Workgroup:	IDR		
Internet-Draft:	draft-cui-idr-flowspec-feedback-roadmap-00		
Published:	6 July 2026		
Intended Status:	Informational		
Expires:	7 January 2027		
Authors:	Y. Cui	Y. Gao	J. Haas
	Tsinghua University	*Zhongguancun Laboratory*	*Juniper*

Problem Statement and Roadmap for BGP FlowSpec Monitoring

Abstract

This document describes the problem space and roadmap for monitoring BGP Flow Specification (FlowSpec) deployments. It outlines the operational motivation for FlowSpec monitoring, identifies representative classes of monitoring information, and positions relevant work on FlowSpec, the BGP Monitoring Protocol (BMP), IP Flow Information Export (IPFIX), and YANG-based operational state within a common framework. The resulting roadmap provides common context for related protocol-specific work in the relevant IETF working groups.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 7 January 2027.

Copyright Notice

Table of Contents

1. Introduction

BGP Flow Specification (FlowSpec) provides a mechanism for distributing traffic filtering and traffic treatment policies using BGP. Existing FlowSpec Version 1 (FSv1), defined in [RFC8955], [RFC8956], and [RFC9117], enables the dissemination of match conditions and actions for use cases such as traffic handling, DDoS mitigation, and policy-based traffic steering. The FlowSpec Version 2 (FSv2) work [draft-ietf-idr-flowspec-v2-04] explores additional policy representation and processing capabilities.

In operational deployments, advertisement of a FlowSpec route does not by itself provide sufficient visibility into how the corresponding policy is realized. Operators may need to determine whether the route was received, validated, accepted, and translated into the intended filtering or forwarding behavior. They may also need information about constrained realization, failures, and resulting traffic-treatment outcomes.

These monitoring needs span multiple sources and protocol mechanisms. Route-related events and statistics may be reported using BGP-oriented telemetry, traffic-treatment observations may be exported using flow telemetry, and structured operational state may be represented using YANG-based models. The Network Telemetry Framework in [RFC9232] classifies these as control-plane, forwarding-plane, and management-plane telemetry, respectively. Related work may therefore span multiple documents and working groups.

This document provides an informational problem statement and roadmap for BGP FlowSpec monitoring. It identifies the roles of FlowSpec, BMP, IPFIX, and YANG-related work and highlights areas in which coordination or additional protocol-specific work may be useful. It does not define new protocol extensions, encodings, data models, or requirements for a specific telemetry transport.

2. Definitions and Acronyms

- NLRI: Network Layer Reachability Information
- FSv1: Flow Specification Version 1, defined in [RFC8955] and [RFC8956]
- FSv2: Flow Specification Version 2, described in [draft-ietf-idr-flowspec-v2-04]
- DDoS: Distributed Denial of Service
- BMP: BGP Monitoring Protocol, defined in [RFC7854]
- REL: Route Event Logging, defined in [draft-ietf-grow-bmp-rel-05]
- IPFIX: IP Flow Information Export, defined in [RFC7011]
- YANG: A data modeling language used to model configuration and operational state data
- Monitoring: The collection, export, correlation, or interpretation of operational information associated with FlowSpec policy realization.
- Route Status: Control-plane state associated with the lifecycle of a FlowSpec route, including reception, validation, acceptance, rejection, update, and withdrawal.

- Enforcement Status: Operational state associated with the realization of a FlowSpec route as filtering, forwarding, or traffic-treatment behavior.

3. Scope and Non-Goals

This document is limited to the monitoring and troubleshooting aspects of BGP FlowSpec deployments. Its scope includes the operational visibility needed to understand how FlowSpec routes are processed and realized, including route reception, validation, policy processing, selection, enforcement status, constrained or partial realization, and traffic-treatment outcomes. It also includes the correlation of information obtained from the control plane, enforcement functions, and data-plane observations.

This document focuses on the overall problem space and the relationship among relevant technical components. It is intended to explain why multiple technologies may be involved in FlowSpec monitoring and why related work may be developed in multiple documents and working groups.

