Relevant for this Network Anomaly	name	Path Name from Yang Model
Y	time	The Unix epoch (or Unix time / POSIX time / Unix timestamp) is the number of seconds that have elapsed since January 1, 1970 (midnight UTC/GMT), not counting leap seconds (in ISO 8601: 1970-01-01T00:00:00Z). Literally speaking the epoch is Unix time 0 (midnight 1/1/1970), but 'epoch' is often used as a synonym for 'Unix time'. time stamp converter: https://www.epochconverter.com/
Y	EncodingPath	The converter on this page converts timestamps in seconds, milliseconds and microseconds to readable dates.
Y	Producer	Name of the device that is the source of the telemetry
Y	acl-in-rpf-packets	number of inbound Access Control List reverse path forwarding packets
N	active-routes-count	Number of active routes present in the routing table for each route source.
Y	af-name	Identifies the type of address family - IPv4 or IPv6
Y	as	This is the autonomous system number, it identifies the the unit of control for the routing policy of a single administrative entity. It can be a single device/subnet or can be a group of subnets/prefixes. *
Y	backup-routes-count	number of backup routes that are configured in the Routing Information Base
Y	bandwidth	This is the bandwith capacity in kilo bits per second =bandwidth number * 1000, e.g. 100,000,000 * 1000 = 100,000,000,000 or 100Gbps

Y	bytes-received	number of bytes received by this port. Also known as ingress bytes
Y	bytes-sent	number of bytes sent by this port. Also known as egress bytes
Y	carrier-transitions	loss or recovery of carrier signal- Signal transition, when referring to the modulation of a carrier signal, is a change from one significant condition to another. Examples of signal transitions are a change from one electric current, voltage, or power level to another; a change from one optical power level to another; a phase shift; or a change from one frequency or wavelength to another.
N	checksum-error-packets	number of packets with checksum errors - Checksums are used to ensure the integrity of data portions for data transmission or storage. A checksum is basically a calculated summary of such a data portion. Network data transmissions often produce errors, such as toggled, missing or duplicated bits. As a result, the data received might not be identical to the data transmitted, which is obviously a bad thing. Because of these transmission errors, network protocols very often use checksums to detect such errors. The transmitter will calculate a checksum of the data and transmits the data together with the checksum. The receiver will calculate the checksum of the received data with the same algorithm as the transmitter. If the received and calculated checksums don’t match a transmission error has occurred.
Y	crc-errors	number of packets with cyclical redundancy check errors - Cyclic Redundancy Check (CRC) Error indicates when data is corrupted. Calculating from all data, CRC validates packets of information sent by devices and verifies it against the data extracted, ensuring its accuracy.

Y	deleted-routes-count	number of routes deleted from routing information base / forwarding information base. The forwarding information base (FIB) is the actual information that a routing/switching device uses to choose the interface that a given packet will use for egress. For example, the FIB might be programmed such that a packet bound to a destination in 192.168.1.0/24 should be sent out of physical port ethernet1/2. There may actually be multiple FIB's on a device for unicast forwarding vs multicast RPF checking, different protocols (ip vs mpls vs ipv6) but the basic function is the same - selection criteria (usually destination) mapping to output interface/encapsulation. Individual FIB's may also be partitioned to achieve concurrent independent forwarding tables (i.e. vrf's). Each FIB is programmed by one or more routing information bases (RIB). The RIB is a selection of routing information learned via static definition or a dynamic routing protocol. The algorithms used within various RIB's will vary - so, for example, the means by which BGP or OSPF determines potential best paths vary quite a bit. The means by which multiple RIB's are programmed into a common (set) of FIB's in a box will vary by implementation but this is where concepts like administrative distance are used (e.g. identical paths are learned via eBGP and OSPF, the eBGP is usually preferred for FIB injection). Again, RIB's may also be potentially partitioned to allow for multiple vrf's, etc
Y	df-unreachable-packets	ICMP destination unreachable message with code that indicates fragmentation needed by do not fragment bit is set. When a router is unable to forward a datagram because it exceeds the Maximum Transfer Unit of the next-hop network and its Don't Fragment bit is set, the router is required to return an ICMP Destination Unreachable message to the source of the datagram, with the Code indicating "fragmentation needed and DF set". To support the Path MTU Discovery technique specified in this memo, the router MUST include the MTU of that next-hop network in the low-order 16 bits of the ICMP header field that is labelled "unused" in the ICMP specification. The high-order 16 bits remain unused, and MUST be set to zero.
Y	discard-packets	number of discarded packets - The packets were received with *no errors* but were dumped before being passed on to a higher layer protocol. A typical cause of discards is when the router/switch needs to regain some buffer space.

