Chapter 29

Instant Virtual System (IVS)

The Instant Virtual System (IVS) gives managed service providers (MSPs) the opportunity to offer cost-effective secure remote access, disaster recovery and managed extranet services to small and medium sized companies. To meet this opportunity, MSPs can deliver managed security solutions from equipment that is located on the subscriber company's premises (Customer Premises Edge router-based) or within the MSP network (Carrier Edge router-based or network-based). Network-based managed security solutions centralize the security gateway equipment in the MSP network. A virtualized IVE allows the MSP to provide managed, network-based SSL VPN services to multiple customers from the same equipment. The basic business model might work something like this:

- The MSP manages the SSL VPN equipment at the MSP site.
- Small and medium-sized companies subscribe to monthly services from the MSP.
- The MSP is responsible for the management of the equipment, but delegates portal administration to an IVS administrator designated by each subscriber company.
- The virtual system supports and enforces an architectural and administrative separation between subscriber companies, providing a completely secure and individualized view for each subscriber.

This system provides a number of benefits to service providers:

- **Expand market share—**The ability to provide secure SSL VPN capabilities to as many as 255 subscriber companies from one IVE offers the MSP economies of scale and the opportunity to expand market share with services targeting small and medium sized businesses.
- **Simplify administration—**Each subscriber administrator can manage their company's IVS instance with no visibility into another subscriber company's administrative interface. The MSP root administrator can manage all hosted companies and can easily monitor or configure hosted company systems.
- **Enhance subscriber security—**Each subscriber company maintains complete separation from other subscriber companies. As far as the subscriber administrator or subscriber users are concerned, they are operating on a completely independent and protected SSL VPN system.

- **Optimize traffic management—**Traffic from end-users or corporate intranet servers stays within each company's VLAN. Subscriber end-users never see services located on another subscriber's intranet.

See the following topics for more information:

- "Licensing: IVS availability" on page 744
- "Virtualized IVE architecture" on page 746
- "Clustering a virtualized IVE" on page 770
- "IVS use cases" on page 785

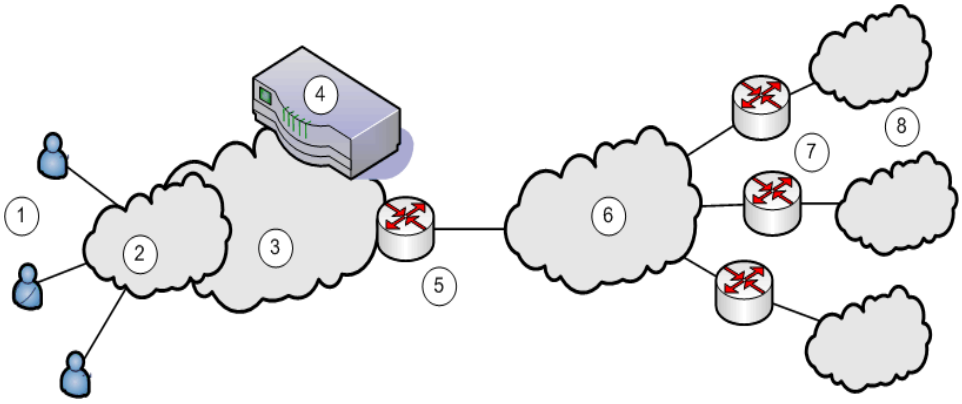
Licensing: IVS availability

- You must have an IVS license to create IVS systems. (Note that IVS licenses are not available for SA 700 appliances.)
- You must have both an IVS license and a Network Connect license to provide centralized DHCP support to your subscribers.

Deploying an IVS

For each subscriber company, the virtualized IVE provides a secure portal for the company's end-users (mobile employees, customers, or partners) to access its internal resources. Authentication servers that reside either on the subscriber's premises or in the MSP network, authenticate end-users who sign in to the IVS. Once authenticated, end-users establish secure sessions through the IVS to their respective company's back-end servers.

Figure 57: MSP deployment scenario



The following numbered list items correspond to the labeled objects in Figure 57

1. End-users sign in to different subscriber company intranets on specified IP addresses.

2. End-users sign-in over an Internet connection using a standard SSL-enabled Web browser.

3. All traffic is directed into the Managed Service Provider's (MSP) network. The MSP is the customer who holds the license to the virtualized IVE hardware and software.

4. All traffic is directed to the virtualized IVE. Each message is evaluated based on its sign-in IP address and, by the virtualized IVE, is assigned a VLAN tag containing a VLAN ID that corresponds to a subscriber company. The IVE supports up to 250 IVS systems, each one representing a single subscriber company IVE. The subscriber is any company that subscribes to hosted SSL VPN services from the MSP.

5. The MSP carrier-edge (CE) router or other Layer 2 device acts as a VLAN termination point, and routes traffic over a secure tunnel to a customer premises edge (CPE) router. Based on the VLAN ID, the router directs the traffic to the appropriate subscriber intranet. During this part of the process, the CE router removes the VLAN tag containing the VLAN ID, as once the message is correctly destined for the appropriate intranet, the ID and tag are no longer needed. The term subscriber intranet is interchangeable with the term company intranet.

6. The CE router routes messages over the service provider backbone to the appropriate customers' premises edge routers through encrypted tunnels, such as IPSec, GRE, PPP, and MPLS tunnels. Untagged traffic is sent over these tunnels to the customer intranet.

7. The CPE routers within the customer intranet on the customer premises can act as a VLAN termination point and routes traffic from the secure tunnel connected to the CE Router, to the customer intranet.

8. The end-user traffic reaches the correct subscriber company's backend resources. The IVE processes any return messages to the end-users from the subscriber intranets following a similar set of steps.

In a typical MSP deployment, firewalls are present in front of the IVE in the MSP's DMZ, behind the IVE, in the MSP network or in the customer's intranet DMZ, or both. Note that a virtualized firewall could potentially exist behind the IVE (a Vsys cluster, for example), in which case it should have the ability to accept VLAN tagged traffic from the IVE and forward it to the proper customer VLAN (and vice versa). Also, most, if not all deployments have Domain Name Server (DNS) or Application servers located either in the MSP network or on the customer intranet.