The following items are outside the scope of this document:

- Defining new FlowSpec actions, route encodings, or attribute formats
- Defining new BMP messages, TLVs, event types, or statistics types
- Defining new IPFIX Information Elements or export procedures
- Defining new YANG modules, nodes, or operational state schemas
- Defining new subscribed-notification or YANG-Push mechanisms
- Selecting or requiring a specific transport for FlowSpec monitoring data
- Standardizing a complete closed-loop control framework for FlowSpec policy validation or optimization
- Defining implementation-specific behavior for a particular platform

This document does not replace protocol-specific solution work. It provides a common problem statement and roadmap for positioning such work and identifying how different technical efforts may contribute to the broader FlowSpec monitoring problem.

4. Operational Motivation and Problem Statement

BGP FlowSpec is often used for time-sensitive operational functions such as DDoS mitigation, targeted traffic filtering, and policy-based traffic steering. Successful distribution of a FlowSpec route does not by itself indicate that the intended traffic-treatment policy has been realized on a receiving system.

Current deployments often rely on fragmented or implementation-specific methods to determine whether a FlowSpec route has been received, validated, accepted by local policy, and realized by the relevant enforcement function. Operators may therefore face a visibility gap between control-plane advertisement, local realization, and observed traffic treatment.

Several operational gaps follow from this:

- There may be insufficient visibility into the lifecycle of a FlowSpec route, including reception, validation, policy processing, update, withdrawal, and failure conditions.
- A receiving system may be unable to fully realize a FlowSpec rule. Unsupported match components, unsupported actions, local policy, unavailable redirect targets, or filtering-resource limitations may result in constrained or partial realization.
- Route status and enforcement status may differ. A FlowSpec route may be accepted by the control plane while the corresponding filtering or forwarding behavior is inactive, constrained, or not successfully programmed.
- Operators may need to observe traffic-treatment outcomes, including match statistics, drop-related observations, redirect-related observations, and, where available, reasons why the intended treatment was not applied.
- Information obtained from the control plane, enforcement functions, and data-plane observations may use different identifiers, scopes, and timestamps. This can prevent an operator from determining whether the observations relate to the same FlowSpec policy.

These gaps become more significant in heterogeneous environments. Implementations may expose different route status, realization details, failure information, and traffic-treatment observations. Consequently, troubleshooting may remain difficult even when the FlowSpec route has been correctly distributed.

The problem addressed by this document is not a single missing protocol element. It is the absence of a coherent framework that identifies the relevant monitoring information, relates that information to the FlowSpec policy lifecycle, and positions ongoing and potential future work in the relevant technical areas.

5. Representative Use Cases and Monitoring Information

One class of use cases concerns reception and lifecycle status of a FlowSpec route. An operator may need to determine whether a receiving system has received the route, validated it, accepted it for processing, updated it, or withdrawn it. Such information is important for basic operational validation.

A second class concerns realization of the policy. A receiving system may accept a FlowSpec route but be unable to fully realize the derived filtering or forwarding behavior because of unsupported features, unavailable dependencies, resource constraints, or local policy. The operator may need to know that realization was constrained and the condition that led to that outcome.

A third class concerns enforcement status. Operators may need to observe whether the filter, firewall entry, or policy object derived from a FlowSpec route is active, constrained, updated, or removed. This information may differ from route status and may be needed to understand how a rule is actually realized in the enforcement path.

A fourth class concerns traffic-treatment outcomes. An operator may need to know whether the intended treatment is being observed in practice. This may include match counts, drop-related observations, redirect-related observations, or reasons for failed treatment where such information is available.

A fifth class concerns correlation across mechanisms. An operator may need to associate a FlowSpec route with related BMP events or statistics, YANG operational state, and IPFIX traffic observations. Source identification, sequence information, and observation timestamps may be needed to correlate those records and detect missing or stale data.

Taken together, these use cases suggest several recurring categories of monitoring information:

- FlowSpec route lifecycle information
- Constrained or partial realization information
- FlowSpec-derived enforcement status information
- Traffic-treatment outcome information
- Correlation information across route status, enforcement status, and data-plane observation

6. Overview of Solution Space

6.1. Conceptual Framework

FlowSpec monitoring may involve multiple functional components spanning policy generation, route dissemination, operational state tracking, policy realization, and data-plane observation. A useful way to understand the overall problem space is therefore to consider a conceptual feedback framework rather than a single protocol mechanism.

