Application Note for Avaya Solutions Platform (ASP) 130 Release **6.0.0.3.0** (KVM on RHEL 8.10) and Earlier Releases.

VLAN & VLAN TRUNKING CONFIGURATION GUIDE

February 2026

Issue 2

Contents

Change History

Issue	Date	Description
1.0	**07/2025**	Initial release. Information in this document will be incorporated into the 'Installing the Avaya Solutions Platform 130 Series R6.0.x' documentation at future time.
2.0	**02/2026**	Updated ASP Software Version applicability

1. Introduction

1.1. Purpose

This application note provides guidance for configuring VLANs and enabling VLAN trunking on ASP R6.0.0.3.0 KVM on Red Hat Enterprise Linux (RHEL) 8.10 solution and earlier releases. It is intended for system administrators and technical users responsible for deploying and managing virtual infrastructure on Avaya Solutions Platform (ASP) compute servers.

The purpose of this document is to ensure that VLAN configurations are implemented consistently and correctly across the ASP R6.0 – R6.0.0.3.0 solution, enabling secure, scalable, and efficient network segmentation for Avaya application virtual machines (VMs). The procedures outlined here apply to both initial VLAN setup and modifications to existing environments, using Cockpit and command-line tools where appropriate.

The configurations described in this document are intended to **complement**, not replace, the existing information documented in the *Installing the Avaya Solutions Platform 130 Series R6.0.x documentation.*

Starting with **ASP R6.0.0.4.0** and later, a new **VLAN and VLAN Trunking Configuration Guide** is available. Customers with hosts running **ASP R6.0.0.4.0 or later** must reference the **ASP 130 R6.0.0.4.0 and Later VLAN and VLAN Trunking Configuration Guide – Rev 1**.

The network configuration script (**configNetwork**) has been significantly enhanced in this release. Customers are strongly advised to update to the latest ASP version to take full advantage of the updated network configuration capabilities when implementing VLAN or network changes.

The information in this document will be incorporated into the Installing the Avaya Solutions Platform 130 Series R6.0.x documentation in a future date. This document will continue to be updated until then. Ensure that you are signed up for Avaya E-notifications so that you will be notified when new issues of this Application Note are posted.

1.2 Overview of ASP 130 R6.0 Supported Network Topologies

Scenario	Supported	Details
Single VLAN per physical adapter	✅	Standard setup using one VLAN per NIC; configured using the configNetwork script.
Multiple VLANs on separate NICs (no bonding)	✅	Each VLAN configured on a different NIC and bridge; allows network segregation without trunking.
Multiple VLANs on same NIC (VLAN trunking)	✅	VLAN tagging (802.1Q) enabled; up to 5 VLANs per 1 Gbps adapter. Requires manual configuration via Cockpit.
VLAN trunking with bonded interfaces	✅	VLANs configured on a bonded interface (bond0); bridges created per VLAN. Recommended for scalable designs.
OOBM VLAN tagging	✅ (Single VLAN)	Supported via configNetwork script; only one VLAN allowed per OOBM NIC. No trunking on OOBM.
Multiple VLANs on a single bridge	❌	Not supported in ASP R6.x. Each VLAN must use its own bridge.
VLAN tagging within guest OS (VM layer)	❌	VLANs must be configured at hypervisor layer only; VM-level tagging is not supported in ASP R6.x.
LAG (802.3ad) / Active-Active bonding	🚫 (Future)	Not currently supported; active-standby bonding only. Future support planned.

2. VLAN Configuration Overview

2.1 VLAN Fundamentals

A VLAN (Virtual Local Area Network) is a logical grouping of devices within a network, designed to segment and isolate traffic for improved security, performance, and management. Devices within the same VLAN can communicate with each other, regardless of their physical location, while devices in different VLANs **require a router** or **layer 3 switch** for communication (Not provided by Avaya).

Note: Link aggregation IEEE 802.2ad (LAG) support will be documented in a future release.

2.2 Recommended Practices

General Considerations

Although bandwidth is not limited by the number of VLANs configured, all traffic—regardless of VLAN segmentation—shares the physical constraints of the underlying link, in this case 1 Gbps ports. Excessive

VLAN configuration can lead to unmanaged traffic that may exceed link capacity if not properly planned, resulting in saturation, degraded performance, and unpredictable network behavior.

VLAN Design & Segmentation

- Use separate VLANs for:
  - Management traffic (e.g., servers, switches, application management traffic)
  - VoIP traffic (e.g., IP phones, voice gateways, Avaya application traffic).
- Avoid placing **all VLANs on a single physical adapter** (server and switch side). Instead, separate high-traffic VLANs using dedicated links for **load spreading** when possible.

Enable 802.1Q Trunking

- Use IEEE 802.1Q to tag VLAN traffic.
- Ensure matching trunk configurations on both ends (Customer Data switches/routers- ASP 130 servers).

Limit Allowed VLANs

- Only allow necessary VLANs on the trunk.
- For the **Avaya ASP R6.0 solution**, allocate **1–5 VLANs max per dedicated 1 Gbps port** to ensure optimal performance.

Apply Quality of Service (QoS)

- Prioritize time-sensitive traffic like VoIP or video:
  - Use **DSCP EF (Expedited Forwarding)** or **802.1p CoS/PCP = 5 or above marking.**
  - Follow each Avaya Application best practices when setting QoS.
- Implement **traffic shaping or prioritization** as needed to prevent congestion (e.g., LLQ or priority queues).
- Ensure low latency (<150 ms), low jitter (<30 ms), and minimal packet loss (<1%) for VoIP traffic.

Bandwidth Monitoring & Capacity Planning

- (Customer Network) Continuously monitor trunk port utilization, using 3rd party NMS tools (not provided by Avaya) such as: PRTG, LibreNMS, NetFlow/sFLOW, ntopng, SolarWinds etc.
- Estimate bandwidth usage (consult with each Avaya application documentation):

VoIP (audio only):

- G.729 (low bandwidth): ~8–24 Kbps per call
- G.711 (standard quality): ~80–100 Kbps per call
- G.722 / Opus (wideband/high-fidelity): ~64–128 Kbps per call

VoIP with video:

- 480p (SD): ~500 Kbps – 1 Mbps
- 720p (HD): ~1 – 1.5 Mbps
- 1080p (Full HD): ~1.5 – 3 Mbps

- 4K (UHD): ~4 – 8 Mbps

VoIP with Audio, Video, and Collaboration

- **Screen sharing or document collaboration typically adds:**
  - **150 – 500 Kbps (static content)**
  - **1 – 2 Mbps (dynamic screen sharing with motion/video)**

Management traffic: Typically low, with occasional spikes during remote sessions, firmware updates, or backups.

- Maintain average trunk utilization **below 80%** to avoid congestion and preserve voice/video quality.

Regularly Audit Traffic Flows

- Verify expected inter-VLAN routing behavior and enforce separation between management and VoIP VLANs.
- Review firewall/ACL rules to minimize unnecessary traffic between VLANs.

⚠️ Warning Signs of Overuse or Saturation

Symptom	Possible Cause
🌐 **Slow network performance**	**Aggregate traffic exceeding 1 Gbps**
📉 **High latency, jitter, VoIP/video struggling**	**Network congestion**
❌ **Dropped packets**	**Buffer overflow from oversubscription**
❌ **Dropped VoIP calls or registration failures**	**QoS misconfiguration or bandwidth saturation**
📦 **Excessive broadcast/multicast**	**Poorly segmented or unmanaged VLANs**
🚦 **Sustained port utilization > 80%**	**Risk of saturation during peak times**
🔁 **Frequent re-transmissions**	**Collisions or congestion-induced packet loss**
🚨 **SNMP/monitoring alerts on CPU or interface load**	**Potential network congestion or broadcast storm**

3 VLAN Configuration Scope, Limitations, and Supportability

This section outlines the supported VLAN deployment models for ASP 130 R6.0 systems running KVM on RHEL 8.10. It defines tested configurations, documents known limitations, and provides clear guidance on what changes are allowed or restricted to preserve supportability across the platform.

Supported and Validated VLAN Configuration Methods

The following VLAN configuration methods are validated and supported on ASP 130 R6.0:

- VLAN tagging must be configured **at the hypervisor level** (host OS layer). VLAN tagging within guest operating systems (VMs) is **not supported**.
- The default VLAN configuration workflow uses the *configNetwork* script for assigning a single VLAN per physical NIC or per bridge (e.g., `bridge0`, `bridgeoob`).

- Advanced VLAN trunking and multi-VLAN configurations are supported **via Red Hat Cockpit**, specifically for:
    - Multiple VLANs on a single NIC
    - VLAN trunking with bonded interfaces (e.g., `bond0`)
- Each VLAN must be mapped to a dedicated Linux bridge (e.g., `br-2011`, `br-2014`). Multiple VLANs on a single bridge are **not supported**.

These supported methods apply to both initial deployments and subsequent reconfigurations of ASP 130 servers.

3.1 Supported and Validated VLAN Configuration Methods

The following VLAN configuration methods are officially supported and validated by Avaya for the ASP 130 R6.0 solution. Any deviations from these methods require prior written approval from Avaya.

Supported Methods

- **Single VLAN per Interface (Standard Configuration):**
  The *configNetwork* script can be used to assign a single VLAN to a physical interface. This is the default and most supported deployment for basic management and application separation.
- **VLAN Trunking on a Single Adapter:**
  VLAN tagging using 802.1Q can be applied to a single NIC via Cockpit. Multiple VLANs are supported, with each VLAN requiring its own Linux bridge (e.g., br-2011, br-2014). This method enables multiple traffic segments over a single 1 Gbps connection.
- **VLAN Trunking with Bonded Interfaces:**
  Bonded interfaces (active-standby only) may be used as parent interfaces for trunked VLANs. VLANs must be created on the bond (e.g., `bond0.1010`, `bond0.2011`) and assigned to independent bridges. This topology offers resiliency and simplifies cable management while preserving VLAN segmentation.

- **OOBM VLAN Support:**
  A single VLAN ID can be applied to the Out-of-Band Management interface using the configNetwork script. VLAN trunking is **not** supported on OOBM interfaces.

⚠️ **Constraints**

- Only the above configurations are validated and supported.
- **VLAN tagging within the guest OS** is not supported.
- **LAG / 802.3ad (active-active bonding)** is not supported as of R6.0.x.

3.2 Configuration Scope and Known Limitations

The following constraints are enforced to ensure system integrity and predictable behavior:

Scope

- VLAN tagging is limited to:
  - Physical NICs for basic single-VLAN configurations
  - Bonded interfaces for trunking with redundancy
- The configNetwork script supports only:
  - One VLAN per physical interface or bridge
  - No support for trunking or multi-VLAN bridges
- VLAN interfaces created through Cockpit must be mapped **one-to-one with individual bridges**

Limitations

- **Out-of-Band Management (OOBM)** is restricted to a single VLAN and cannot participate in trunking
- **LAG/802.3ad** (link aggregation) is **not supported** in this release
- Cockpit must **not** be used to modify:
  - bridge0 or bridgeoob when configured via the script
- VLAN tagging **within the VM guest OS** is unsupported

⚠️ *Unsupported changes may lead to network failure or require a full host re-image to restore connectivity.*

3.3 Supportability Guidelines and Change Control

Strict adherence to supported configurations is required to maintain eligibility for Avaya support. Any deviation from these guidelines should be treated as a controlled change.

Support Guidelines

- Only the VLAN configuration procedures outlined in this document are validated by Avaya
- Use of system tools such as `nmcli` is permitted only as outlined in this document. Any other tools, commands, or procedures not documented here are, by default, considered unsupported.
- Changes to `OOBM`, `bridge0`, or existing bonded interfaces via Cockpit are **not supported** if those components were originally configured using the script

Change Control Requirements

- Submit a request to Avaya support before applying custom VLAN or bond configurations outside the documented models
- Maintain configuration backups and change logs before applying VLAN changes
- If unsupported configurations are applied and connectivity is lost, a full re-image of the host may be required

📌 *To confirm whether a specific VLAN topology is supported, customers are advised to contact Avaya technical support prior to implementation.*

4 Supported VLAN Topologies in the ASP 130 R6.0 Solution

Red Hat Enterprise Linux (RHEL) offers a variety of options and configurations for VLAN setup and 802.1Q VLAN tagging. While the Red Hat vendor does not provide a single "best" recommended configuration, it is important to note that for Avaya ASP R6.0, the only tested and supported configuration methods are the ones included in this document.

