Why Network Segmentation Projects Fail, and What to Do About It

Results from Cisco's 2026 Segmentation Survey.

1. Introduction

Network segmentation has long been core to an organization's security strategy. By dividing networks into isolated zones, segmentation limits the spread of attacks, reduces blast radius, and safeguards critical assets.

Despite its importance, segmentation projects are prone to failure, all too often stalling out before achieving desired outcomes. According to the Cisco® 2025 Segmentation Report, 79% of security professionals say that segmentation is a top priority for their organizations, but only 33% have fully implemented both macro- and micro-segmentation.

The industry has long recognized that segmentation is hard. The common barriers—complex environments, limited visibility, and tooling gaps—are well documented. What has been missing is a clear explanation of **why specific projects fail**, and whether factors like project scope, segmentation approach, or organizational context shape the outcome.

This year's edition of the Cisco Segmentation Report sets out to answer those questions. We commissioned an independent market research firm to survey network security practitioners about 400 failed segmentation projects at U.S.-based organizations with more than 500 employees. The findings reveal distinct patterns in how these projects fail—and point to practical steps that can improve the odds of success.

Key takeaways

- **Segmentation project failures fall into four distinct categories:**
  - About half of failed segmentation projects run into a "perfect storm"—a wide range of challenges hitting at once.
  - Another third fail due to accumulated friction across multiple fronts, with no single dominant cause.
  - About one in twelve fail because segmentation policies became too difficult to maintain.
  - About one in thirteen fail because scope expanded beyond what the team could handle given the complexity of the environment.
- **Differences in segmentation method and environment shape how projects fail:**
  - Projects that include campus networks tend to fail either from a broad spectrum of simultaneous challenges or from unexpected changes in scope due to complex environments.
  - Projects that include IoT environments tend to fail from accumulated friction across multiple fronts or from struggles with policy maintenance.
  - Projects using Layer 2 segmentation approaches most often fail because of inadequate visibility across complex environments.
- **There is a disconnect between diagnosed failures and proposed fixes:**
  - More than 70% of proposed fixes focus on general IT project management rather than segmentation-specific remedies—even when the project failed primarily for segmentation-specific reasons.

2. Segmentation project failures can be classified into four distinct categories

Pinpointing why an IT project fails is rarely straightforward. Multiple factors usually contribute, and their relative weight varies from one project to the next. To understand why segmentation projects fail, we evaluated each of the 400 failed projects against twelve factors—six related to general IT project management, and six specific to segmentation. For every project, each factor was rated on a scale of 1 (strongly disagree that it contributed to failure) to 5 (strongly agree).

Table 1. The twelve factors evaluated for each failed project

General IT Project Management Factors	Segmentation-Specific Factors
Goals were unclear or inconsistently defined at the outset.	The complexity of the environment (e.g., hybrid cloud, containers, legacy systems) made segmentation difficult to implement successfully.
Senior leadership sponsorship and project leadership were insufficient.	We lacked sufficient visibility into assets to design effective segmentation policies.
The project experienced scope creep or changing requirements.	Identifying legitimate communication flows between systems was more difficult than anticipated.
The project timeline was unrealistic given the available resources.	Segmentation policies required excessive manual effort to create and maintain.
Issues and risks were not identified, tracked, or addressed effectively during project execution.	Limitations or immaturity of segmentation tools (including third-party products) contributed significantly to project failure.
Coordination and communication among stakeholders were ineffective.	Concerns about application outages or business disruption constrained how fully segmentation could be deployed.

With twelve factors rated across 400 projects, patterns began to emerge in the data. When we analyzed those patterns, the failed projects fell into four distinct categories:

- **Perfect storm:** Projects that failed due to a wide range of issues across both general IT project management and segmentation-specific technical challenges. Anything that could go wrong, did.
- **Diffuse friction:** Projects that faced multiple points of moderate friction, with no single dominant cause. The cumulative effect was enough to stall the effort.
- **Operational drag:** Projects that failed under the operational burden of creating and maintaining segmentation policies, compounded by a reluctance to deploy aggressively due to outage risk.
- **Scope and visibility trap:** Projects where scope expanded beyond what was originally planned, while the team faced insufficient asset visibility, a complex environment, unrealistic timelines, and outage concerns.