In such a framework, an upper-layer controller, mitigation system, or operational application derives traffic handling intent and generates FlowSpec policy. The control plane distributes the policy and maintains state associated with route processing. Enforcement functions realize the resulting filtering or forwarding behavior, while the data plane produces observable traffic-treatment outcomes. Monitoring information from these functions may be exported for operational analysis and may also be used as input to higher-layer policy processing.

The Network Telemetry Framework in [RFC9232] classifies telemetry according to the source of the observed information. In the FlowSpec monitoring context, BMP can provide control-plane telemetry, IPFIX can provide forwarding-plane traffic-treatment observations, and YANG-based mechanisms can provide management-plane access to structured operational state. This classification describes the source and role of the information; it does not require a particular deployment architecture.

This conceptual framework is intended only as a functional view of the monitoring problem space. It does not prescribe a specific architecture, protocol mapping, signaling mechanism, telemetry transport, or implementation model. Its purpose is to show that FlowSpec monitoring

is not limited to route advertisement itself, but may also involve route lifecycle state, constrained realization, filtering or forwarding status, observable traffic-treatment outcomes, and feedback into policy handling logic.

An example conceptual framework is illustrated below:

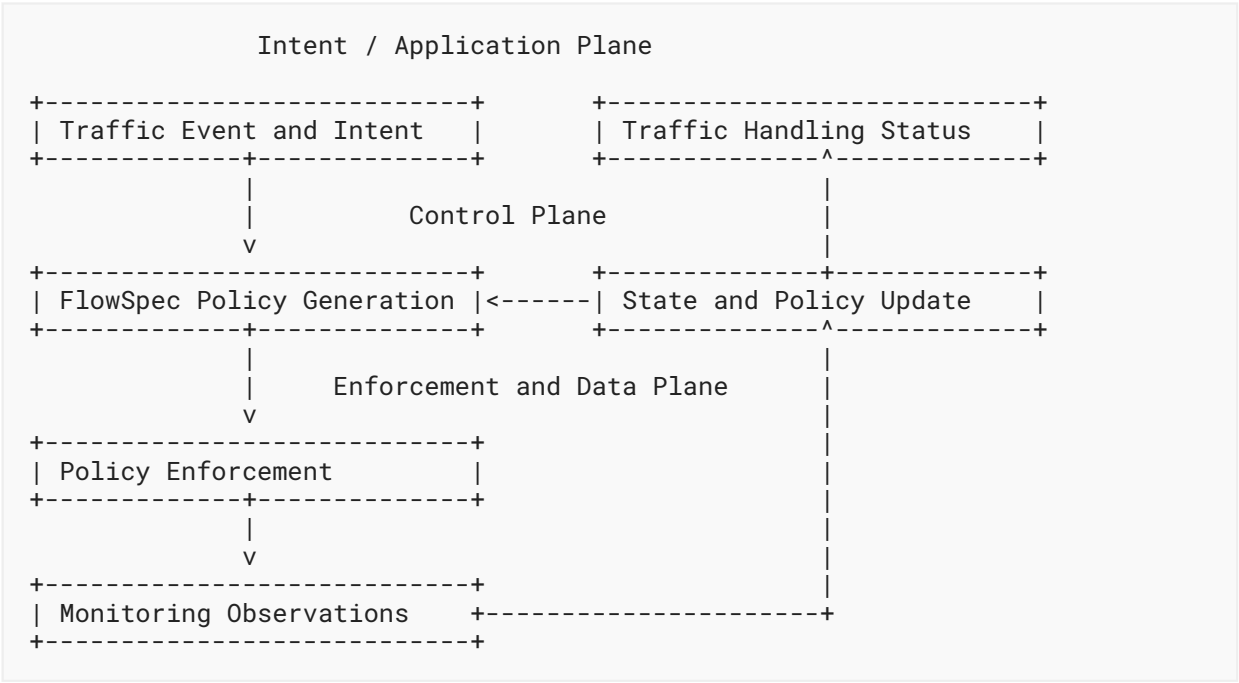

Figure 1: Example Conceptual Feedback Framework for FlowSpec Monitoring

In this example, traffic handling intent is translated into FlowSpec policy generation in the control plane. The policy is then realized in the data plane through filter or firewall enforcement. Statistical information and other monitoring observations may be exported through telemetry mechanisms. Such information may be used for external observability or as input to state or rule update functions in the control plane. Use of monitoring information as input does not by itself imply that policy changes are automatic; that behavior depends on the deployment and is outside the scope of this document.

