Internet Engineering Task Force (IETF)
Request for Comments: 5810
Category: Standards Track
ISSN: 2070-1721

A. Doria, Ed.
Lulea University of Technology
J. Hadi Salim, Ed.
Znyx
R. Haas, Ed.
IBM
H. Khosravi, Ed.
Intel
W. Wang, Ed.
L. Dong
Zhejiang Gongshang University
R. Gopal
Nokia
J. Halpern

March 2010

Forwarding and Control Element Separation (ForCES) Protocol Specification

Abstract

This document specifies the Forwarding and Control Element Separation (ForCES) protocol. The ForCES protocol is used for communications between Control Elements(CEs) and Forwarding Elements (FEs) in a ForCES Network Element (ForCES NE). This specification is intended to meet the ForCES protocol requirements defined in RFC 3654. Besides the ForCES protocol, this specification also defines the requirements for the Transport Mapping Layer (TML).

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5810.

Copyright Notice

Table of Contents

1. Introduction

Forwarding and Control Element Separation (ForCES) defines an architectural framework and associated protocols to standardize information exchange between the control plane and the forwarding plane in a ForCES Network Element (ForCES NE). RFC 3654 has defined the ForCES requirements, and RFC 3746 has defined the ForCES framework. While there may be multiple protocols used within the overall ForCES architecture, the terms "ForCES protocol" and "protocol" as used in this document refer to the protocol used to standardize the information exchange between Control Elements (CEs) and Forwarding Elements (FEs) only.

The ForCES FE model [RFC5812] presents a formal way to define FE Logical Function Blocks (LFBs) using XML. LFB configuration components, capabilities, and associated events are defined when the LFB is formally created. The LFBs within the FE are accordingly controlled in a standardized way by the ForCES protocol.

This document defines the ForCES protocol specifications. The ForCES protocol works in a master-slave mode in which FEs are slaves and CEs are masters. The protocol includes commands for transport of LFB configuration information, association setup, status, event notifications, etc.

Section 3 provides a glossary of terminology used in the specification.

Section 4 provides an overview of the protocol, including a discussion on the protocol framework and descriptions of the Protocol Layer (PL), a Transport Mapping Layer (TML), and the ForCES protocol mechanisms. Section 4.4 describes several protocol scenarios and includes message exchange descriptions.

While this document does not define the TML, Section 5 details the services that a TML MUST provide (TML requirements).

The ForCES protocol defines a common header for all protocol messages. The header is defined in Section 6.1, while the protocol messages are defined in Section 7.

Section 8 describes the protocol support for high-availability mechanisms including redundancy and fail over.

Section 9 defines the security mechanisms provided by the PL and TML.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.