In a virtualized IVE deployment, the front-end is considered the external interface and is the end-user or Internet-facing interface. The back-end is considered the internal interface and is the subscriber company intranet-facing interface.

The IVE tags *inbound traffic* sent by end-users and destined for a server in the subscriber intranet or MSP network, with VLAN tags containing the VLAN ID. Inbound traffic can arrive over the IVE appliance's internal interface or external interface.

Outbound traffic, which is traffic transmitted over the IVE backend and destined for servers located on MSP network or subscriber intranet, can be sourced by the IVE itself. For example, traffic destined for authentication, DNS, or application servers, is outbound traffic, as is traffic forwarded by the IVE, such as Network Connect traffic.

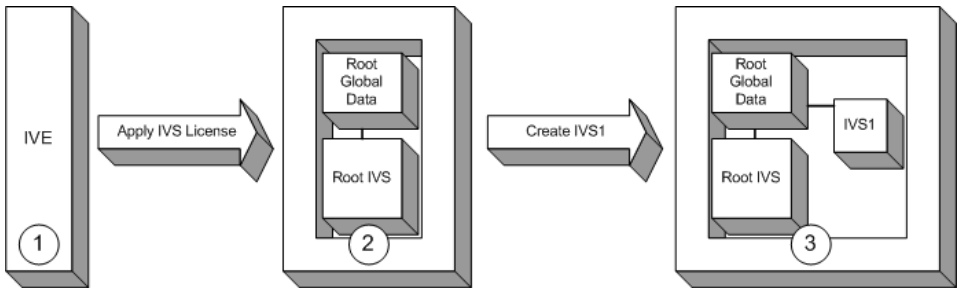
If the traffic arrives as inbound traffic to an IP address that has been designated for an IVS system that uses a VLAN, that traffic is tagged with the VLAN tag on arrival. When it has been identified and directed to the proper backend destination, the VLAN termination device strips the VLAN tag from the Ethernet frame and forwards the traffic to the backend destination.

Virtualized IVE *architecture*

The virtualized IVE framework consists of a root system and any subscriber IVS systems the MSP root administrator creates subsequently. Subscriber IVS administrators can only manage resources on their particular IVS system. The root administrator can manage resources on all IVS systems on the appliance.

The IVS license converts the IVE system to a root system that is functionally identical to the IVE, with the added capability of provisioning virtual systems. The root system consists of system-level global data and a single default root IVS, which encompasses the access management subsystem.

Figure 58: IVS architecture



The root administrator (root administrator) is the super-administrator of the root system. Often, the root administrator is the same thing as the IVE administrator. The root administrator has administrative control over the root system and all subscriber IVS systems. The root administrator can provision IVS systems on the root system, create IVS administrators, edit IVS configuration. The root administrator can override configuration changes made by any IVS administrator.

NOTE: The instructions for configuring the root and IVS systems are meant to be read by a root administrator. The pronoun *you*, in these sections, denotes the **root administrator**. If a task can be performed by someone in a role other than the root administrator, the text makes a distinct reference to the role in the task description.

As shown in Figure 58:

1. The IVE administrator applies an IVS license to an IVE appliance containing a Secure Access license.

2. The resulting system contains the root global data and a root IVS, in effect, a virtualized IVE.

3. From the root IVS, the root administrator can create multiple subscriber IVS systems, each IVS completely separate from any other IVS.

The root system contains a superset of all capabilities of the system. You, as the root administrator, define all global network settings and root administrator settings on the root system. For each subscriber, you provision one or more IVS systems and manage them from the root system.

The subscriber IVS contains a unique instance of the access management framework. When you create an IVS for each subscriber company, you also create an IVS administrator (IVS administrator) account. The IVS administrator has complete administrative control over the IVS. The IVS administrator uses an administrative admin console that contains a subset of the root administrator capabilities.

Signing in to the root system or the IVS

You can configure sign-in URLs using different methods:

- Sign-in URL prefix per IVS
- Virtual ports
- VLAN ports

You can use both of these methods on the same IVS.

Signing-in using the sign-in URL prefix

This feature enables end-users to access an IVS by way of a single hostname and and IVS-specific sign-in URL prefix. By using this method, administrators can ensure that users can access multiple IVS systems by way of a single IP address on the IVE.

Additionally, the use of path-based URLs results in:

- **Savings in certificate costs**—You need only supply one device certificate.
- **Fewer DNS entries**—You need only one DNS entry across all IVS systems hosted on a single IVE.

Administrators and end-users can sign into an IVS system using sign-in URLs similar to the following (assuming the managed service provider URL is www.msp.com):

- Company A sign-in URL: www.msp.com/companyA
- Company B sign-in URL: www.msp.com/companyB
- Company A IVS administrator sign-in URL: www.msp.com/companyA/admin
- Company B IVS administrator sign-in URL: www.msp.com/companyB/admin

You can continue to restrict access by implementing additional sign-in URLs that are segregated by certain criteria, as follows:

- www.msp.com/companyA/sales
- www.msp.com/companyA/finance
- www.msp.com/companyA/hr

If you do not specify a URL prefix, the IVE defaults to sign-in over virtual ports. If you do specify a path-based sign-in URL prefix, the following rules apply:

- You cannot specify a multilevel path for the URL prefix, by using the / character.
- End-users can sign in to an IVS on the internal port, external port, VLAN interface, or virtual port that has not already been assigned to an IVS using the selected URL prefix, in other words, where the hostname is the DNS name assigned to one of the interface IP addresses.