A related way to view the monitoring problem is as a state-oriented model of FlowSpec policy realization. In such a model, monitoring information may reflect not only route lifecycle events, but also whether policy realization has completed, whether the rule has matched traffic, and whether the observed effect is consistent with the intended policy objective. The following example illustrates one possible conceptual state machine.

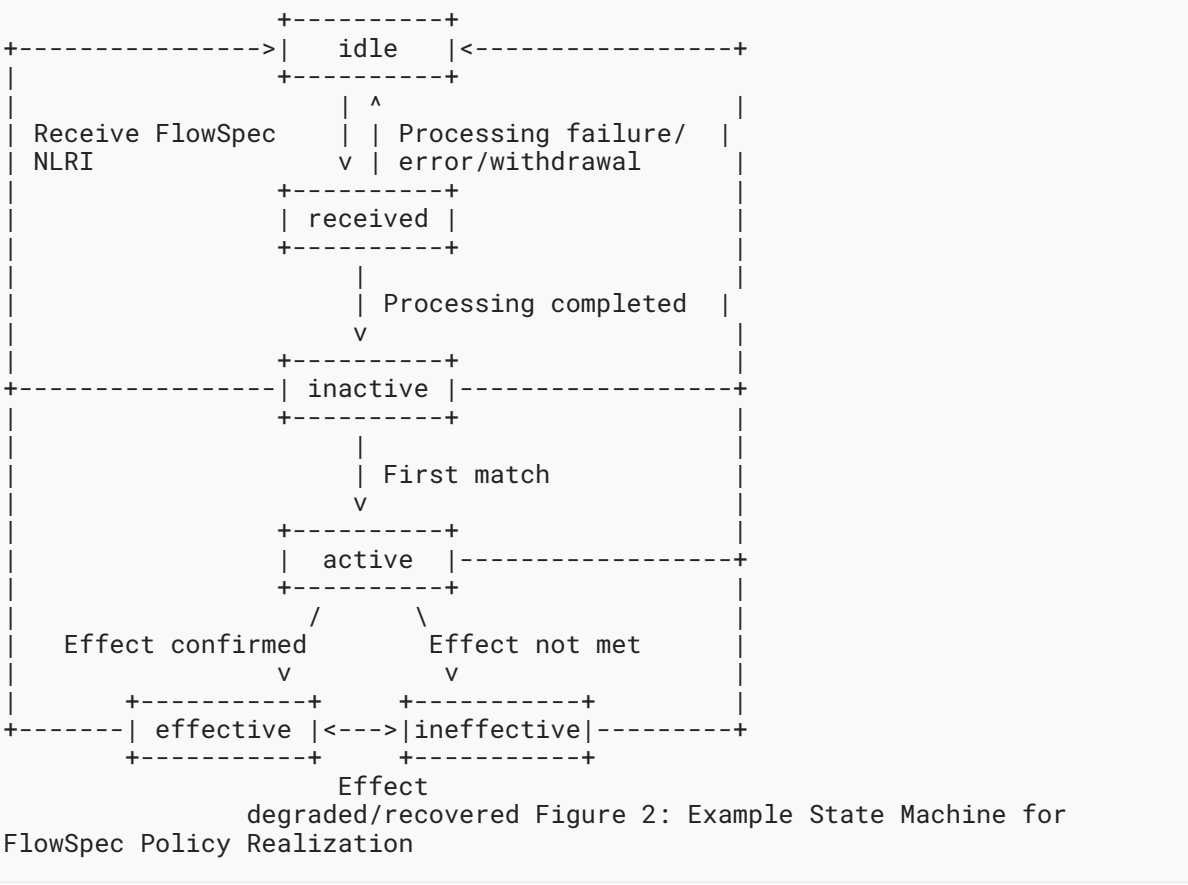

Figure 2: Example State Machine for FlowSpec Policy Realization

In this example, "received" indicates that the FlowSpec NLRI is visible to the receiving system and is undergoing validation and local processing. "Inactive" indicates that processing and realization have completed but no matching traffic has been observed. "Active" indicates that matching traffic has been observed. Where a deployment has an explicit policy objective and sufficient observations to evaluate it, "effective" and "ineffective" indicate whether the observed outcome is consistent with that objective. Validation, policy, realization, or withdrawal failures can return the rule to "idle" or generate an event for operational analysis.