Notably, more than half of all failed projects fall into the Perfect Storm category, where everything goes wrong at once. Another third land in Diffuse Friction, where projects face moderate but broad friction. Given the complexity of modern networks, it's perhaps unsurprising that more than 80% of failed segmentation projects stumble on multiple fronts at once (see Figure 1).

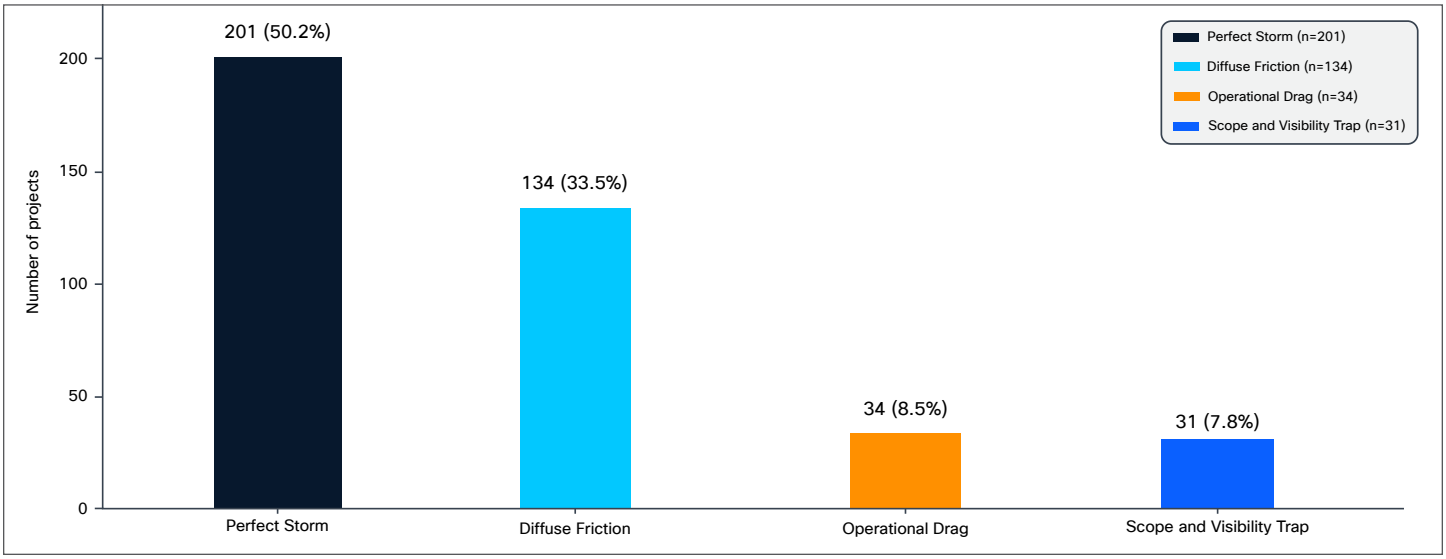

Figure 1. 84% of failures are due to the presence of most (or all) failure factors in the segmentation project

3. Differences in segmentation method and environment cause projects to fail in different ways

Segmentation projects vary greatly in terms of model (macro- vs. micro-segmentation), approach (Layer 2, Layer 3, etc.), and network types (public cloud, campus, etc.). This diversity has historically made it difficult to pin down the actual causes of project failures. Correlating failure categories with the characteristics of the underlying projects provides valuable insights (see Figures 2 and 3).

For example, projects that include campus environments often fail because of a wide range of issues hitting at once (Perfect Storm) or because of inadequate visibility relative to the complexity of the environment (Scope and Visibility Trap). Campus environments typically combine heterogeneous devices (desktops, laptops, mobile devices, routers), networks (corporate Wi-Fi, guest Wi-Fi, Ethernet), and users (full-time employees, part-time employees, contractors, visitors). The sheer number of variables, combined with the complexity of creating and enforcing segmentation policies across them, means anything that can go wrong often does.

Similarly, segmentation projects in IoT networks tend to fail because of friction accumulated across multiple factors (Diffuse Friction) or because of the complexity of maintaining segmentation policies (Operational Drag). Again, this is due to the inherent diversity of IoT devices in these types of environments. These aren't just different flavors of laptops or mobile devices. Factory floors are home to sensors, robots, security cameras, and other smart devices—each with its own connectivity patterns and policy needs. It's the same story with hospital networks (thin clients, imaging machines, label printers, security cameras), warehouses (surveillance systems, robots), and other environments that rely on the interconnectivity of IoT devices. Managing segmentation policies across these devices requires expertise and careful planning.

