Schema

OpenC2-Command (Record)

ID	Name	Type	#	Description
1	action	Action	1	The task or activity to be performed (i.e., the 'verb').
2	target	Target	1	The object of the action. The action is performed on the target.
3	args	Args	0..1	Additional information that applies to the command.
4	actuator	Actuator	0..1	The subject of the action. The actuator executes the action on the target.

Action (Enumerated)

ID	Name	Description
3	query	Initiate a request for information.
6	deny	Prevent a certain event or action from completion, such as preventing a flow from reaching a destination or preventing access.
8	allow	Permit access to or execution of a target.
16	update	Instruct a component to retrieve, install, process, and operate in accordance with a software update, reconfiguration, or other update.
20	delete	Remove an entity (e.g., data, files, flows.

Target (Choice)

ID	Name	Type	#	Description
16	features	Features	1	A set of items used with the query action to determine an actuator's capabilities
10	file	File	1	Properties of a file.
11	ip_addr	IP-Addr	1	The representation of one or more IP addresses (either version 4 or version 6).
15	ip_connection	IP-Connection	1	A network connection that originates from a source and is addressed to a destination.
1024	slpf	slpf:Target	1	Targets defined in the Stateless Packet Filter Profile

Actuator (Choice)

ID	Name	Type	#	Description
1024	slpf	slpf:Specifiers	1	Actuator specifiers and options as defined in the Stateless Packet Filter profile

Args (Map)

ID	Name	Type	#	Description
1	start_time	Date-Time	0..1	The specific date/time to initiate the action
2	stop_time	Date-Time	0..1	The specific date/time to terminate the action
3	duration	Duration	0..1	The length of time for an action to be in effect
4	response_requested	Response-Type	0..1	The type of response required for the action
1024	slpf	slpf:Args	0..1	Command arguments defined in the Stateless Packet Filter profile

OpenC2-Response (Map)

ID	Name	Type	#	Description
1	status	Status-Code	0..1	An integer status code (Duplicates message status code)
2	status_text	String	0..1	A free-form human-readable description of the response status
6	versions	Version	0..n	Supported OpenC2 Language versions
7	profiles	jadn:Uname	0..n	List of profiles supported by this actuator
8	schema	jadn:Schema	0..1	Syntax of the OpenC2 language elements supported by this actuator
9	pairs	Action-Targets	0..n	List of targets applicable to each supported action
10	rate_limit	Number	0..1	Maximum number of requests per minute supported by design or policy

1024	slpf	slpf:Results	0..1	Response data defined in the Stateless Packet Filter profile

Status-Code (Enumerated.ID)

ID	Description
102	Processing -- an interim response used to inform the client that the server has accepted the request but not yet completed it.
200	OK -- the request has succeeded.
400	Bad Request -- the consumer cannot process the request due to something that is perceived to be a client error (e.g., malformed request syntax.)
500	Internal Error -- the consumer encountered an unexpected condition that prevented it from fulfilling the request.
501	Not Implemented -- the consumer does not support the functionality required to fulfill the request.

Features

Type Name	Base Type	Description
Features	ArrayOf(Feature) [0..n]	A target used to query Actuator for its supported capabilities

File (Map)

ID	Name	Type	#	Description
1	name	String	0..1	The name of the file as defined in the file system
2	path	String	0..1	The absolute path to the location of the file in the file system
3	hashes	Hashes	0..1	One or more cryptographic hash codes of the file contents

IP-Addr

Type Name	Base Type	Description
IP-Addr	Binary (ip-addr)	32 bit IPv4 address or 128 bit IPv6 address

IP-Connection (Record)

ID	Name	Type	#	Description
1	src_addr	IP-Addr	0..1	source address
2	src_port	Port	0..1	source TCP/UDP port number
3	dst_addr	IP-Addr	0..1	destination address
4	dst_port	Port	0..1	destination TCP/UDP port number
5	protocol	L4-Protocol	0..1	Protocol (IPv4) / Next Header (IPv6)

Message-Type (Enumerated)

ID	Name	Description
0	notification	A message that does not solicit a response
1	request	A message for which a response is requested
2	response	A message containing a response to a request

Request-Id

Type Name	Base Type	Description
Request-Id	Binary	A value of up to 128 bits that uniquely identifies a particular command

Date-Time

Type Name	Base Type	Description
Date-Time	Integer	Milliseconds since 00:00:00 UTC, 1 January 1970.

Duration

Type Name	Base Type	Description
Duration	Integer	Milliseconds

Hashes (Map)

ID	Name	Type	#	Description
1	md5	Binary	0..1	MD5 hash as defined in RFC3121
4	sha1	Binary	0..1	SHA1 hash as defined in RFC3174
6	sha256	Binary	0..1	SHA256 as defined in RFC6234

L4-Protocol (Enumerated)

ID	Name	Description
1	icmp	Internet Control Message Protocol – RFC 792
6	tcp	Transmission Control Protocol – RFC 793–
17	udp	User Datagram Protocol – RFC 768
132	sctp	Stream Control Transmission Protocol – RFC 4960

Port

Type Name	Base Type	Description
Port	Integer [0..65535]	Transport Protocol Port Number, RFC 6335

Feature (Enumerated)

ID	Name	Description
1	versions	List of OpenC2 language versions supported by this actuator
2	profiles	List of profiles supported by this actuator
3	schema	Definition of the command syntax supported by this actuator
4	pairs	List of supported actions and applicable targets
5	rate_limit	Maximum number of supported requests per minute

Response-Type (Enumerated)

ID	Name	Description
0	none	No response
1	ack	Respond when command received
2	status	Respond with progress toward command completion
3	complete	Respond when all aspects of command completed

Version

Type Name	Base Type	Description
Version	String	Major.Minor version number

Action-Targets (Array)

ID	Type	#	Description
1	Action	1	action -- An action supported by this actuator
2	Target.*	1..n	targets -- List of targets applicable to this action