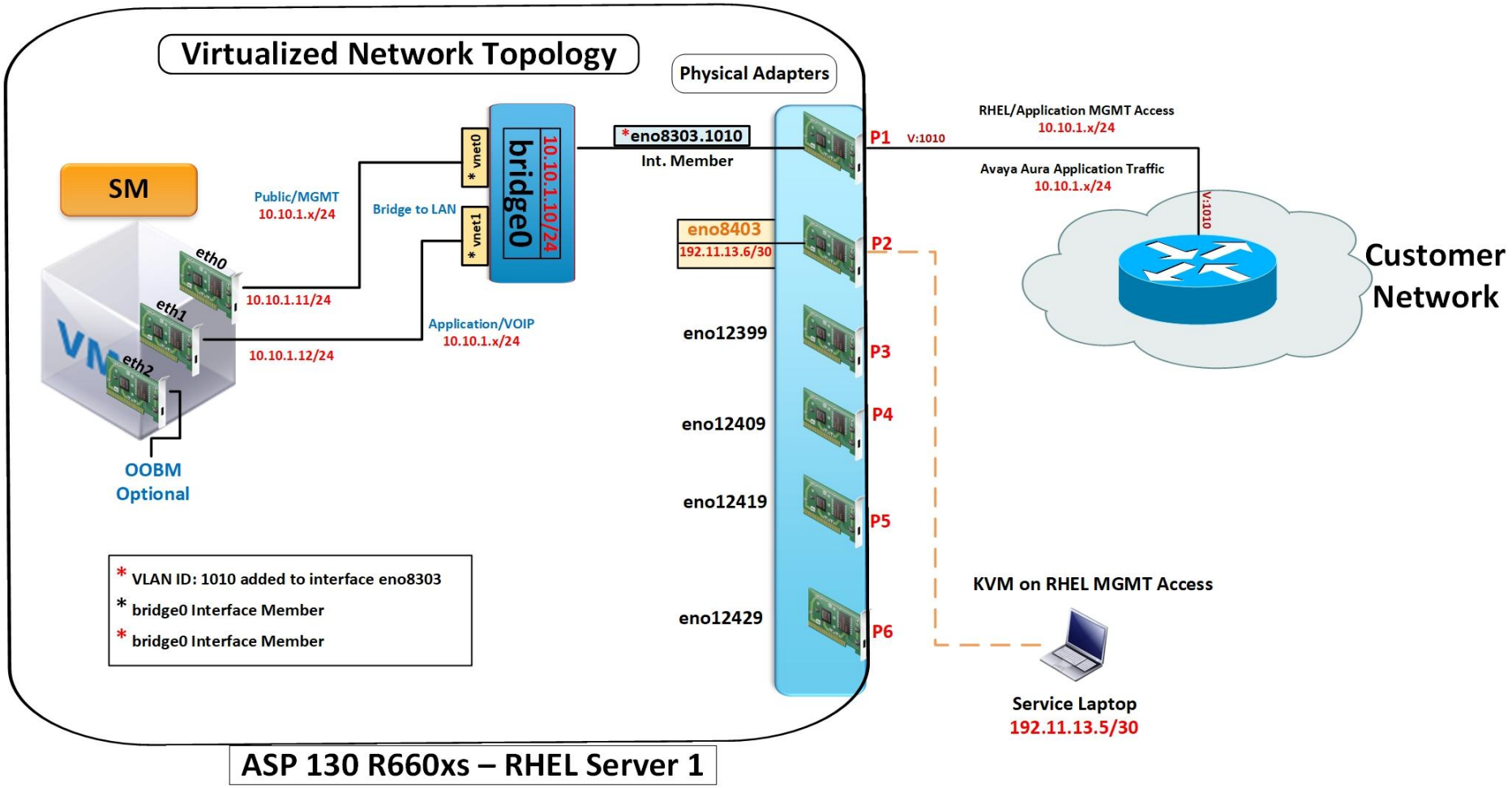
Warning While alternative configurations may be supported, they require prior approval from Avaya. If the desired configuration is not listed in this section, contact Avaya support for approval before proceeding with implementing network changes on the host.

Note: Following topologies are also applicable to customers with ASP 130 R640 KVM on RHEL 8.10 servers.

Note: For details on network port mapping and physical interface differences between Dell R640 and R660xs servers, refer to the **NIC assignment mapping** section in the *Installing the Avaya Solutions Platform 130 Series* guide.

4.1 Single VLAN configuration in an ASP 130 R6.0 – Hypervisor Layer:

Note: In this topology, the VLAN ID is assigned to the physical adapter.

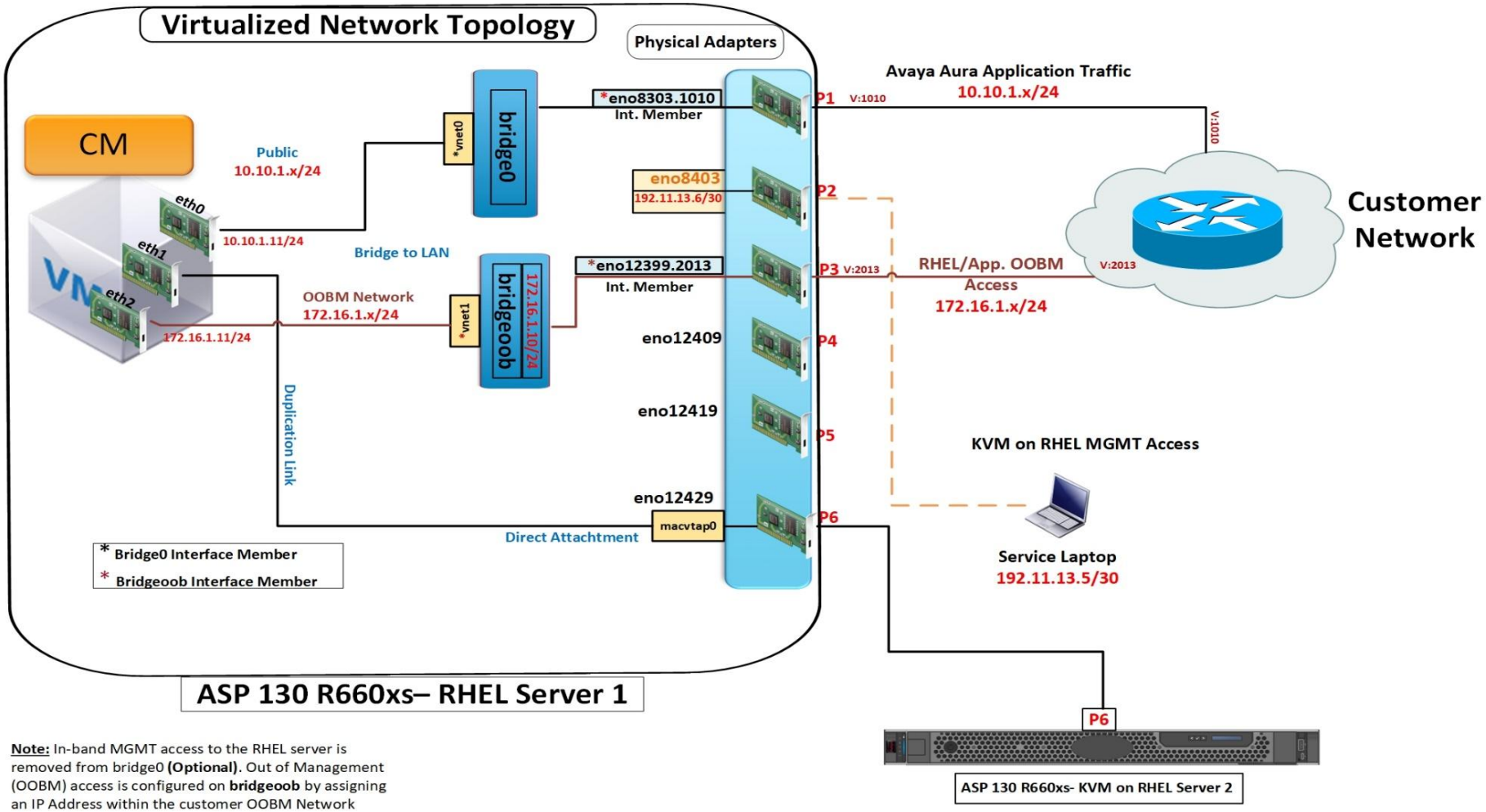


- ASP 130 KVM on RHEL Network Topology with a single VLAN configured. Bonding & OOBM is not configured.

Figure 1 – Single VLAN Configuration

4.2 Single VLAN configuration with OOBM, no Bond in an ASP 130 R6.0 – Hypervisor Layer:

Note: In this topology, each VLAN ID is assigned to a physical adapter.



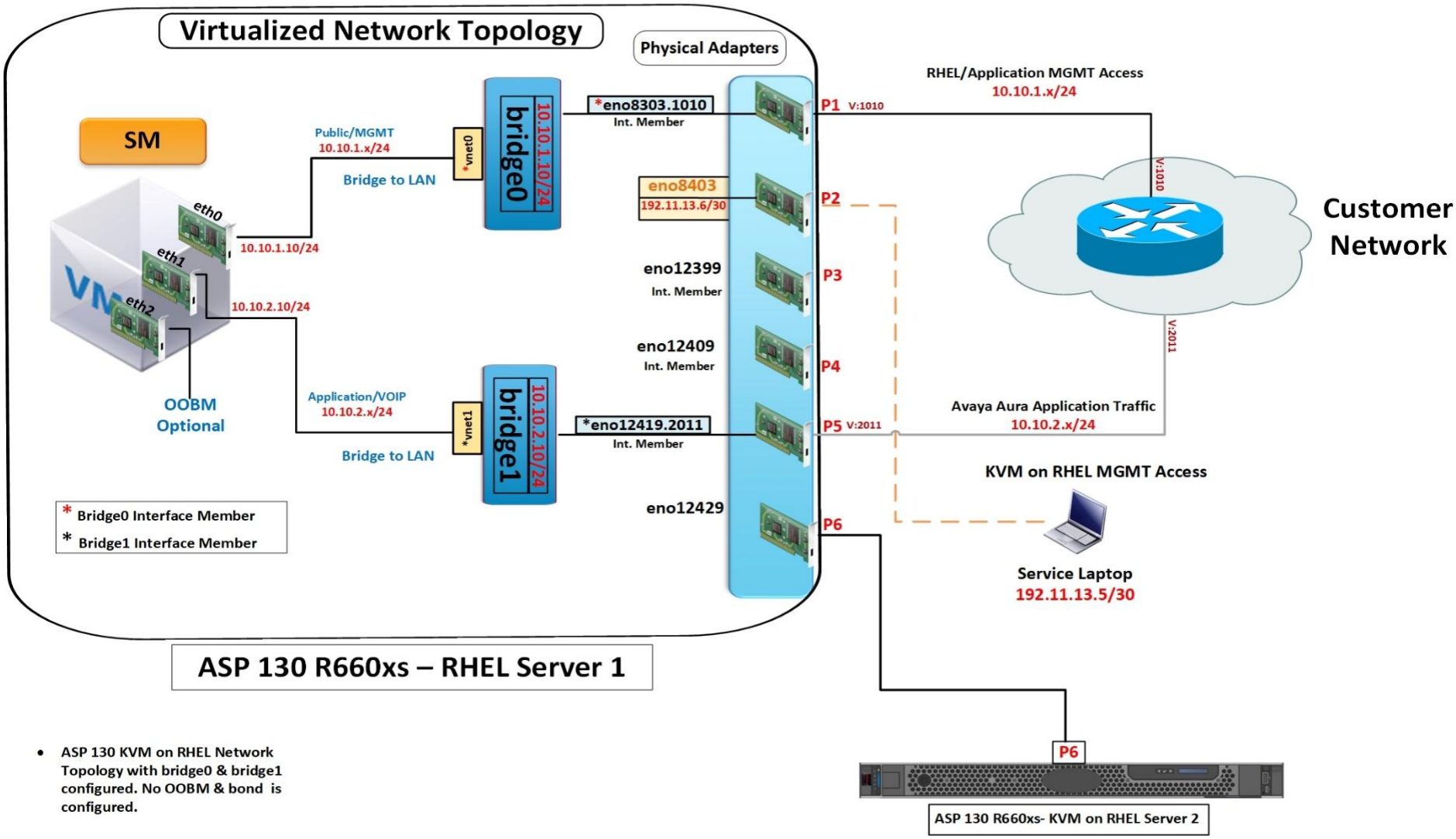
Note: In-band MGMT access to the RHEL server is removed from bridge0 **(Optional)**. Out of Management (OOBM) access is configured on **bridgeoob** by assigning an IP Address within the customer OOBM Network segment.

- **ASP 130 RHEL 8 Network Topology with OOBM configured and no bonding.**

Figure 2 – Single VLAN Configuration with OOBM

4.3 Multiple VLAN configuration on separate bridges in an ASP 130 R6.0 – Hypervisor Layer:

Note: In this topology, each VLAN ID is assigned to a unique physical adapter. Bonding is not configured.

