Unicast-flood detection

Successfully pass the free certification exam at IW Academy and become an Infinet Certified Engineer.

To the certification exam

Unicast-flood occurs when the unicast frame's destination MAC-address is unknown for the switch (not included in its routing table), it sends this frame to all interfaces of the network, besides the sender interface. The most common reasons of unicast-flood are:

- MAC address table overflow (a common problem in large networks)
- Hosts with ARP timers longer than the ARP cache time on switches
- Incorrect STP settings
- Incorrect switch groups settings (in particular, when the IDs of switch groups for the receiving and sending traffic are different).

The unicast-flood process on devices is the following: if the frame's destination MAC-address is not included in the unit's MAC switch forwarding table, then this frame is flooded to all interfaces besides the sender interface. The distribution occurs until the unit receives a frame with this MAC-address as the sender (i.e., the interface to which the frame was destinated to respond). After that, the device will learn: it will add this MAC address to the MAC switch forwarding table and map it with the interface from which it was received. If the device does not learn in 4 seconds, and frames still arrive, then traffic to this direction will be blocked for 4 seconds. Then the process repeats.

This process has the following representation in the unit's interfaces and links graphs:

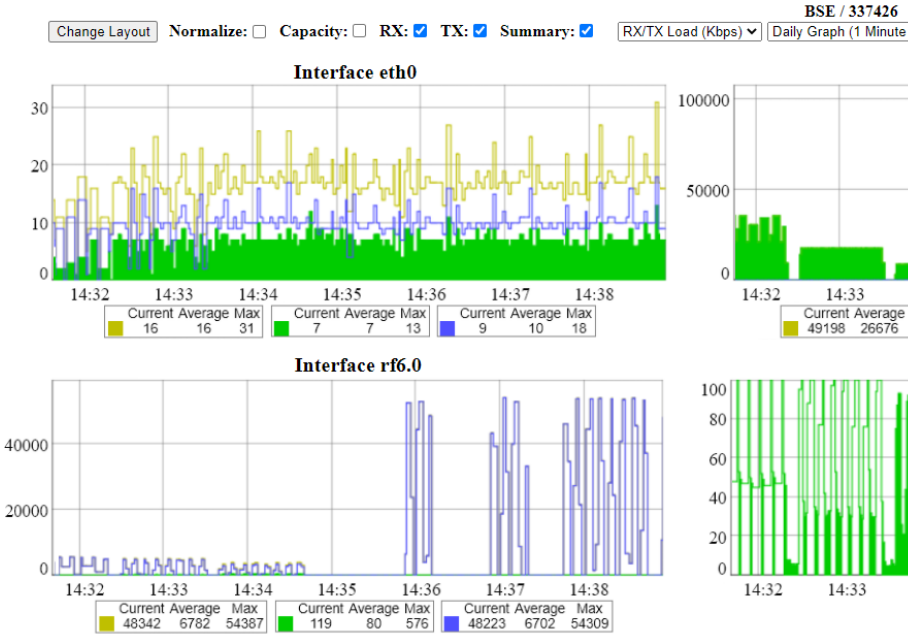


Figure - Unicast-flood example in the interfaces graphs

Also, unicast-flooding can be detected in the "Switch Statistics" → "Device Status" tab in "Flood" column:

ID	Unicast	Broadcast	Flood	STP
kernel	3779	2	0	0
1	2276	1791	0	0
2	0	20	5330077	0

Figure - Unicast-flood detection in switch statistics

Infinet Wireless units provide unicast-flood protection. If necessary, you can allow unlimited unicast-flood without protection filter through the switch group by setting the check box in "Basic Settings" → "MAC Switch" settings:

Title

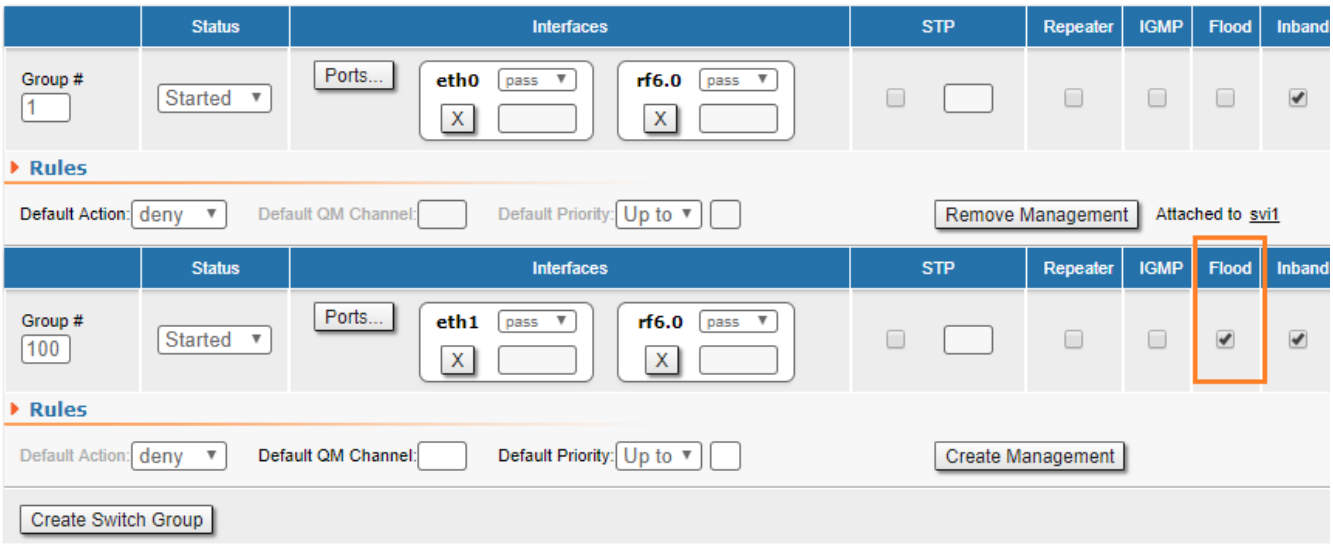


Figure - How to allow unicast-flood without protection filter

Devices react to unidirectional traffic (which is not a unicast-flood) in a similar manner. This happens, for example, in case of generating "artificial" traffic (using specialized units or software) or when the real traffic is unidirectional. In these cases, it is recommended to allow unlimited unicast-flood through the switch group without protection filter.