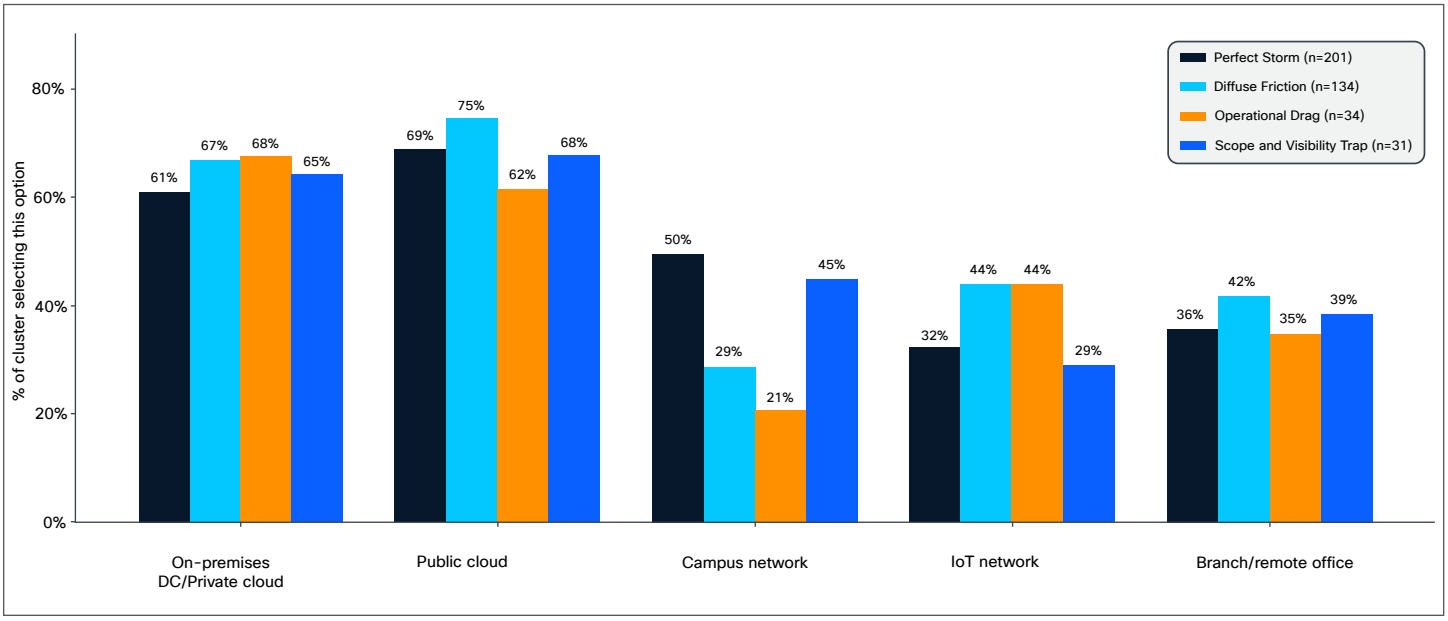

Figure 2. Failure patterns differ between campus and IoT environments.

Projects using Layer 2 approaches (for example, VLANs) tend to fail due to unexpected changes in scope—most likely because of visibility gaps (Scope and Visibility Trap). These projects may have started with a defined scope but expanded as new assets were incrementally discovered. It is likely that they began with inadequate visibility into the assets on the network and faced pressure to leave existing workflows untouched.

