

DoS Host Alert 124690

Duration: Mar 17 20:00 - 20:05 (0:06)

DETAILS Time: Alert Timeframe Units: pps View: Router

Router (Severity): MTC-GR-01 (391%)

Summary

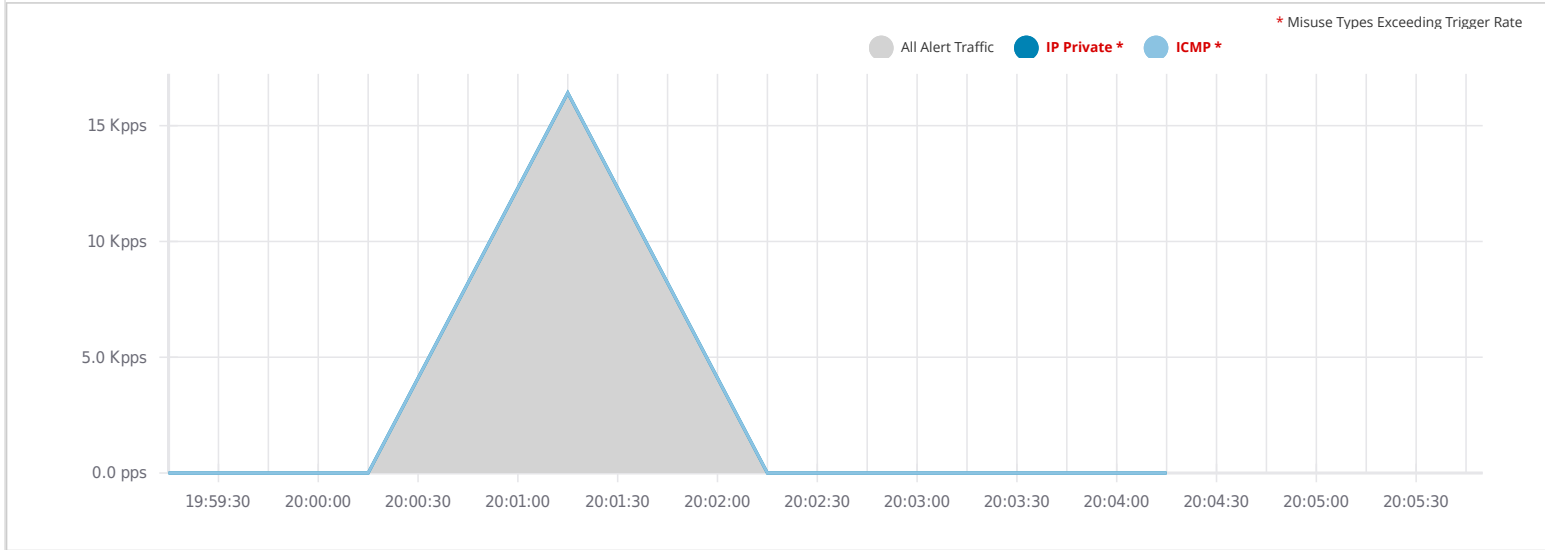
No data detected on the Network Boundary. Data shown below is for Router 'MTC-GR-01 (391%)'.

KEY INFORMATION

Severity Level	Max Severity Percent	Top Misuse Type	Max Impact of Alert Traffic	Direction	Misuse Types	Managed Object	Target
High Fast Flood	391.0% of 10 Kpps	ICMP	36.2 Mbps/39.1 Kpps at MTC-GR-01	Outgoing	ICMP, IP Private	Global Detection	ff02::16

ALERT TRAFFIC

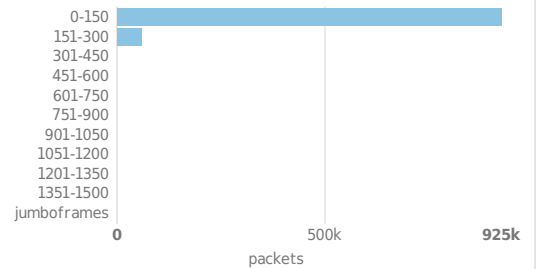
Misuse Types



Alert Characterization

Misuse Types	IP Private (3)	100.00%
Misuse Types	ICMP (0)	100.00%
Source IP Addresses	fe80::/64	100.00%
Source IP Addresses	fe80::a66c:2aff:fe76:b400/128	25.58%
Source IP Addresses	fe80::200:0:0:0/72	25.26%
Destination IP Addresses	ff02::16/128	100.00%
Protocols	ipv6-icmp (58)	100.00%
Source Countries	Unknown	100.00%
Source ASNs	NULL (0)	100.00%
Destination ASNs	NULL (0)	100.00%
ICMP Types	IPv6 Unassigned 0 (code 143)	100.00%