This state machine is illustrative. It aligns monitoring observations with a policy lifecycle but does not require implementations to expose these states.

6.2. Monitoring Information Categories

The monitoring information associated with FlowSpec deployments can be grouped into the following categories:

In this document, realization information, enforcement status information, and traffic-treatment outcome information describe different aspects of the FlowSpec policy lifecycle. Realization information describes whether and to what extent a received FlowSpec route was successfully

translated into the intended filtering or forwarding behavior. Enforcement status information describes the current operational state of the resulting enforcement objects. Traffic-treatment outcome information describes the observed handling of traffic matching the FlowSpec rule.

1. **Route lifecycle information**

   This includes whether a FlowSpec route was received, validated, accepted, rejected, updated, withdrawn, or otherwise processed by a receiving system.

2. **Constrained or partial realization information**

   This includes whether and to what extent a received FlowSpec route was successfully translated into the intended filtering or forwarding behavior, and whether realization was constrained by platform limitations, unsupported features, unavailable dependencies, resource limitations, local policy, or other local conditions.

3. **FlowSpec-derived enforcement status information**

   This includes the current operational state of filter entries, firewall rules, policers, redirect state, or similar enforcement objects derived from the FlowSpec route, such as whether they are installed, active, inactive, constrained, or removed.

4. **Traffic-treatment outcome information**

   This includes observations of how matching traffic was handled in the forwarding or enforcement path, such as counters, hit statistics, drop-related observations, redirect-related observations, observed rate-limiting behavior, or other treatment results. Where supported, it may also include reasons associated with observed drops or other treatment outcomes.

5. **Correlation and evaluation information**

   This includes information that links a FlowSpec route, its control- plane lifecycle, its enforcement status, and its observed impact on traffic treatment. Correlation information can include a policy identifier, source identity, observation timestamp, and sequence information. It may also include information used to determine whether observed outcomes are consistent with the intended policy objective.

6.3. Candidate Technical Components

Different technical components may contribute to different parts of the overall solution space.

1. **FlowSpec**

   FlowSpec distributes the policy and provides the context with which monitoring information needs to be associated. FlowSpec-related signaling may identify a policy for which feedback is requested and carry parameters used to associate subsequent monitoring information with that policy. It does not itself convey the resulting route events, aggregate statistics, operational state, or traffic-treatment observations.

2. **BMP**

BMP provides control-plane telemetry for BGP. For FlowSpec, relevant capabilities include event-driven reporting of exceptional conditions, RIB-level statistics, and information describing changes within a statistics reporting interval. BMP extensions may therefore contribute to visibility into FlowSpec route processing without being used to report packet-level traffic observations.

3. **IPFIX and similar flow telemetry mechanisms**

   IPFIX provides a framework for exporting forwarding-plane flow observations. Existing or future Information Elements may be used to report traffic-treatment outcomes associated with FlowSpec-derived behavior, including traffic counts, applied treatment, and, where available, drop or redirect outcomes. Such records need a means to associate the observation with the relevant FlowSpec policy.

4. **YANG-based operational models**

   YANG-based models may represent structured FlowSpec operational state, including the relationship between a FlowSpec route and derived filtering or forwarding objects. The subscribed-notification and YANG-Push mechanisms in [RFC8639] and [RFC8641] can provide periodic or on-change updates for state represented in a YANG datastore. [draft-ietf-netconf-notif-envelope-05] defines source, sequence, and observation-time metadata that can assist correlation with information obtained through other telemetry mechanisms.

Some categories of monitoring information may require more than one technical component. For example, troubleshooting may require a BMP event that identifies a control-plane failure, YANG operational state that represents the resulting device state, and IPFIX observations that describe the traffic outcome.

This document does not prescribe a one-to-one mapping between information categories and protocol mechanisms. Rather, it highlights that the overall solution space is likely to involve multiple complementary components. Correlation across those components may use a policy identifier together with source, scope, sequence, and observation- time information.

7. Relationship to Ongoing Work and Working Groups

The monitoring problem described in this document spans policy association, control-plane telemetry, forwarding-plane observations, and management-plane operational state. Existing work addresses different parts of this problem and is complementary. This section positions that work without redefining the scope of the relevant working groups or presuming adoption of additional work.

