Configuring Avaya Identity Engines Ignition Guest Tunneling

Release 9.1
NN47280-504
Issue 01.01
August 2015

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

The *Configuration Avaya Identity Engines Ignition Guest Tunneling* explains how to install, configure, and manage Ignition Guest Tunneling (IGT).

Related resources

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Subscribing to e-notifications

Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

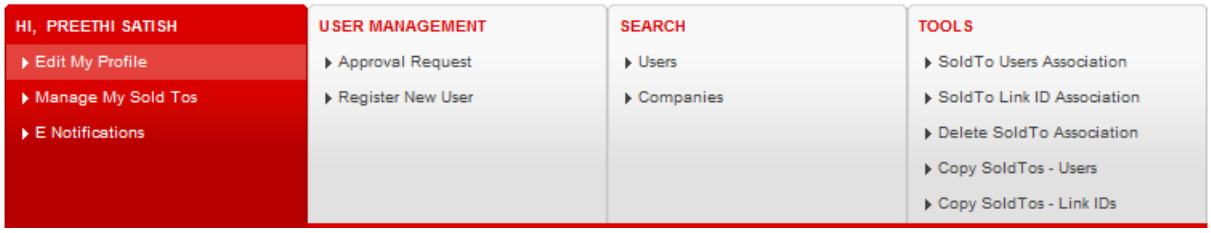
About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing Switch 8800.

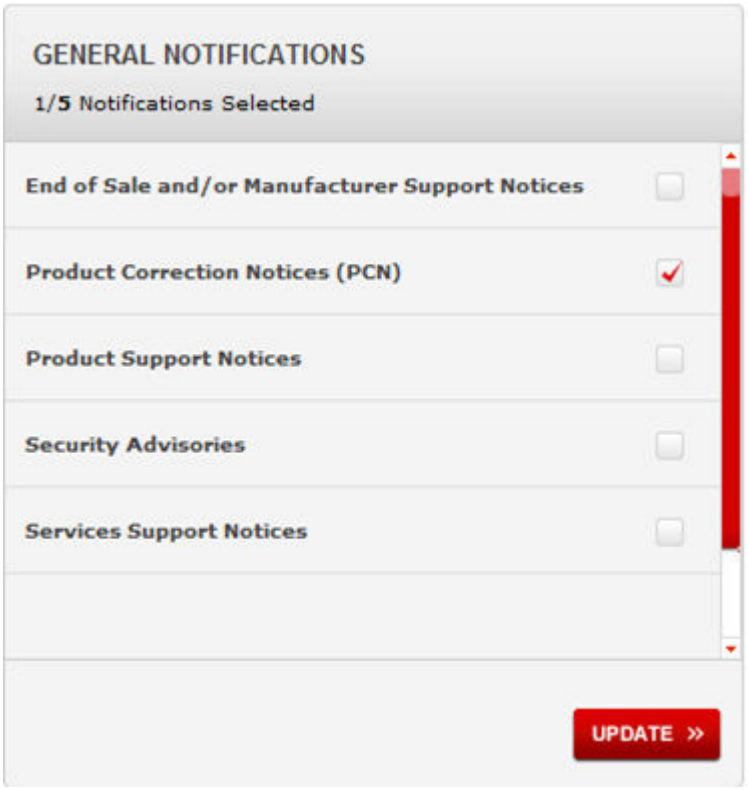
Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Click **MY PROFILE**.

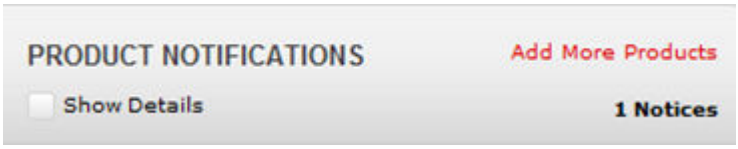
4. On the site toolbar, click your name, and then click **E Notifications**.



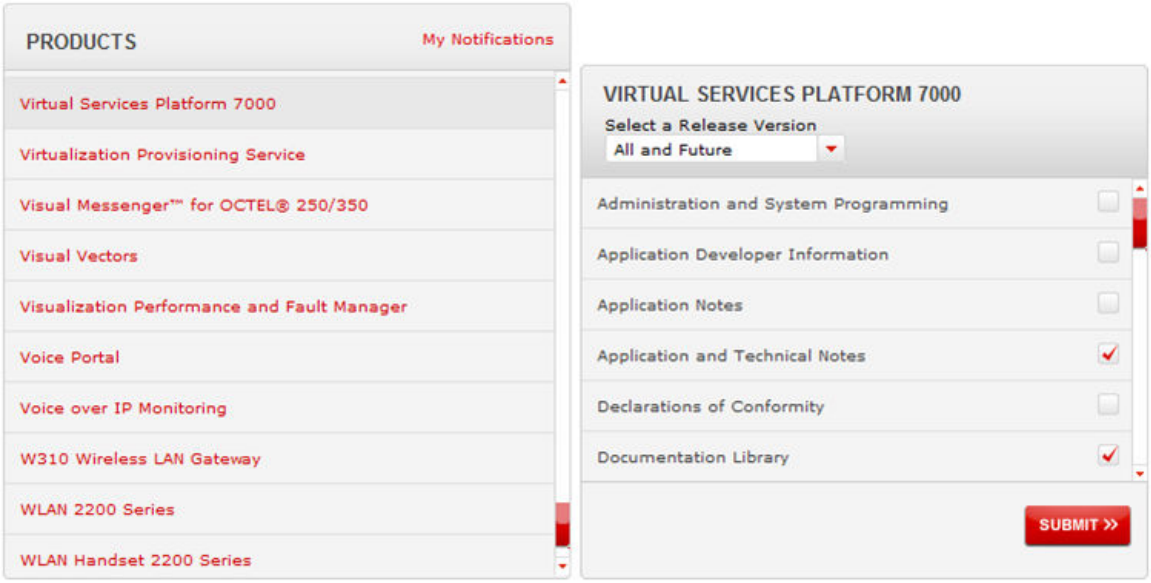
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.



8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.



11. Click **Submit**.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.
3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks

- Include Comments

6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

Configuring Avaya Identity Engines Ignition Guest Tunneling, NN47280–504 is a new document for IGT Release 9.1, so all the features are new in this release. See *Avaya Identity Engines Ignition Guest Tunnelling Release Notes*, NN47280-402 for full list of features.

Chapter 3: IGT Introduction

Avaya Identity Engines Ignition Guest Tunneling (IGT) virtual appliance is an Avaya Identity Engines portfolio product which provides Wireless Local Area Network (WLAN) 9100 guest user traffic isolation solution using Generic Routing Encapsulation (GRE) tunneling technology.

Common Guest Network Isolation

Guest Network Isolation is a security requirement for network access control to separate the guest traffic from intranet and to separate intranet from guest traffic.

Common Guest Network Isolation method includes:

- Mapping Service Set Identifier (SSID) and VLAN
- Tunneling from WLAN controller to Demilitarized Zone (DMZ)
- Enforcing through security policy and Firewall

Guest Network Isolation for IGT

IGT uses Guest Network Isolation to separate the guest traffic from intranet and to separate intranet from guest traffic.

Guest Network Isolation method for IGT includes:

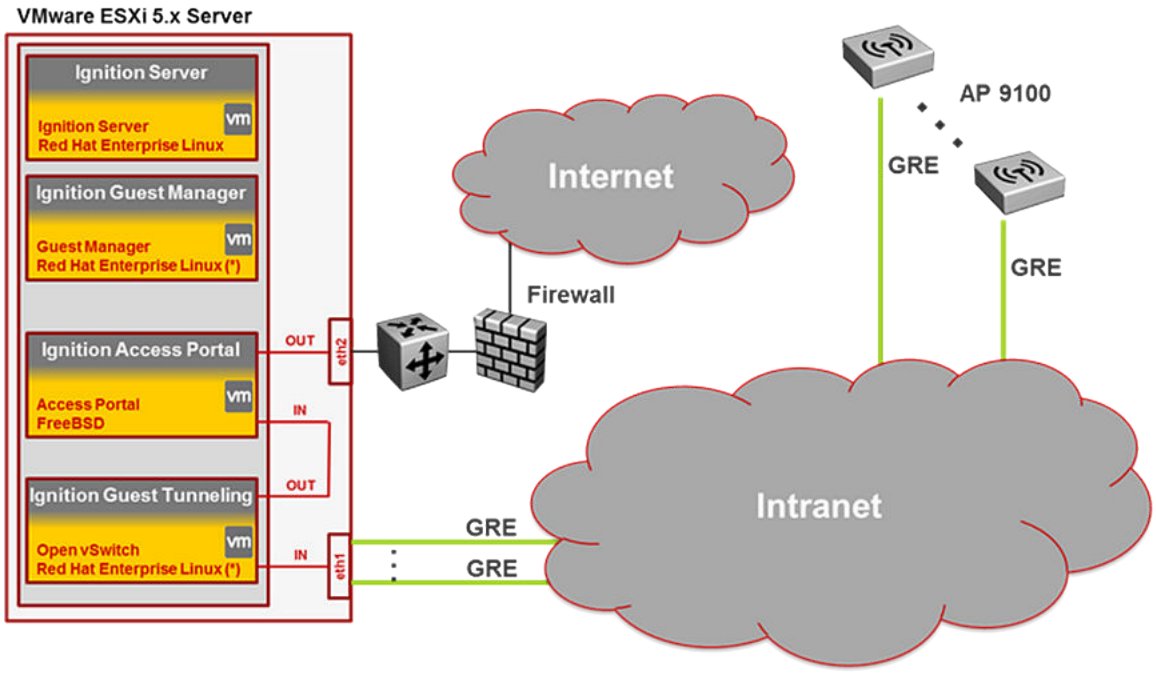
- Mapping SSID and VLAN
- Tunneling to IGT through the SSID and GRE tunneling

Use case examples

Following are the two use cases of GRE-based Guest Network isolation.

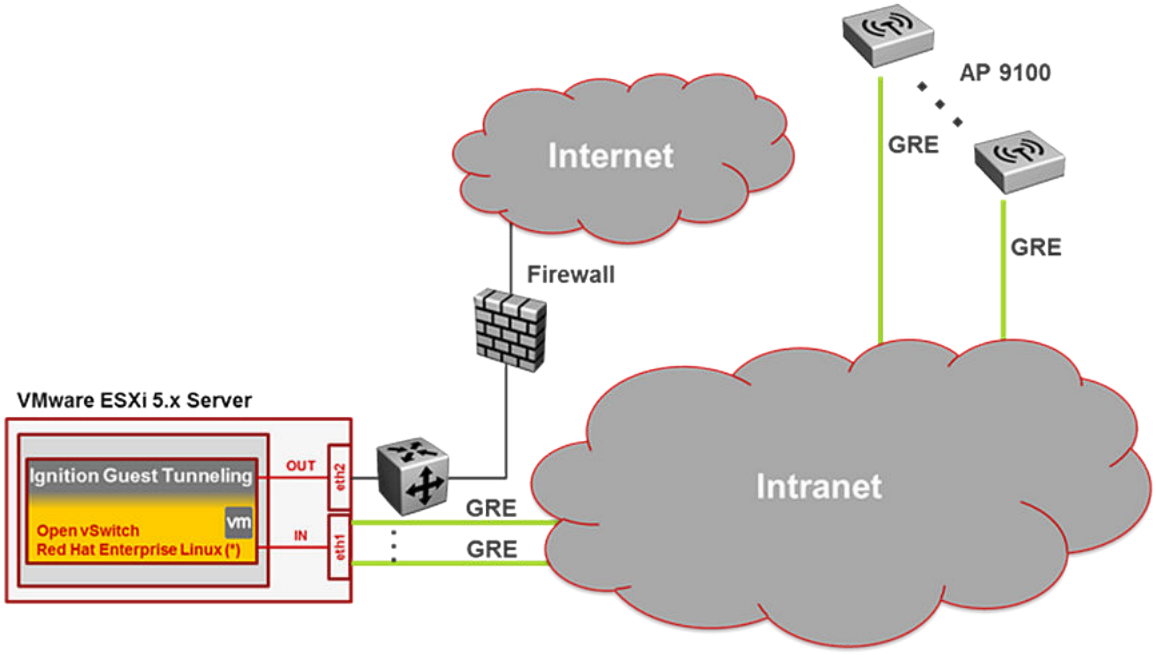
GRE-based Guest Isolation Deployment

GRE-based Guest Isolation Deployment deals with isolating guest traffic by making use of IGT and IDE Access Portal that acts as an external captive portal. The IGT's IN-interface is configured as the remote end point on the AP 9100. The AP tunnels the guest traffic to the IGT appliance. The appliance on receiving client traffic, decapsulates the packets and forwards it to the Access Portal. The Access Portal OVA can be deployed on the same server that hosts the IGT appliance. In this situation, the OUT interface of IGT is connected to the IN interface of the Access Portal. A Dynamic Host Configuration Protocol (DHCP) server can reside on the IN interface of the Access Portal. The OUT interface of Access Portal will be connected to the Internet or DMZ. Hence, guest traffic is routed from the AP to the guest tunneling appliance and later through the access portal. In case, the access point sends out client traffic on different VLAN, then IGT needs to be configured to strip the VLAN tag and forward the client traffic to the access portal as untagged.