For example, assume that your IVE ports are assigned to specific DNS names, as follows:

- Internal Port = MSP-internal
- External Port = MSP-external
- VLAN Port 10 = MSP-vlan10
- Virtual Port X = MSP-virtualx

Now, consider that VLAN Port 10 and Virtual Port X are not assigned to an IVS. If you host the Company A IVS, and the Company A sign-in URL prefix is specified as companyA in the IVS profile, then end-users can sign-in to the Company A IVS using any of the following URLs:

- MSP-internal/companyA
- MSP-external/companyA
- MSP-vlan10/companyA
- MSP-virtualx/companyA

The path-based URL feature carries a few restrictions, as follows:

- An end-user or administrator can sign into only one IVS from a given browser instance. If you attempt to sign in to another IVS from a new browser window of the same browser instance, your sign in attempt is rejected. You must create a new browser instance to sign in to multiple IVS systems.
- You cannot establish multiple concurrent sessions, with all sessions using Host Checker, from the same end-point to different IVE systems. You cannot establish multiple concurrent sessions from the same end-point to multiple IVS systems, regardless of the sign-in method.

- If you configure an IVS with a path-based sign-in URL prefix, you cannot use the persistent session cookie (DSID) and maintain the ability to sign in to multiple IVS systems from the same browser using the URL prefix. The limitation does not apply to users signing in to the IVS with a sign-in IP address, because the system creates a different DSID per target IVS in that case.

- Pass-through proxy based on port numbers is supported. However, you cannot specify a pass-through proxy policy when using virtual hosts, unless the virtual host DNS entry maps to the IVS sign-in IP address. If the virtual host DNS entry points to the IVE, when the user signs in he will sign-in to the root IVS sign-in page.

- When using Secure Meeting, if a user is not already signed in to their IVS and you have enabled the option **require IVE users**, all meeting invitation emails will contain a link to the root IVS sign-in page.

- If an IVS user bookmarks pages while using web rewriting, signs out, then reopens the browser and selects the bookmark, he will display the root IVS sign-in page.

Signing-in over virtual ports

You may have reasons for configuring virtual ports for sign in. Virtual ports provide significant segregation of traffic. If you choose to use virtual ports, keep in mind that:

- **Must provide multiple certificates**—You need to supply one device certificate per virtual port address.

- **Must configure multiple DNS entries**—You need to supply DNS entries for each IVS system hosted on a single IVE.

The sign-in request's target IP address drives the sign-in to the root system or IVS. To sign in to the root system or an IVS, users browse to a hostname-based URL. You map the URL, by way of external DNS, to the IP address or to an IP alias of the IVE system's external interface.

For example, consider an MSP with host name msp.com, that provides SSL VPN gateway services to two subscribers: s1 and s2.

- Root administrator sign-in URL: http://www.msp.com

- S1 sign-in URL: http://www.s1.com

- S2 sign-in URL: http://www.s2.com

External DNS must map these URLs to unique IP addresses, which must correspond to IP addresses or aliases hosted on the IVE, typically a virtual port defined on either the internal or external port.

To summarize signing-in, IVS users can sign in on:

- A virtual port configured on the external interface of the IVE.

- A virtual port configured on the internal interface of the IVE (untagged).

- A VLAN interface configured on the internal interface (tagged).

Root system users can also sign in directly over the internal or external interface. For more information about signing in, see “Configuring sign-in policies” on page 183 and “Configuring sign-in pages” on page 187.

Signing-in over a VLAN interface

In addition to the sign-in capabilities provided over the external interface (or the internal interface, if configured) by the root administrator, end-users can sign in over any VLAN interface the root administrator assigns to their IVS. In other words, the IVS administrator can provide the VLAN port IP address to end-users for sign-in.

NOTE: You cannot map an explicit device certificate to any IP addresses mapped to a VLAN. When signing in over a VLAN interface, the system chooses the device certificate that is already assigned to the IVS. If there is no certificate associated with the IVS, the system assigns the certificate from the top of the IVE device certificate list. This list can be re-ordered when a certificate is added or removed, which can result in an unpredictable certificate during configuration. Once an IVS is in a production state, this should not present a problem, as the IVS VIP is mapped to a specific certificate.

Navigating to the IVS

Only root administrators can navigate to an IVS from the root system. On the virtualized IVE, the admin console navigation for the root system includes an additional drop-down menu listing the configured IVS systems, on all page headers. You can navigate to an IVS and administer it by selecting an IVS from the drop-down menu. IVS administrators must sign-in directly to the IVS through a standard administrative sign-in page.

The root administrator creates the initial IVS administrator account. An IVS administrator can create additional IVS administrator accounts, using the standard procedure for creating administrator accounts, as described in “Creating and configuring administrator roles” on page 728.

Determining the subscriber profile

In order to configure the system to properly steer inbound traffic to the correct subscriber IVS, and outbound traffic to the correct VLAN, the MSP root administrator needs to compile a profile for each subscriber company.

IVS Configuration Worksheet

When creating a new virtual system, you must create a number of other system objects, and specify several pieces of data, including IP addresses, VLAN IDs, virtual ports, and DNS settings. You can use this worksheet to plan and keep track of the system data while creating each IVS. The worksheet presents data in the general order in which you should define the IVS.

Depending on the specific topology of the subscribers' networks, you may need to collect additional information, or may not use all of the information listed on the form.

Date:		Created by:	
Subscriber:			
Account #:			
Comment:			
Subscriber VLAN (System > Network > VLANs)			
VLAN Settings			
	VLAN Port Name:		
	VLAN ID (1-4095):		
VLAN Port Information			
	IP Address:		
	Netmask:		
	Default Gateway:		
Subscriber Sign-in Virtual Port Configuration (System > Network > Port 1 > Virtual Ports > New Virtual Port)			
	External Virtual Port Name (for sign-in):		
	IP Address:		
	Internal Virtual Port Name (optional):		
	IP Address:		
Install Device Certificate for IVS hostname			
	IVS Hostname:		
	Internal Port:		
	External Port:		
Subscriber IVS (System > Virtual Systems > New Virtual System)			
	Name (Subscriber):		
	Description:		
Administrator			
	Username:		
	Password (at least 6 characters in length):		
Properties			
	Max Concurrent Users:		
	Default VLAN:		

	Selected Virtual Ports: (Internal Interface)	
	Selected Virtual Ports: (External Interface)	
	Network Connect IP Pool:	
Static Routes (System > Network > Routes > New Routes)		
	Destination Network/IP:	
	Netmask:	
	Gateway:	
	Interface:	
	Metric:	
DNS Settings (Subscriber IVS > System > Network > Overview)		
	Hostname:	
	Primary DNS:	
	Secondary DNS:	
	DNS Domain(s):	
	WINS:	

Administering the root system

Once you apply the IVS license to the IVE, the new **Virtual Systems** tab appears in the administrator UI. After you apply the IVS license, you can see an explicit display of the root system in the drop down menu that appears in the admin console header area.