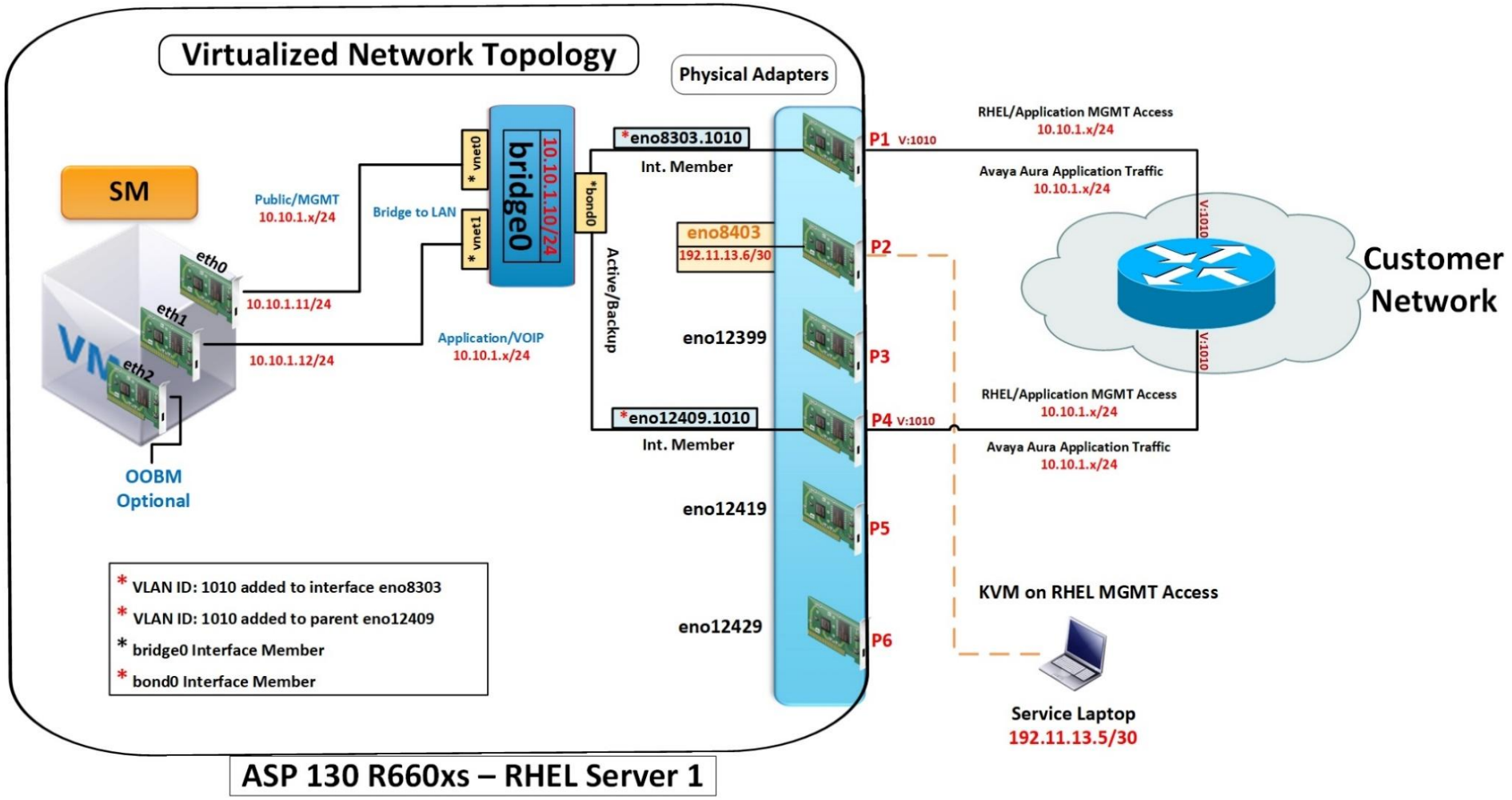


- ASP 130 KVM on RHEL Network Topology with bridge0 & bridge1 configured. No OOBM & bond is configured.

Figure 3 – Multiple VLAN Configuration on Separate Bridges

4.4 Single VLAN configuration with bonding in an ASP 130 R6.0 – Hypervisor Layer:

Note: In this topology, the VLAN ID is assigned to each physical adapter rather than the bond.

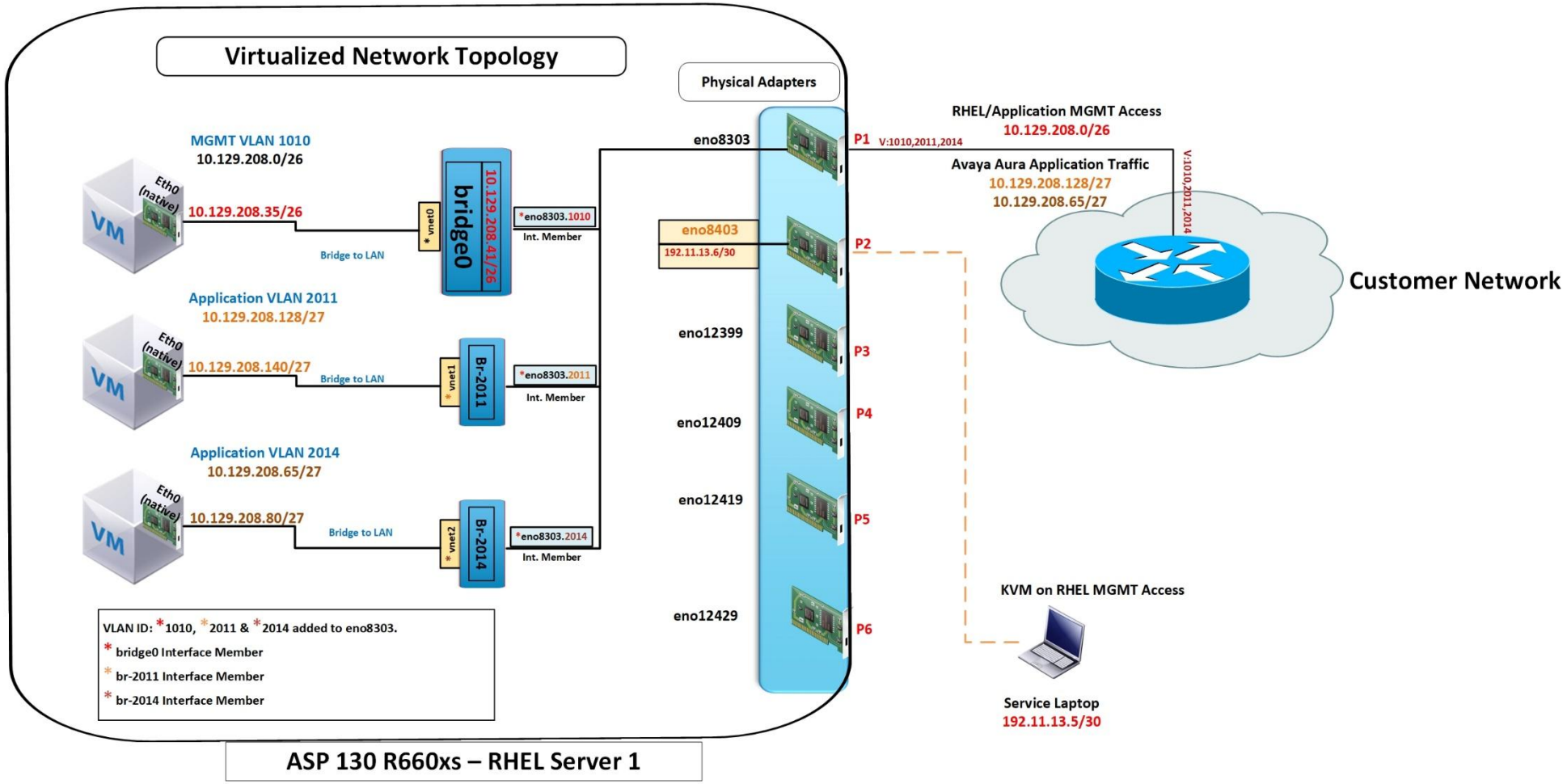


- ASP 130 RHEL Network Topology with bond0 and a single VLAN is configured. No OOBM is configured.

Figure 4 – Single VLAN Configuration with Bonding

4.5 Multiple VLAN configuration with no bonding in an ASP 130 R6.0 – Hypervisor Layer:

Note: In this topology, each VLAN ID is assigned to a physical adapter.



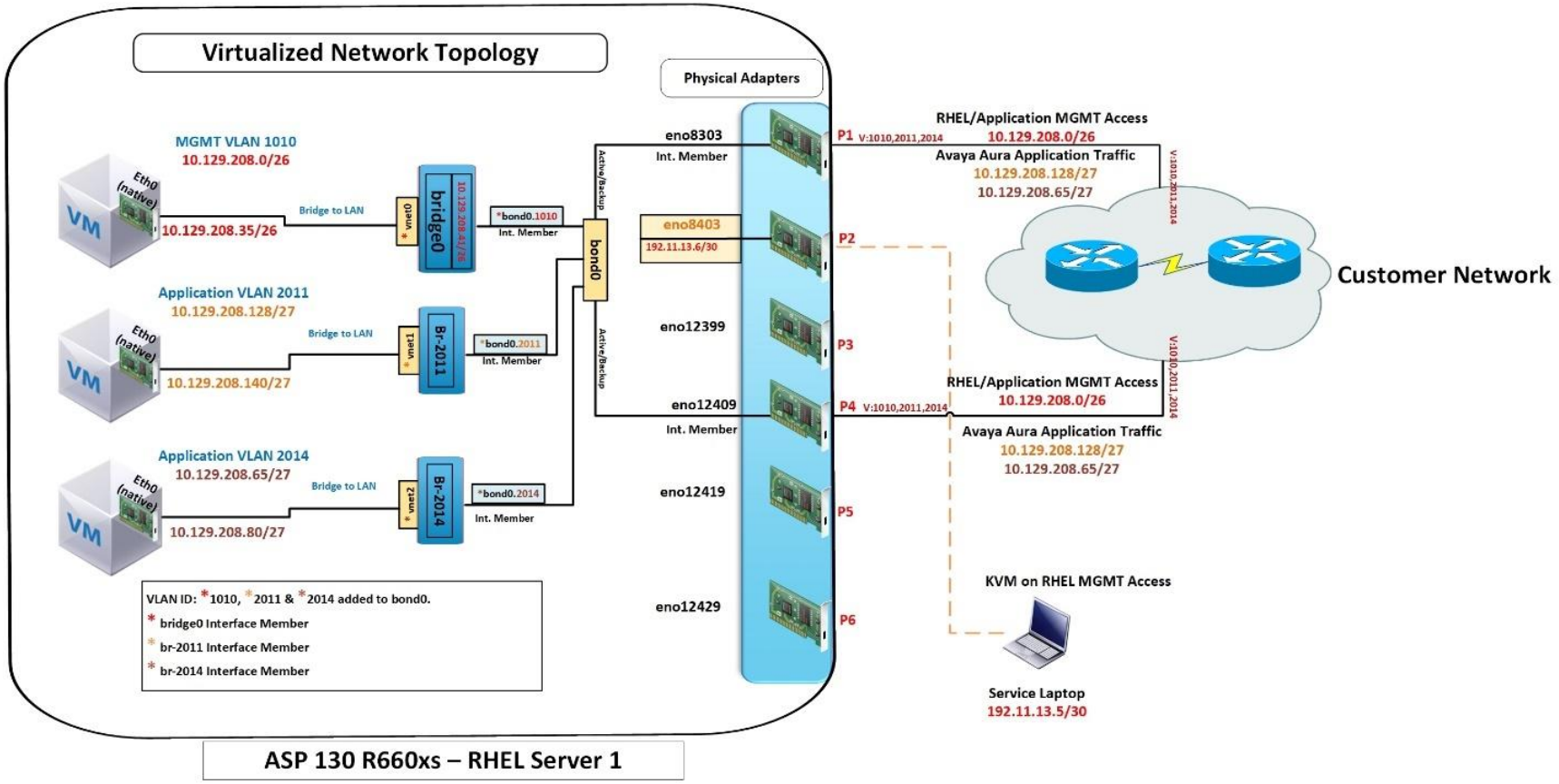
- ASP 130 KVM on RHEL Network Topology with multiple VLAN configuration. Bonding & OOBM is not configured.

Figure 5 – Multiple VLAN Configuration with no Bonding

4.6 Multiple VLAN configuration with bonding in an ASP 130 R6.0 – Hypervisor Layer:

Note: This topology can support up to two bonds if necessary, leaving one remaining NIC (physical adapter) available for either Out-of-Band Management (OOBM) or Communication Manager (CM) duplication traffic.

Note: In this topology, each VLAN ID is assigned to the bond rather than the physical adapter.



- ASP 130 KVM on RHEL Network Topology with multiple VLAN configuration. Bonding is configured. OOBM is not configured.

Figure 6 – Multiple VLAN Configuration with Bonding

5 VLAN Deployment Procedures for ASP 130 R6.0

5.1 Single VLAN Deployment

5.1.1 Configure KVM on RHEL 8.10 Server Management Interface for VLAN Tagging

The KVM on RHEL 8.10 management interface can be configured to support VLAN tagging (IEEE 802.1Q). The following guidelines provide instructions for configuring the appropriate NICs on the server to enable this functionality.

The network configuration script "`configNetwork`" available with the ASP 130 R6.0 software image allows the configuration of VLAN tagging, however, for more complex network configurations Cockpit (user web interface for Red Hat Enterprise Linux) can be used.

In this configuration example, a single **VLAN** will be created and assigned to **bridge0**. However, the same process can be followed when configuring a VLAN ID to OOBM interface.

Prerequisites

- During the maintenance activity, the customer network administrator must configure the appropriate VLAN ID on the data switch port that connects the server to the management network and enable VLAN tagging (IEEE 802.1Q) on that port. Failure to do so will result in the server (hypervisor) being disconnected from the network after the VLAN configuration changes are applied.

5.1.2 Adding a VLAN ID using the network configuration script

Note: When making network configuration changes to the primary interface, it is necessary to connect to the server via the designated services port. As the script applies changes, network services will be restarted, which will terminate any existing connections over the primary interface. In the event of misconfiguration, the server will only be accessible through the services port or console.

