straightforward. The work involves understanding current authorisation policies and rewriting them in FreeRADIUS policy language.

Policy optimisation: This is where effort goes. Migration creates an opportunity to clean up accumulated legacy configuration, integrate with existing user management systems, simplify authorisation logic, and establish documentation practices.

Many organisations find that migration effort is less about FreeRADIUS complexity and more about addressing technical debt that accumulated in ISE.

The flexibility trade-off

ISE limits you to Cisco's development roadmap and integration options.

FreeRADIUS-based implementations offer unlimited customisation. If you need integration with a system that wasn't anticipated, you can build it. If you need authorisation logic that doesn't fit standard patterns, you can write it.

The trade-off is that you're writing policies rather than clicking through GUI options. For organisations with in-house expertise or strong professional services relationships, this flexibility is valuable. For organisations that prefer turnkey solutions, the ISE approach may be more comfortable.

7. Evaluating TACACS+ solutions: A decision framework

Feature checklists tell you what a TACACS+ solution can do. They don't reveal how it will perform in your specific environment. Ask these questions instead.

Multi-vendor support questions

"What happens when we deploy equipment from a vendor you haven't explicitly tested?"

This reveals architecture. Strong answers:

- "We'll update our configuration dictionaries to support it."
- "Let's capture what the equipment is sending and adjust policies."
- "We've deployed with similar vendors and can apply that experience."

Weak answers:

- "We'll need to add that to our development roadmap."
- "It should work fine." (assumption without evidence)
- "You'll have to wait for software releases."

"What's your actual experience with our specific vendors?"

Listen for concrete examples. Experience means describing specific issues encountered and how they were solved. Lack of experience means generic claims about standards compliance without specifics.

"Show examples of solving vendor-specific implementation issues."

Experienced vendors can describe specific vendor attribute formats they've handled, authorisation model variations they've accommodated, and non-standard implementations they've worked around.

Discovery and deployment questions

"How do you handle vendor-specific TACACS+ implementations?"

Strong answers explain the process for analysing vendor behaviour, determining authorisation models, tools used for discovery, and typical timelines.

Weak answers claim everything "just works" without explaining how, or can't describe a clear process.

“Walk through your discovery process for new equipment.”

This should include initial configuration, log analysis, policy adjustment, validation testing, and documentation. If the vendor can’t describe a clear process, they likely don’t have one.

Configuration flexibility questions

“How do you handle different vendor authorisation models?”

Look for policy language flexibility, ability to write conditional logic, integration with external systems, and examples of handling different models (command-by-command, permission lists, local equivalence).

Be sceptical of “our GUI has options for all that.” This limits flexibility to pre-defined options.

“Show me your policy language.”

If the vendor uses procedural configuration, examine example policies. Evaluate readability, support for conditional logic, integration capabilities, and complexity management.

If the vendor uses declarative configuration, ask what happens when you need something the GUI doesn’t support.

Migration support questions

“Walk me through a typical ISE migration.”

Strong answers address understanding current configuration, translating authorisation policies, integration with existing directories, timeline estimates, testing approach, and cutover strategy.

Weak answers claim it’s “straightforward” without explaining why or how, or can’t provide timeline estimates.

“How do you handle legacy configuration cleanup?”

This reveals whether they understand organisational challenges: defining current roles, mapping users to new structure, documentation requirements, and change management.

Vendors who focus only on technical migration may underestimate the effort required.

Standards participation questions

“How do you stay current with TACACS+ standards evolution?”

Look for active participation in IETF working groups, contributions to RFC specifications, tracking of draft standards, and plans for implementing upcoming features (such as TACACS+ over TLS).

Vendors who contribute to standards development understand the protocol deeply and will implement new standards promptly.

8. Conclusion: Making the choice

The decision involves more than selecting a TACACS+ server. You're choosing between vendor flexibility and single-vendor optimisation, integration with existing infrastructure and standalone systems, adaptation speed and software release schedules.

What complexity actually involves

The TACACS+ protocol is straightforward. Complexity comes from vendor diversity in implementation, documentation gaps, legacy configuration accumulation, and organisational challenges in defining roles and permissions.

Success requires both technical expertise in TACACS+ and understanding of your specific infrastructure.

The architectural trade-off

Commercial TACACS+ solutions typically offer declarative configuration through graphical interfaces. This works well when your requirements fit within pre-defined options, you're comfortable with vendor lock-in, you prefer turnkey solutions, and your environment is relatively homogeneous.

FreeRADIUS-based approaches offer procedural configuration through policy languages. This works well when you have multi-vendor equipment, need integration with existing infrastructure, want customisation capability, need vendor-neutral architecture, and want to avoid per-user or per-device licensing.

Neither approach is universally superior. The right choice depends on your environment, your team's capabilities, and your organisational preferences.

The InkBridge approach

InkBridge Networks contributed to RFC 8907 (the TACACS+ standard) and continues active participation in the IETF working group developing TACACS+ TLS specifications. The team has decades of experience with the protocol and has deployed TACACS+ solutions for major ISPs and enterprises with complex multi-vendor environments.

The architectural priorities:

- Vendor-neutral design that adapts to any equipment
- Integration with existing infrastructure
- Policy language flexibility to handle any authorisation model
- Professional services that understand your environment

InkBridge Networks

Next steps

Audit your environment: Document your equipment vendors and their TACACS+ characteristics. Which authorisation models do they use? What are your MFA requirements? Where will TACACS+ traffic flow?

Calculate current costs: If you're using a commercial solution, calculate true costs including licensing, constraints on equipment vendor selection, delays supporting new vendors, and professional services for customisation.

Identify integration requirements: List existing systems that should integrate with TACACS+ authentication, such as user directories, databases, logging systems, and automation tools.

Understand timeline constraints: When do you need to support new equipment? Planned expansions, pending acquisitions, equipment refresh cycles, and cloud migrations all affect whether you need architectural flexibility.

About InkBridge Networks

InkBridge Networks engineers, supports, and installs foundational network solutions for authentication and network security. The core team at InkBridge Networks founded and continues to maintain FreeRADIUS, the world's most popular RADIUS server. InkBridge Networks provides solutions engineering, support packages, consulting, and training optimised for medium to large enterprises, Internet service providers, and universities.

For more information, visit inkbridgenetworks.com or contact info@inkbridge.io.

InkBridge Networks