GRE-based Traffic Isolation Deployment

In GRE-based Traffic Isolation Deployment there is no captive portal. The AP to guest tunneling appliance connectivity remains similar to the GRE-based Guest Isolation Deployment. The IGT instead of forwarding the guest traffic to the access portal after decapsulating, forwards it to the next hop switch that in turn forwards the packet to the internet or DMZ through a firewall similar to how the rest of traffic is forwarded. This scenario supports both tagged and untagged client traffic with suitable modifications on the ESXi server.



Chapter 4: Installing IGT

This chapter describes the procedure to install Ignition Guest Tunneling (IGT) as a virtual appliance on a VMware ESXi server.

System requirements

The following table describes the minimum system requirements to install IGT:

Software	Software Compatibility	Comments
Ignition Guest Tunneling	• VMware ESXi versions 5.1 or 5.5 • Installation on a VMware ESXi server is done using an OVA file which already incorporates the OS Red Hat Enterprise Linux.	• The VM requires a x86_64 capable environment • Number of CPUs - minimum 2 Dual-core CPUs • Memory - minimum 4GB • Storage (HDD or Flash) - minimum 20GB (VMware thin provisioning is allowed) • Minimum 1 physical NIC (preferably 3 NICs. Management, IN and OUT) • See https://www.vmware.com/ for a list of supported hardware platforms for ESXi.

Warning:

Avaya provides Ignition Guest Tunneling as a Virtual Appliance. Do not install or configure any other software on the VM shipped by Avaya.

- Avaya does not support the installation of any VMware specific, Red Hat Enterprise Linux (RHEL) specific, or any third-party vendor package or Red Hat Package Manager (RPM) on its VM, other than what Avaya ships as a package, image, or OVA.
- Do not install or uninstall any software components unless Avaya specifically provides the software and/or instructs you to do so. Do not modify the configuration or the properties of any software components of the VMs (including VMware Tools) unless Avaya

documentation and/or personnel specifically instructs you to do so. Avaya does not support any deviation from these guidelines.

- Avaya determines which VMware Tools to install and configure. When required, Avaya provides these tools as part of the installation package. VMware Tools configures the kernel and network settings and unless Avaya tests and approves these tools, Avaya cannot guarantee that the VM will work after the tool is installed and configured.

Note:

In this release, Avaya do not support installing VMware tools.

Turn off automatic VMware Tools updates if you have enabled them. Refer to the following instructions to disable automatic updates.

Network configuration for IGT

IGT has three network interfaces:

- **Management VLAN (br0)** is a vSwitch Port Group instance dedicated for management of the devices. All the devices used in IGT provides Web or CLI based administration. Hence, having dedicated interface for management provides more security and agility.
- **AP VLAN (br1)** is a vSwitch Port Group instance dedicated for AP and Guest Tunneling GRE connectivity.
- **Mobility VLAN (br2)** is a vSwitch Port Group instance dedicated for Wireless LAN clients. All wireless client IP addresses and Ignition Access Portal IN interface will be part of Mobility VLAN subnets.

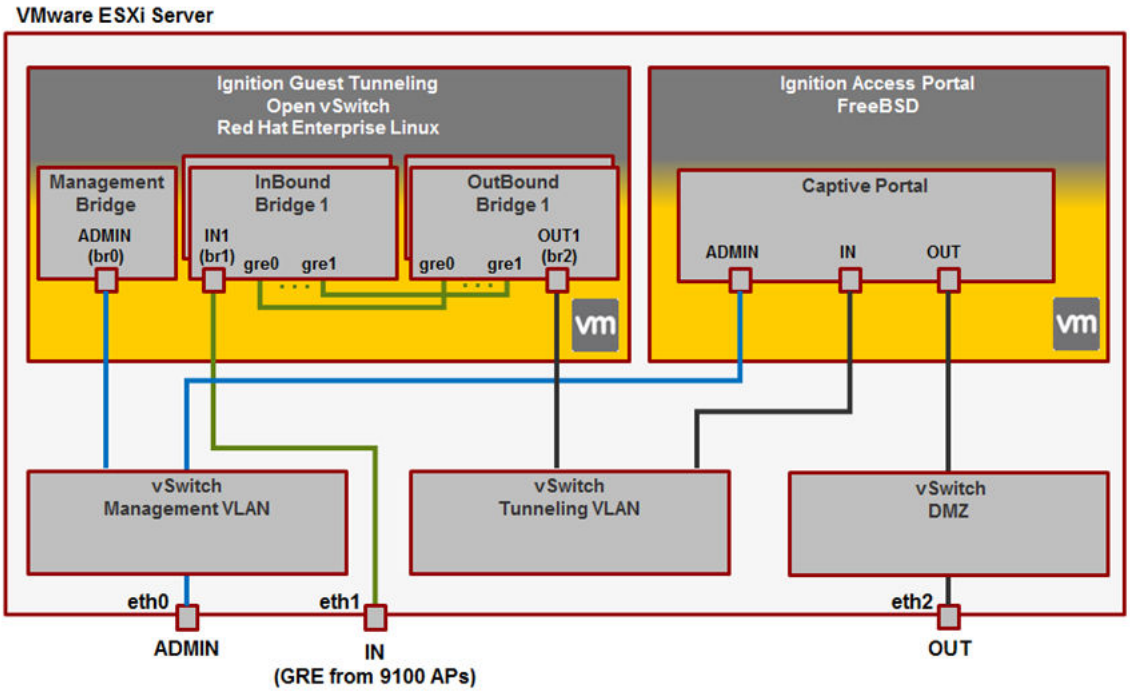


Figure 1: IGT Architecture

Configuration Overview

Follow the below procedures in sequence to install and configure IGT:

1. Install VMware ESXi server. For more information, see Installing IGT virtual appliance on page 16.
2. Install Avaya WLAN 9100 Wireless Orchestration System (WOS). For more information, see Installing WLAN 9100 Wireless Orchestration System on page 19.
3. Configure Ignition Guest Tunneling. For more information, see Configuring IGT virtual appliance on page 20.
4. Configure AP GRE tunnel through WOS / WMI. For more information, see WLAN 9100 Configuration using WOS / WMI on page 27.

Installing IGT virtual appliance

About this task

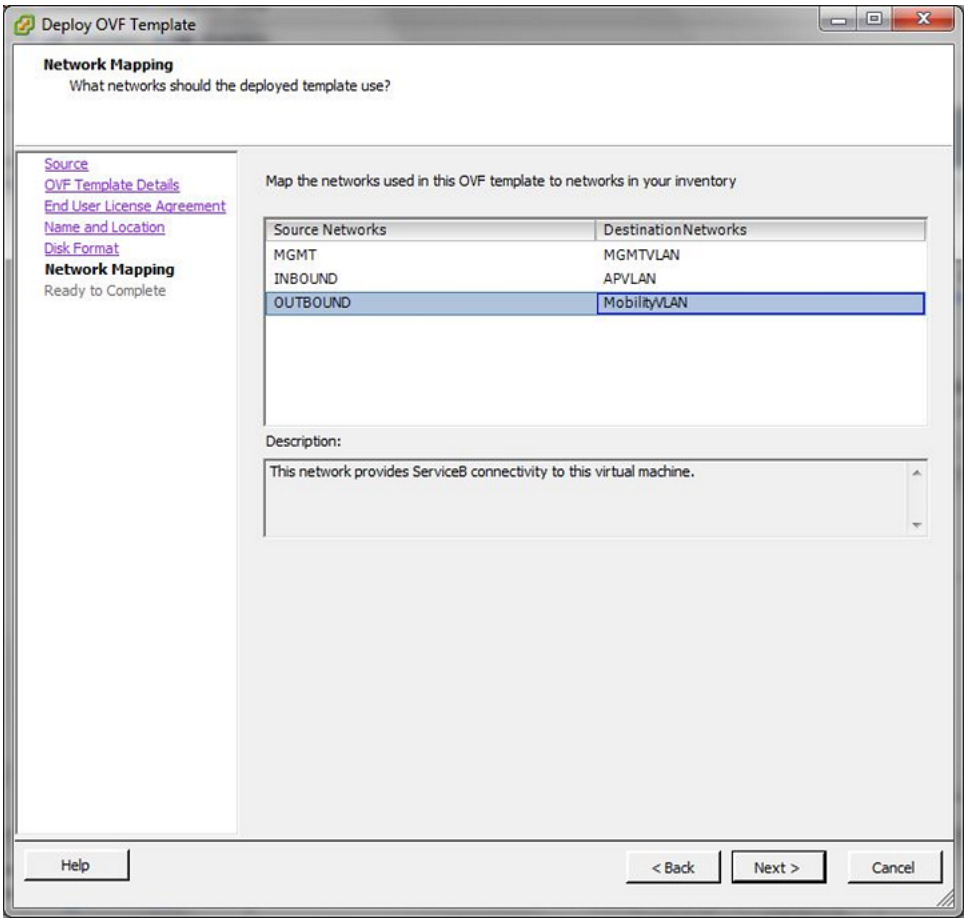
Avaya recommends that you use VMware vSphere Client to deploy the VM into your system. Start the VMware vSphere Client and log in to the ESXi server on which you want to install IGT.

Procedure

1. Select **File** > **Deploy OVF Template** from the vSphere Client.
2. Click **Browse** to select the location to import the IGT virtual appliance and click **Next**.
3. Click **Accept** to accept the license and click **Next**.
4. Enter a **Name** for the virtual machine and click **Next**.
5. Select one of the following format to store the virtual disks and click **Next**.
   - **Thick Provision Lazy Zeroed** : Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created.
   - **Thick Provision Eager Zeroed**: A type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. This format takes longer time to create disks than to create other types of disks.
   - **Thin Provision**: For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the disk size. Uses only as much datastore space as the disk needs for its initial operations.

   By default, **Thick Provision Lazy Zeroed** format is selected.

6. Associate the IGT network interfaces to the correct VM network, based on site configuration.



7. Review your settings. Click **Finish** to start the import.

Note:

Ensure that the **Promiscuous mode** is set to **Accept** for the newly created OUT interface.