Procedure

5.1.2.1 Connect to the KVM on RHEL server using the services port connection.

5.1.2.2 Log in to the KVM on RHEL host by using a Secure Shell (SSH) client e.g., PuTTY.

5.1.2.3 Authenticate using the existing `custadm` credentials or `sroot` if EASG enabled.

5.1.2.4 Execute the following CLI command: `configNetwork`

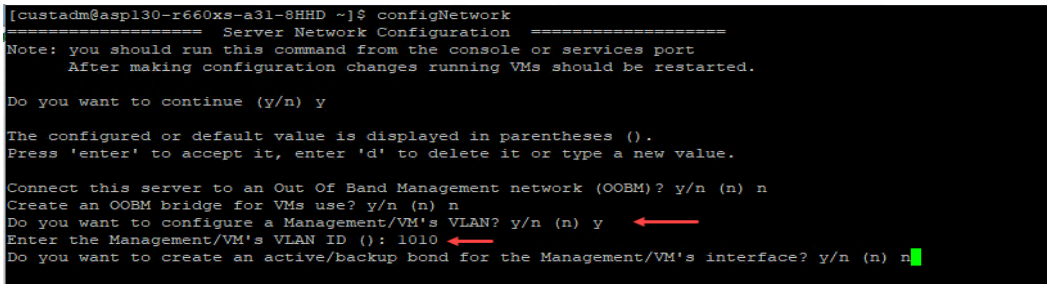
5.1.2.5 Follow the script prompts:

- `Do you want to continue (y/n)`**:** Type **y** to continue if the connection is via services port.
- `Connect this server to an Out of Band Management Network (OOBM) y/n (n)`**:** Type **n** to continue (OOBM configuration is not part of this procedure).

Consideration:

The network script automatically detects if ***OOBM*** has been previously configured on the management interface. If OOBM is found, the script will display a "**Y**" by default. To retain the current OOBM configuration, simply press Enter without making any changes to keep the existing OOBM configuration intact.

- `Create an OOBM bridge for VMs use? y/n (n):` Type **n** to continue.
- `Do you want to configure a Management/VM's VLAN? y/n (n):` Type **y**
- `Enter the Management/VM's VLAN ID ():` Type VLAN ID for example 1010.
- Type **n** to continue (Bond configuration is not part of this procedure).



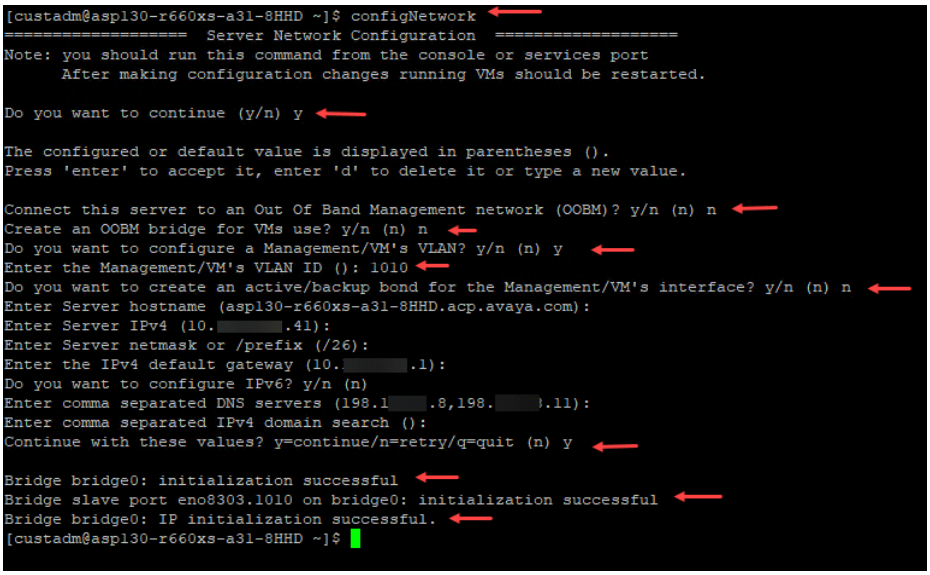
Consideration:

The network script automatically detects if a bond has been previously configured on the management interface. If a ***bond*** is found, the script will display a "**Y**" by default. To retain the current bond configuration, simply press Enter without making any changes to keep the existing bonding configuration intact.

- Press **Enter** key (7 times) until prompt displays *`Continue with these values? y=continue/n=retry/q=quit (n).`* If satisfied with current selections, type **y.**

  Note: Although multiple changes at the same time are supported by the network script, IP address changes are not part of this procedure.

Example Output with a VLAN Configured – No Bonding.



Example Output with a VLAN and Bonding Configured

```
[root@aspl30-r660xs-a31 ~]# configNetwork
==================  Server Network Configuration  ==================
Note: you should run this command from the console or services port
      After making configuration changes running VMs should be restarted.

Do you want to continue (y/n) y

The configured or default value is displayed in parentheses ().
Press 'enter' to accept it, enter 'd' to delete it or type a new value.

Connect this server to an Out Of Band Management network (OOBM)? y/n (n) n
Create an OOBM bridge for VMs use? y/n (n) n
Do you want to configure a Management/VM's VLAN? y/n (n) y
Enter the Management/VM's VLAN ID (): 1010
Do you want to create an active/backup bond for the Management/VM's interface? y/n (y)
 0) eno12409
 1) eno12419
 2) eno12429
 3) eno12399
Enter the port # to use in the bond (eno12409):
Note: port eno12409 must not be used as a direct attachment interface for any VM
Create an active/backup bond with eno8303 and eno12409? y/n (y)
Enter Server hostname (aspl30-r660xs-a31.acp.avaya.com):
Enter Server IPv4 (10.      1):
Enter Server netmask or /prefix (/26):
Enter the IPv4 default gateway (10.1      .1):
Do you want to configure IPv6? y/n (n)
Enter comma separated DNS servers (198.      11,198.      8):
Enter comma separated IPv4 domain search (acp.avaya.com):
Continue with these values? y=continue/n=retry/q=quit (n) y

Bridge bridge0: initialization successful
Bond: initialization successful
Bond port bond0-port1 eno8303.1010 initialization successful
Bond port bond0-port2 eno12409.1010 initialization successful
Bridge bridge0: IP initialization successful.
[root@aspl30-r660xs-a31 ~]#
```

5.1.2.6 Execute the following CLI command for bond configuration validation: `nmcli con`

Example Output: VLAN configuration without NIC bonding.

```
[custadm@aspl30-r660xs-a31-8HHD ~]$ nmcli con
NAME              UUID                                  TYPE      DEVICE
Mgmt_VM_Network   131f7fc1-fa8e-40af-8782-8f9a58d4ab7b  bridge    bridge0
Services          8a85c6cf-dae9-46d3-853e-2c7fc7d7c3e4  ethernet  eno8403
bridge0-port      4264e99e-f252-455e-a272-e3cb9e84ab33  vlan      eno8303.1010
eno12399          a22e2c35-3a60-4b9d-bc0c-71a06b8e080c  ethernet  --
eno12409          29c06695-9947-4789-8881-174564fcc74c  ethernet  --
eno12419          ea2eb3ff-d7ba-4098-8942-3583ac2e2114  ethernet  --
eno12429          b9db8b4c-c8ef-424f-b82b-380446afc13d  ethernet  --
eno8303           58913a34-8c99-4ea4-87bc-b68984fbec30  ethernet  --
ens1f0np0         44eaa2b3-7521-41bc-8ef2-993ca8961f4a  ethernet  --
ens1f1np1         bf4f745f-bele-4f6f-8902-9ea57ba07553  ethernet  --
[custadm@aspl30-r660xs-a31-8HHD ~]$
```

Output example: VLAN configuration with NIC bonding.

```
[custadm@aspl30-r660xs-a31 ~]$ nmcli con
NAME              UUID                                  TYPE      DEVICE
Mgmt_VM_Network   90f517bb-bc6b-47ea-a4af-8ef84210ab66  bridge    bridge0
Services          f21f3299-a47f-414c-a8a1-b3324701b681  ethernet  eno8403
vnet0             077e3e2f-8f3d-4962-bd20-2b422c9e2706  tun       vnet0
vnet1             16b28e57-ba2c-4c3e-b4e6-a4d0ebf8fab6  tun       vnet1
vnet3             42468248-17d8-426d-8b44-fd4f717a8153  tun       vnet3
bond0-port1       cc7bdc6c-8801-4e89-bf4a-89840db063fb  vlan      eno8303.1010
bond0-port2       6f91a1b9-e261-4523-9b14-e64d63e132e7  vlan      eno12409.1010
bridge0-port      adb11f85-6567-4f47-afed-eaa4e5375838  bond      bond0
```

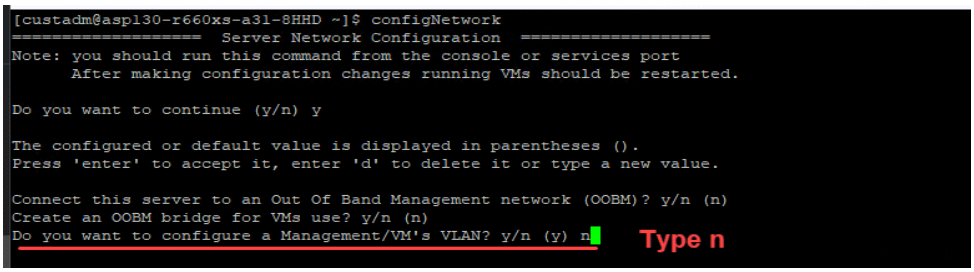
5.1.2.7 (Optional) if a VLAN ID ***needs to be changed***, re-run the `configNetwork` script and repeat all previous steps.

Warning Unless instructed by Avaya, Do **NOT** use Cockpit to make changes to either **bridge0** or **bridgeoob** if OOBM is configured on the server. Doing so will break the `configNetwork` script, and the server will require re-imaging.

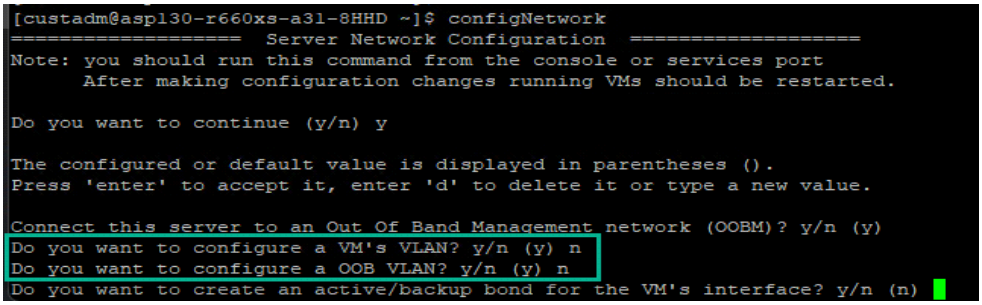
5.1.2.8 (Optional) If a VLAN ID ***needs to be removed,*** re-run the `configNetwork` script and answer **n** when the script asks for the appropriate VLAN.

Warning Unless instructed by Avaya, Do **NOT** use Cockpit to make changes to either **bridge0** or **bridgeoob** if OOBM is configured on the server. Doing so will break the `configNetwork` script, and the server will require re-imaging.

Output example when OOBM has not been previously configured.



Output example when OOBM has been previously configured.



5.1.3 Configuring a VLAN ID on a new Bridge using Cockpit

About this task

Putting VoIP and Data on separate networks is a recommended best practice and industry standard. Isolating VoIP traffic from Data/Management Traffic helps to enhance network security and enables customers to implement QoS adequately. It also helps by simplifying network traffic management and troubleshooting as each network can be monitored independently. By independently monitoring each network, a network administrator can quickly identify and address issues specific to either VoIP or data/management services, improving response times and minimizing downtime.

Note: Call signaling in VoIP communications, whether directed to Communication Manager (CM), Session Manager (SM), or media servers, is still classified as VoIP traffic, even if media (RTP packets) is not transmitted as part of the call signaling process.

Note: Currently, the network configuration script supports assigning a single VLAN ID to either `bridge0` (MGMT), `bridgeoob` (OOBM) or both; however, it does not yet support configuring multiple VLANs on a single bridge.

Before you begin

- It is expected to have at least one extra physical interface apart from the one designated for the Hypervisor management interface (eno8303).
- Connect the designated server port (for example, eno12419) to the customer's data switch. For a network topology illustration of this configuration, refer to Figure 15: A single VLAN configuration on separate bridges in an ASP 130 R6.0 – Hypervisor Layer on page 77 of the ASP 130 Installation document.
- Customer data switch port connecting server must be already configured with the corresponding VLAN ID and VLAN tagging (IEEE 802.1Q) enabled.

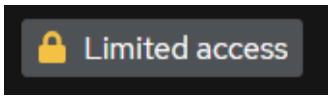
Note: In the event of a misconfiguration with the primary interface, the server Cockpit UI will only be accessible through the services port.