Setting up the system requires a series of basic procedures. Once the hardware is connected:

1. Boot the system.

2. Apply the IVS license through the **Maintenance > System > Upgrade/Downgrade** page of the admin console.

3. Configure the root system from the admin console, as described in "Provisioning an IVS" on page 753.

Regardless of how many subscriber administrators you define on the subscriber IVS systems, you always maintain control over the entire system and have visibility into the settings on all IVS systems.

Configuring the root administrator

Configuring the root administrator is similar to the task of creating a new administrator on a standalone IVE. You can create an administrator account through the **Authentication > Auth. Servers > Administrators > Users** page of the admin console, or by using the serial console, as described in "Connecting to an IVE appliance's serial console" on page 807.

If you upgrade from an earlier IVE version to the 5.1 version software or later, the system considers any administrator in the root system who maps to the **.Administrators** role to be a root administrator for the IVE. If you re-image the IVE appliance or install a brand new piece of hardware, you create a primary administrator during the initial configuration steps, in the serial console. For more information about setting up the system from the serial console, see "Connecting to an IVE appliance's serial console" on page 807.

Provisioning an IVS

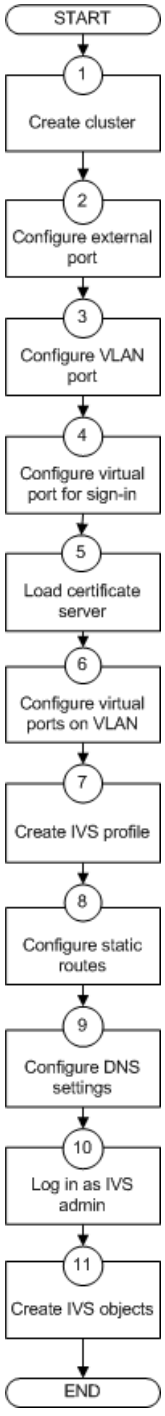
This section describes the tasks involved in provisioning an IVS, including:

- "Understanding the provisioning process" on page 754
- "Configuring sign-in ports" on page 757
- "Configuring a Virtual Local Area Network (VLAN)" on page 759
- "Loading the certificates server" on page 762
- "Creating a virtual system (IVS profile)" on page 763
- "Configuring role-based source IP aliasing" on page 766
- "Configuring policy routing rules on the IVS" on page 768
- "Clustering a virtualized IVE" on page 770
- "Configuring DNS for the IVS" on page 771
- "Configuring Network Connect for use on a virtualized IVE" on page 773
- "Configuring authentication servers" on page 778
- "Accessing standalone installers" on page 781
- "Performing export and import of IVS configuration files" on page 781
- "Monitoring subscribers" on page 783
- "Troubleshooting VLANs" on page 784

Understanding the provisioning process

Figure 59 illustrates the basic tasks required to provision an IVS.

Figure 59: Basic process of provisioning an IVS



Provisioning an IVS consists of the following steps, as illustrated in Figure 59:

1. Configure one or more clusters, if needed, through the **System > Clustering > Create Cluster** page.
2. Configure and enable external port. The external port is in a disabled state, by default. You must enable the port and configure it, to provide sign-in capabilities from outside the network.
3. Create at least one VLAN port for each subscriber company. You must define a unique ID for each VLAN. A subscriber company can have multiple VLANs on the IVE.
4. Configure at least one virtual port on the external port to enable end-users to sign in. You can also configure virtual ports on the internal port, for signing in from behind the firewall, if needed.
5. Load one certificate server per subscriber company.
6. If you intend to use virtual ports, for example, to support IP sourcing, create them at this point in the process.
7. Create an IVS profile for each subscriber company. The IVS profile establishes the connection between the company, the VLAN, and the available virtual ports.
8. Configure static routes to backend servers. If you intend to provide shared access to resources on the MSP network, you add static routes to the VLAN route tables that point to those resources.
9. Configure DNS settings, so that any traffic destined for resources on the MSP network first goes through the MSP's DNS server.
10. Log in as the IVS administrator.
11. Configure users, roles, realms, and resource policies for the IVS.

When you create the IVS, the IVS name appears in the drop down menu located in the header of the admin console. You can perform operations on each IVS by selecting the IVS name in the drop down menu and clicking the **Go** button.

Task Summary: Provisioning an IVS

To provision an IVS system, you must:

1. Create a cluster, if necessary. For instructions, see "Clustering" on page 699.
2. Configure an external port, which consists of enabling the port and configuring virtual ports to allow end-users to sign-in from outside the MSP network. For instructions, see "Configuring sign-in ports" on page 757.
3. Configure a VLAN, which includes defining the VLAN port and specifying a VLAN ID. For instructions, see "Configuring a Virtual Local Area Network (VLAN)" on page 759.

4. Load the certificates server, which allows the MSP and subscriber companies to certify traffic. For instructions, see “Loading the certificates server” on page 762.

5. Configure virtual ports on the VLAN for IP sourcing or for clustering. For instructions, see “Configuring a virtual port for sign-in on the internal port” on page 758.

6. Create the IVS profile, which defines the subscriber company’s environment on the virtualized IVE. For instructions, see “Creating a new IVS profile” on page 763.

7. Configure static routes to support backend servers, Network Connect users, and to provide shared services on the MSP network. For instructions, see “Adding static routes to the VLAN route table” on page 761.