By default, a guest operating system's virtual network adapter only receives frames that are meant for it. Because, IGT is acting as a tunneling server for the wireless clients, it has to check for packets that are meant to the wireless clients. Placing the guest's network adapter in promiscuous mode causes it to receive all frames passed on the virtual switch that are allowed under the VLAN policy for the associated port group.

8. Set the **Promiscuous Mode** to **Accept** for the newly created network. For more information, see Setting Promiscuous Mode for newly created network on page 19
9. Select the VM created from the tree on the left side of the **vSphere Client** window.
10. Start IGT by clicking the **Power on the virtual machine** link in the **Getting Started** tab.

    You can see the Avaya Ignition Guest Tunneling summary in the **Summary** tab.

Setting Promiscuous Mode for newly created network

About this task

Set the Promiscuous Mode to Accept for the newly created OUT interface.

Procedure

1. Click **VMware ESXi** IP address on the left of the **vSphere Client**.
2. Navigate to **Configuration** tab.
3. In the **Hardware** section, click **Networking**
4. Click **Properties** of the **Standard Switch: vSwichx**.
5. Select the new network created and click **Edit**.
6. Select the **Security** tab.
7. Select the **Promiscuous Mode** check box.
8. Select **Accept** from the drop-down list and click **OK**.

   In the vSwitchx Properties window in the **Effective Policies** section, you can see the Promiscuous Mode changed to **Accept**.
9. Click **Close** to close the vSwitchx Properties window.

Installing WLAN 9100 Wireless Orchestration System

About this task

This section describes the procedure to install Avaya WLAN 9100 Wireless Orchestration System (WOS) on ESXi Server. For more information about using the WOS, see *Using the Avaya Wireless Orchestration System*, NN47252-103.

Before you begin

Start the VMware vSphere Client and log in to the ESXi server on which you want to install Avaya WLAN 9100 WOS.

Procedure

1. Select **File** > **Deploy OVF Template** from the vSphere Client.
2. Click **Browse** to select the location to import the Avaya WLAN 9100 WOS and click **Next**.
3. Enter the **Name** of the virtual machine and click **Next**.
4. Select one of the following format to store the virtual disks and click **Next**.
   - **Thick Provision Lazy Zeroed**: Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created.

- **Thick Provision Eager Zeroed**: A type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. This format takes longer time to create disks than to create other types of disks.
- **Thin Provision**: For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the disk size. Uses only as much datastore space as the disk needs for its initial operations.

By default, **Thick Provision Lazy Zeroed** format is selected.

5. Associate the IGT network interfaces to the correct VM network, based on site configuration.
6. Review your settings. Click **Finish** to start the import.
7. Select the VM created from the tree on the left side of the **vSphere Client** window.
8. Start Avaya WLAN 9100 WOS by clicking the **Power on the virtual machine** link in the **Getting Started** tab.

   You can see the Avaya WLAN 9100 WOS summary in the **Summary** tab.

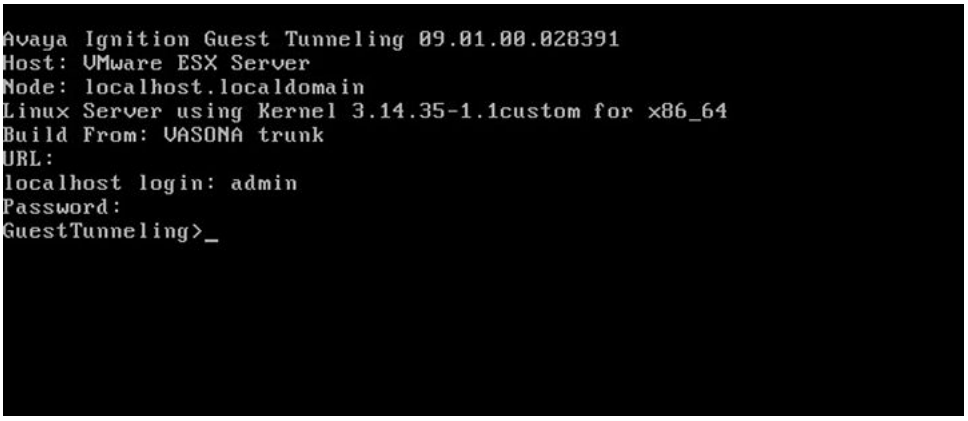
Configuring IGT virtual appliance

About this task

After you power on the IGT VM, configure the VM settings to start Ignition Guest Tunneling.

Procedure

1. Power on the VM and launch the Ignition Guest Tunneling console.
2. Enter the **username** and **password**. The default **username** and **password** is `admin` and `admin`.



3. Configure the management interface:

   `interface br0 ipaddr <IP Address>/<netmask>`

4. Configure the inbound interface:

   `interface br1 ipaddr <IP Address>/<netmask>`

5. Configure the outbound interface:

   `interface br2 ipaddr <IP Address>/<netmask>`

6. Configure the default route for the inbound interface:

   `route add <subnet>/<prefix> <gateway>`

   Note:

   - Setting a default route to bridge interface is optional. Ensure that the network connectivity with AP is Up.
   - Ensure that br0 bridge interface should not be configured with the default route. Because, packets that do not belong to br1 and br2 will get routed over br0 interface. This can cause leakage of traffic into the br0 network.
   - Promiscuous mode should be enabled only on br2 interface and it should be marked as **Reject** on other interfaces.

7. Configure the static route for the management interface:

   `route add <subnet>/<prefix> <gateway>`

Example

Following is the example to configure IGT appliance.

Configure management interface:

```
interface br0 ipaddr 10.10.10.1/24
```

```
7: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
link/ether 00:50:56:b0:2b:39 brd ff:ff:ff:ff:ff:ff
inet 10.10.10.1/24 brd 10.140.251.255 scope global br0
valid_lft forever preferred_lft forever
inet6 fe80::250:56ff:feb0:2b39/64 scope link
valid_lft forever preferred_lft forever
```

Configure the inbound interface:

```
interface br1 ipaddr 10.10.10.2/16
```

```
8: br1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
link/ether 00:50:56:b0:7f:65 brd ff:ff:ff:ff:ff:ff
inet 10.10.10.2/16 scope global br1
valid_lft forever preferred_lft forever
inet6 fe80::250:56ff:feb0:7f65/64 scope link
valid_lft forever preferred_lft forever
```

Configure the outbound interface:

```
interface br2 ipaddr 10.10.10.3/16
```

```
6: br2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
link/ether 00:50:56:b0:55:93 brd ff:ff:ff:ff:ff:ff
inet 10.10.10.3/16 scope global br2
valid_lft forever preferred_lft forever
inet6 fe80::250:56ff:feb0:5593/64 scope link
valid_lft forever preferred_lft forever
```

IGT Web User Interface

Launch IGT Web User Interface to import, export the GRE Tunnel configuration .csv or .tar file, add, display or delete the GRE Tunnel in the IGT appliance.

Follow the below steps to configure and manage IGT GRE tunnel:

- Add GRE Tunnel. For more information, see Adding GRE tunnel on page 22.
- Display GRE Tunnel Status. For more information, see Displaying Guest Tunneling Status on page 23.
- Import GRE Tunnel. For more information, see Importing GRE tunnel on page 23.
- Export GRE Tunnel. For more information, see Exporting GRE Tunnel on page 24.

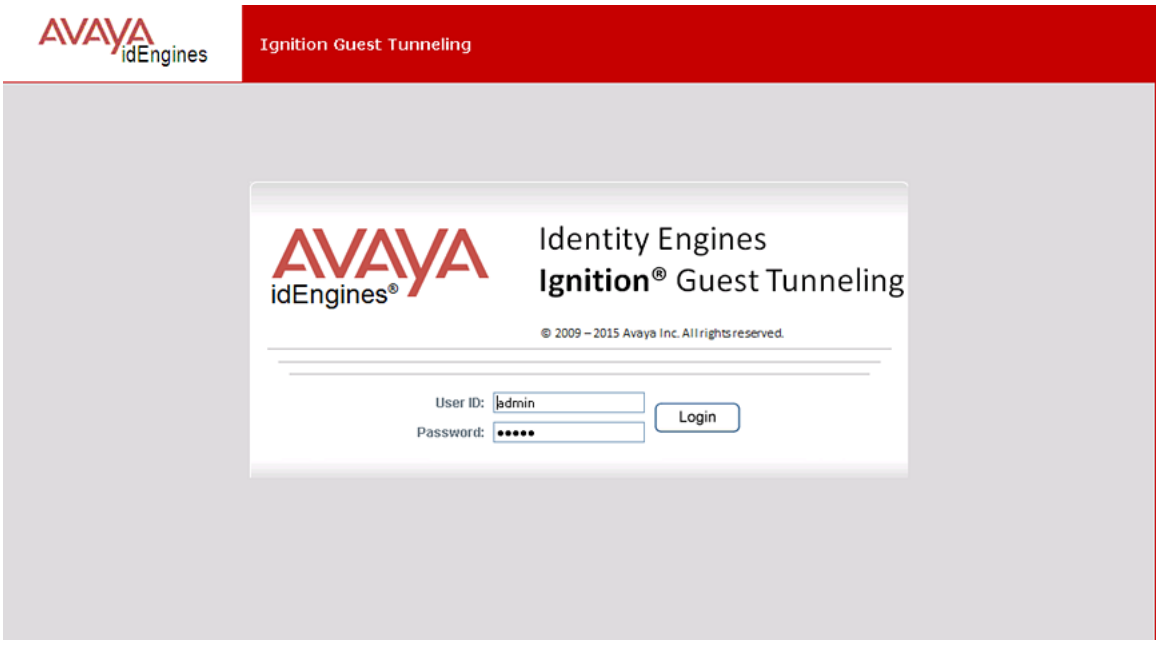
Adding GRE tunnel

About this task

Add individual GRE tunnel into IGT.

Procedure

1. In a supported web browser, enter the IP address of IGT Appliance management (https://<*IGT Appliance mgmt IP address*>).
2. Enter **User ID** and **Password**. The default **User ID** and **Password** is `admin` and `admin`.



3. In the **Tunnel** menu, click **Add** to add new GRE tunnel.
4. Enter the tunnel remote endpoint.

5. Click **Add** to save the new GRE tunnel.

   The user interface adds the tunnel remote endpoint into IGT and displays the success message.

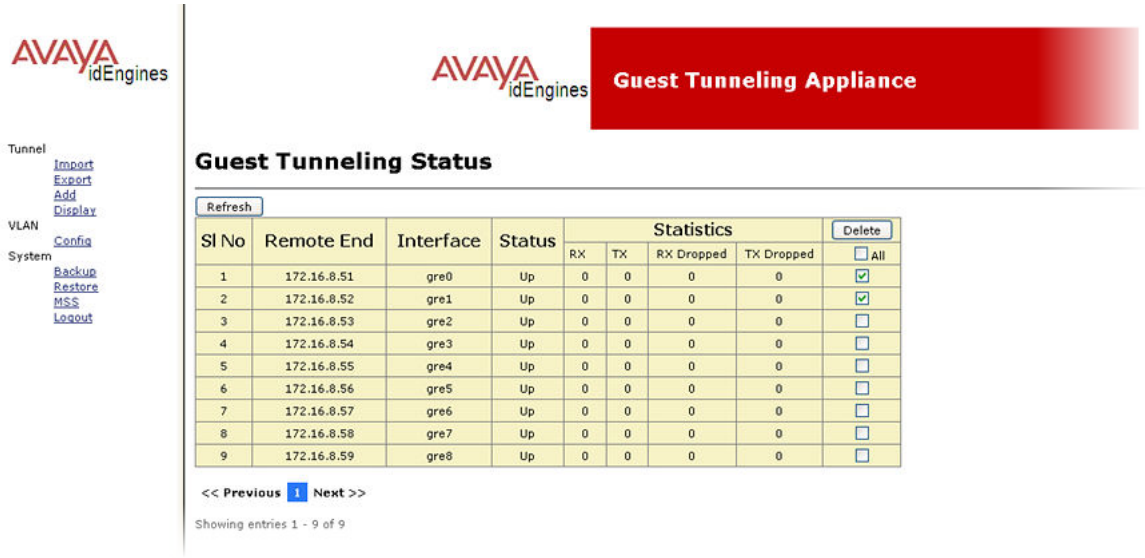
Displaying Guest Tunneling Status

About this task

Display the status of Guest Tunneling.