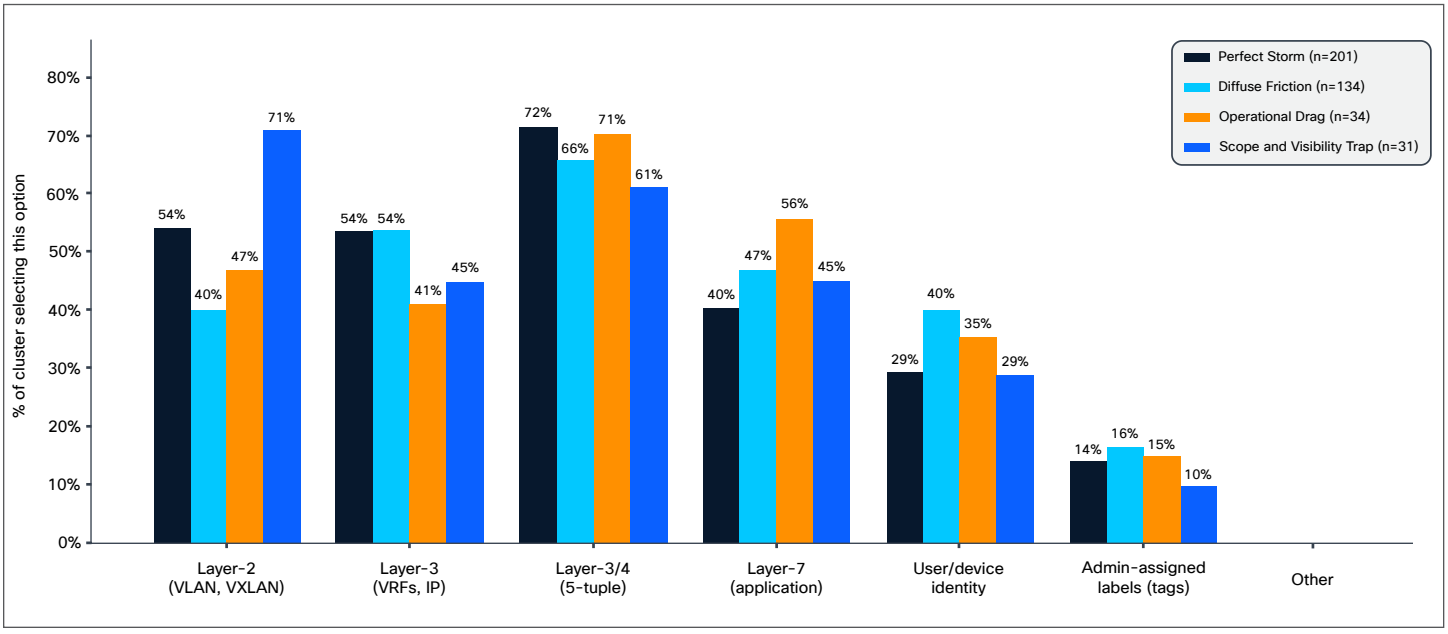

Figure 3. Layer 2 segmentation projects most often fail because of misaligned scope due to gaps in network visibility.

Notably, failure categories do not significantly differ by workload type, suggesting that the failure patterns arise regardless of whether the environment runs bare metal, virtualized, containerized, or serverless workloads. Instead, the differences emerge primarily from segmentation model, approach, and network type.

4. There is a disconnect between diagnosed failures and proposed fixes

When asked how they would fix these project failures, practitioners across the board proposed general IT project management fixes—such as more flexible project timelines, better coordination between teams, a more defined scope, and stronger leadership. This held true even when segmentation-specific challenges were identified as the main cause of project failure. In fact, the ratio between general IT project management fixes and segmentation-specific fixes is consistently approximately 70:30 across all four failure categories (see Figure 4).