Procedure

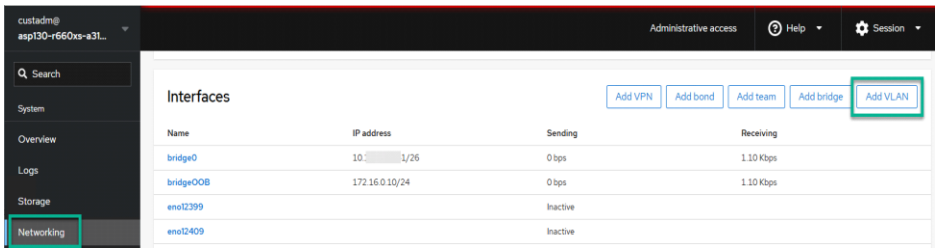
5.3.1.1 Using a Web browser tab, navigate to the KVM on RHEL server IP Address e.g.: https://192.11.13.6:9090

5.3.1.2 Authenticate using the existing *custadm* credentials.

5.3.1.3 If not already in *"Administrative access"*, click on the upper-right corner *"Limited access"* and enter the password for the *custadm* account.

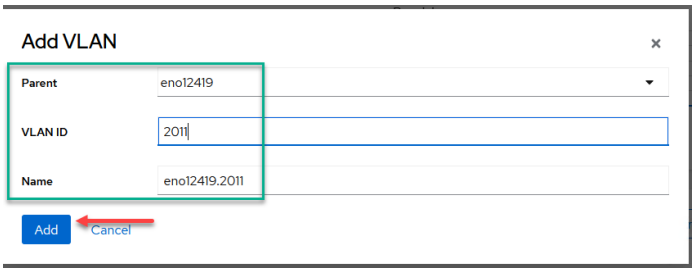


5.3.1.4 From the left-pane menu, select ***Networking>Add VLAN.***

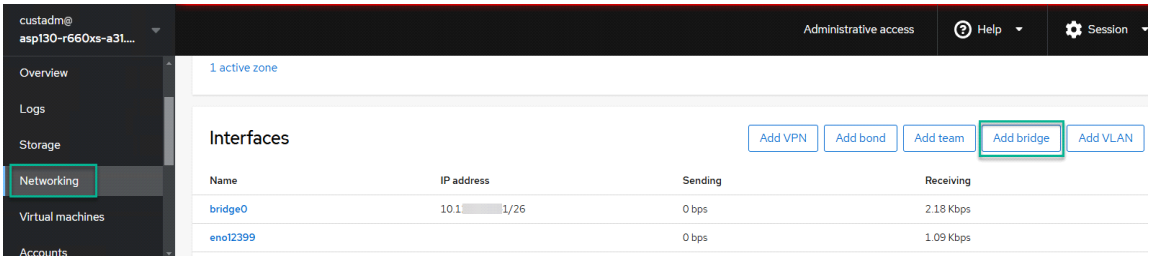


5.3.1.5 Select the following:

- Parent: <Select corresponding **Physical Adapter**> e.g. **eno12419**
- VLAN ID: <Enter corresponding VLAN ID typically 1-4094> e.g. **2011**.
- Name: Leave default value
- Click ***Add*** button to create the new VLAN interface.



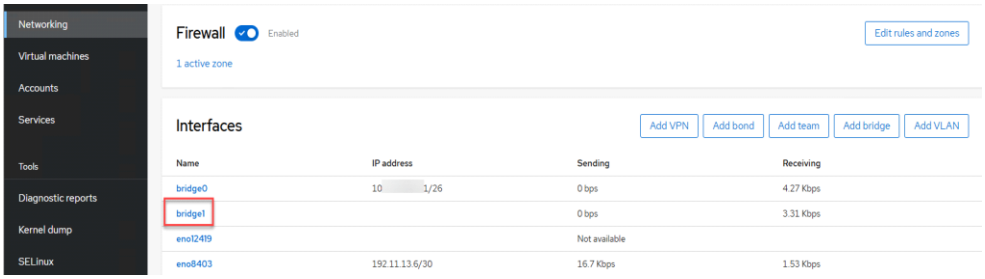
5.3.1.6 From the left-pane menu, click on **Networking>Add bridge**.



5.3.1.7 Select the following:

- Name: **bridge1**
- Ports: previously created VLAN port e.g. ***eno12419.2011.***
- Click ***Add*** button to create bridge.

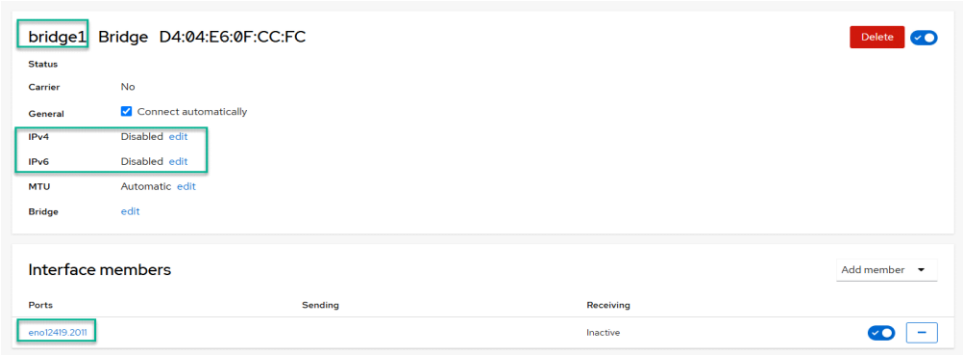
5.3.1.8 Under ***Interfaces*** select the newly created ***bridge1.***



5.3.1.9 Click edit for **IPv4** and validate the following:

- Address is set to ***disabled.*** If not, for Addresses, select from the drop-down menu ***Disabled.***
- All entries are greyed out for DNS, DNS search domains and Routes.
- Click Save.

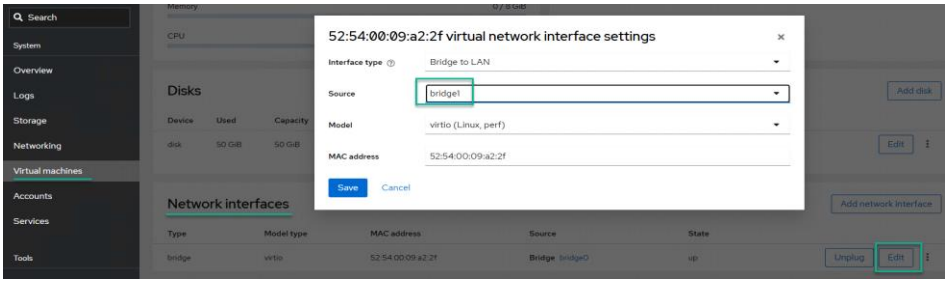
5.3.1.10 Repeat steps for **IPv6.**



5.3.1.11 Migrate the Avaya application virtual network interfaces to the appropriate newly created bridge.

Note: Virtual machines must be powered off before making any network changes.

Note: When segregating networks, a new network segment for VoIP will be provisioned. Coordinate with the customer's network administrators to ensure that Avaya Aura applications are re-IPed accordingly.



5.4 Configuring VLAN trunking on A Single Physical Adapter

About this task

VLAN trunking is a networking technique that enables the transmission of traffic from multiple Virtual Local Area Networks (VLANs) over a single physical network link. Using industry-standard protocols such as IEEE 802.1Q, VLAN trunking adds a unique VLAN identifier to each Ethernet frame, ensuring that traffic remains logically segmented across the shared link. This method improves network scalability and efficiency **by reducing the need for multiple physical interfaces** and simplifying cable management.

Putting VoIP and Data on separate networks is a recommended best practice and industry standard. Isolating VoIP traffic from Data/Management Traffic helps enhance network security and allows customers to implement QoS adequately. It also helps by simplifying network traffic management and troubleshooting as each network can be monitored independently. By independently monitoring each network, a network administrator can quickly identify and address issues specific to either VoIP or data/management services, improving response times and minimizing downtime.

Note: VoIP call signaling, including messages sent to Communication Manager (CM), Session Manager (SM), media servers, Session Border Controller or other SIP/Proxy servers, should always be classified and treated as VoIP traffic. This classification remains essential even when the call does not involve media (RTP) streams at that stage, as signaling is a critical component of the VoIP session setup and control.

Note: For ASP R6.0, VLAN tagging is configured exclusively at the hypervisor layer. VLAN configuration is not applied within the VM guest operating system or application layer.

Warning Server port assignment and configuration for Avaya Communication Manager duplication traffic are not part of this procedure. **DO NOT** make changes to the Avaya CM duplication interface or to the hypervisor when configuring VLAN trunking.

Consideration

- Currently, the network configuration script supports assigning a single VLAN ID to either `bridge0` (MGMT), `bridgeoob` (OOBM) or both; however, it does not yet support configuring multiple VLANs on a single bridge.

Prerequisites

- The customer's data switch port connected to the server must already be configured with the appropriate VLAN ID, and IEEE 802.1Q VLAN tagging must be enabled.
- One VLAN ID is expected to be already configured on the management interface – reference to Configure KVM on RHEL 8.10 Management Interface in the Server for VLAN Tagging

Note: In this example, an additional VLAN ID will be configured on the same physical adapter that provides in-band management access to the KVM on a RHEL 8.10 host (e.g., `eno8303`).

Note: This same procedure can be repeated to configure additional VLANs on the same host NIC. However, a new bridge must be created for every additional VLAN, as described in **Multiple VLAN configuration with no bonding in an ASP 130 R6.0 – Hypervisor Layer**

Note: In the event of a misconfiguration with the primary interface, the server Cockpit UI will only be accessible through the services port.

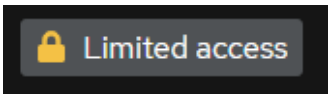
5.4.1 High-Level Workflow

5.4.1.1 Verify that one VLAN is already configured. If not, run the network configuration script to set up the initial VLAN on the host's management interface.
5.4.1.2 Add a second VLAN to the same physical adapter used by the network script in step 1 (e.g., **eno8303.2011**).
5.4.1.3 Disable IPv4 and IPv6 on the newly created VLAN interface.
5.4.1.4 Create a new bridge for the newly created VLAN interface, using appropriate naming and port assignment (e.g., bridge name: **br-2011**, port member: **eno8303.2011**).
5.4.1.5 Edit the VM's network configuration to connect its virtual network interface to the newly created bridge (e.g., br-2011), enabling the VM to send and receive traffic on the corresponding VLAN.
5.4.1.6 Repeat steps for configuring 1-5 VLANs onto the same physical adapter.

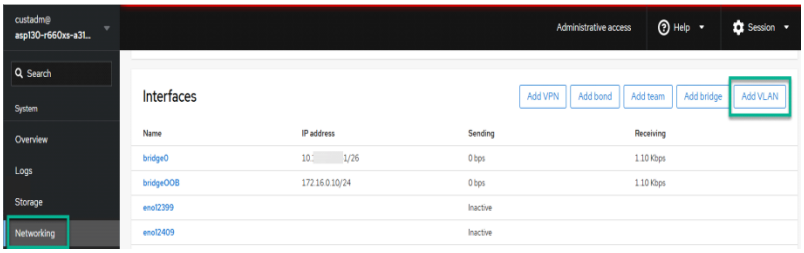
5.4.2 STEP by STEP Procedure

5.4.2.1 Using a Web browser tab, navigate to the KVM on RHEL server IP Address e.g.: https://192.11.13.6:9090
5.4.2.2 Authenticate using the existing *custadm* credentials.

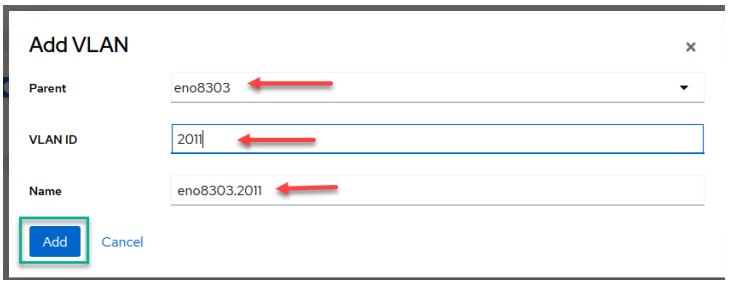
5.4.2.3 If not already in "*Administrative access*", click on the upper-right corner *"Limited access"* and enter the password for the *custadm* account.



5.4.2.4 From the left-pane menu, select ***Networking>Add VLAN.***



- Select the following:
  - Parent: <Select management **Physical Adapter**> e.g. `eno8303`
    - VLAN ID: <Enter corresponding VLAN ID typically 1-4094> e.g. `2011`
    - Name: Leave default value
- Click the ***Add*** button to create the virtual interface.