Procedure

1. In the **Tunnel** menu, click **Display** to display the status of Guest Tunneling.



   The Display Guest Tunneling Status window appears listing all the Guest Tunneling information.

2. **(Optional)** To remove a Tunnel, select the required tunnel check box and click **Delete**.
3. **(Optional)** Click **Refresh** to refresh the **Guest Tunneling Status** table.

Importing GRE tunnel

About this task

Import the GRE tunnel configuration .csv file from WLAN 9100 Orchestration server.

Procedure

1. In the **Tunnel** menu, click **Import**.
2. Browse and select the .csv file from your local hard disk.

The .csv is exported from the WOS to configure the GRE Tunnels on IGT. For more information see, Exporting WLAN Access Point configuration on page 31

3. Click **Import** to import the .csv file.

   The user interface parses the .csv file and import only tunnel information into the IGT .

   After parsing, it displays a success message with the count of tunnels added.

Exporting GRE Tunnel

About this task

Export GRE tunnel from IGT.

Note:

Ensure to take backup of the GRE Tunnels before making any config changes, because when IGT VM is updated it replaces it with a new VM.

Procedure

1. In the **Tunnel** menu, click **Export**.

   The Export tunnel remote endpoint window appears.

2. Click **Export** to export the GRE tunnel.

   The Save as window appears.

3. Select the location in your local hard disk to save the .tar file.

Configuring IGT GRE Tunnel VLAN

About this task

Configure the IGT GRE tunnel VLAN to untag the VLAN traffic.

Procedure

1. In the **VLAN** menu, click **Config**.

   The Guest VLAN Untagging Configuration window appears.

2. Enter the **Guest VLAN ID** for which you want the IGT to untag the VLAN traffic and forward.

   Enter **VLAN ID** range between 1 and 4095.

3. Click **Untag VLAN**.

   The VLAN ID entered gets configured as **Guest Tunnel VLAN**.

Managing IGT GRE Tunnel System

Use the following procedures to backup system configuration, restore it, configure Maximum Segment Size (MSS) and logout of the appliance.

- Backup System Configuration. For more information, see Taking Backup of IGT System Configuration on page 25.
- Restore System Configuration. For more information, see Restoring IGT System Configuration on page 25.
- TCP MSS Value Configuration. For more information, see Configuring TCP MSS value on page 26.
- Logout. For more information, see Logging out of Guest Tunneling Appliance on page 26.

Taking Backup of IGT System Configuration

About this task

Take Backup of IGT system configuration.

Note:

- The IGT system backup does not contain the tunnel configuration. For more information on exporting tunnel configuration, see Exporting GRE Tunnel on page 24
- Ensure to take backup of the IGT system configuration before making any configuration changes, because when IGT VM is updated it replaces it with a new VM.

Procedure

1. In the **System** menu, click **Backup**.
2. Click **Export**.

   The Save as window appears.
3. Select the location in your local hard disk to save the .tar file.
4. Click **Save** to save the .tar file.

Restoring IGT System Configuration

About this task

Restore the IGT system configuration.

Procedure

1. In the **System** menu, click **Restore**.
2. Click **Browse** to select the **Backup** .tar file from your local hard disk.
3. Click **Import** to restore the system configuration.

Note:

System will reboot automatically after import.

Configuring TCP MSS value

About this task

Configure TCP Maximum Segment Size (MSS) value to change the default value 1350 bytes.

Procedure

1. In the **System** menu, click **MSS**.
2. Uncheck the **Use Default** check box and enter the **TCP MSS** value (TCP MSS value ranges between 577 and 1422 bytes).

3. Click **Save**.

   MSS value gets saved and displays a success message.

Logging out of Guest Tunneling Appliance

About this task

Logout from Guest Tunneling appliance.

Procedure

In the **System** menu, click **Logout**.

The **Guest Tunneling Appliance** login page is displayed.

Chapter 5: WLAN 9100 Configuration using WOS / WMI

GRE Tunnel configuration on WLAN 9100 access points can be done through WLAN 9100 WOS and Access Point Web Management Interface (WMI).

WLAN 9100 WOS is a management application used to manage multiple access points. For more information about configuring GRE tunnel on WLAN 9100 WOS, see GRE Tunnel Configuration on WLAN 9100 Orchestration System on page 27.

Access Point WMI is a GUI used to manage a single access point. For more information about configuring GRE tunnel on WLAN 9100 WMI, seeGRE Tunnel Configuration on WLAN 9100 Web Management Interface on page 32.

GRE Tunnel Configuration on WLAN 9100 Orchestration System

Use the following procedure in sequence to configure GRE tunnel on WLAN 9100 Orchestration System.

1. Launching WLAN 9100 Orchestration System. For more information, see Launching WLAN 9100 Orchestration System on page 27.
2. Configuring SSID. For more information, see Configuring SSID using WLAN 9100 Orchestration System on page 28.
3. Configuring GRE tunnel. For more information, see Configuring GRE tunnel on WLAN 9100 Orchestration System on page 29.
4. Associating the GRE tunnel to SSID. For more information, see Associating the GRE tunnel to SSID on page 30.
5. Exporting WLAN Access Point configuration. For more information, see Exporting WLAN Access Point configuration on page 31.

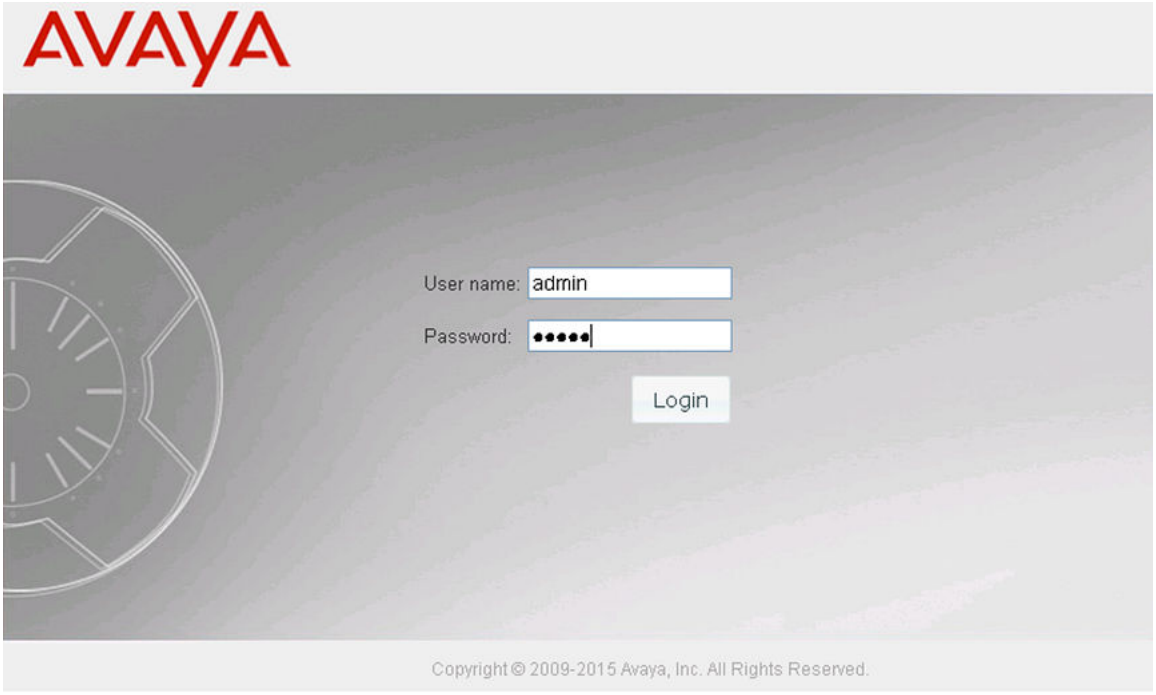
Launching WLAN 9100 Orchestration System

About this task

Launch WLAN 9100 Orchestration System to configure tunnel.

Procedure

1. In a supported web browser, enter the IP address of the WOS (https://<*WOS IP Address*>).



2. Enter the **Username** and **Password**. The default **Username** and **Password** is `admin` and `admin`.

Configuring SSID using WLAN 9100 Orchestration System

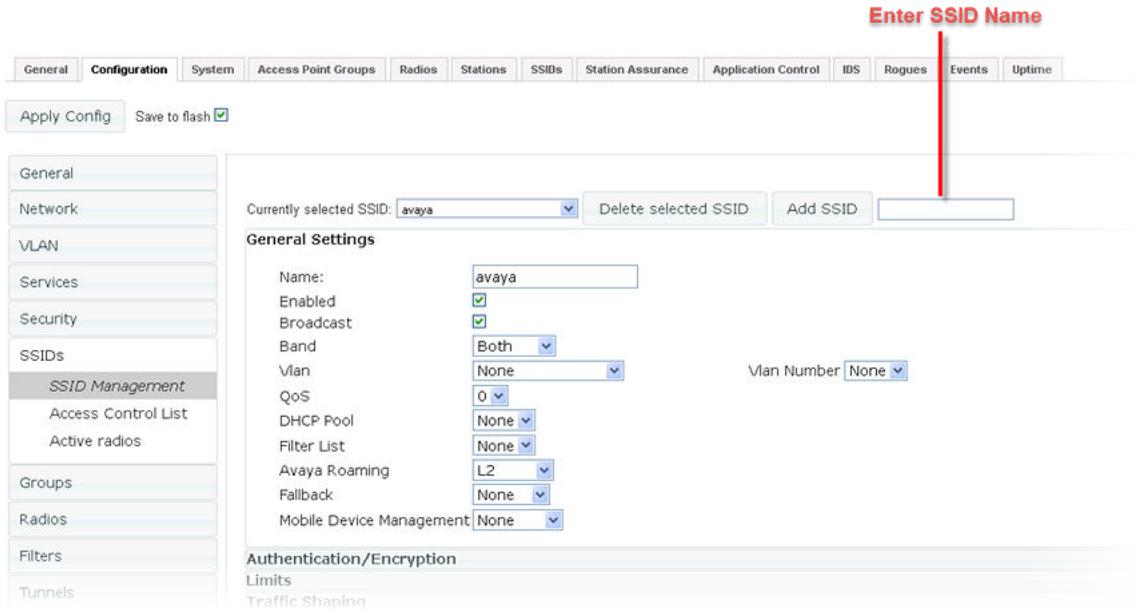
About this task

Configure SSID on AP using WLAN 9100 Orchestration System.

Procedure

1. Go to **Monitor** > **Access Points** > **<*AP instance*>** > **Configuration**.
2. Click **SSIDs** > **SSID Management**.