Packet Size Distribution



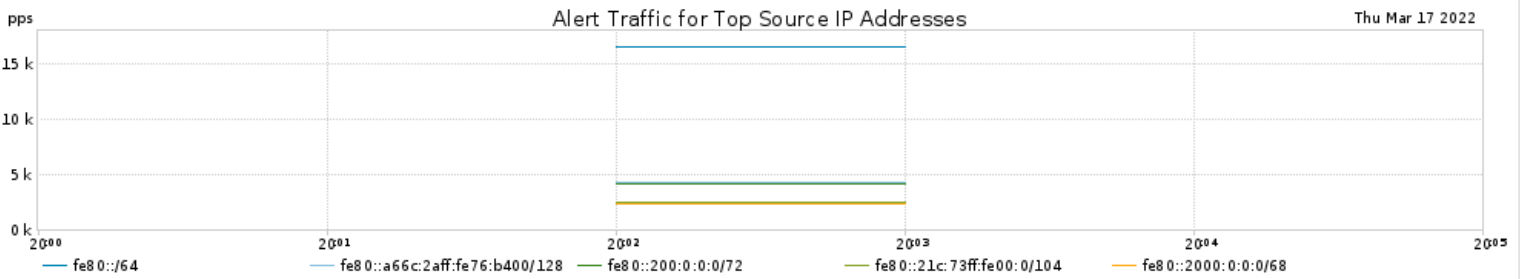
Top Traffic Patterns (last 5 min of selected timeframe)

	Source	Protocol	Flags	Src Port	Destination	Dest Port	Router	Alert Traffic
1.	fe80::/64	ICMPV6	--	--	ff02::16/128	--	MTC-GR-01	16.42 Kpps
2.	fe80::a66c:2aff:fe76:b400/128	ICMPV6	--	--	ff02::16/128	--	MTC-GR-01	4.20 Kpps
3.	fe80::200:0:0:0/72	ICMPV6	--	--	ff02::16/128	--	MTC-GR-01	4.15 Kpps
4.	fe80::21c:73ff:fe00:0/104	ICMPV6	--	--	ff02::16/128	--	MTC-GR-01	2.46 Kpps
5.	fe80::2000:0:0:0/68	ICMPV6	--	--	ff02::16/128	--	MTC-GR-01	2.28 Kpps

### Traffic Details

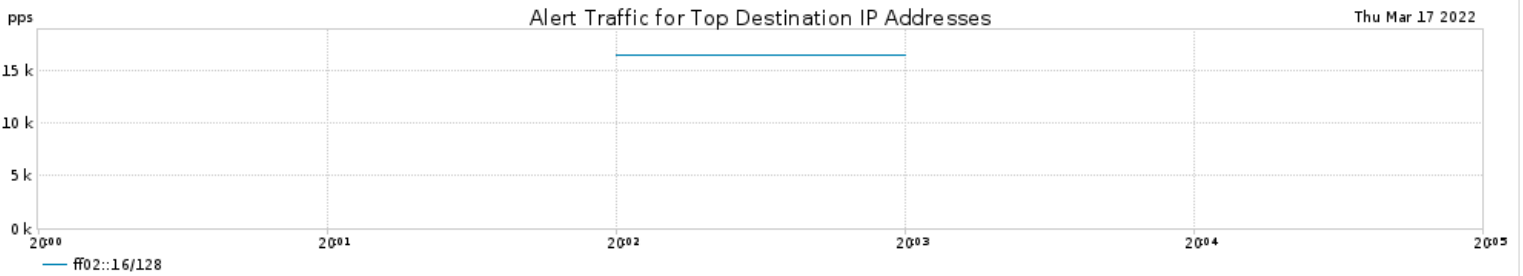
	Source	Protocol	Flags <sup>1</sup>	Src Port	Destination	Dest Port	Router	Alert Traffic <sup>▼</sup>
1.	fe80::/64	ICMPV6	--	--	ff02::16/128	--	MTC-GR-01	16.42 Kpps
2.	fe80::a66c:2aff:fe76:b400/128	ICMPV6	--	--	ff02::16/128	--	MTC-GR-01	4.20 Kpps
3.	fe80::200:0:0:0/72	ICMPV6	--	--	ff02::16/128	--	MTC-GR-01	4.15 Kpps
4.	fe80::21c:73ff:fe00:0/104	ICMPV6	--	--	ff02::16/128	--	MTC-GR-01	2.46 Kpps
5.	fe80::2000:0:0:0/68	ICMPV6	--	--	ff02::16/128	--	MTC-GR-01	2.28 Kpps