8. Configure DNS settings, to force traffic to go through the MSP DNS server. If you are running Network Connect, you must configure DNS. For instructions, see “Configuring DNS for the IVS” on page 771.

9. Configure Network Connect, if necessary. For instructions, see “Configuring Network Connect for use on a virtualized IVE” on page 773.

Configuring sign-in ports

You must configure virtual ports by which end-users can sign in to the subscriber company intranet. A virtual port activates an IP alias on a physical port and shares all of the network settings of that port. For more information about virtual ports in general, see “Configuring virtual ports” on page 562.

This section contains the following topics:

- “Configuring the external port” on page 757
- “Configuring a virtual port for sign-in on the external port” on page 758
- “Configuring a virtual port for sign-in on the internal port” on page 758

Configuring the external port

You need to enable and configure the external port to allow IVS end-users to sign in from outside the network.

To enable and configure the external port:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than Root, select Root from the menu and click **Go**.

2. Select **System > Network > Port 1 > Settings**.

3. Select **Enabled**.

4. Enter a valid IP address for the external port.
5. Enter a valid netmask for the IP address.
6. Enter the default gateway address.
7. Click **Save Changes**.

The system enables the port.

Configuring a virtual port for sign-in on the external port

You need to configure a virtual port to enable IVS end-users to sign-in from outside the network over the external port. For example, if users sign in over the Internet, they use the virtual port defined on the external port.

To configure the virtual port for sign-in:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than Root, select Root from the menu and click **Go**.
2. Select **System > Network > Port 1 > Virtual Ports**.
3. Click **New Port**.
4. Enter a unique name for the virtual port.
5. Enter a valid IP address, provisioned by the subscriber company's network administrator.
6. Click **Save Changes**.

The system adds the port, displays the **Virtual Ports** tab, and restarts the network services. This virtual port is available for use during the process described in "Creating a virtual system (IVS profile)" on page 763. Define as many virtual ports as needed for sign-in.

Configuring a virtual port for sign-in on the internal port

You need to enable and configure the internal port to allow IVS end-users to sign in from inside the network.

To configure the virtual port for sign-in:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than Root, select Root from the menu and click **Go**.
2. Select **System > Network > Internal Port > Virtual Ports**.
3. Click **New Port**.
4. Enter a unique name for the virtual port.

5. Enter a valid IP address, provisioned by the subscriber company's network administrator.

6. Click **Save Changes**.

The system adds the port, displays the **Virtual Ports** tab, and restarts the network services. You can assign this virtual port to an IVS profile as described in "Creating a virtual system (IVS profile)" on page 763. Define as many virtual ports as needed for sign-in.

Task Summary: Configuring IVS sign-in ports

To configure IVS sign-in ports, you must:

1. Configure the external port. For instructions, see "Configuring the external port" on page 757.

2. Configure a virtual port for sign-in on the external port. For instructions, see "Configuring a virtual port for sign-in on the external port" on page 758.

3. Configure a virtual port for sign-in on the internal port (optional). For instructions, see "Configuring a virtual port for sign-in on the internal port" on page 758.

Configuring a Virtual Local Area Network (VLAN)

By defining at least one Virtual Local Area Network (VLAN) on each subscriber IVS, the MSP can take advantage of VLAN tagging, by which the virtualized IVE tags traffic with 802.1Q VLAN IDs before transmitting the traffic over the backend. The carrier infrastructure uses the VLAN tag to direct the packets to the appropriate subscriber intranet.

VLAN tagging provides separation of the traffic the IVE transmits over the backend, destined for subscriber intranets. Traffic coming in over the front-end—that is, inbound traffic—does not have VLAN tags. The IVS adds the tag to a message upon its arrival over one of the IVE ports.

Each VLAN is assigned a VLAN ID which is part of an IEEE 802.1Q-compliant tag that is added to each outgoing Ethernet frame. The *VLAN ID* uniquely identifies each subscriber and all subscriber traffic. This tagging allows the system to direct all traffic to the appropriate VLAN and to apply respective policies to that traffic.

The *VLAN termination point* is any device on which VLAN-tagged traffic is identified, stripped of the VLAN tag, and forwarded to the appropriate tunnel to the backend. The VLAN termination point can be a CE router, CPE router, L2 switch, firewall, or other device capable of VLAN routing.

You must define a VLAN port for each VLAN. The root administrator assigns the specific VLAN ID when defining the VLAN port.

For each VLAN you configure, the virtualized IVE provisions a unique, logical VLAN interface, or port, on the internal interface. There is no relationship between the internal port IP address and any VLAN port IP address. Each VLAN port has its own route table.

Each VLAN port definition consists of:

- **Port Name.** Must be unique across all VLAN ports that you define on the virtualized IVE or cluster.
- **VLAN ID.** An integer in the range from 1 to 4095 that uniquely identifies the subscriber/customer VLAN.
- **IP Address/Netmask.** Must be an IP address or netmask from the same network as the VLAN termination point, because the virtualized IVE connects to the VLAN termination point on a Layer 2 network connection. VLAN IP addresses must be unique. You cannot configure a VLAN to have the same network as the internal port. For example, if the internal port is 10.64.4.30/16 and you configure a VLAN as 10.64.3.30/16, you may get unpredictable results and errors.
- **Default gateway.** The IP address of the default router, typically the CE or CPE router. The default gateway could act as the VLAN termination point, or could reside behind the VLAN termination point.
- **Other network settings.** Inherited from the internal port.

NOTE: If you do not specify a VLAN for the subscriber company, you must configure the IVS to transmit traffic over the internal interface by selecting it as the default VLAN.

Configuring VLANs on the virtualized IVE

The relationship between a VLAN and a given IVS allows the root system to separate and direct traffic to different subscribers, as described in "Licensing: IVS availability" on page 744. You can define multiple VLANs for a subscriber IVS.

Configuring a VLAN port

Before creating a new virtual system, create a VLAN port to identify the specific subscriber traffic.