3. Enter the **Name** of SSID that you want to add.



4. Click **Add SSID**.
5. Click **Apply Config** to save the configuration.

Configuring GRE tunnel on WLAN 9100 Orchestration System

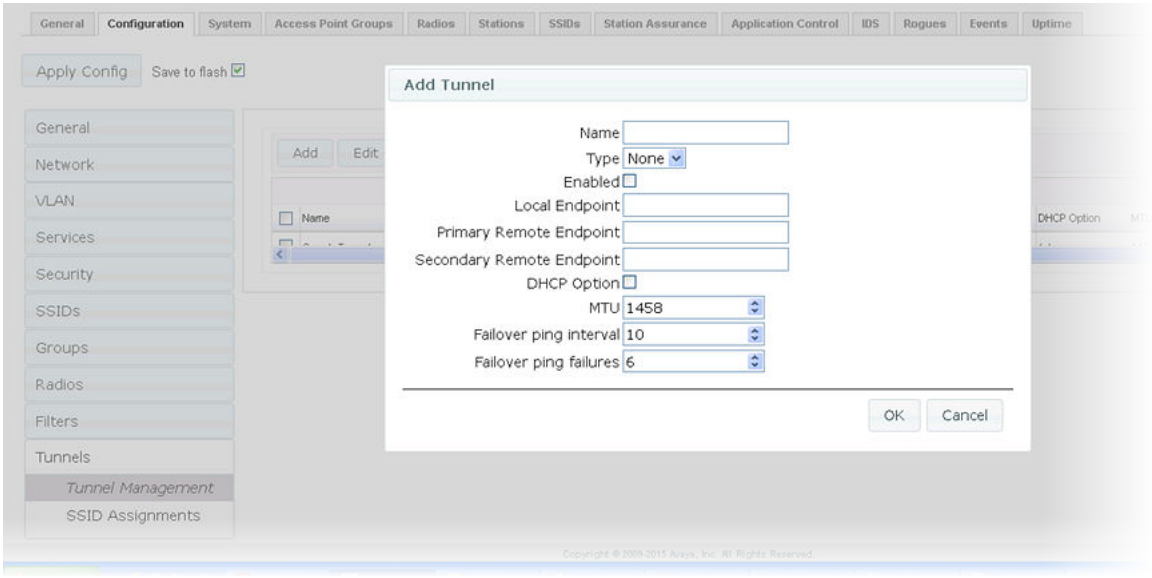
About this task

Configure GRE tunnel on AP using WLAN 9100 Orchestration System.

Procedure

1. Go to **Monitor** > **Access Points** > ***<AP instance>*** > **Configuration**.
2. Click on **Tunnels** > **Tunnel Management**.

3. Click **Add**. The Add new tunnel window displays.



To edit existing tunnel information, select the tunnel and click **Edit**.

4. Select **Type** as `gre` from the drop-down list.
5. Enter the **Local EndPoint** IP address (Access Point address).
6. Enter the **Primary Remote EndPoint** IP address (IGT inbound interface IP).
7. **(Optional)** Enter the **Secondary Remote EndPoint** IP address, for failover and redundancy purposes.
8. Click **Add**.
9. Click **Apply Config** to save the configuration.

Associating the GRE tunnel to SSID

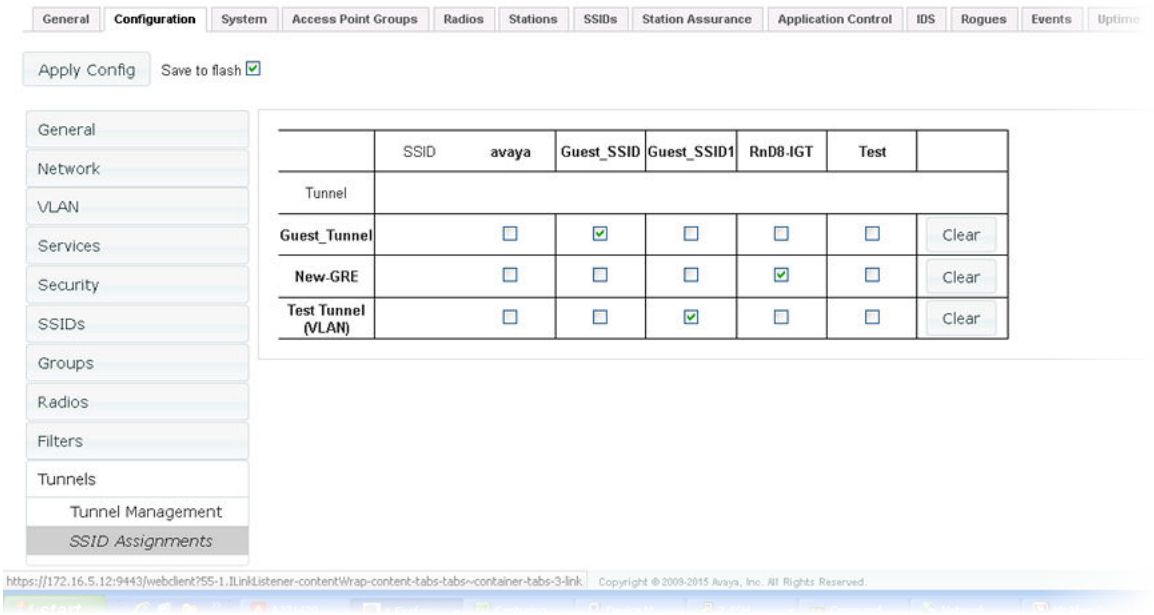
About this task

Associate the GRE tunnel to SSID using WLAN 9100 Orchestration System.

Procedure

1. Go to **Monitor** > **Access Points** > **<*AP instance*>** > **Configuration**.
2. Click **SSID Assignments**.

3. Select the **SSID check box** to associate the GRE tunnel to SSID.



4. Click **Apply Config** to save the configuration.

Exporting WLAN Access Point configuration

About this task

Export the Access Point configuration in .csv format.

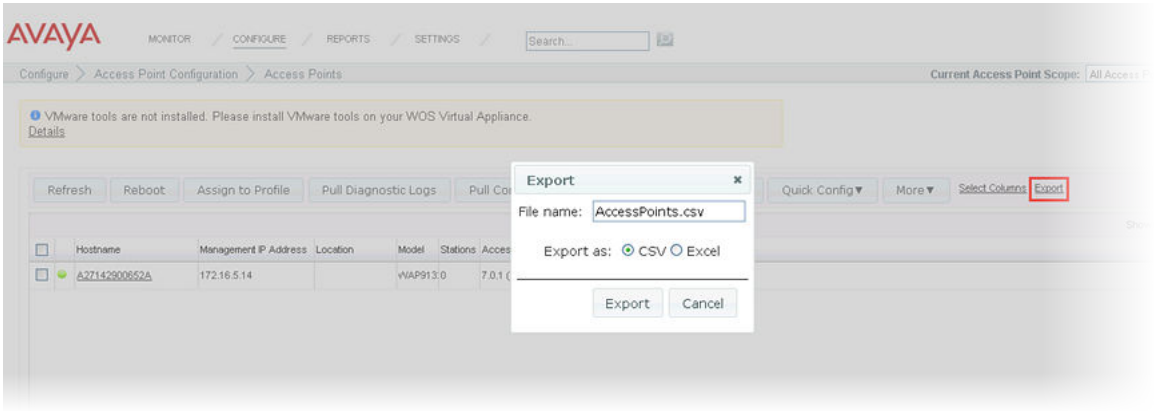
Note:

Ensure to take backup of the WLAN Access Point configuration before making any configuration changes, because when IGT VM is updated it replaces it with a new VM.

Procedure

1. Go to **Configure** > **Access Point Configuration** > **Access Point**.

2. Click **Export link**.



3. Browse and select the .csv file.
4. Click **Export**.

GRE Tunnel Configuration on WLAN 9100 Web Management Interface

Use the following procedure in sequence to configure GRE tunnel on WLAN 9100 Web Management Interface (WMI).

1. Launching the WLAN 9100 WMI. For more information, see Launching WLAN 9100 Web Management Interface on page 32.
2. Configuring SSID. For more information, see Configuring SSID on Avaya WLAN 9100 WMI on page 33.
3. Configuring GRE tunnel. For more information, see Configuring GRE tunnel on Avaya WLAN 9100 WMI on page 34.
4. Associating GRE tunnel to SSID. For more information, see Associating the GRE tunnel to SSID on page 35.

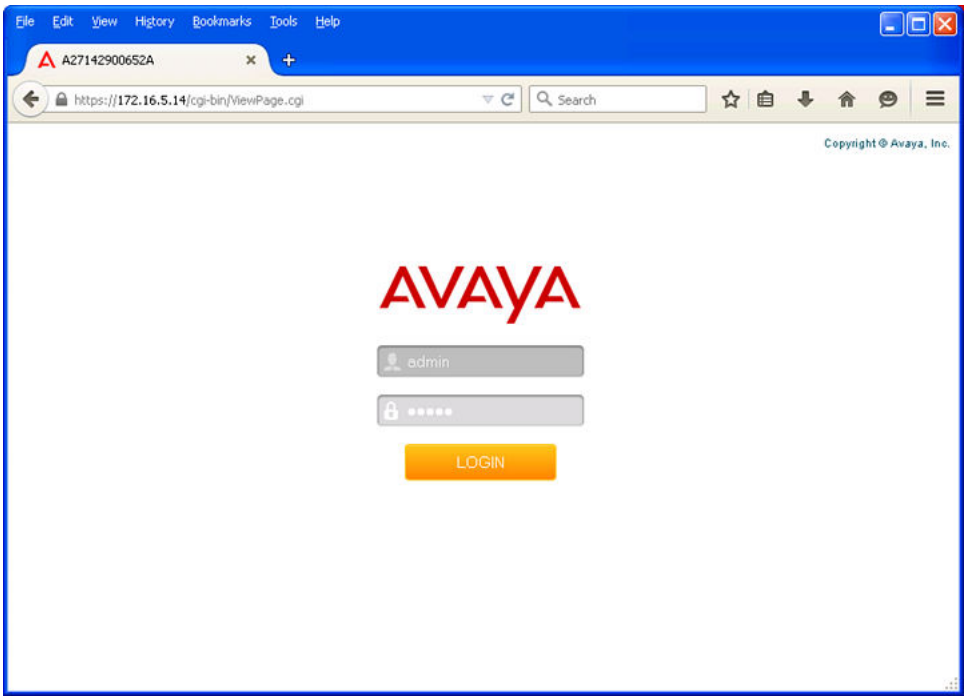
Launching WLAN 9100 Web Management Interface

About this task

Launch WLAN 9100 Web Management Interface to configure tunnel.

Procedure

1. In a supported web browser, enter the IP address of the AP (https://<*AP IP Address*>).



2. Enter the **Username** and **Password**. The default **Username** and **Password** is `admin` and `admin`.

Configuring SSID on Avaya WLAN 9100 WMI

About this task

Configure SSID on AP using Avaya WLAN 9100 Web Management Interface.

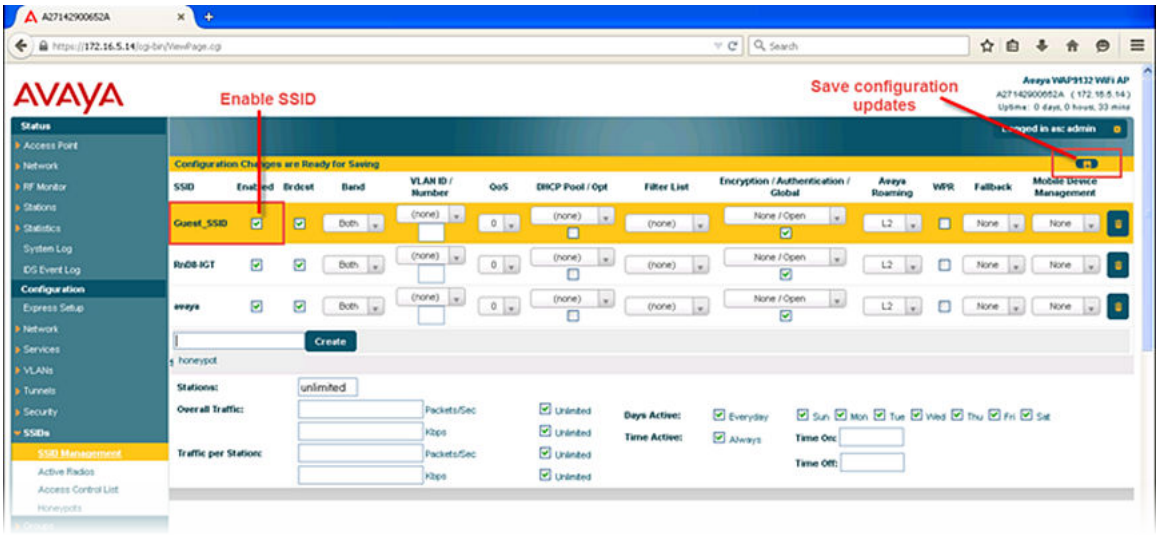
Procedure

1. Go to **Configurations** > **SSIDs** > **SSID Management**.
2. Enter the **Name** of the SSID.
3. Click **Create**.

   A message box is displayed with the following note:

   “Note: New SSID created is disabled. Enable after configuration.”
4. Click **OK**.
5. Select the **Enabled** check box.