### Top 5 Items by Alert Traffic



### Source IP Addresses

fe80::/64	2.74 Kpps	100.00%
fe80::a66c:2aff:fe76:b400/128	700.00 pps	25.58%
fe80::200:0:0:0/72	691.00 pps	25.26%
fe80::21c:73ff:fe00:0/104	409.00 pps	14.95%
fe80::2000:0:0:0/68	380.00 pps	13.89%



### Destination IP Addresses

ff02::16/128	2.74 Kpps	100.00%
--------------	-----------	---------

No Data

### Source TCP Ports

No items available.

# No Data

### Destination TCP Ports

No items available.

# No Data

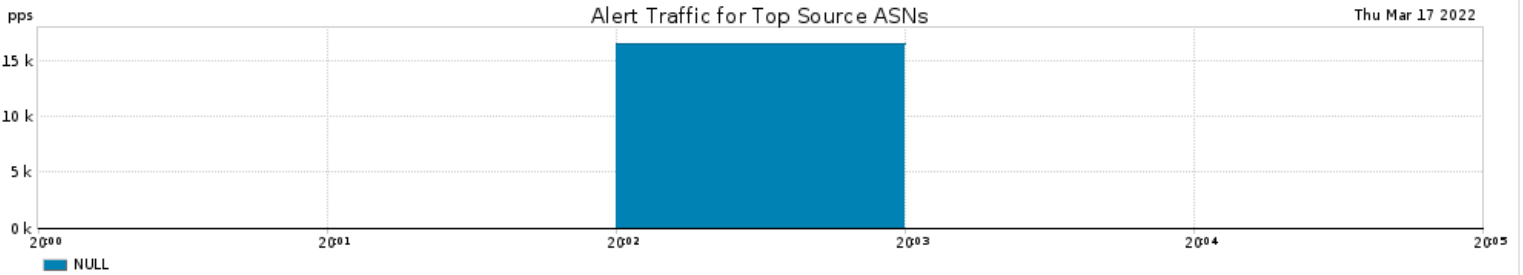
### Source UDP Ports

No items available.

