# BIG-IP System: Configuring the System for Layer 2 Transparency

Version 13.1

# Table of Contents

# Overview: Configuring the BIG-IP system as a Layer 2 device with wildcard VLANs

### Introduction

To deploy a BIG-IP® system without making changes to other devices on your network, you can configure the system to operate strictly at Layer 2. By deploying a virtual wire configuration, you transparently add the device to the network without having to create self IP addresses or change the configuration of other network devices that the BIG-IP device is connected to.

A *virtual wire* logically connects two interfaces or trunks, in any combination, to each other, enabling the BIG-IP system to forward traffic from one interface to the other, in either direction. This type of configuration is typically used for security monitoring, where the BIG-IP system inspects ingress packets without modifying them in any way.

---

***Important:*** *The virtual wire feature is not available on systems provisioned for Virtual Clustered Multiprocessing (vCMP).*

---

### Sample configuration

This illustration shows a virtual wire configuration on the BIG-IP system. In this configuration, a VLAN group contains two VLANs tagged with VLAN ID 4096. Each VLAN is associated with a trunk, allowing the VLAN to accept all traffic for forwarding to the other trunk. Directly connected to a Layer 2 or 3 networking device, each interface or trunk of the virtual wire is attached to a wildcard VLAN, which accepts all ingress traffic. On receiving a packet, an interface of a virtual wire trunk forwards the frame to the other trunk and then to another network device.

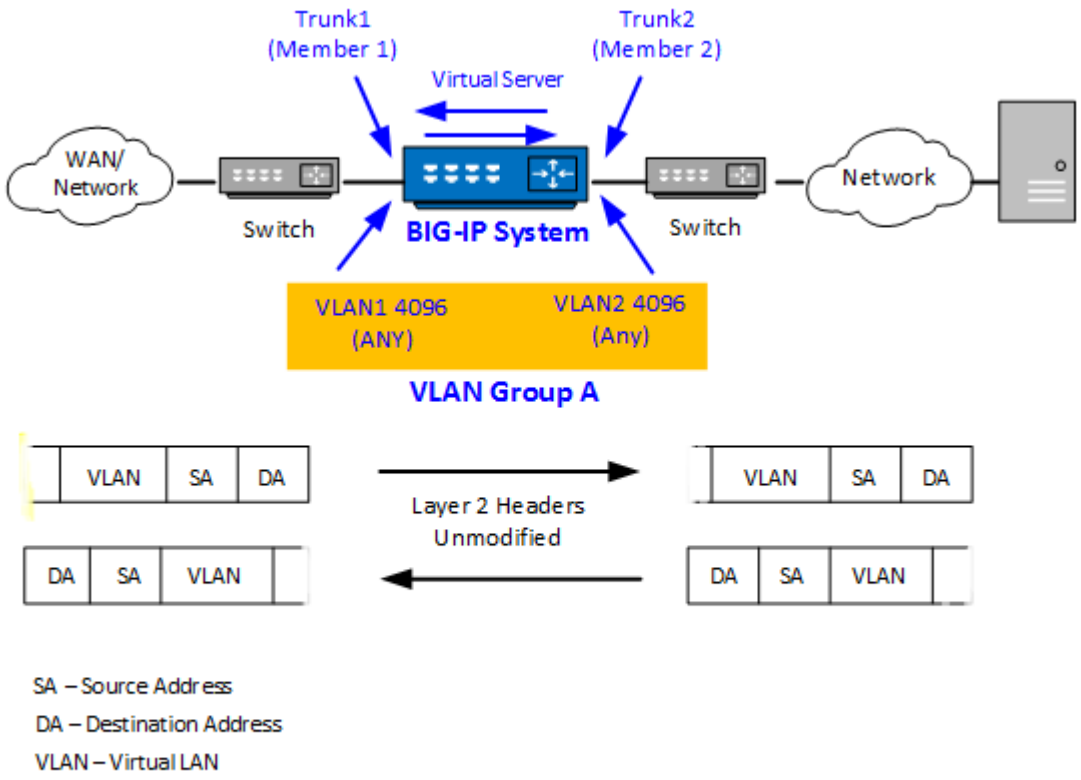


**Figure 1: Virtual wire configuration for bi-directional Layer2 transparency**

Optionally, you can create a forwarding virtual server that applies a security policy to ingress traffic before forwarding the traffic to the other trunk.

### Key points

There are a few key points to remember about virtual wire configurations in general:

- An interface accepts packets in promiscuous mode, which means there is no packet modification.
- The system bridges both tagged and untagged data.
- Source MAC address learning is disabled.
- Forwarding decisions are based on the ingress interface.
- Neither VLANs nor MAC addresses change.

---

***Note:*** *VLAN double tagging is not supported in a virtual wire configuration.*

---

*About memory consumption*

## About memory consumption

When you use the BIG-IP Layer 2 Transparency feature, the BIG-IP device switches the traffic at Layer 2, in the absence of any virtual server on the system that matches the traffic. In this case, the device maintains a "connection" state with a default age of 300 seconds. If the number of these connections is large, the BIG-IP device can experience high memory consumption.

To alleviate this, F5 recommends that you take one of the following actions:

- Configure one or more matching virtual servers to handle all traffic.

- If you are unaware of all traffic patterns, configure a wildcard virtual server instead, of type Forwarding (IP) or Performance (Layer 4). This enables the device to perform a connection close operation much more quickly and therefore mitigate high memory consumption.
- Configure a lower threshold for the BigDB variable `tm.l2forwardidletimeout`.