7.1. Relationship to FlowSpec Work in IDR

FlowSpec provides the policy distribution context and identifies the policy object to which monitoring information relates. Work in IDR may define how a feedback request and correlation information are associated with a FlowSpec route, while the resulting monitoring information is exported through other mechanisms.

[draft-cui-idr-flowspec-feedback-binding-00] explores this association by defining feedback-binding information for a FlowSpec route. From the perspective of this roadmap, such work can identify the policy for which feedback is requested and provide an identifier for correlating subsequent reports.

FlowSpec evolution may also affect this association. Changes in policy representation, action structure, or object identity, including those explored by [draft-ietf-idr-flowspec-v2-04], may need to be considered when defining stable correlation across a policy lifecycle.

7.2. BMP-Related Work in GROW

BMP is the principal component in this roadmap for exporting BGP control-plane information. Relevant BMP work falls into three areas: event-driven reporting, RIB-level statistics, and reporting-interval statistics.

First, [draft-ietf-grow-bmp-rel-05] defines the Route Event Logging (REL) message for alerting, reporting, and on-change analysis. [draft-geng-grow-bmp-rel-enhancement-01] defines additional REL event types for selected FlowSpec validation and action-processing failures. These mechanisms provide event-driven visibility into exceptional conditions. Additional event types or recovery indications may be useful as FlowSpec capabilities and operational experience evolve.

Second, BMP provides views of Adj-RIB-In, Adj-RIB-Out, and Loc-RIB through [RFC7854], [RFC8671], and [RFC9069]. [RFC9972] defines additional global and per-AFI/SAFI RIB statistics. Potential future work may define FlowSpec-specific BMP Statistics Types for aggregate monitoring of FlowSpec route processing and realization.

Third, [draft-ietf-grow-bmp-stats-informational-tlv-00] defines additional information for gauge-type BMP statistics during a reporting interval, including minimum, maximum, average, median, and observation time for selected values. This mechanism can supplement, but does not define, FlowSpec-specific statistics.

[draft-ietf-grow-bmp-tlv-20] provides a general extensibility framework for carrying optional TLVs in BMP messages, including indexed TLVs that can be associated with an NLRI in a Route Monitoring message. It is an encoding foundation for BMP extensions rather than a separate class of FlowSpec monitoring information.

7.3. IPFIX-Related Work in the Operations and Management Area

IPFIX, defined in [RFC7011], provides a framework for exporting forwarding-plane flow observations. In this roadmap, IPFIX-related work may report traffic-treatment information associated with FlowSpec- derived behavior; it is not used to report BGP route status.

Potential future work could specify how existing IPFIX Information Elements are used, and whether additional Information Elements are needed, to associate a flow record with a FlowSpec policy and report the observed treatment.

7.4. YANG-Based Operational State and Incident Correlation

YANG-related work may define structured operational state for FlowSpec policy realization, including the relationship between a FlowSpec route and derived filtering or forwarding objects. A FlowSpec-specific operational model could complement BMP events and statistics by providing a structured view of current state.

At a higher level, [draft-ietf-nmop-network-incident-yang-09] defines a technology-independent model for correlating alarms, logs, metrics, and other observations into network incidents. FlowSpec-related failures or unexpected traffic-treatment outcomes may be inputs to such incident management. The incident model provides higher-level correlation and is independent of any FlowSpec-specific operational model.

7.5. YANG-Push Work in NETCONF

[RFC8639] defines a framework for subscribed notifications, and [RFC8641] defines periodic and on-change subscriptions for updates from a YANG datastore. These mechanisms can be used to deliver FlowSpec operational state if such state is represented in a YANG model.

[draft-ietf-netconf-notif-envelope-05] defines an extensible YANG-Push notification envelope with source identification, sequence information, and an observation timestamp. This metadata can assist in correlating YANG operational state with BMP events or statistics and IPFIX observations.

7.6. Planned Future Work

Existing work provides many of the building blocks described by this roadmap, but protocol-specific gaps may remain. Potential future work may include:

- FlowSpec-specific BMP Statistics Types for aggregate control-plane monitoring;
- IPFIX usage or extensions for FlowSpec-related traffic-treatment observations; and
- a YANG operational model for FlowSpec policy realization.

Coordination may also be needed to ensure that a policy identifier, source identity, scope, sequence information, and observation time can be used consistently when correlating information across these mechanisms. Each protocol-specific document is expected to define its own data, encoding, procedures, and security considerations.