To create a VLAN port, perform the following steps:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than Root, select Root from the menu and click **Go**.
2. Select **System > Network > VLANs** to open the VLAN Network Settings tab.
3. Click **New Port**.
4. Under **VLAN settings**, enter a name for the VLAN port.

5. Enter a VLAN ID.

NOTE: The VLAN ID must be between 1 and 4095 and must be unique on the system. The root system uses untagged traffic and cannot be changed.

6. Enter the IP address for the VLAN.
7. Enter a netmask for the VLAN.
8. Enter a default gateway for the VLAN.
9. Click **Save Changes**.

Assigning a VLAN to the root IVS

In order to assign a VLAN to a role, you must assign the VLAN to the root IVS, first. If you have not assigned a VLAN to the root IVS, the VLAN is not available in the VLAN drop down menu in the **Users > User Roles >** *Select Role* **> VLAN/Source IP page**.

To assign a VLAN to the root IVS

1. Select **System > Virtual Systems > Root**.
2. Under Properties, select the VLAN from the **Available VLANs** list.
3. Click **Add ->** to move the VLAN name to the **Selected VLANs** list.
4. Click **Save Changes**.

Adding static routes to the VLAN route table

When you create a new VLAN port, the system creates two static routes, by default:

- The default route for the VLAN, pointing to the default gateway.
- The interface route to the directly connected network.

In addition, you can static routes to shared servers in the MSP network.

To add static routes to a VLAN route table:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than Root, select Root from the menu and click **Go**.
2. Select **System > Network > VLANs**.
3. Either click **New Port** or select an existing VLAN for which to add a static route.
4. At the bottom of the VLAN port page, click the **Static Routes** link.
5. From the drop-down menu, select the VLAN for which to create static routes, if not already selected.

6. Click **New Route**.
7. On the **New Route** page, enter the destination network/IP address.
8. Enter the destination netmask.
9. Enter the destination gateway.
10. Select the interface from the **Interface** drop down menu.
11. Enter the metric.

    The metric is a number between 0 and 15, and usually signifies the number of hops that traffic can make between hosts. You can set the metric of each route to specify precedence. The lower the number, the higher the precedence. Therefore, the device chooses a route with a metric of 1 over a route with a metric of 2. A router that uses metrics compares a dynamic route metric with the static route metric and chooses the route with the lowest metric.

12. If you want to add static routes to shared services, for example, you should perform one of the following steps:

    - Click **Add to** *[VLAN]* **route table**, where *[VLAN]* is the name of an available VLAN, to add the route to a selected VLAN. This action adds the static route to a particular subscriber company's VLAN route table and excludes access from all other VLANs, including from users of the MSP network.
    - Click **Add to all VLAN route tables** to add the route to all VLANs defined on the system. For example, if the root administrator wants to share some service among all end-users of all subscriber company's, select this option.

NOTE: You can also use static routes if you want to configure shared services on the MSP network. To accomplish this:

1. Add a static route to the shared resource in either your own VLAN route table, if the root system has a VLAN, or in the main IVE route table, if the root system uses the internal interface.
2. Click **Add to all VLAN route tables**, which populates all VLAN route tables with the static route. When you add the static route to all VLAN route tables, all IVS profiles can access the shared services.

Deleting a VLAN

You cannot delete a VLAN that is associated with an IVS. First, you must either delete the IVS or remove the relationship between the IVS and the VLAN port.

To delete a VLAN:

1. Select **System > Network > VLANs**.
2. Select the checkbox next to the name of the VLAN to delete.
3. Click **Delete**.

Loading the certificates server

On the root system, you can load certificates using the procedure described in “Importing certificates into the IVE” on page 595.

You must associate the virtual ports that you have defined as sign-in ports for IVS end-users with the device certificate. You can specify virtual ports on the **Certificate Details** page, as described in “Associating a certificate with a virtual port” on page 600.

On an IVS, you can only import Trusted Client CAs and Trusted Server CAs, as described in “Using trusted client CAs” on page 601 and in “Using trusted server CAs” on page 614.

NOTE: You cannot share certificates across IVS systems. You must have a unique IP and certificate for each IVS.

You can only configure the root IVS to re-sign IVE applets/controls in the admin console. The admin consoles for subscriber IVS systems do not show the re-signing option. You should take note of the following information:

- All root and subscriber end-users see the same applets/controls: either all of the default Juniper controls, or all of the controls signed by the root IVS.
- If you do not want subscriber IVS systems to see controls signed by the certificate from the root IVS, then you should not re-sign the controls. If you re-sign the controls, the subscriber IVS systems have access to them.

Creating a virtual system (IVS profile)

After creating a VLAN port, proceed with the task of creating the new virtual system (IVS profile) for the subscriber company.

This section contains the following topics:

- “Creating a new IVS profile” on page 763
- “To define the IVS profile:” on page 763
- “To define sign-in properties, VLAN, and port settings:” on page 764

Creating a new IVS profile

The IVS profile defines the subscriber IVS and any elements required to reach the subscriber’s intranet, such as DNS settings and authentication servers. You must specify a *default VLAN* for each IVS. The significance of the default VLAN for a given IVS is that when an end-user attempts to sign into a particular realm within that IVS, the IVS sends traffic to the authentication server for that realm over the default VLAN interface.

To define the IVS profile:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than **Root**, select **Root** from the menu and click **Go**.
2. Select **System > Virtual Systems**.
3. Click **New Virtual System** to display the **IVS - Instant Virtual System** page.
4. Enter the name of the subscriber company.
5. Enter a description (optional).
6. Select **Enabled**, if it is not already selected.

NOTE: If you ever need to prohibit a subscriber and the subscriber's end-users from accessing the IVS due to billing or other problems, disable their account here. By disabling the account, you can resolve any customer issues and then enable access without having to delete the subscriber account and lose all the configuration data.

7. Under **Administrator**, create a username for the IVS administrator.
8. Create a password for the IVS administrator.

NOTE: The IVS administrator username and password are available in the IVS profile the first time you create the IVS. Subsequently, if you edit the IVS, these fields are not available, for security purposes. However, if you need to access the IVS administrator username and password, you can do so through the IVS configuration page, by going to the Administrators authentication server.