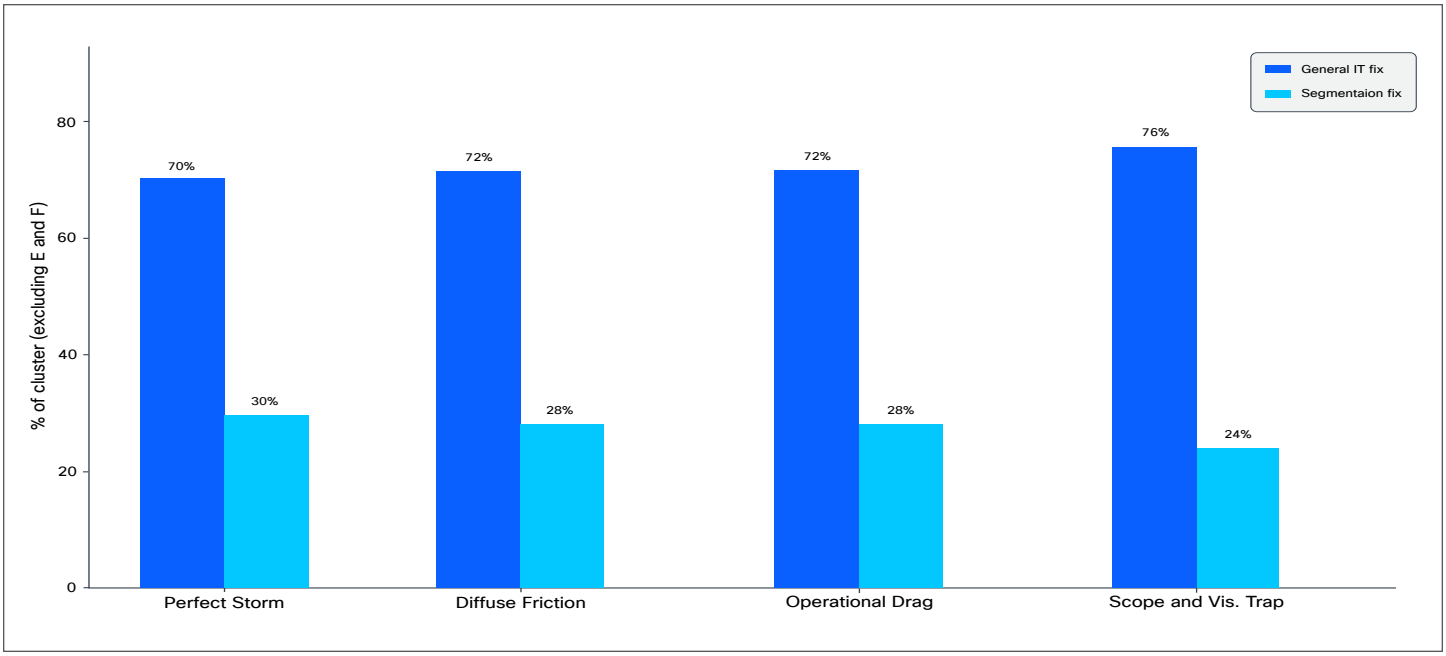

Figure 4. Proposed fixes disproportionately favored general IT project management over segmentation-specific fixes across all four failure categories.

The reasons for this disconnect vary:

- When a project struggles with broader management issues, it can leave the impression that the whole effort was mishandled—even if the actual cause of failure was a specific technical challenge. The proposed fix then reflects that broader sentiment rather than the proximate cause.
- Good project management might have surfaced technical challenges early enough to resolve them before they became fatal. From this view, general IT project management fixes aren't contradicting the diagnosis—they're targeting the conditions that allowed the technical problem to derail the project in the first place.
- Segmentation is, at its core, a technology designed to divide—and it is applied to networks, which are built to connect. That tension between isolating and connecting may naturally push the blame toward how the project was run rather than toward the technical segmentation work.

Whatever the reason, improving success rates depends on getting project management right and making sure participants believe the project is worthwhile and has a realistic chance of success. But when a segmentation-specific failure is identified, it is that failure that needs direct attention. General IT project management fixes alone will not make a segmentation-specific problem go away.

5. Recommendations

Understanding how segmentation projects fail provides an opportunity to plan ahead and improve the odds of success. Here are three pieces of practical guidance for teams planning segmentation projects:

a) Enter the project with the understanding that segmentation is hard. Segmentation projects typically touch different network types, use multiple approaches at once, and require coordination across multiple teams. This complexity is a significant reason that more than 80% of failed segmentation projects stumble on multiple fronts at once rather than on a narrow set of issues. Recognizing this up front—and scoping the project, timeline, and resourcing accordingly—reduces the risk of being overwhelmed mid-execution.

b) Get project management right. Strong project management is a necessary foundation for segmentation success. That means defining a clear and realistic scope; setting timelines that reflect the actual complexity of the environment; establishing coordination across the network, security, and application teams that will be involved; and tracking risks actively throughout execution. Executive sponsors play a critical role here—not in solving technical problems, but in providing the authority and resources needed to resolve blockers when they arise. Good project management sets the conditions under which technical challenges can be surfaced early and addressed before they derail the effort.

c) Address segmentation-specific issues too. Good project management sets the stage, but it cannot substitute for resolving segmentation-specific technical problems. When these issues are identified, they need direct attention with the right technical fixes:

a. A visibility gap needs a discovery and asset inventory solution, not just better coordination.

b. A policy maintenance burden needs automation and better tooling, not just a clearer scope.

c. A tooling limitation needs the right type of tool for the problem—not just more tools. Tools designed for one kind of segmentation won't necessarily solve a different kind.

d. A complex environment needs a segmentation approach suited to it, not just more meetings.

e. Outage concerns need safe policy testing and phased rollout mechanisms, not just stronger executive backing.