5.4.2.5 Under ***Networking>Interfaces***, click on the newly created virtual interface e.g. `eno8303.2011`

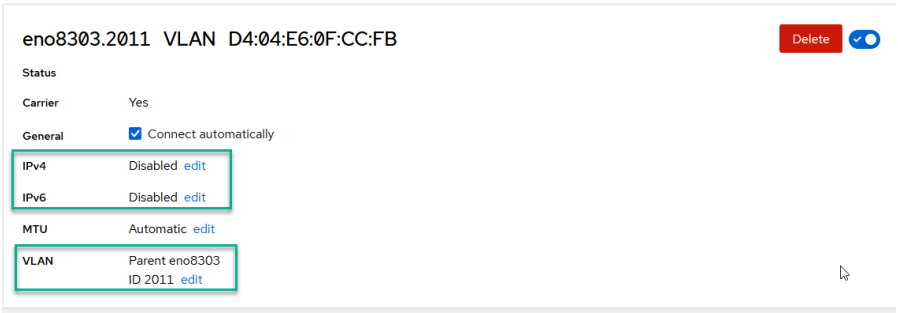
5.4.2.6 Click edit for **IPv4** and validate the following:

5.4.2.7 Address is set to ***disabled.*** If not, for Addresses, select from the drop-down menu ***Disabled.***

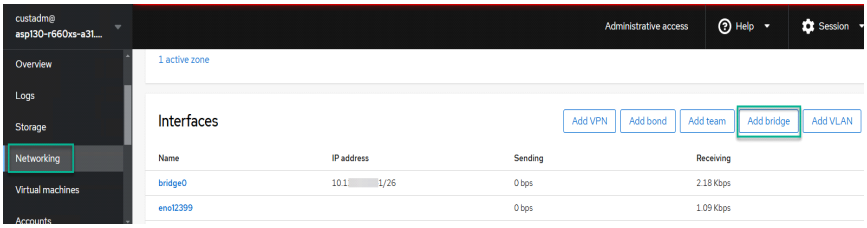
5.4.2.8 All entries are greyed out for DNS, DNS search domains and Routes.

5.4.2.9 Click ***Save***.

5.4.2.10 Repeat steps for **IPv6.**



5.4.2.11 From the left-pane menu, select ***Networking>Add Bridge.***

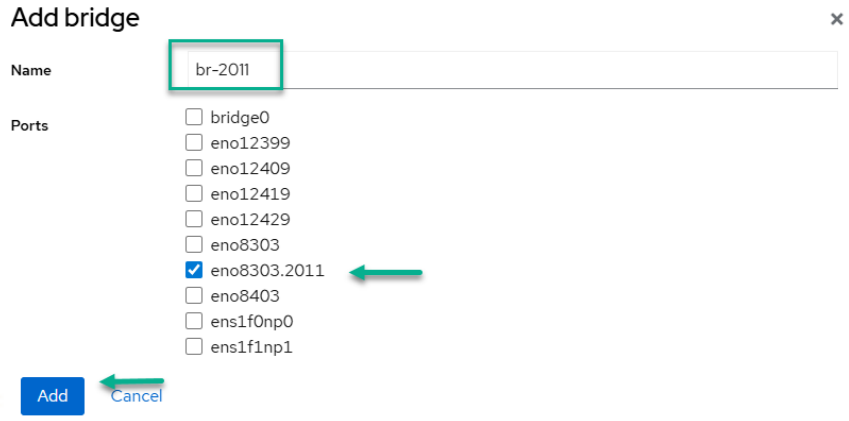


5.4.2.12 Complete the following:

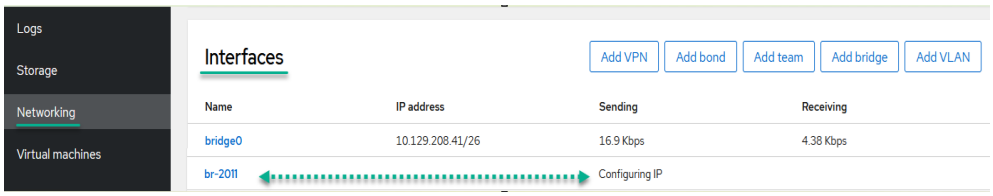
- Name: <Enter new bridge label e.g. `br-2011, VoIP-2011, etc`>

Note: As best practice, it is recommended to label the new bridge with the corresponding VLAN tag that was previously configured.

- Ports: select the previously created VLAN port e.g. `eno8303.2011`
- Click the ***Add*** button to create the new bridge.



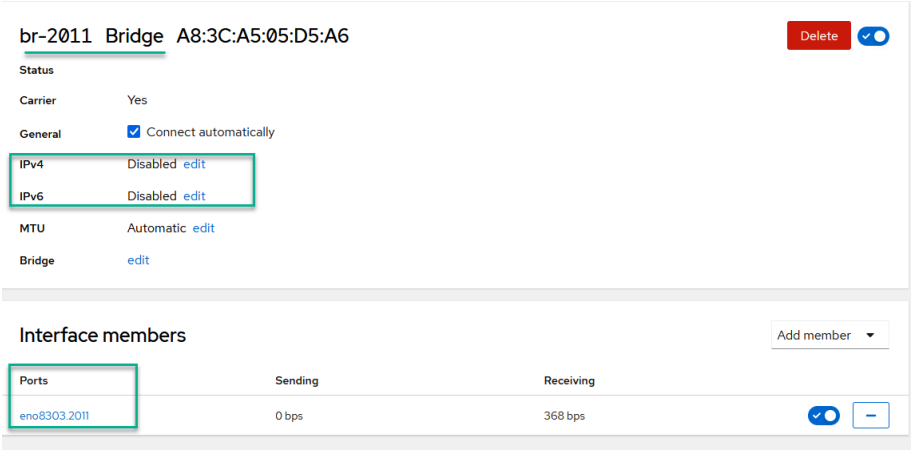
5.4.2.13 Under ***Networking>Interfaces*** select the newly created bridge e.g., `br-2011`.



5.4.2.14 Click edit for **IPv4** and validate the following:

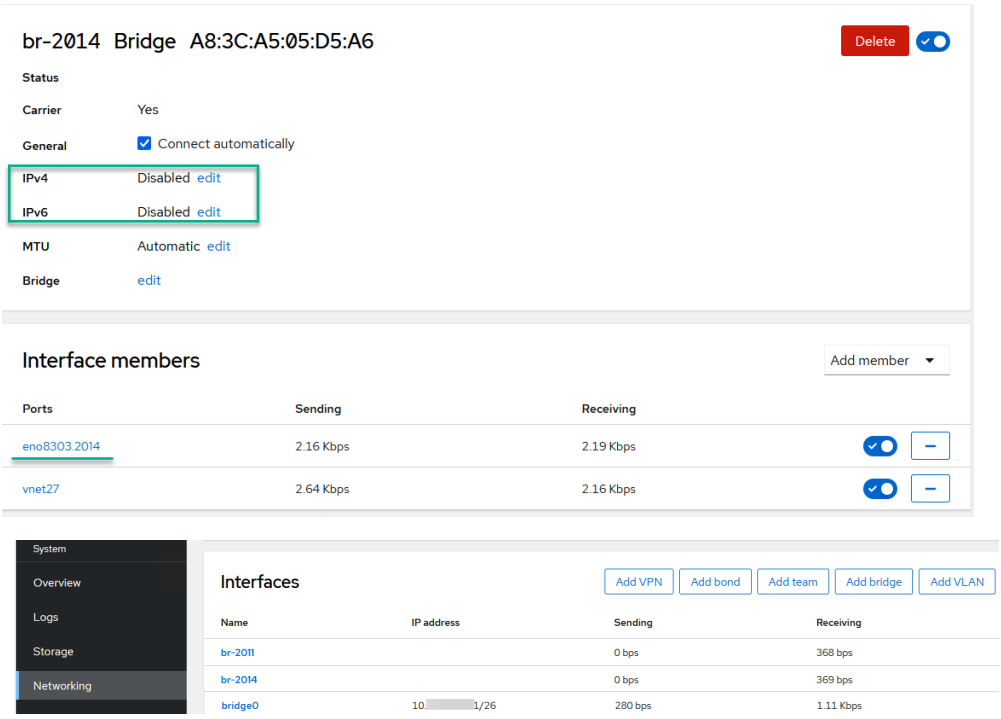
- Address is set to ***disabled.*** If not, for Addresses, select from the drop-down menu ***Disabled.***
- All entries are greyed out for DNS, DNS search domains and Routes.

- Click Save.
- Repeat steps for **IPv6.**



Note: The same procedure can be used to configure new VLANs on other physical adapters, except for the physical adapter used for in-band management access.

In the following screen example, in addition to VLAN 2011, VLAN 2014 has also been configured on the host to simulate a different application traffic type—separate from the default management VLAN configured on bridge0, as illustrated in the **Example diagram of multiple VLAN configuration with no bonding in an ASP 130 R6.0 – Hypervisor Layer**

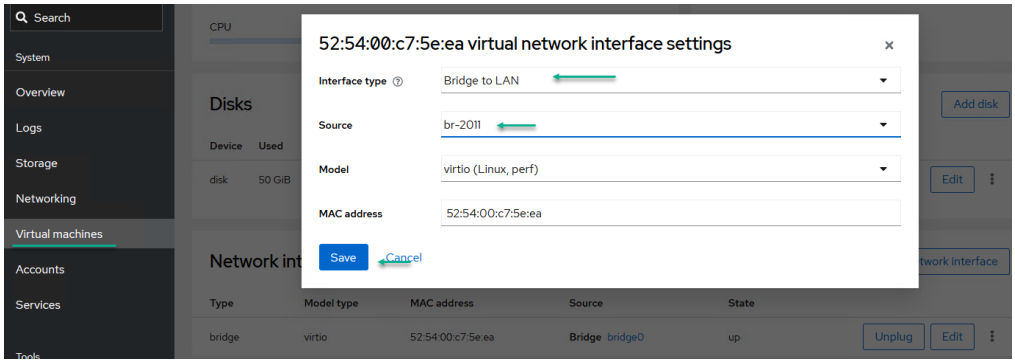


5.4.2.15 Navigate to the ***Virtual machines*** tab and Migrate Avaya Aura applications virtual network interfaces to the newly created bridge accordingly.

Note: Virtual machines must be powered off before making any network configuration changes.

Note: When segregating networks, a new network segment will be provisioned for VoIP traffic. Coordinate with the customer's network administrators to ensure that Avaya Aura applications are re-IP'd accordingly (If needed).

In the following example, the newly created bridge `br-2011` is assigned to the test virtual machine.



5.4.2.16 Repeat the procedure as needed to configure additional VLANs and bridges on the same physical interface, without using bonding.

5.5 Configuring VLAN trunking with bonded interfaces

About this task

VLAN trunking is a networking technique that enables the transmission of traffic from multiple Virtual Local Area Networks (VLANs) over a single physical network link. Using industry-standard protocols such as IEEE 802.1Q, VLAN trunking adds a unique VLAN identifier to each Ethernet frame, ensuring that traffic remains logically segmented across the shared link. This method improves network scalability and efficiency **by reducing the need for multiple physical interfaces** and simplifying cable management.

Putting VoIP and Data on separate networks is a recommended best practice and industry standard. Isolating VoIP traffic from Data/Management Traffic helps enhance network security and allows customers to implement QoS adequately. It also helps by simplifying network traffic management and troubleshooting as each network can be monitored independently. By independently monitoring each network, a network administrator can quickly identify and address issues specific to either VoIP or data/management services, improving response times and minimizing downtime.

Note: VoIP call signaling, including messages sent to Communication Manager (CM), Session Manager (SM), media servers, Session Border Controller or other SIP/Proxy servers, should always be classified and treated as VoIP traffic. This classification remains essential even when the call does not involve media (RTP) streams at that stage, as signaling is a critical component of the VoIP session setup and control.

Consideration

- Currently, the network configuration script supports assigning a single VLAN ID to either `bridge0` (MGMT), `bridgeoob` (OOBM) or both; however, it does not yet support configuring multiple VLANs on a single bridge.
- Beginning with the release of this document, when VLAN trunking is used in conjunction with bonded interfaces, the VLAN tag must be applied to a bonded interface rather than to an individual physical interface. This represents a change from the original single VLAN configuration method currently supported by the network script.
- As part of this procedure, the existing VLAN configuration must be removed to apply the new VLAN method.

Prerequisites

- The customer's data switch ports connected to the ASP server must already be configured with the appropriate VLAN IDs, and IEEE 802.1Q VLAN tagging must be enabled.


Note: In the event of a misconfiguration with the primary interface, the host Cockpit UI will only be accessible through the services port.


Warning Server port assignment and configuration for Avaya Communication Manager duplication traffic are not part of this procedure. **DO NOT** make changes to the Avaya CM duplication interface or to the hypervisor when configuring VLAN trunking.

5.5.1 High-Level Workflow

5.5.1.1 Remove existing VLAN configuration using the network configuration script, while preserving or configuring a network bond e.g. **bond0**.

5.5.1.2 If applicable, use **Cockpit** to remove any single VLAN interfaces previously configured on network bridges other than **bridge0**, except for Out of Band Management OOBM. OOBM interface will retain its existing single-VLAN configuration.

5.5.1.3 Use **Cockpit** to configure initial VLAN for Host and application management traffic, using **bond0** as the parent interface e.g. **bond0.1010**.

5.5.1.4 Use cockpit to configure additional VLANs for Application and VoIP traffic (e.g. **bond0.2011**, **bond0.2014**, etc.).

5.5.1.5 Disable IPv4 and IPv6 on each newly created VLAN interfaces.

5.5.1.6 Remove **bond0 port member** association from **bridge0**.

5.5.1.7 Add the newly created VLAN interface for Host and Application management traffic (e.g. **bond0.1010)** as a port member to **bridge0**.

5.5.1.8 Create a new bridge (or re-label existing ones, excluding **bridge0**), for each of the remaining VLAN interfaces. Use appropriate naming and port assignments (e.g. bridge name: **br-2011**, port member: **bond.2011**, bridge name: **br-2014** port member: **bond.2014**, etc).

5.5.1.9 Edit the VM's network configuration to connect its virtual network interface to the newly created bridge (e.g., bridge0, br-2011, br-2014), enabling the VM to send and receive traffic on the corresponding VLAN.