6. Click **Save** icon on top right corner below the **Logged in as: username**.



Configuring GRE tunnel on Avaya WLAN 9100 WMI

About this task

Configure GRE tunnel on AP using WLAN 9100 Web Management Interface.

Procedure

1. Go to **Configuration** > **Tunnels** > **Tunnel Management**.
2. Enter the **New Tunnel Name** and click **Create**.

   A message box is displayed with the following note:

   “Note: New tunnel created is disabled. Enable after configuration”.
3. Click **OK**.
4. Select the **Enabled** check box.
5. Select the **Type** to `gre` from the drop-down list.
6. Enter the following endpoints.
   - **Local Endpoint** (the AP address).
   - **Primary remote Endpoint** (the Ignition Guest Tunneling inbound interface IP).
   - **Secondary remote Endpoint** for failover and redundancy purposes.
7. Click **Save** icon on the right-top corner.

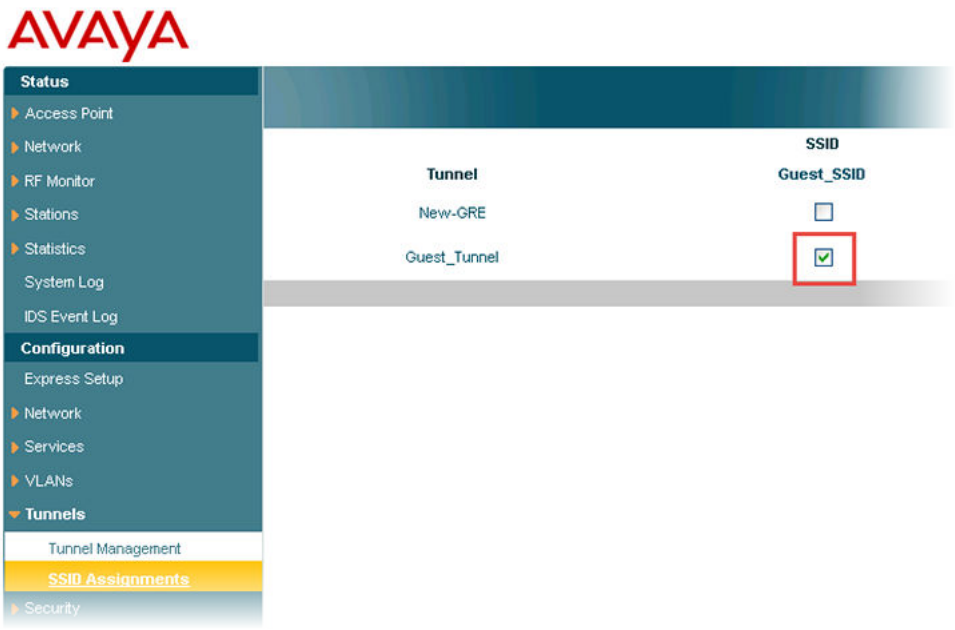
Associating the GRE tunnel to SSID

About this task

Associate the GRE tunnel to SSID using Avaya WLAN 9100 Web Management Interface.

Procedure

1. Go to **Configuration** > **Tunnels** > **SSID Assignments**.
2. Select the **SSID** check box to associate it with the GRE tunnel.



3. Click **Save** icon on the right-top corner.

Chapter 6: Configuring AP 9100 and IGT to support VLANs

The AP 9100 supports VLAN tagging. After configuring the AP 9100, it sends encapsulated client traffic through transport VLAN (tunnel VLAN) to IGT. The IGT decapsulates the packets received on the GRE tunnel, removes the tagging on the VLAN and forwards the untagged packet to the Ignition Access Portal.

Configuring VLANs on AP 9100

About this task

Configure client VLANs on AP 9100.

Procedure

1. In a supported browser, enter the IP address of the AP (https://<*AP IP Address*>).
2. Enter the **Username** and **Password**. The default **Username** and **Password** is `admin`.
3. Go to **Configuration** > **VLANs** > **VLAN Management**.
4. Enter the **New VLAN Name** and **Number**.
5. Click **Create**.

   Create two VLANs, one for client traffic and another for tunneling.
6. **(Optional)** Add an interface IP in case a static IP address is being assigned.
7. **(Optional)** Select the **DHCP** check box, in case an external DHCP server is configured to grant an IP for these VLANs.
8. **(Optional)** Select the **Management** check box to enable Management, in case management traffic needs to flow on these VLANs.
9. Create a new SSID and enable it. For more information, see Configuring SSID on Avaya WLAN 9100 WMI on page 33.

   Assign the created guest VLAN to the SSID that is being used for guests to connect.
10. Select the VLAN to the SSID from **VLAN ID / Number** drop-down list, in the **SSID Management** page.

11. Create a GRE tunnel to associate with the SSID you created. For more information, see Configuring GRE tunnel on Avaya WLAN 9100 WMI on page 34.

    Note:

    When you create a GRE tunnel on the AP, ensure that the tunnel's local end point IP address is same as the Tunnel VLAN that is created.

12. Click **Save** icon on the right-top corner.

Configuring Tunnel VLAN on AP 9100

About this task

Configure tunnel VLAN on AP 9100.

Procedure

1. Create GRE tunnel. For more information, see Configuring GRE tunnel on Avaya WLAN 9100 WMI on page 34.
2. Go to **Configuration** > **VLANs** > **VLAN Management**.
3. Enter **New VLAN Name** and **Number**.
4. Click **Create**.

   The newly created tunnel VLAN list appears.
5. **(Optional)** Add an interface IP in case a static IP address is being assigned.
6. **(Optional)** Select the **DHCP** check box, in case an external DHCP server is configured to grant an IP for these VLANs.
7. **(Optional)** Select the **Management** check box to enable Management, in case management traffic needs to flow on these VLANs.
8. Enter the **IP Address**.

   Ensure that the GRE tunnel's **Local Endpoint** and Tunnel VLAN **IP Address** should be the same.
9. Enter the **Subnet Mask**.
10. Click **Save** icon on the right-top corner.

Configuring VLAN on ESXi Server for IGT IN interface

About this task

Configure VLAN on VMware ESXi Server for IGT IN interface.

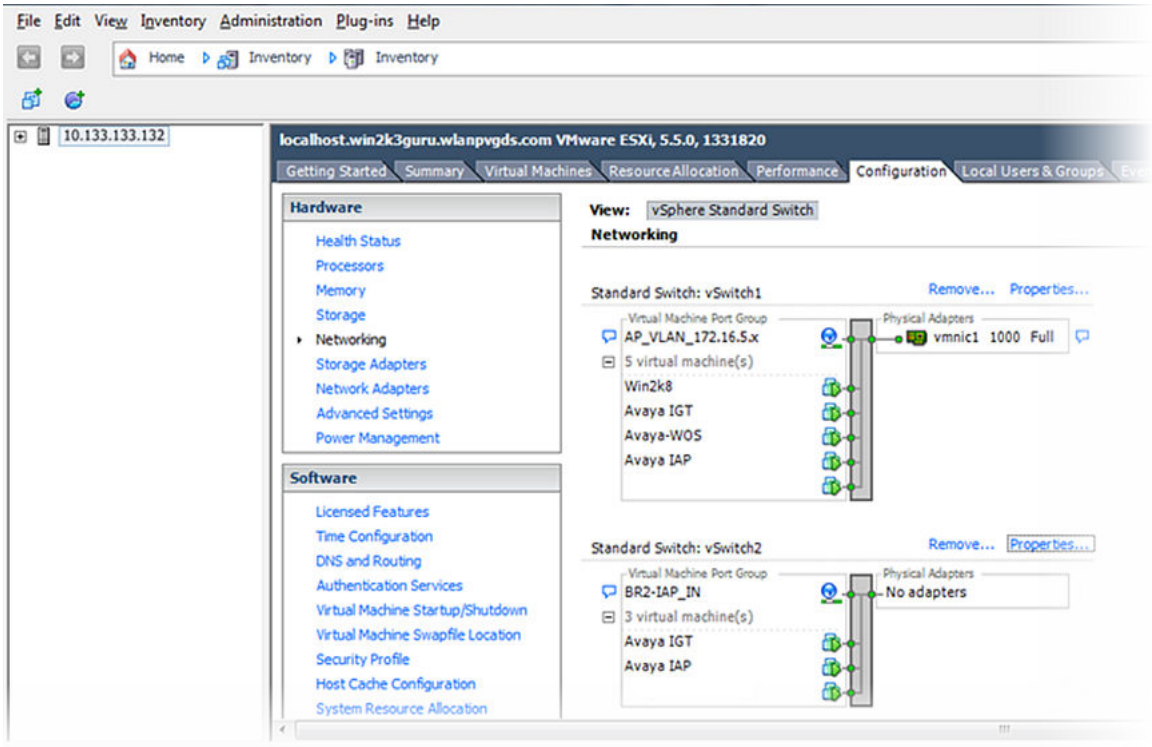
Before you begin

Install the Ignition Guest Tunneling appliance. For more information, see Installing IGT on page 14.