8. Operational Considerations for Deployment

FlowSpec monitoring needs to support incremental deployment. Not all devices in a network will expose the same monitoring information, and a device may support only a subset of the relevant mechanisms. Monitoring applications therefore need to distinguish an unreported state from a reported negative state and remain useful when visibility is incomplete.

Heterogeneous environments may differ in how FlowSpec routes are realized, which failures are reported, what operational state is represented, and which traffic-treatment observations are available. Protocol-specific work needs common semantics where interoperability is required while allowing implementation-specific diagnostic detail.

Information from different telemetry mechanisms may be generated and delivered at different times. An observation timestamp identifies when state or traffic was observed, while an export or notification timestamp may identify when a report was generated. Source identification and sequence information can help detect missing, duplicated, reordered, or stale reports. Correlation based on time assumes sufficient clock alignment for the intended operational use.

The choice of reporting mode affects both timeliness and overhead. Event-driven BMP reporting and on-change YANG-Push subscriptions can reduce unnecessary periodic updates but may generate bursts during a large failure. Periodic BMP statistics, periodic YANG-Push updates, and IPFIX export require appropriate reporting or aggregation intervals. Sampling and reporting intervals are distinct and need to be interpreted accordingly.

Detailed events, counters, state updates, and flow records can create load on monitored devices, transport paths, and collectors. Protocol- specific solutions need to consider scoping, filtering, aggregation, rate control, threshold-based reporting, and data retention. Recovery or clearing information is also important so that collectors do not treat a historical failure as a current condition.

9. IANA Considerations

This document has no IANA actions.

10. Security Considerations

Monitoring information associated with FlowSpec policy may reveal operational details about filtering policy, route realization, platform capabilities, firewall state, deployment state, and traffic treatment behavior. Such information may be sensitive in some operational environments.

Protocol-specific solutions need to consider confidentiality, integrity, source authentication, and access control for the generation, export, transport, storage, and use of monitoring data. These considerations apply to feedback-request signaling as well as to BMP, IPFIX, and YANG-based reporting.

An attacker that can forge, modify, replay, delay, or suppress monitoring information could cause an operator or automated system to draw an incorrect conclusion about FlowSpec policy realization. Correlation identifiers, source identities, sequence information, and observation timestamps therefore need appropriate integrity protection and replay or staleness handling in the protocol that carries them.

A feedback request, high-frequency subscription, or large number of events and flow records can consume resources on monitored devices and collectors. Protocol-specific solutions need to address authorization, rate limiting, filtering, and aggregation to limit resource-exhaustion or amplification risks.

Where monitoring information is used as input to automated policy processing, implementations need safeguards against unstable feedback, incorrect correlation, and actions based on incomplete or stale data. The design of an automated closed-loop controller remains outside the scope of this document.

11. References

11.1. Normative References

[RFC8955] Loibl, C., Hares, S., Raszuk, R., McPherson, D., and M. Bacher, "Dissemination of Flow Specification Rules", RFC 8955, DOI 10.17487/RFC8955, December 2020, <https://www.rfc-editor.org/rfc/rfc8955>.

[RFC8956] Loibl, C., Ed., Raszuk, R., Ed., and S. Hares, Ed., "Dissemination of Flow Specification Rules for IPv6", RFC 8956, DOI 10.17487/RFC8956, December 2020, <https://www.rfc-editor.org/rfc/rfc8956>.

[RFC9117] Uttaro, J., Alcaide, J., Filsfils, C., Smith, D., and P. Mohapatra, "Revised Validation Procedure for BGP Flow Specifications", RFC 9117, DOI 10.17487/RFC9117, August 2021, <https://www.rfc-editor.org/rfc/rfc9117>.

[RFC7854] Scudder, J., Ed., Fernando, R., and S. Stuart, "BGP Monitoring Protocol (BMP)", RFC 7854, DOI 10.17487/RFC7854, June 2016, <https://www.rfc-editor.org/rfc/rfc7854>.

[draft-ietf-idr-flowspec-v2-04] Hares, S., 3rd, D. E. E., Yadlapalli, C., and S. Maduschke, "BGP Flow Specification Version 2", April 2024, <https://datatracker.ietf.org/doc/draft-ietf-idr-flowspec-v2/04/>.