# No Data

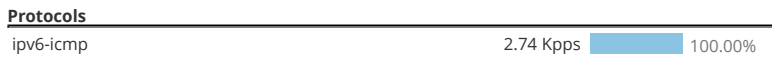
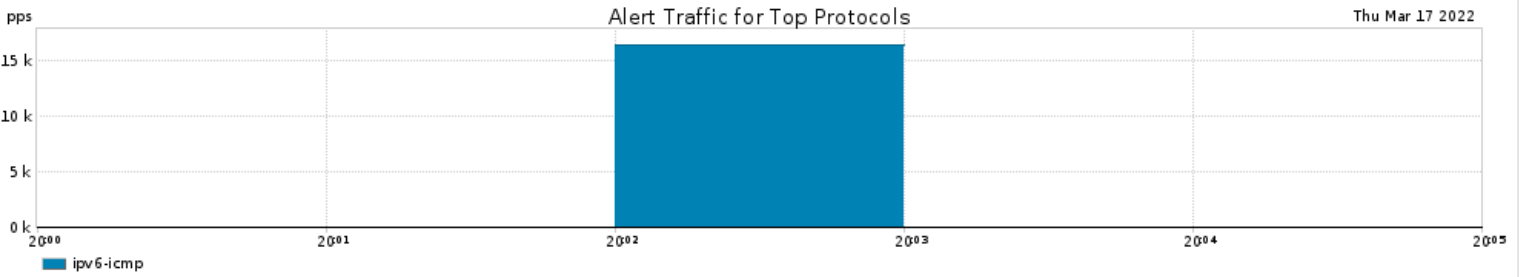
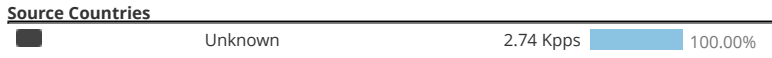
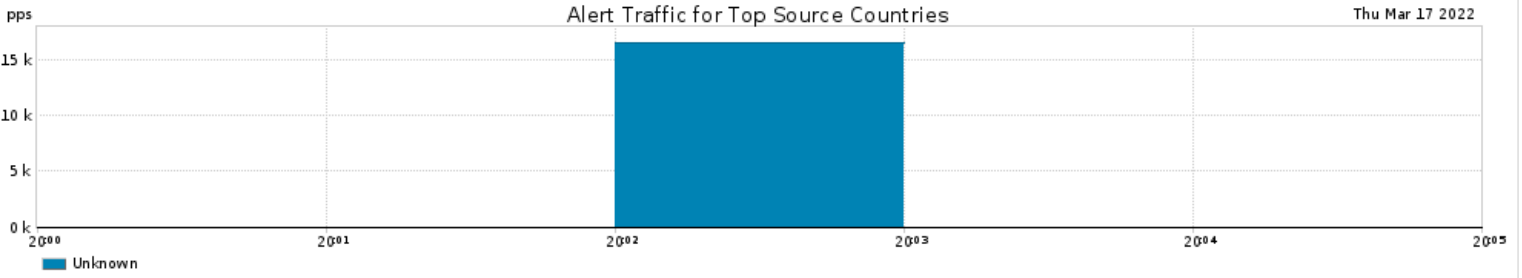
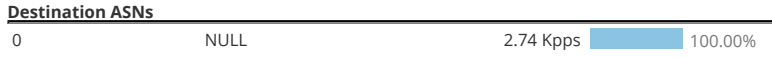
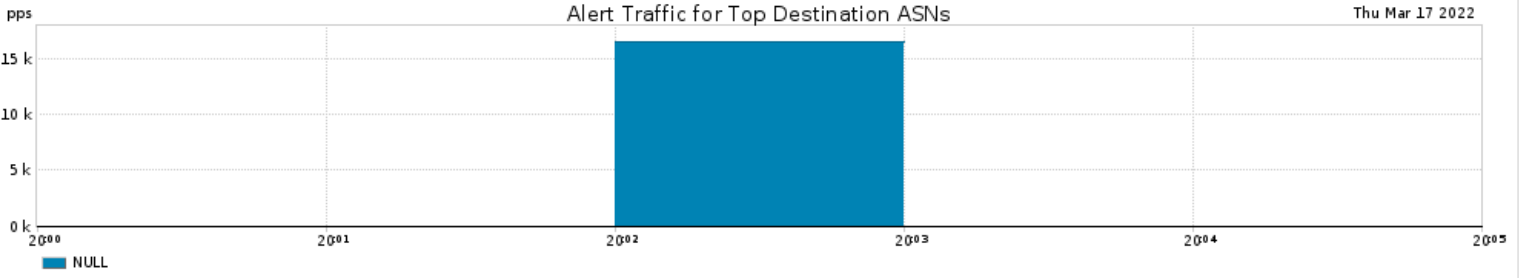
### Destination UDP Ports

No items available.