Procedure

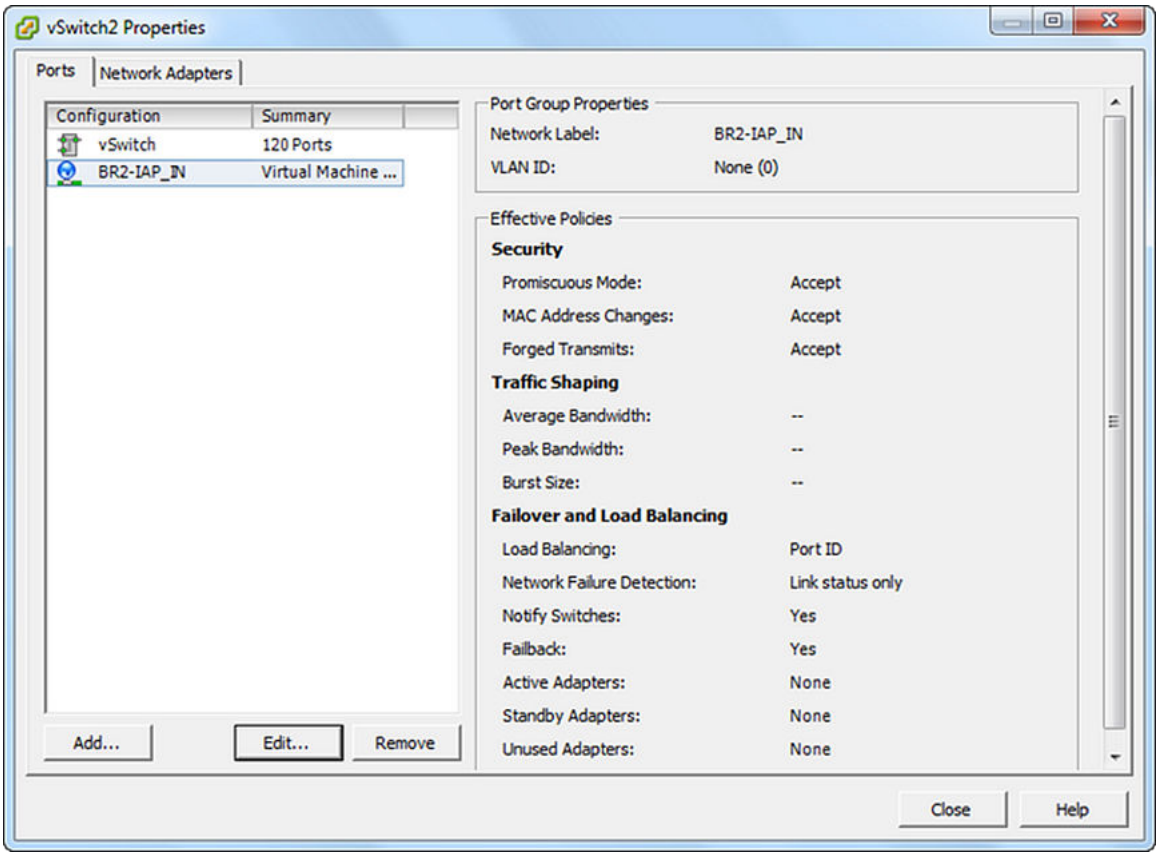
1. Navigate to **Configuration** tab in **vSphere Client**.
2. Click **Networking** in the **Hardware** section.

   The vSphere Standard Switch Structure displays.



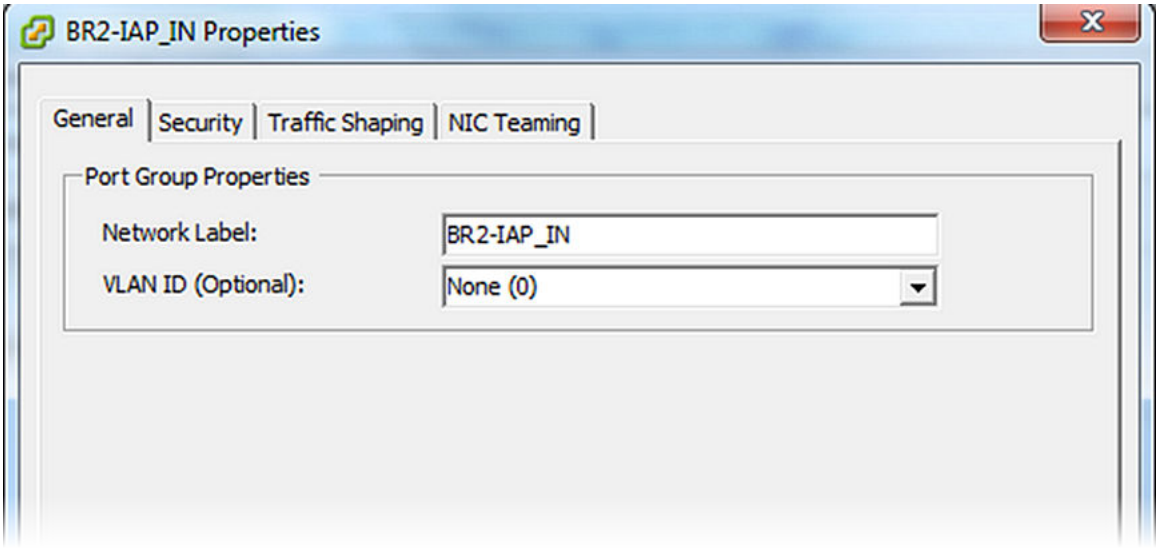
3. Create a virtual machine port group for the vSwitch to which the **IN** interface of the IGT appliance is mapped.
4. Click **Properties**.

5. Select the network interface mapped to the vSwitch and click **Edit**.



The interface properties window displays.

6. Enter the VLAN ID of the Tunneling VLAN and click **OK**.



After the virtual machine port group is created, the network interface assigned to the VM instance expects the tagged VLAN traffic with the VLAN ID to be same as the tunneling VLAN present on the AP.

Configuring VLAN on IGT

About this task

Configure VLAN on IGT using Guest Tunneling Appliance.

Procedure

1. In a supported web browser, enter the IP address of the IGT (https://<*IGT IP Address*>).
2. Enter the **Username** and **Password**. The default **Username** and **Password** is `admin`.
3. Navigate to **VLAN** > **Config** to configure guest tunnel VLAN.

   The **Guest VLAN Untagging Configuration** window displays.
4. Enter the **Guest VLAN ID** and click **Untag VLAN**.
5. Configure the IGT appliance GRE tunnel, to configure GRE tunnel see Adding GRE tunnel on page 22.

Chapter 7: Multiple VLAN Support

In multiple VLAN support scenario, IGT does not untag the multiple VLAN IDs from AP. IGT forwards the packet to OUTBOUND interface with a tag and rely on the adjacent switch to untag the VLAN IDs.

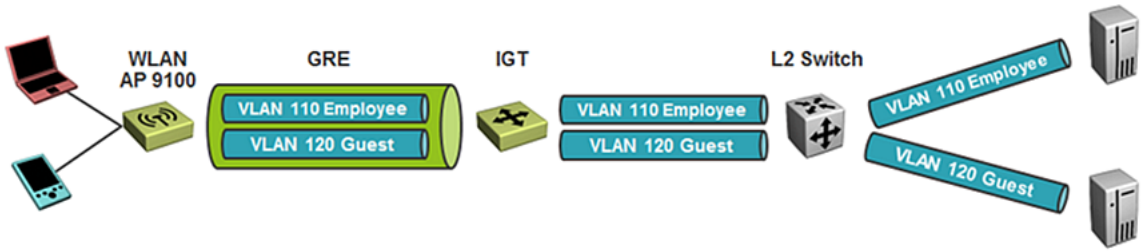


Figure 2: Topology diagram of multiple VLAN support in IGT

Configuring Multiple VLANs on AP 9100

About this task

Configure multiple VLANs on AP 9100.

Procedure

1. In a supported web browser, enter the IP address of AP (https://<*AP IP Address*>).
2. Enter the **Username** and **Password**. The default **Username** and **Password** is `admin` and `admin`.
3. Go to **Configuration** > **VLANs** > **VLAN Management**.
4. Create tunneling VLAN, for more information see Configuring Tunnel VLAN on AP 9100 on page 37.
5. Create multiple VLANs, create multiple SSIDs and map to respective VLANs and create GRE tunnel and assign to SSID on AP 9100.

   Ensure that the Local Endpoint and Tunnel VLAN IP address is the same.

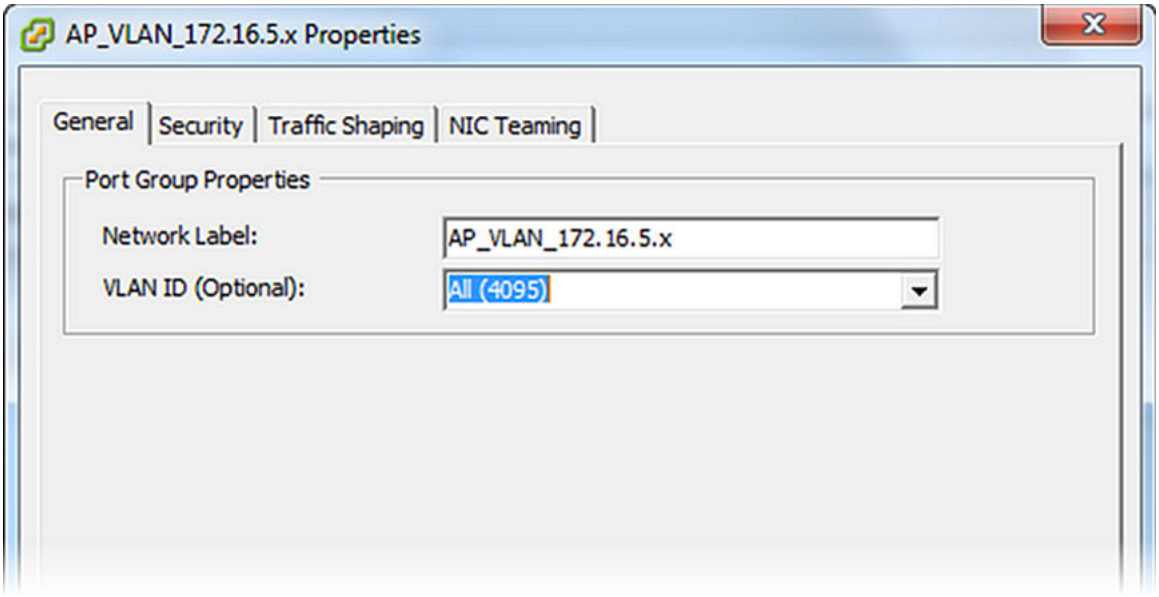
Configuring VLAN on ESXi Server for IGT OUT interface

About this task

Configure VLAN on ESXi Server for IGT OUT interface.

Procedure

1. Navigate to **Configuration** tab in **vSphere Client**.
2. Click **Networking** in the **Hardware** section.
3. Create a virtual machine port group for vSwitch that is mapped to the **OUT** interface of IGT appliance.
4. Click **Properties**.
5. Select the network interface mapped to the vSwitch and click **Edit**.
6. Select the **VLAN ID (Optional)** to (All) 4095 from the drop-down list.



Configuring Dynamic Client VLAN assignment through IDE Server

About this task

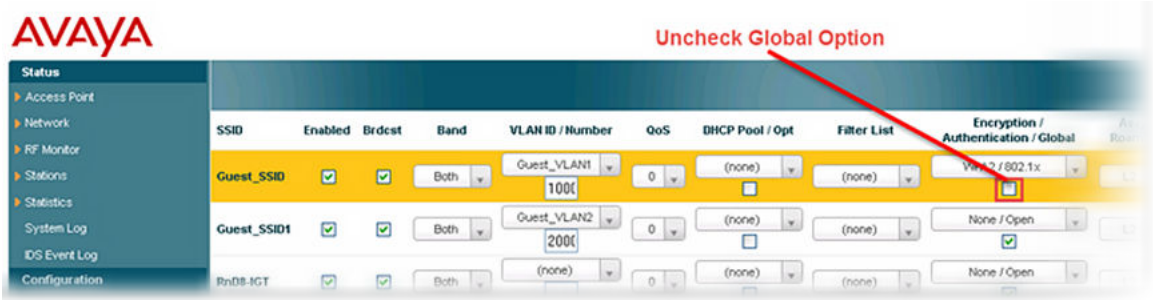
This section describes the procedure to configure Dynamic Client VLAN assignment through IDE Server.

In this scenario AP 9100 is configured with only one SSID. The SSID will have the authentication type as 802.1X with the IDE server configured as the external radius server. After user

authenticates, the IDE server maps the user on the specific VLAN and the traffic flows on the GRE tunnel to the IGT appliance.

Procedure

1. Create an SSID on the AP. For more information, see Configuring SSID on Avaya WLAN 9100 WMI on page 33.
2. Select **Encryption / Authentication / Global** type as `WPA2/802.1X`.
3. Uncheck the **Encryption / Authentication / Global** check box.