Y	encapsulation-failure-packets	number of packets where packets encapsulation failed IP fragmentation is an Internet Protocol (IP) process that breaks datagrams into smaller pieces (fragments), so that packets may be formed that can pass through a link with a smaller maximum transmission unit (MTU) than the original datagram size. The fragments are reassembled by the receiving host. If the do not fragment bit is set in the IP header, the packet will be dropped
N	fragmentation-consumed-packets	number of consumed fragmentation packets
N	fragmentation-failure-packets	number of failed fragmented packets
N	free-application-memory	amount of free application memory in bytes
Y	free-physical-memory	amount of free physical memory in bytes
Y	global__established-neighbors-count-total	number of established neighbors -The fact that routers are neighbors is not sufficient to guarantee an exchange of route/link state updates; they must form adjacencies to exchange route / link-state updates. Adjacency is an advanced form of neighborship formed by routers that are willing to exchange routing information after negotiating parameters of such an exchange. Routers reach a FULL state of adjacency when they have synchronized information
Y	global__neighbors-count-total	total number of neighbors (see above for neighbor description)
Y	global__nexthop-count	number of next hops - Next hop is a routing term that refers to the next closest router a packet can go through. The next hop is among the series of routers that are connected together in a network and is the next possible destination for a data packet.
Y	global__restart-count	number of session restarts - This is the number of

Y	gre-error-drop	number of gre packet drops
N	gre-lookup-failed-drop	number of gre lookup failures
N	incomplete-adjacency-packets	incomplete adjacency packets
Y	input-data-rate	number of input data rate in bytes
Y	input-drops	number of input packet drops
Y	input-errors	number of input packet errors
Y	input-ignored-packets	number of input packet ignored
Y	input-load	input bandwidth load
Y	input-packet-rate	input packet rate
Y	input-queue-drops	number of input queue drops
Y	instance-name	name that uniquely identifies a routing process
Y	interface-name	interface name
Y	lisp-decap-error-drops	number of lisp decapsulation drops
N	lisp-encap-error-drops	number of lisp encapsulation drops
N	lisp-punt-drops	number of lisp punt drops
N	load-interval	number of seconds for load calculation of an interface for load averages

Y	mpls-disabled-interface	mpls interface forwarding in a disabled state
N	multi-label-drops	number of multi-label drops
N	no-route-packets	number of no route packets
y	node-name	Name of the node
y	null-packets	total number of null packets
y	output-buffer-failures	Number of output buffer failures
y	output-data-rate	output data rate in bytes
y	output-drops	number of output drops
y	output-errors	number of output errors
y	output-load	output bandwidth load in X bytes per second
y	output-packet-rate	output packet rate in packets per second
y	output-queue-drops	number of output queue drops
y	packets-received	number of packets received
y	packets-sent	number of packets sent
y	paths-count	number of learned route paths
y	peak-input-data-rate	peak input data rate in bytes

y	peak-input-packet-rate	peak input packet per second rate
y	peak-output-data-rate	peak output data rate in bytes
y	peak-output-packet-rate	peak output packet per second rate
y	performance-statistics__global__configuration-items-processed	number of configuration items processed
y	performance-statistics__global__ipv4rib-server__is-rib-connection-up	identifies RIB stats as up (true) or down (false)
y	performance-statistics__global__ipv4rib-server__rib-connection-up-count	identifies the type of address family - IPv4 or IPv6
y	performance-statistics__vrf__inbound-update-messages	number of inbound update messages to vrf
y	protocol-route-memory	the amount of route memory in use
y	punt-unreachable-packets	number of packets punted to route processor for IP addressed with an unreachable destination
y	ram-memory	amount of RAM in bytes
y	reliability	reliability rates achieved by each process in the system
y	route-table-name	total number of routes
y	routes-counts	number of route
y	rp-destination-drop-packets	number of packet drops destined for route processor
y	rpf-check-failure-packets	number of reverse path forwarding failure packets
Y	saf-name	Service Advertisement Framework name

Y	system-ram-memory	system RAM
Y	total-cpu-fifteen-minute	CPU load for last 15 minutes
Y	total-cpu-five-minute	CPU load for last 5 minutes
Y	total-cpu-one-minute	CPU load for last 1 minutes
Y	total-number-of-drop-packets	total number of dropped packets
Y	unresolved-prefix-packets	number of unresolved route prefix packets
Y	unsupported-feature-packets	number of unsupported feature packets
Y	vrf-name	virtual routing and forwarding name
Y	vrf_neighbors-count	number of neighbor counts for virtual routing and forwarding name
Y	vrf_network-count	number of network counts for virtual routing and forwarding name
Y	vrf_path-count	number of path counts for virtual routing and forwarding name
Y	vrf_update-messages-received	number of update messages received for virtual routing and forwarding name