

Bridging

<https://campus.barracuda.com/doc/95258939/>

A Layer 2 bridge checks the destination MAC address of each incoming frame. If the MAC address is assigned to the bridge computer, the frame is processed by it as the destination. If the MAC address is not assigned to the bridge computer, the network bridge notes the source address of the frame and the port on which the frame was received and either creates or refreshes an entry in a Layer 2 bridge table. The port is a number that identifies the network adapter and its corresponding LAN segment. Each entry in the Layer 2 bridge table consists of a MAC address, the port number corresponding to the LAN segment on which a frame from the MAC address was received, and a timeout value. Entries in the Layer 2 bridge table persist for 5 minutes before being removed.

- [How to Configure Layer 2 Bridging](#)
- [How to Configure Routed Layer 2 Bridging](#)
- [How to Configure Layer 3 Bridging](#)

For more information on bridging parameters, see [Bridging Configuration Settings](#).

Bridging Type Feature Comparison

To help you decide which method to use, the following table compares the features that are available for each bridging method:

Features	Transparent Layer 2 Bridging	Routed Layer 2 Bridging	Layer 3 Bridging
MAC Transparent	Yes	Yes	No
Routing-Bridging-Forwarding	No	Yes	Yes
Local Firewall Traffic (Gateway)	No	Yes	Yes
Auto Learning of Network Nodes	Yes	Yes	No
Active Learning of Network Nodes	No	Yes	No
Next Hop Bridging	Yes	Yes	No
Broad-Multicast Propagation	Yes	Yes	Yes
High Availability	Yes	Yes	Yes
VLAN capable	Yes	Yes	Yes
IP and ARP Forwarding	Yes	Yes	Yes
Non IP Protocols Forwarding	No	No	No
IPv6	No	No	No
IPS	Yes	Yes	Yes

Application Control (Application Detection)	Yes	Yes	Yes
SSL Inspection	No	Yes - default route required	Yes - default route required
URL Filter	Yes - default route required	Yes - default route required	Yes - default route required
Virus Scanning	No	Yes - default route required	Yes - default route required
ATP	No	Yes - default route required	Yes - default route required
Safe Search	No	Yes - default route required	Yes - default route required
YouTube for Schools	No	Yes - default route required	Yes - default route required
Google Accounts	No	Yes - default route required	Yes - default route required
File Content Filtering	Yes	Yes - default route required	Yes - default route required
User Agent Filtering	Yes	Yes	Yes
Custom Block Pages	No	Yes	Yes

Bridging on VMware ESXi

Before configuring a Layer 2 bridge on a virtual Barracuda CloudGen Firewall running on a VMware ESXi hypervisor, you must enable promiscuous mode for all network interfaces and vSwitches that are used by the bridge.

Security Weaknesses and Solutions

Because bridging heavily depends on broadcasts for establishing connectivity, this results in a few weak points that you must carefully consider. Try to implement bridging in a trusted environment. Broadcasts in huge environments also consume a lot of bandwidth. The CloudGen Firewall offers different methods to help prevent the following common attacks.

Preventing IP or ARP Spoofing over Layer 2 Bridges

Network nodes may use the IP addresses of fake ARP responses in order to fake network traffic with arbitrary IP addresses. Because firewall security is enforced on Layer 3, the security policy is

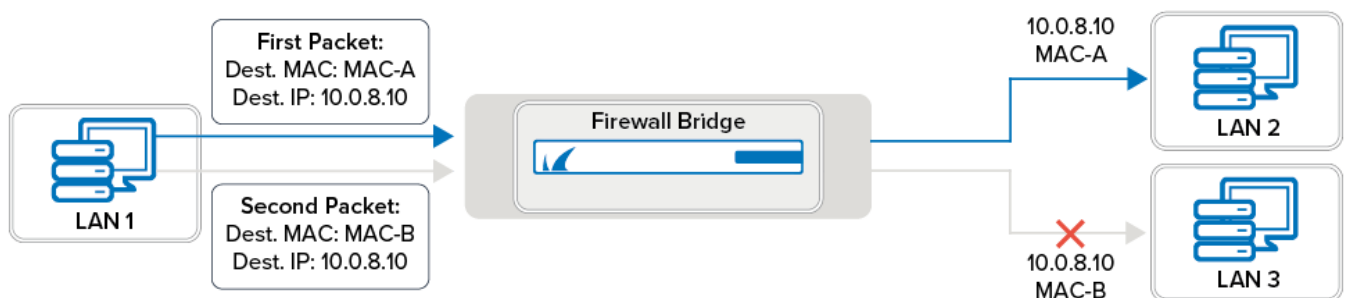
bypassed. These issues can be solved by taking the following measures:

- **Segment Access Control Lists (Bridging Interface ACLs)** – Specify which IP addresses are allowed on a segment.
- **Static Bridge ARP Entries** – Statically specify IP addresses, MAC addresses, and segments to avoid learning via ARP.
- **MAC-based Access Rules** – Define source MAC conditions for network objects.
- **ARP Change Reporting** – Specify which types of the IP-MAC-Segment relationship changes must be reported in the access cache and log.

Prevent Destination MAC Spoofing

Another security issue in bridged environments is the possible exploitation of security enforcement on Layer 3 and traffic delivery on Layer 2. You can prevent these issues by enforcing Layer 2 when a Layer 3 session is granted. MAC addresses for a session are fixed when the session is created and remain enforced until the session ends.

In the figure below, a client from LAN 1 tries to force a connection grant to a client in LAN 3. To do so, it sends a packet to the client in LAN 2 using MAC-A as a destination MAC address and 10.0.8.10 as the destination IP address. After the session has been granted through the bridge and communication has been allowed, it sends a second packet exchanging the MAC address for the client in LAN 2 with the MAC address for the client in LAN 3, leaving the IP address the same. If MAC enforcement is configured, the connection with the spoofed MAC address will not be allowed.



Figures

1. br_mac_spoofing.png

© Barracuda Networks Inc., 2021 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.