9. Specify the sign-in properties, VLAN, and port settings for the IVS.

To define sign-in properties, VLAN, and port settings:

1. Enter the maximum number of concurrent end-users allowed on the IVS.

NOTE: The number of concurrent end-users must be fewer than the number of assigned users on the entire system.

2. Select a VLAN from the **Available** list box and click **Add ->** to move the name of the VLAN to the **Selected VLANs** list box. You can add multiple VLANs to an IVS. You can select the internal port as a VLAN even if you have added other VLANs to the Selected VLANs list. Unlike other VLAN interfaces, you can add the internal port to multiple IVS profiles. If you have not defined a VLAN, you must select the internal interface instead.

3. To specify the default VLAN for the IVS, select the VLAN name in the **Selected VLANs** list box, then click **Set Default VLAN**. The IVS marks the VLAN name with an asterisk (*). The virtualized IVE uses the default VLAN to provide authentication server access. The IVE consults the default VLAN's route table to look up the route to authentication servers for a given IVS.

NOTE: You must specify the internal port as the default VLAN for the root IVS.

4. If you want to define a sign-in URL prefix that your end-users can sign in over rather than over a virtual port, add the prefix to the **Sign-in URL Prefix** field. The prefix is the equivalent of the first node in the URL, for example, companyA in the following URL:

   http://www.mycompany.com/companyA

   For more information about using the prefix, see "Signing-in using the sign-in URL prefix" on page 747.

5. If you have defined virtual ports for either the internal interface or the external interface, you can select them in the **Available** list boxes and click **Add ->** to move them to the **Selected Virtual Ports** list boxes for the respective interfaces. For more information about virtual ports, see "Configuring virtual ports" on page 562.

6. Enter the address or range of IP addresses that are available for Network Connect clients (end-users). If you intend to configure a DNS server on the IVS, for a server located on the subscriber intranet, you must add the available Network Connect IP address pool values here. For more information, refer to "Specifying IP filters" on page 542.

7. Click **Save Changes**.

For information on how to sign in to the IVS as an IVS administrator, see "Signing in directly to the IVS as an IVS administrator" on page 765.

Signing in directly to the IVS as an IVS administrator

Signing in directly to the IVS as an IVS administrator is different than picking the IVS from the virtual system drop down menu in the Web-based administrator UI console. If you, as the root administrator, want to sign in the same way that all IVS administrators must sign in to the IVS, perform the following steps:

1. Sign-out of the root IVE.

2. Enter the sign-in URL in the address bar of a valid browser, using either the hostname or the IP address. For example:

   https://www.company.com/admin

   or

https://10.9.0.1/admin

This example assumes that you assigned the IP address 10.9.0.1 as a virtual port for sign-in. The format depends on whether or not you defined a DNS entry for the sign-in host name. When logging in, the administrator can enter the host name or the IP address defined as the virtual port for sign-in. If the administrator signs in from within the network, he should use the IP address you configured for signing in over the internal port. If the administrator signs in from outside the network, he should use the IP address you configured for signing in over the external port.

3. Press **Enter**.
4. Enter the IVS administrator username.
5. Enter the IVS password.
6. Click the **Sign in** button.

Assuming the credentials are valid, the **System Status** page for the IVS appears.

When either the root or an IVS administrator exits the IVS, the appliance immediately severs the connection.

Configuring role-based source IP aliasing

If the subscriber company employs policy evaluation devices/firewalls in their network for the purpose of separating traffic based on the source IP address as it enters the intranet from the IVS, you, the root administrator, must configure the IVS to generate traffic with different source IP addresses. The role-based source IP aliasing feature, also known as VIP sourcing, provides the capability to map end-user roles to VLANs and specific source IP addresses (the IP address of any one of the virtual ports hosted on the VLAN interface). All traffic generated by the IVS over the back-end on behalf of the end-user carries the source IP address configured for the end-user's role.

For example, assume that the traffic to a particular subscriber intranet needs to be differentiated based on whether it originates from customers, partners, or employees. There are two ways to accomplish this:

- Provision three different VLANs for the subscriber, create three roles corresponding to customers, partners and employees, and map each role to a different VLAN.
- Provision a single VLAN for the subscriber, configure three virtual ports with unique IP addresses, and map customers, partners and employee roles to the same VLAN but to different source IP addresses.

This section contains the following topics:

- "Associating roles with VLANs and the source IP address" on page 766
- "Configuring virtual ports for a VLAN" on page 767

Associating roles with VLANs and the source IP address

You can use role-based source IP aliasing whether or not you have defined a VLAN. In the case of a non-VLAN configuration, you define a virtual port, then assign that port to a role's source IP. For more information, see "Configuring virtual ports" on page 562.

When using a VLAN, you can set the source IP address of a role to either the VLAN port IP address or to an IP alias configured on a VLAN port.

Configuring virtual ports for a VLAN

To configure virtual ports for a VLAN, perform the following steps:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than Root, select Root from the menu and click **Go**.
2. Select **System > Network > VLANs**.
3. Click on the VLAN name of the VLAN to which to add virtual ports.
4. Select the **Virtual Ports** tab.
5. Click **New Port**.
6. Enter a name for the new virtual port.
7. Enter a valid IP address.

   If defining the port to provide subnetting and traffic separation capabilities to the subscriber, you need to get the IP address from the subscriber. You define the virtual port with the IP address that the subscriber's policy evaluation devices validate in order to separate traffic to different locations on the subscriber intranet. You can specify any the virtual port IP as any IP from a VLAN defined on the IVS.
8. Click **Save Changes**.

   The virtualized IVE restarts certain services on the appliance.

The IVS administrator can then create users and assign them to roles which are associated with the source IP addresses you have defined.

