White Paper

OSPF versus EIGRP: The Case for Open Standards-based Routing

The Ease of Migration and Benefits for Procurement

By Dan Conde, ESG Analyst

December 2016

This ESG White Paper was commissioned by Juniper Networks and is distributed under license from ESG.

Contents

Introduction

Networking products based on open standards confer significant benefits upon their end-users: increased product choice, interoperability, enhanced security, and lower total cost of ownership. For government customers and end-users, deployment of open standard-based equipment also enables compliance with federal laws, regulations, and White House guidance that mandates full and open competition in IT acquisitions.

ESG recently surveyed 306 IT professionals representing enterprise-class (1,000 employees or more) organizations in North America, of which 31% were in midmarket and 69% in enterprise. The survey found that 74% of organizations rely on the acceptance of open standards to choose the network infrastructure technologies they deploy.[1]

What Is an Open Standard?

Respected engineering standards communities, such as the Internet Engineering Task Force (IETF), convene stakeholders (industry, academia, etc.) to analyze engineering specifications. The purpose is to achieve consensus around specifications that will be accessible to all stakeholders for implementation and deployment.

In network routing, one well-established routing protocol is Open Shortest Path First (OSPF). The IETF established OSPF as the standard for interior routing. Any router manufacturer can implement OSPF into its products, and most of them have.

Is EIGRP Open Standard?

No, the Enhanced Interior Gateway Routing Protocol (EIGRP) developed by Cisco is not an open standard. EIGRP is a routing protocol that is proprietary to Cisco. Although Cisco submitted a portion of EIGRP to the IETF for consideration as a potential standard, the entire protocol has not been accepted as a standard and remains proprietary to Cisco.

Business Case for Open Standards

Increased Product Choice

Acquisition and deployment of IT and networking products based on open standards makes good business sense because open standards confer more choice among products. By definition, every vendor or manufacturer can base its IT products on open standard protocols. This means increased competition among manufacturers and more choice for IT end-users.

Lower Total Cost of Ownership

The increased competition among manufacturers leads to lower product prices and thus decreased capital expenditure for IT end-users. In addition, the wider availability of personnel trained on open standards can lead to a reduction in operational expenses.

Adoption of a proprietary protocol such as EIGRP, on the other hand, can raise an end-user's costs when the number of suppliers is limited to a single source.

Interoperability

Because multiple router manufacturers have implemented a routing protocol based on open standards (for example, OSPF is an internationally accepted open standard protocol) into their products, devices from different manufacturers can interoperate and function together within the same network. This provides great flexibility, agility, and choice.

[1] Source: ESG Research Report, *Trends in Data Center Networking*, February 2016.

Enhanced Security

Open standard-based protocols can improve a network's security posture. Open standards enable the integration of different solutions from multiple sources that conform to the same protocols. This supports concepts such as defense in depth for cybersecurity.

When different products use the same protocols with different software implementations, organizations can benefit from software diversity and avoid network monoculture or homogeneity. The organization can avoid the situation where a vulnerability exploited in one product will affect the entire organization, as can happen in an organization with all devices operating on the same software implementation. Such a "single point of failure" circumstance could produce significant consequences.

With a heterogeneous network based on open standards, any impact of a security event attempting to exploit a vulnerability in one affected product can more likely be contained as the system allows for greater redundancy, providing a built-in mitigation.

OSPF's support for modern security capabilities such as IPSec authentication enables compatibility with modern security infrastructure.

U.S. Government Procurement Requirements

Federal law, regulations, and White House guidance require agencies to acquire networking equipment under the rubric of full and open competition. This means that agencies should procure equipment in a manner that is brand- and technology-neutral. Basing products upon open standards is essential to compliance with these requirements because such standards are, by definition, brand- and technology-neutral.

Migrating from EIGRP to OSPF

IT organizations that want to migrate from EIGRP to OSPF have three options:

1. Integrated—a new network build-out combined with a protocol migration. This approach is suited for those who are adding OSFP devices to a network and will migrate existing devices from EIGRP to OSPF.

2. Redistribution—migration performed one segment at a time. The benefit is that each section of the network can be kept on either EIGRP or OSPF. This requires a careful analysis and understanding of the network architecture.

3. Overlay—running EIGRP and OSPF simultaneously on all routers. The two protocols are kept separate on the network so they do not interface with each other. This is simple to set up, but the problem is that an end-user continues to run both protocols throughout the network.

These well-known methods allow organizations to determine how best to reduce risk and cost while migrating toward OSPF.

The Bigger Truth

The procurement of network routers needs to be revisited with a view based on modern technology standards and should not rely on what seemed to work in the past. The adoption of open standard-based protocols, such as OSPF, has enabled the creation of a broad ecosystem of vendors offering interoperable, innovative, and secure products. Such an ecosystem enables full and open competition, one of the major federal requirements for IT procurement.

Multiple methods for migrating to an OSPF-based environment provide choices depending on the journey that an end-user chooses to undertake. These methods are documented and tested, which reduces operational risk. Migrating to open standards will pay off in the long term with lower capital and operational expenses, and will also provide great flexibility and network capability in the long term.

References

Standards Documents
Internet Engineering Task Force: OSPF Version 2 Request for Comments: 2328. https://tools.ietf.org/html/rfc2328
Internet Engineering Task Force: OSPF for IPv6 Request for Comments: 5340. https://tools.ietf.org/html/rfc5340
Procurement and Security Guidelines
Federal Acquisition Regulation, Subpart 6.1—Full and Open Competition
Federal Acquisition Regulation, Subpart 39—Appropriate Security policies
National Security Agency, Information Assurance Directorate. "Defense in Depth"
https://www.iad.gov/iad/library/reports/defense-in-depth.cfm
OMB Circular A-11: General procurement guidelines
OMB Circular A-130: Management of Federal Information Resources - guidelines on security plans
OMB Memorandum M-06-13: Competitive Sourcing

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188