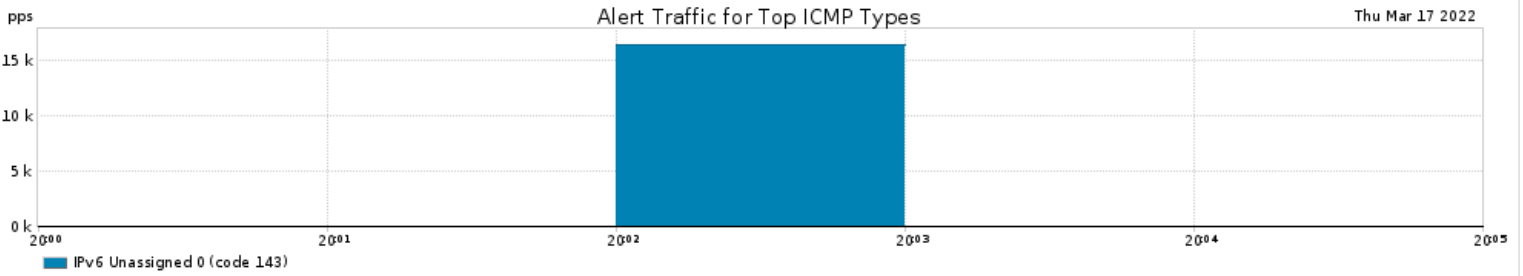
### Source ASNs

0 NULL 2.74 Kpps 100.00%



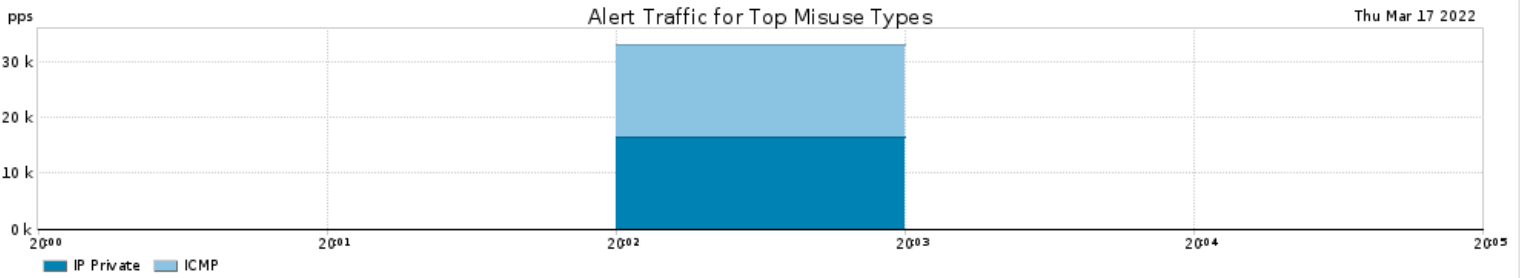
No Data

**TCP Flags** No items available.



#### ICMP Types

IPv6 Unassigned 0 (code 143) 2.74 Kpps 100.00%

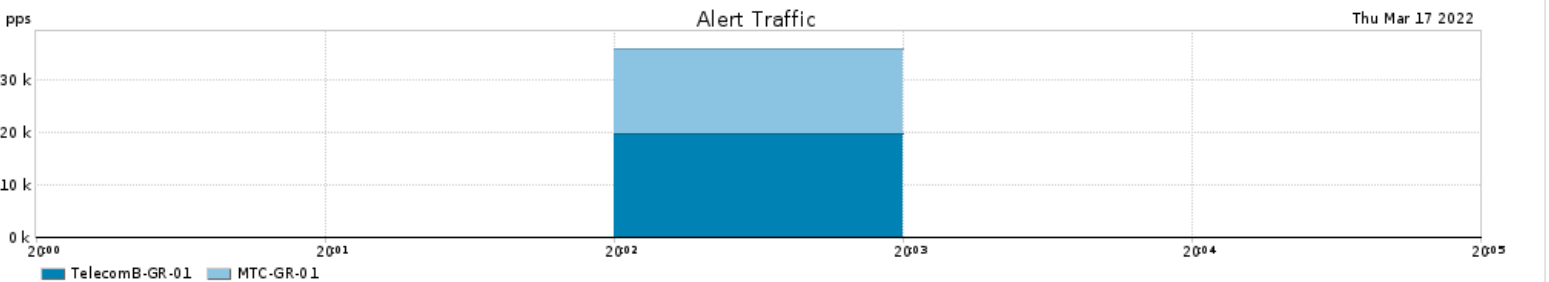


#### Misuse Types

IP Private 2.74 Kpps 100.00%

ICMP 2.74 Kpps 100.00%

#### Routers



Name (# Interfaces)	Severity	Interface Direction	Interface Boundary	Interface ASNs	Avg Packet Size	Max Observed	Average Observed
<b>TelecomB-GR-01</b> (2)	Medium	-	-	-	115	18.1 Mbps 19.6 Kpps	3.0 Mbps 3.3 Kpps
<b>Filtered by Router</b>		OUT			115	18.1 Mbps 19.6 Kpps	3.0 Mbps 3.3 Kpps
<b>HundredGigE0/9/0/3</b> MICE Arista port Eth6/14		IN	Network		115	18.1 Mbps 19.6 Kpps	3.0 Mbps 3.3 Kpps
<b>MTC-GR-01</b> (3)	High	-	-	-	119	15.7 Mbps 16.4 Kpps	2.6 Mbps 2.7 Kpps
<b>Filtered by Router</b>		OUT			119	15.7 Mbps 16.4 Kpps	2.6 Mbps 2.7 Kpps
<b>BVI3</b> Midwest Internet Cooperative Exchange (MICE)		IN	Network		120	7.2 Mbps 7.4 Kpps	1.2 Mbps 1.2 Kpps
<b>TenGigE0/0/0/6</b> Loop to Te-0-2-0-6 for MICE I1 access		IN	Network		118	8.5 Mbps 9.0 Kpps	1.4 Mbps 1.5 Kpps

#### Annotations

##### Alert Classification Possible Attack

The "IP Private" host alert signature has been triggered at router "MTC-GR-01". (expected rate: 2.50 Kpps, observed rate: 14.90 Kpps)  
auto-annotation on Thu Mar 17 20:00:10

This alert was generated due to fast flood detection. The "ICMP" host alert signature has been triggered at router "MTC-GR-01". (expected rate: 2.50 Kpps, observed rate: 14.90 Kpps)  
auto-annotation on Thu Mar 17 20:00:10

For assistance with this product, please contact support at <https://support.arbornetworks.com>

About