In practice, the upstream project management conditions and the proximate technical barriers may need to be addressed at the same time. Treating either one alone is rarely enough.

6. Conclusion

The Cisco 2026 Segmentation Report provides valuable insights into why segmentation projects fail and how organizations can mitigate these challenges to improve success rates. Key takeaways from the research include:

- More than 80% of failed segmentation projects struggle on multiple fronts at once, across both general IT project management and segmentation-specific technical factors.
- Segmentation projects that include campus or IoT networks, and those that use Layer 2 approaches, are especially prone to failure.
- Strong project management is necessary for segmentation success, but it is not sufficient. When segmentation-specific technical challenges arise, they need direct technical attention.

Segmentation is hard, but the patterns behind its failures are no longer hidden. Teams that enter their projects aware of these patterns—and prepared to address both the organizational and the technical dimensions of the work—are better positioned to succeed.

7. About the Research

Cisco commissioned independent market research specialist Vanson Bourne to conduct this research. The study surveyed 400 network security practitioners at U.S.-based companies with at least 500 employees. Each respondent was asked to answer the survey questions based on their experiences with a single failed segmentation project that had occurred within the previous 24 months. Most respondents have undertaken multiple segmentation projects during their careers. Respondents were screened for eligibility, and their responses were quality-checked before being included in the final dataset.

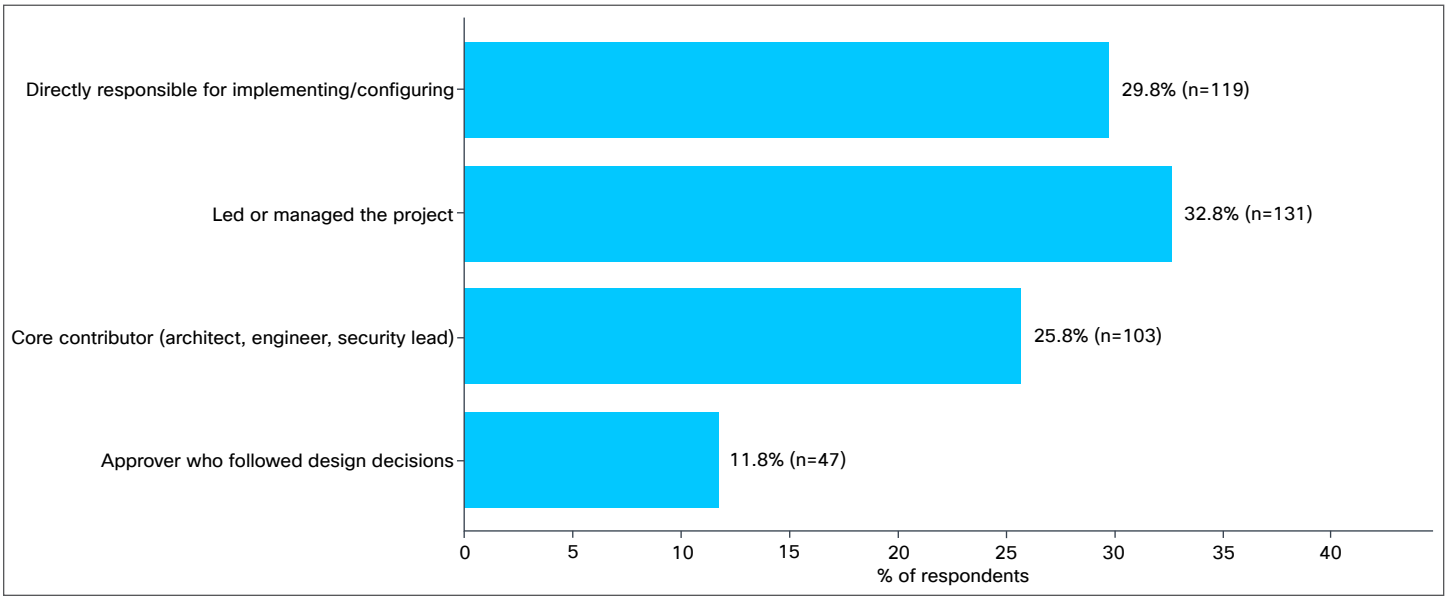

Figure 5. Role distribution of respondents.