5.5.1.10 **When applicable**, disconnect and remove cables no longer associated with the host network configuration.

5.5.1.11 Repeat steps for configuring VLAN trunking on a second bonded interface. Max 5 VLANs per bonded interface

5.5.2 VLAN Removal and Bond Configuration on the Host Management Interface

About this task

As part of this procedure, **all existing VLAN configuration will be removed from the host**, including VLANs not connected to **bridge0**. The only exception is the **Out-of-Band Management (OOBM)** interface, which, if configured on the host, will retain its existing single-VLAN configuration and dedicated NIC.

Following this VLAN reset, network traffic will be consolidated onto a single **bonded interface**, which will be configured to support **VLAN trunking**. This updated topology simplifies both the network design and ongoing management by allowing multiple VLANs to **pass through** the same physical link.

As part of this VLAN and Network Port consolidation, **NICs previously dedicated to application-specific traffic will be removed from the host networking configuration** (Example diagram of multiple VLAN configuration on separate bridges in an ASP 130 R6.0 – Hypervisor Layer), and their associated cabling will be disconnected.

Note: When possible, Avaya recommends adopting this updated topology when configuring hosts with bonded interfaces and VLAN trunking. However, if necessary, NICs dedicated to application-specific traffic may remain configured on the host.

Warning Server port assignment and configuration for Avaya Communication Manager duplication traffic are not part of this procedure. **DO NOT** make changes to the Avaya CM duplication interface or to the hypervisor when configuring VLAN trunking.

Procedure

5.5.2.1 Connect to the KVM on RHEL server using the services port connection.

5.5.2.2 Log in to the KVM on RHEL host by using a Secure Shell (SSH) client e.g., PuTTY.

5.5.2.3 Authenticate using the existing `custadm` credentials or `sroot` if EASG enabled.

5.5.2.4 Execute the following CLI command: `configNetwork`.

5.5.2.5 Follow the script prompts:

6 Type **y** to continue if the connection is via services port.

7 Type **Enter** to continue (OOBM configuration is not part of this procedure).

8 `Create an OOBM bridge for VMs use? y/n (n)`: Type **Enter** to keep existing configuration.

- `Do you want to configure a Management/VM's VLAN? y/n (y)` : Type **n** to unconfigure previously assigned VLAN.

- `Do you want to create an active/backup bond for the Management/VM's interface? y/n (y)` : Type **y** to configure an active/backup bond.

Note: If a bond has already been configured for the management interface, the existing configuration may be retained, as it will be leveraged when VLANs are subsequently added to the bonded interface.

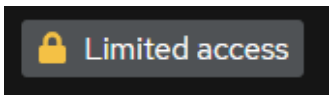
- `Enter the port # to use in the bond (eno12409)` : <Leave existing bond configuration or select proper port>
- `Create an active/backup bond with eno8303 and eno12409? y/n (y)` : Type **y** to configure/maintain bond.
- Press **Enter** key (7 times) until prompt displays *Continue with these values? y=continue/n=retry/q=quit (n).* If satisfied with current selections, type **y.**

Note: While the network script supports configuring multiple network parameters simultaneously, IP address changes are not part of this procedure.

5.5.2.6 Using a Web browser tab, navigate to the KVM on RHEL services IP Address https://192.11.13.6:9090

5.5.2.7 Authenticate using the existing *custadm* credentials.

5.5.2.8 If not already in "*Administrative access*", click on the upper-right corner *"Limited access"* and enter the password for the *custadm* account.



5.5.2.9 From the left-pane menu, select ***Networking***

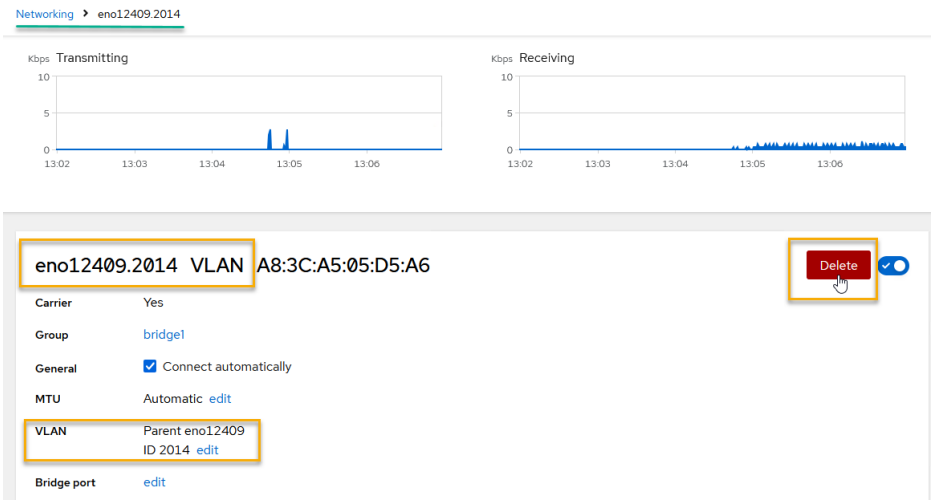
5.5.2.10 Carefully review the existing bridge and VLAN configuration on the host. If additional VLANs and bridges have been configured for specific VM (application) traffic, as illustrated in the topology example ***'Example diagram of multiple VLAN configuration on separate bridges in an ASP 130 R6.0 – Hypervisor Layer'***—they must be removed before proceeding. Ensure that all remaining VLANs are removed from the host, if present.

Note: Previously configured bridges, apart from `bridge0`, can be reused if appropriate labels are set.

Note: In the following example, VLAN 2014 on interface `eno12409.2014`, which is currently assigned to `eno12409` (a member of bridge bridge1), will be deleted. Later in the process, VLAN 2014 will be re-added as part of the VLAN trunking configuration on the bonded interface.

5.5.2.11 Select `bridge1 >` Under ***Interface members*** select `eno12409.2014`

5.5.2.12 Click the ***Delete*** button to remove VLAN 2014 from the host network configuration.



5.5.2.13 Repeat steps as needed to delete all remaining VLANs from the host network configuration.

5.3.3 Configuring multiple VLANs on a Bonded Interface

Prerequisites

At this point, no VLANs should be configured on the host. Refer to VLAN Removal and Bond Configuration on the Host Management Interface if needed.

Note: if necessary, NICs dedicated to application-specific traffic may remain configured on the host.

At least one bond should already be configured for both Host Management and application traffic. Refer to VLAN Removal and Bond Configuration on the Host Management Interface

About this Task

This section outlines the implementation of the following topology: **Example diagram of multiple VLAN configuration with bonding in an ASP 130 R6.0 – Hypervisor Layer.** However, the same logic and procedure apply when configuring VLAN trunking on a secondary bonded interface.

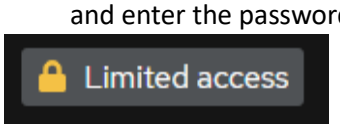
Note: For guidance on configuring a second network bond refer to Configuring NIC Bonding (only available in ASP R6.0.0.1 and later) in the ASP 130 Installation document.

Procedure

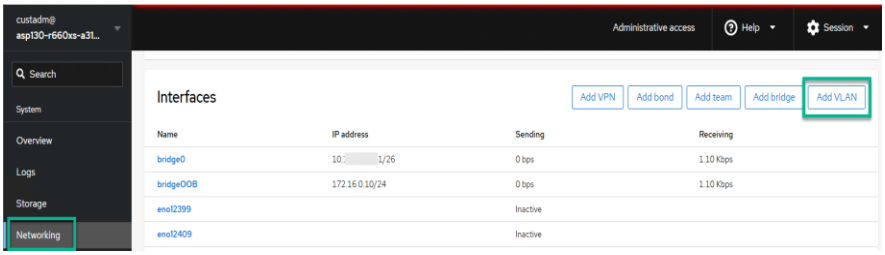
5.3.3.1 Using a Web browser tab, navigate to the KVM on RHEL services IP Address: https://192.11.13.6:9090

5.3.3.2 Authenticate using the existing *custadm* credentials.

5.3.3.3 If not already in *"Administrative access"*, click on the upper-right corner *"Limited access"* and enter the password for the *custadm* account.



5.3.3.4 From the left-pane menu, select ***Networking>Add VLAN.***

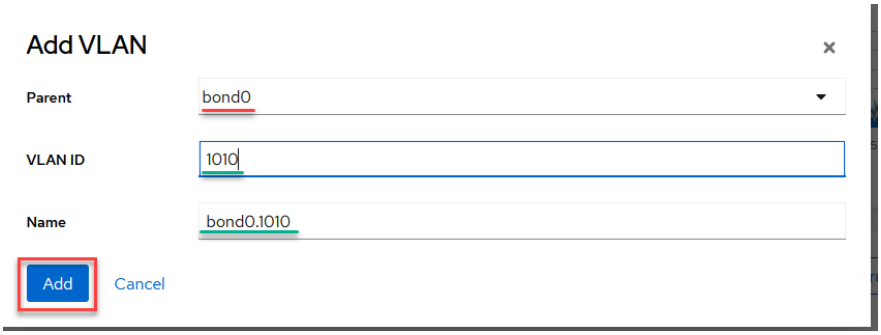


Select the following:

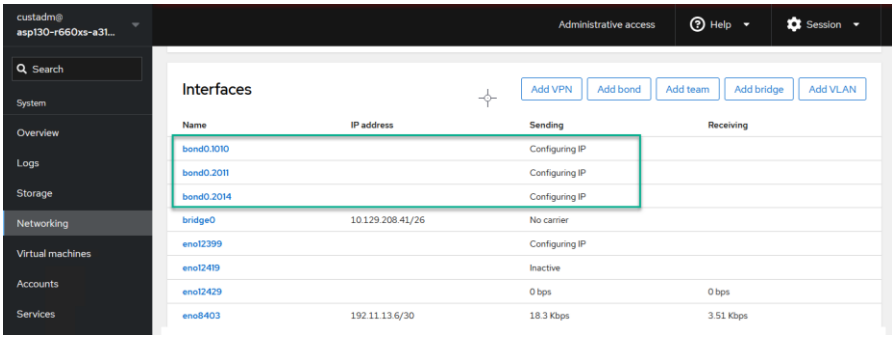
- Parent: `bond0`
- VLAN ID: <Enter corresponding VLAN ID 1-4094> e.g. `1010`

Note: In this example, the first VLAN added is for management traffic. While it is not mandatory to follow this order, it is recommended to maintain a consistent and structured process, especially when replicating the same configuration across multiple servers.

- Name: Leave default value
- Review selections, when ready, click the ***Add*** button to create the virtual interface.



5.3.3.5 Repeat as needed to create additional VLANs for VoIP or other application-specific traffic. In this example, VLANs 2011 and 2014 will also be created.



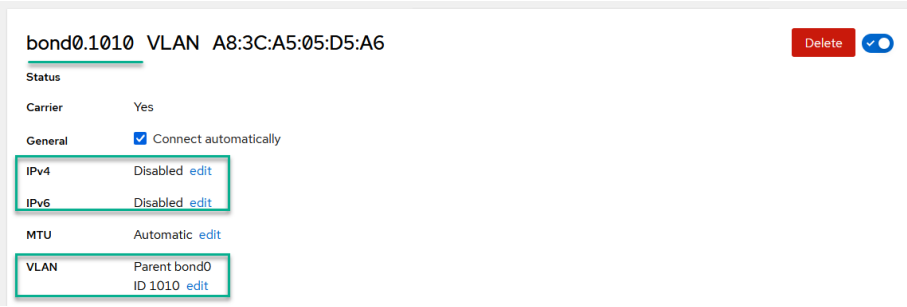
5.3.3.6 Under ***Networking>Interfaces*** select the newly created VLAN for **Management** e.g. `bond0.1010`.

5.3.3.7 Click edit for **IPv4** and validate the following:

- Address is set to ***disabled.*** If not, for Addresses, select from the drop-down menu ***Disabled.***
- All entries are greyed out for DNS, DNS search domains and Routes.
- Click ***Save***.

5.3.3.8 Repeat steps for **IPv6.**

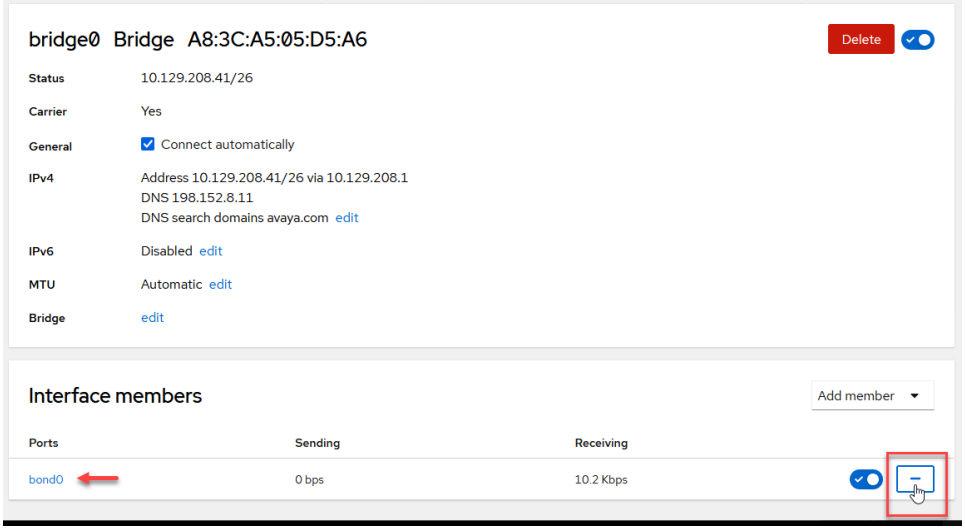
5.3.3.9 Repeat steps for remaining VLANs in this example `bond0.2011 and bond0.2014`.