11.2. Informative References

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <https://www.rfc-editor.org/rfc/rfc7011>.

[RFC8639] Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and A. Tripathy, "Subscription to YANG Notifications", RFC 8639, DOI 10.17487/RFC8639, September 2019, <https://www.rfc-editor.org/rfc/rfc8639>.

[RFC8641] Clemm, A. and E. Voit, "Subscription to YANG Notifications for Datastore Updates", RFC 8641, DOI 10.17487/RFC8641, September 2019, <https://www.rfc-editor.org/rfc/rfc8641>.

[RFC8671] Evens, T., Bayraktar, S., Lucente, P., Mi, P., and S. Zhuang, "Support for Adj-RIB-Out in the BGP Monitoring Protocol (BMP)", RFC 8671, DOI 10.17487/RFC8671, November 2019, <https://www.rfc-editor.org/rfc/rfc8671>.

[RFC9069] Evens, T., Bayraktar, S., Bhardwaj, M., and P. Lucente, "Support for Local RIB in the BGP Monitoring Protocol (BMP)", RFC 9069, DOI 10.17487/RFC9069, February 2022, <https://www.rfc-editor.org/rfc/rfc9069>.

[RFC9232] Song, H., Qin, F., Martinez-Julia, P., Ciavaglia, L., and A. Wang, "Network Telemetry Framework", RFC 9232, DOI 10.17487/RFC9232, May 2022, <https://www.rfc-editor.org/rfc/rfc9232>.

[RFC9972] Srivastava, M., Ed., Liu, Y., Lin, C., Ed., and J. Li, "Advanced BGP Monitoring Protocol (BMP) Statistics Types", RFC 9972, DOI 10.17487/RFC9972, May 2026, <https://www.rfc-editor.org/rfc/rfc9972>.

[draft-cui-idr-flowspec-feedback-binding-00] Cui, Y., Gao, Y., and L. Zhang, "BGP Flow Specification Extension for Feedback Binding", October 2025, <https://datatracker.ietf.org/doc/draft-cui-idr-flowspec-feedback-binding/00/>.

[draft-ietf-grow-bmp-rel-05] Lucente, P. and C. Cardona, "Logging of Routing Events in BGP Monitoring Protocol (BMP)", March 2026, <https://datatracker.ietf.org/doc/draft-ietf-grow-bmp-rel/05/>.

[draft-geng-grow-bmp-rel-enhancement-01] Geng, N., Gao, Y., Zhuang, S., and H. Wang, "Log More Routing Events in the BGP Monitoring Protocol (BMP)", June 2026, <https://datatracker.ietf.org/doc/draft-geng-grow-bmp-rel-enhancement/01/>.

[draft-ietf-grow-bmp-tlv-20] Lucente, P., Gu, Y., Younsi, M., and P. Francois, "BMP v4: Extended TLV Support for BGP Monitoring Protocol (BMP)", March 2026, <https://datatracker.ietf.org/doc/draft-ietf-grow-bmp-tlv/20/>.

[draft-ietf-grow-bmp-stats-informational-tlv-00] Srivastava, M. K., Kolenchery, S., and C. Lin, "BMP Statistics Information TLV", May 2026, <https://datatracker.ietf.org/doc/draft-ietf-grow-bmp-stats-informational-tlv/00/>.

[draft-ietf-nmop-network-incident-yang-09] Hu, T., Contreras, L. M., Wu, Q., Davis, N., and C. Feng, "A YANG Data Model for Network Incident Management", June 2026, <https://datatracker.ietf.org/doc/draft-ietf-nmop-network-incident-yang/09/>.

[draft-ietf-netconf-notif-envelope-05] Feng, A. H., Francois, P., Graf, T., and B. Claise, "Extensible YANG Model for YANG-Push Notifications", May 2026, <https://datatracker.ietf.org/doc/draft-ietf-netconf-notif-envelope/05/>.

Authors' Addresses

Yong Cui
Tsinghua University
Beijing
Beijing, 100084
China
Email: cuiyong@tsinghua.edu.cn

Yujia Gao
Zhongguancun Laboratory
Beijing, 100094
China
Phone: +86-185-1028-7458
Email: gaoyj@zgclab.edu.cn

Jeff Haas
Juniper
United States of America
Email: jhaas@juniper.net