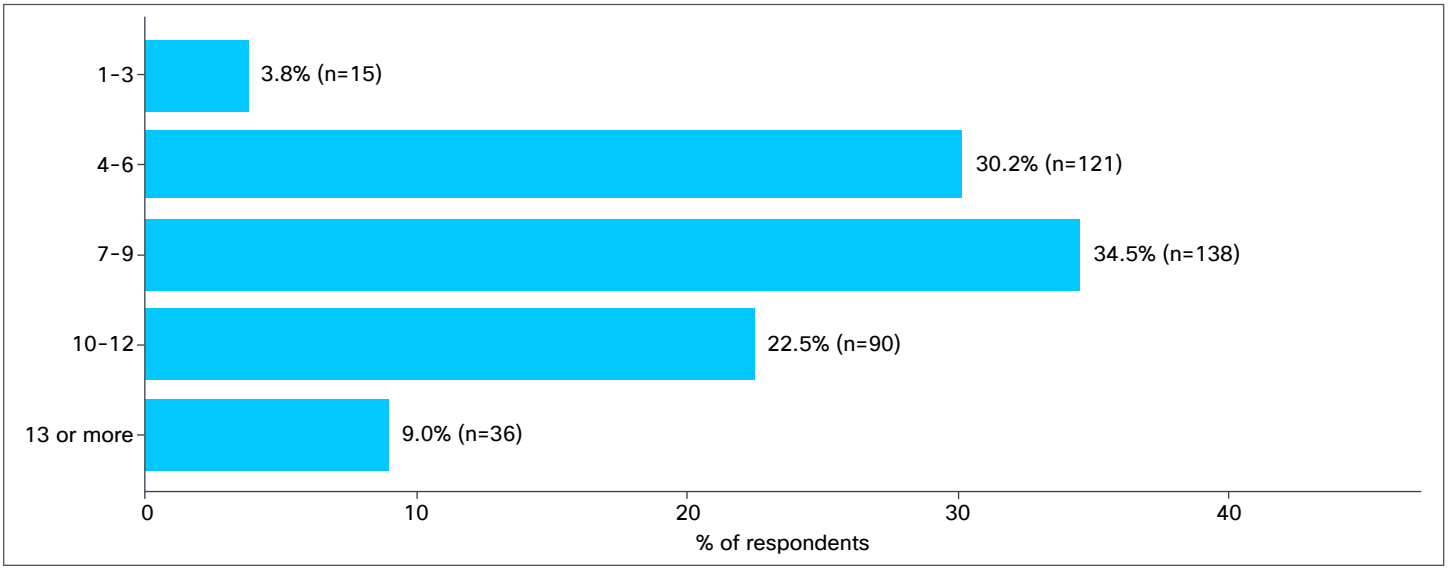

Figure 6. Segmentation projects undertaken by respondents over their careers.

8. References

[1] R. Dube, “Why Network Segmentation Projects Fail,” arXiv, 2026. https://arxiv.org/abs/2604.08632

[2] Cisco Systems Inc., “The Segmentation Report,” Oct. 2025. https://www.cisco.com/c/en/us/products/collateral/security/hypershield/segmentation-report.pdf

[3] R. Dube, “A Taxonomy of Segmentation in Network Security,” IEEE Access, vol. 14, pp. 16921–16935, 2026. https://ieeexplore.ieee.org/document/11364135

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision-makers across technical and business functions in all business sectors and all major markets. For more information, visit vansonbourne.com.

About Cisco

Cisco is the worldwide technology leader that securely connects everything to make anything possible.
Our purpose is to power an inclusive future for all by helping our customers reimagine their applications, power hybrid work, secure their enterprise, transform their infrastructure, and meet their sustainability goals.
For more information visit cisco.com.