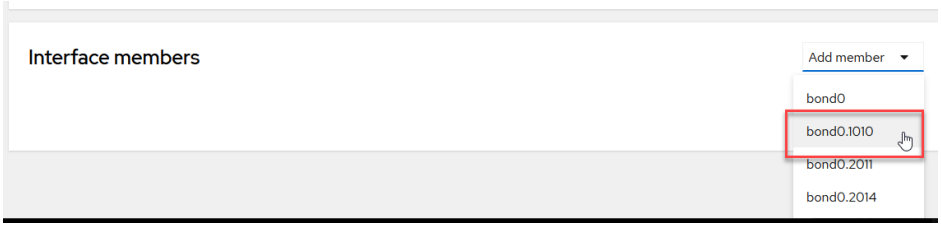
5.3.3.10 Under ***Networking>Interfaces*** select `bridge0`

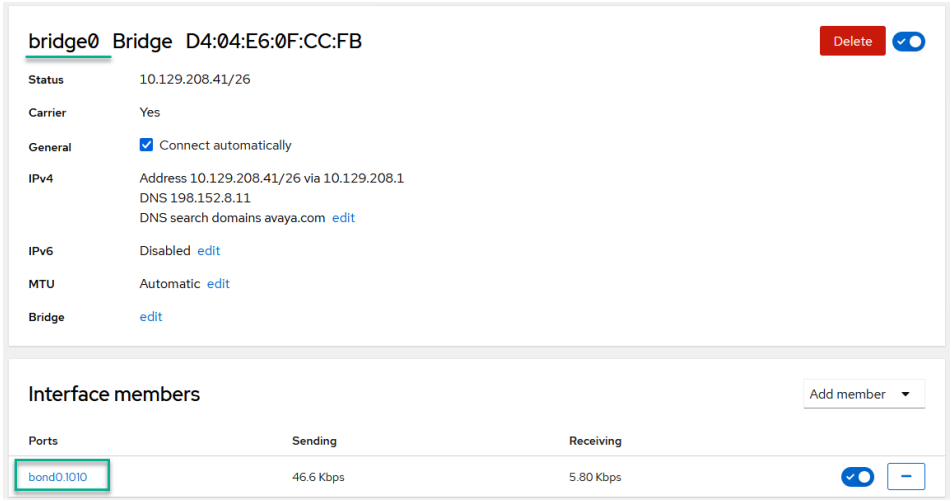
5.3.3.11 Under ***Interface Members*** select the 'minus' icon to remove from `bridge0` the bonded interface `bond0`.

⚠️ **Warning:** Do **not** select the **Delete** button, as this will remove bridge0 from the host configuration.



5.3.3.12 Under ***Interface Members,*** click the ***Add member*** drop-down menu, and select the management VLAN that was previously created, in this example `bond0.1010`





5.3.3.13 Return to the ***Networking*** view and select **`bond0 .`**

5.3.3.14 Click edit for **IPv4** and validate the following:

- Address is set to ***disabled.*** If not, for Addresses, select from the drop-down menu ***Disabled.***
- All entries are greyed out for DNS, DNS search domains and Routes.
- Click ***Save***.

5.3.3.15 Repeat steps for **IPv6.**

Note: When `bond0` is removed from bridge0, it reverts to its default state, which uses DHCP for both IPv4 and IPv6. The interface will attempt to obtain an IP address; when this fails, it eventually times out and appears as **inactive**. This can be misleading, as the interface may appear down—even though traffic is still flowing. In **ASP 130 R6.0**, bonded interfaces are **not expected** to have an IP address configured.

5.3.3.16 At this point, connectivity to the host (KVM) management interface and any VMs configured to use **bridge0** should be restored. Perform appropriate network testing to verify that connectivity has been fully re-established on the expected interfaces for both the host and the VMs.

5.3.3.17 For the remaining configured VLANs (in this example VLANs 2011,2014), you must either configure a new bridge or re-configure an existing bridge (other than bridge0) accordingly.

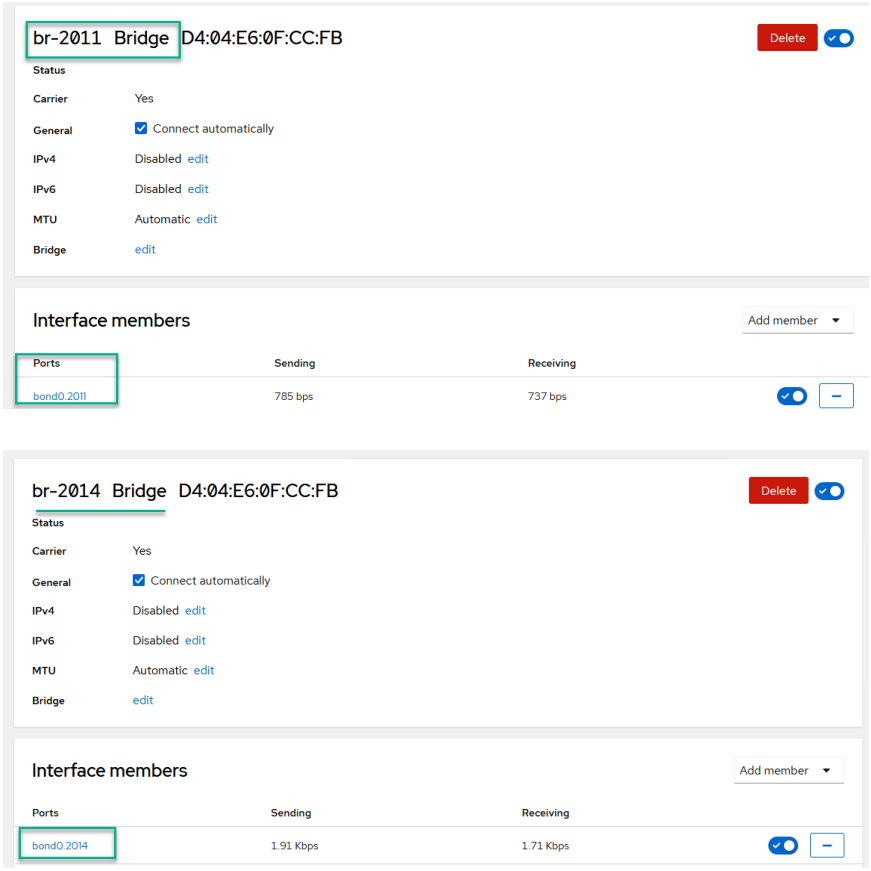
5.3.3.17.1 ***If configuring a new bridge***

- From the left-pane menu, select ***Networking>Add bridge.***
- Complete the following fields:

  Name – As a best practice, bridges should be clearly labeled to include the VLAN tag. For example, for **VLAN 2011**, use names such as br-2011 or bridge-2011.

  Ports – Select the corresponding previously added VLAN interface (e.g., **bond0.2011**).
- Review selections and click Save.

In this example, bridge **br-2011 and br-2014** will also be configured for application traffic on VLAN 2011 and 2014.

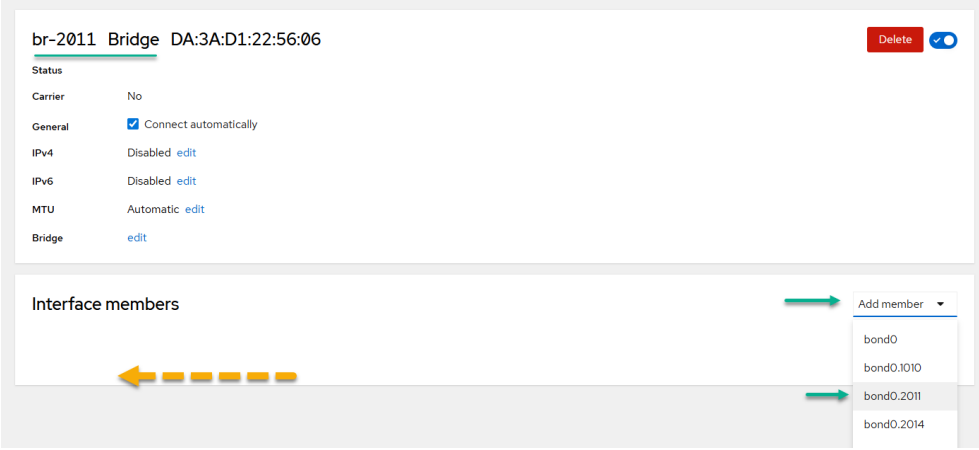


5.3.3.17.2 *To re-configure an existing bridge*

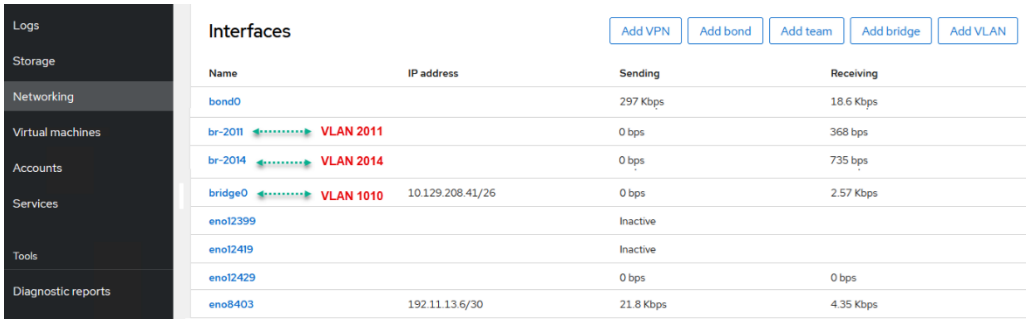
Note: In this example, **bridge1** will be reconfigured to handle traffic tagged with VLAN **2011**, however, the same steps apply to VLAN 2014, to align with the screenshots provided in the previous section.

- From the ***Networking*** page select ***bridge1***
- Click the edit button next to ***Bridge***.

- For the ***Name*** field, as a best practice, bridges should be clearly labeled to include the VLAN tag. For example, for VLAN 2011, use names such as br-2011 or bridge-2011.
- Ignore other fields (Ports, Options) and click ***Save.***
- As part of the bridge relabeling, all previously associated members will be removed. This is expected, proceed with selecting the corresponding member by selecting the ***Add member*** drop-down selection.
- Select previously configured VLAN interface, for this example ***bond0.2011***



- Repeat steps as required to reconfigure bridges for other remaining VLANs.
- The final configuration should resemble the example below: one bridge per configured VLAN, with each VLAN tagged on the bonded interface



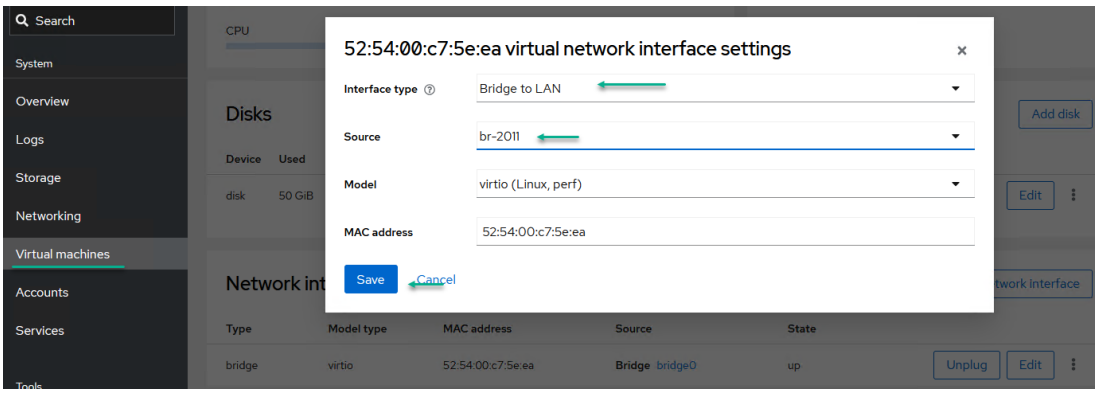
Note: For systems with more than one bond configured (e.g. `bond1`), the same steps and logic can be applied when configuring VLAN trunking on a second bonded interface.

5.3.3.18 Navigate to the ***Virtual machines*** tab and Migrate Avaya Aura applications virtual network interfaces to the newly created bridge accordingly.

Note: Virtual machines must be powered off before making any network configuration changes.

Note: When segregating networks, a new network segment will be provisioned for VoIP traffic. Coordinate with the customer's network administrators to ensure that Avaya Aura applications are re-IP'ed accordingly (If needed).

- In the following example, the newly created bridge `br-2011` is assigned to the test virtual machine.



- Repeat the procedure as needed to configure additional VLANs and bridges on the bonded interface.

5.3.3.19 **<u>When applicable</u>**, disconnect and remove cables no longer associated with the host network configuration.