*Overview: Configuring the BIG-IP system as a Layer 2 device with wildcard VLANs*

*Overview: Configuring the BIG-IP system as a Layer 2 device with wildcard VLANs*

*Naming conventions for virtual wire-related objects*

For virtual wire-related configuration objects, the BIG-IP system manages object naming in specific ways. See the following table for details.

# Supported platforms for virtual wire configuration

The ability to implement Layer 2 transparency using the virtual wire feature is supported on these F5 hardware platforms:

| Platform Name | Platform ID |
|---|---|
| VIPRION B2250 blade | A112 |
| VIPRION B4450 blade | A114 |
| BIG-IP i10800, i10600 | C116 |
| BIG-IP i7800, i7600 | C118 |
| BIG-IP i5800, i5600 | C119 |
| BIG-IP i15800, i15600 | D116 |
| BIG-IP i12800, i12600 | D117 |

# Create BIG-IP objects for Layer 2 transparency

To configure the BIG-IP® system as an inline device operating in Layer 2 transparency mode, you first need to create a virtual wire configuration object. Creating a virtual wire object causes the BIG-IP system to automatically perform these actions:

- Create trunks for accepting all VLAN traffic, with Link Aggregation Protocol (LACP) enabled.
- Set the trunk members (interfaces) to virtual wire mode.
- Create two VLANs with tag 4096 that allow all Layer 2 ingress traffic.
- Create a VLAN group to logically connect the VLANs.

1. On the Main tab, click **Network** > **Virtual Wire**.

   This object appears on certain BIG-IP platforms only.

   The Virtual Wire screen opens.
2. Click **Create**.
3. In the **Name** field, type a name for the virtual wire object.
4. On the right side of the screen, click the double-arrow symbol to expand the Shared Objects panel.
5. Click within the Trunks heading area.
   This displays a list of existing trunks, and displays the + symbol for creating a trunk.
6. Click the + symbol.
7. In the **Name** field, type a name for the trunk, such as `trunk_external` or `trunk_internal`.
8. In the **Interfaces** list, select the check boxes for the interfaces that you want to include in the trunk.
9. From the **LACP** list, select **Enabled**.
   This enables the Link Aggregation Control Protocol (LACP) to monitor link availability within the trunk.
10. Click **Commit**.

    If you do not see the **Commit** button, try using a different browser.

    This creates the trunk that you can specify as an interface when you complete the creation of the virtual wire object.
11. Repeat steps 6 through 10 to create a second trunk.
12. In the Member 1 column, from the **Interfaces/Trunks** list, select a trunk name, such as `trunk_external`.
13. In the Member 2 column, from the **Interfaces/Trunks** list, select another trunk name, such as `trunk_internal`.
14. In the VLAN Traffic Management Configuration column, for the **Define VLANs** list, use the default value of **No**.
15. Click **Done Editing**.
16. Click **Commit Changes to System**.

After you perform this task, the BIG-IP system contains a virtual wire object, two trunks, two VLANs, and a VLAN group.

## Naming conventions for virtual wire-related objects

For virtual wire-related configuration objects, the BIG-IP system manages object naming in specific ways. See the following table for details.

| Object type | System-named? | Naming convention |
|---|---|---|
| Virtual wire | No | User-defined |
| Trunk | No | User-defined |
| VLAN | Yes | `virtual-wire-name`_vlan_4096_`member_number_xx` |
| VLAN group | Yes | Same name as the virtual wire object |

# Create a listener for bi-directional traffic

You create a virtual server when you want the BIG-IP® system to listen for client-side and server-side ingress traffic at Layer 2, without performing any packet modifications such as address translation.

1. Log in to the BIG-IP Configuration utility using the system's management IP address.
2. On the Main tab, click **Local Traffic** > **Virtual Servers** .

   If your BIG-IP system user account restricts you to using TMSH (TMOS® Shell) only, skip this step.
3. Click **Create**.
4. In the **Name** field, type a name, such as `my_virtual_wire_vs`.
5. From the **Type** list, select **Forwarding (Layer 2)**.
6. In the **Destination Address** field, type the IP address in CIDR format. The supported format is address/prefix, where the prefix length is in bits. For example, an IPv4 address/prefix is `10.0.0.1` or `10.0.0.0/24`, and an IPv6 address/prefix is `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`. When you use an IPv4 address without specifying a prefix, the BIG-IP system automatically uses a /32 prefix.
7. In the **Service Port** field, type a port number or select a service name from the **Service Port** list.
8. From the **VLAN and Tunnel Traffic** list, select the name of the virtual wire you previously created.
9. Click **Finished**.

# Configuration results

When you complete the Layer 2 transparency mode configuration, the BIG-IP® system contains these objects:

- Two trunks that represent `Member 1` and `Member 2` interfaces of the virtual wire. Each interface of a trunk has its forwarding mode set to **Virtual Wire**.
- A tagged VLAN for the `Member 1` trunk with a tag of 4096, assigning the `Member 1` trunk to the VLAN.
- A tagged VLAN for the `Member 2` trunk with a tag of 4096, assigning the `Member 2` trunk to the VLAN.
- A VLAN group with the transparency mode set to **Virtual Wire**, where the VLAN group name matches the name of the virtual wire object.
- A virtual server that listens for both client-side and server-side traffic. The virtual server forwards the client-side traffic to the `Member 2` trunk and forwards the server-side traffic to the `Member 1` trunk.

# Legal Notices

## Legal notices

### Publication Date

This document was published on January 25, 2019.

### Publication Number

MAN-0683-00

### Copyright



### Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

All other product and company names herein may be trademarks of their respective owners.

### Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*.

### Link Controller Availability

This product is not currently available in the U.S.

### Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

### RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

### FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a

residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

### Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

### Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

# Index