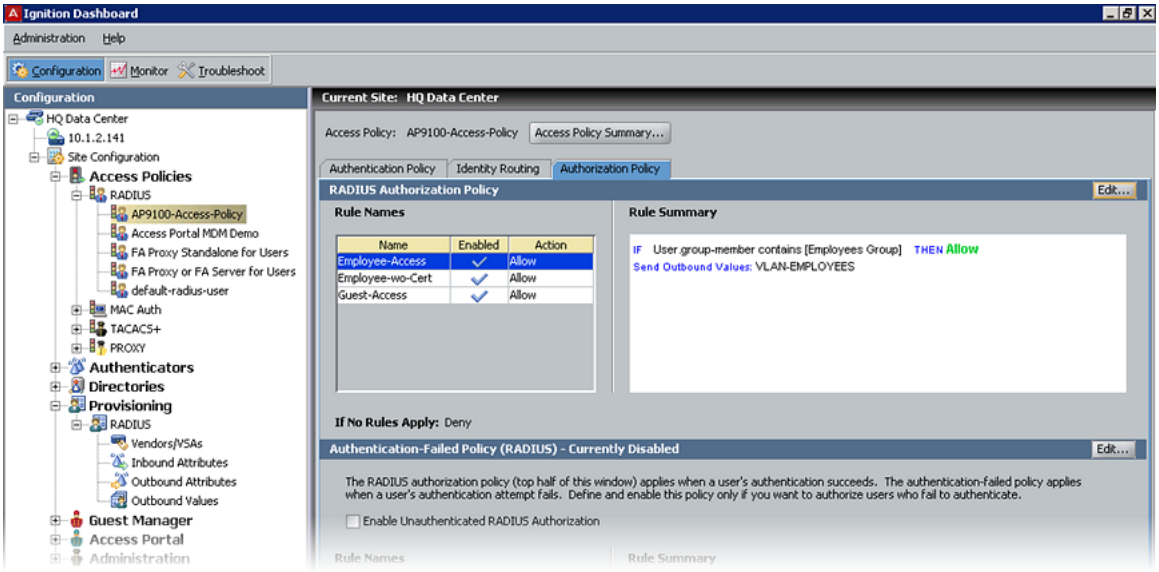
The **Authentication Service Configuration** displays for the SSID.

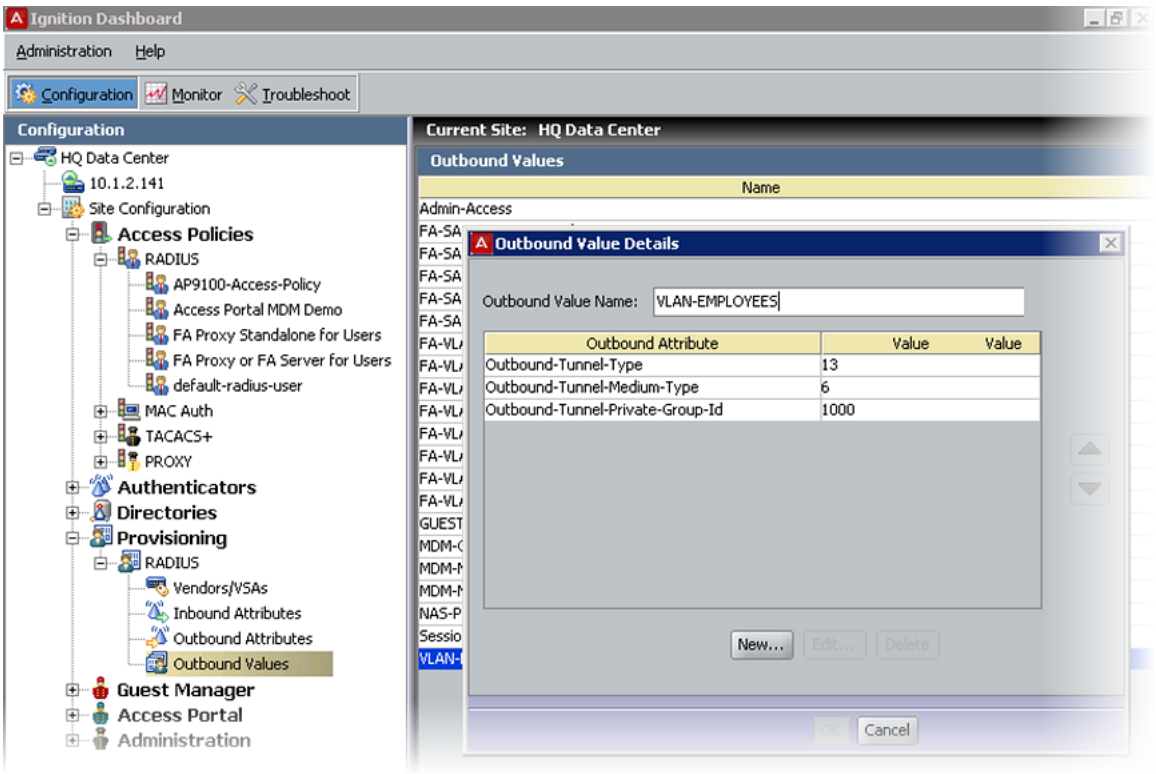
4. Configure the Ignition Server as the external radius server by entering the **Primary Host / IP Address** and **Shared Secret** for the ports 1812 and 1813.
5. Configure VLAN. For more information, see Configuring VLANs on AP 9100 on page 36.

   Note:

   Do not associate any VLAN ID with the SSID.

6. Configure the Ignition server to authenticate user and push a RADIUS outbound attribute with the Guest VLAN ID as shown in the following screenshots. For more information on configuring IDE server, see *Administering Avaya Identity Engines Ignition Server*, NN47280–600.





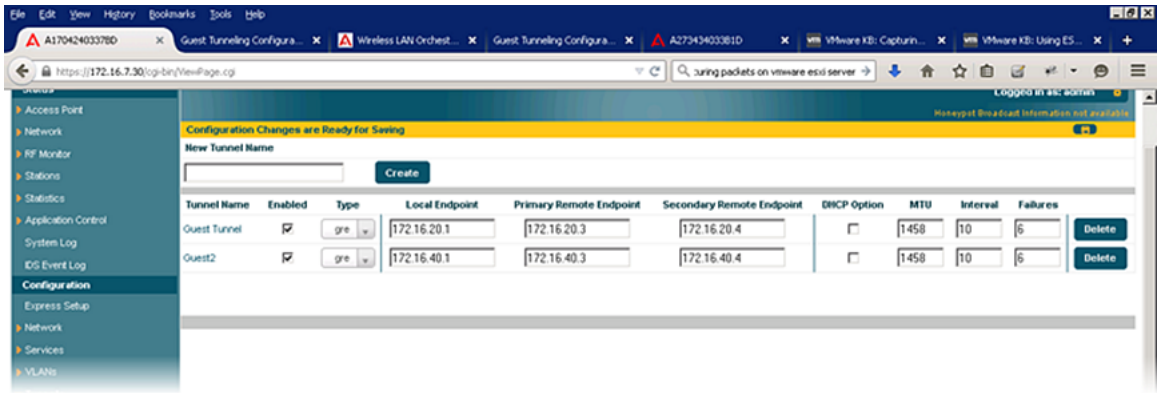
7. To configure multiple VLANs on ESXi Server. For more information, see Configuring VLAN on ESXi Server for IGT IN interface on page 37.

Chapter 8: IGT High Availability

IGT High Availability is delivered by running two IGT virtual instances, which acts as primary and secondary servers.

The redundancy is achieved through the 9100 AP functionality. AP keeps checking for the availability of the GRE tunnel on primary server. If GRE tunnel on primary server does not respond, the packets are sent to GRE tunnel on secondary server.

Example



Chapter 9: Troubleshooting

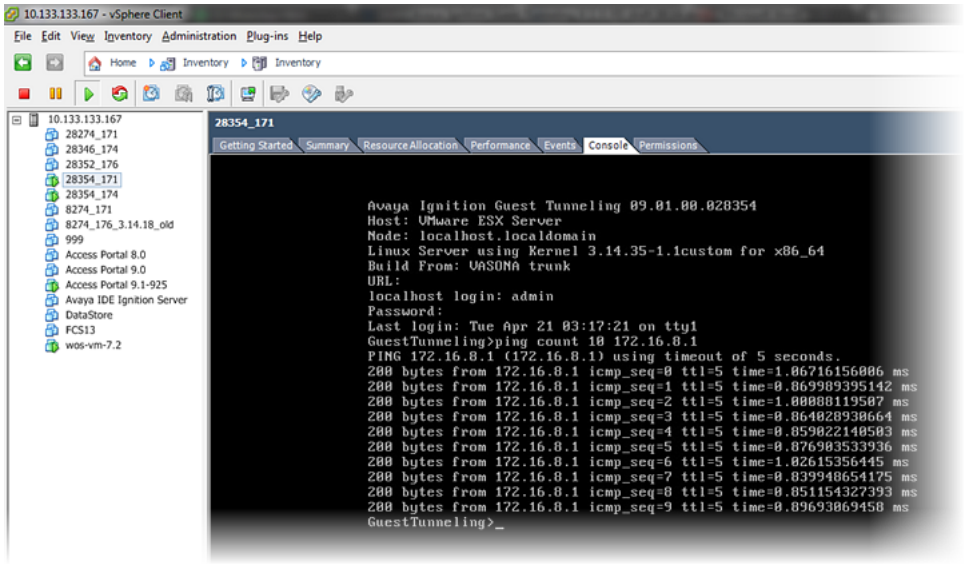
Verifying the connectivity for IGT appliance

Ping functionality can be used to verify the network connectivity for IGT appliance.

`Ping <TTL / Count> <IP Address>`

For example,

1. `ping 20.20.20.1`
2. `ping ttl 10 20.20.20.1`
3. `ping count 10 20.20.20.1`



Tunnel is not responding

- Ensure that SSID to tunnel mapping is correct on the AP.
- Ensure that local IP configured on the AP is same as tunnel remote endpoint configured on the IGT.
- Check the network connectivity.

Issue with wireless client getting an IP address

- Ensure that **Promiscuous** mode is configured as **Accept** on br2 interface.
- Ensure that the configuration of ESXi vSwitch and DHCP server is correct.

Client getting an IP address in the management VLAN

- Ensure that tunnel configuration is correct.
- Ensure that tunnel status is Up.

Debugging issues using tcpdump

Use following procedure to capture packets using tcpdump.

1. Login to IGT console using root or debug user
2. Capture packets on all interfaces of IGT

```
tcpdump -texieth0 -w /tmp/eth0.cap &
tcpdump -texibr0 -w /tmp/br0.cap &
tcpdump -texieth1 -w /tmp/eth1.cap &
tcpdump -texibr1 -w /tmp/br1.cap &
tcpdump -texieth2 -w /tmp/eth2.cap &
tcpdump -texibr2 -w /tmp/br2.cap &
```

Stop packet capture

Use the following command to stop all the tcpdump.

```
killall tcpdump
```

Checking CPU and memory status

Use the following commands to check the CPU and memory usage.

```
top -b -n 1
vmstat
ovs-dpctldump-flows -m
ovs-dpctlshow -s
arp
tar czvfopenswitch_log.tgz /var/log/openvswitch/ /var/log/messages
dmesg
```

Collecting running configuration

Use the following commands to collect the OVS configuration and OVS system configurations.

- OVS configuration

  ```
  ovs-vsctlshow
  ovs-vsctlfind Interface
  ```

- OVS system configurations

  ```
  ifconfig -a
  netstat-nr
  uname-a
  tar czvfoperational.tgz /operational/
  tar tmp_arch.tgz /tmp/
  ```

Packet capture on AP using WOS

Use the following procedure to capture packet on AP using WOS.

1. Go to **Monitoring** > **Access Points** > ***<Access Point>*** and click **Packet Capture**.
2. Select **Capture source** as `Network`.
3. Select **Interface** as `Gig1`.
4. Specify **Capture time** and click **OK**.