Associating roles with source IP addresses in an IVS

Assuming that the root administrator has already configured a VLAN, virtual ports for the VLAN, and the IVS, the IVS administrator can associate roles with the virtual ports as follows:

1. Log in to the IVS as the IVS administrator.
2. Choose **Users > User Roles**.
3. Click **New Role**.

4. Name the role.
5. Select the **Source IP** checkbox.
6. Select any other options and the features you want a user with this role to be able to access (Optional).
7. Click **Save Changes**.

   The page refreshes and a set of tabs now appears.
8. Select the **VLAN/Source IP** tab.
9. Select the VLAN, if the root administrator has defined more than one VLAN for this IVS.
10. Select the source IP from the **Select Source IP** drop down menu.
11. Click Save Changes.
12. Repeat the process for each new role.

When creating new users, the IVS administrator can then assign each user to one of the roles, which determines what source IP address each user can access.

Configuring policy routing rules on the IVS

The virtualized IVE uses a policy routing framework that depends on rules, route tables, and route entries that are configured on the system.

When you create a VLAN, the system provisions a new route table for that VLAN. VLAN route tables exist in addition to the main route table for the IVE. Only the root administrator can manage VLAN route tables. IVS administrators cannot view or access the route tables.

Each VLAN route table contains the following route entries:

- Automatically-created route entries
- Manually-created route entries

Automatically-created route entries

- **Default route 0.0.0.0**. Points to the default gateway you have configured for the VLAN interface. The IVE creates this route internally when it creates the VLAN interface. End-users can reach most of their company's resources through the default route.
- **Interface route**. Network route corresponding to the VLAN interface IP address.

Manually-created route entries

- Static routes to servers within the same VLAN that are accessible through routers other than the default gateway.

- Static routes to server IP addresses on other VLAN ports within the same subscriber company intranet, or VLAN ports within the MSP network. For example, you might define in a VLAN route table static routes to DNS or authentication servers in either a subscriber company intranet or in the MSP network.
- Static routes to server IP addresses accessible through the internal interface. These are usually required if your MSP network is connected to the internal interface.

This section contains the following topics:

- "Routing Rules" on page 769
- "Overlapping IP address spaces" on page 769
- "Define Resource policies" on page 770

Routing Rules

A number of rules have been built into the system to enable the correct routing of traffic to the appropriate subscriber intranets. For example, rules exist to map:

- The Network Connect IP pool address for each Network Connect end-user session to a corresponding VLAN route table.

  To construct this rule, the system determines an end-user's role when the user establishes an Network Connect session. The system can then search the role for the associated VLAN.

- A configured source IP address to a corresponding VLAN route table.

  The system creates this rule whenever you configure a virtual port or source IP alias on a VLAN port.

NOTE:

- There are no explicit rules governing the flow of traffic between the subscriber or MSP networks and end-users. Traffic arriving at the IVE over the backend has a destination IP address set to the configured IP address of one of the network interfaces, either the external interface, VLAN interface, or a Network Connect tunnel interface. An IVE application automatically handles the processing.
- You cannot access the rules table. This section includes a description of the rules table and how rules are constructed to help you understand how the system operates.

For details about rules regarding authentication server access, see "Rules governing access to authentication servers" on page 779.

For an example of how policy routing might be applied, see "Policy routing rules resolution use case for IVS" on page 786.

Overlapping IP address spaces

The virtualized IVE supports overlapping IP addresses in subscriber intranets, and overlapping source IP addresses for Network Connect. At this time, the virtualized IVE does not support multiple VLAN interfaces with identical IP addresses.

The virtualized IVE supports overlapping IP addresses among customer networks that are tied to VLANs in different IVS systems, because IVS systems do not share route tables.

Assume that Company 1 and Company 2 both have internal networks that use IP addresses 10.64.0.0/16. Because these addresses are internal to each company's network, and because each company has a completely separate IVS, identified by a unique VLAN ID, the MSP can support them, even though, technically, they overlap.

Define Resource policies

Both you, as the root administrator, and the IVS administrator can create policies for end-users. For more information on resource policies, refer to "Resource policy components" on page 84.

You can also customize which policies are visible to IVS administrators. However, you must customize each IVS independently. Also, if you are in the root IVS context and you customize the admin console, you are only customizing the console as it appears to you or other administrators who are permitted to view the root IVS console. To customize any IVS admin console, you must be in the context of that IVS. For more information, see "Customizable admin console elements overview" on page 815

Clustering a virtualized IVE

You can cluster the entire IVE, including all IVS systems. You cannot cluster an individual IVS system. The clustering rules and conditions in a standard IVE network also apply to clusters in an IVS network, with the following exceptions:

- **Virtual port replication**—Any virtual port you define on the Active node is replicated to the Passive node. The virtual port's name and address is the same on both Active and Passive nodes.
- **Virtual port source IP**—Given an end-user who maps to a particular role, and a backend connection from any node on behalf of that end-user, the source IP of the backend connection is the same as the source IP of the virtual port configured for the end-user's role.
- **VLAN port replication**—When you create or delete a VLAN port on an Active cluster node, the IVE system automatically adds or deletes the VLAN port on the Passive node.
- **VLAN definition**—For any given VLAN port, the slot, logical name, VLAN ID, netmask, and default gateway are the same across all cluster nodes.

- **VLAN port IP address**—The IP address for each VLAN port is node-specific. Corresponding VLAN ports on an Active/Passive cluster are configured on the same IP network. You can only configure an IP address/netmask combination for a VLAN port on the standby node if the resulting network corresponds to the VLAN port in the Active cluster node. VLAN IP addresses must be unique. You cannot configure a VLAN to have the same network as the internal port. For example, if the internal port is 10.64.4.30/16 and you configure a VLAN as 10.64.3.30/16, unpredictable behavior and errors can occur.
- **Policy routing**—You can configure route settings per node and per interface, either physical or VLAN, however, those route settings are synchronized across the cluster when you edit them.
- **IVS profiles**—IVS profiles are replicated across cluster nodes, and are not partitioned across cluster nodes.
- **Network Connect**—If you deploy the virtualized IVE as an Active/Passive cluster, the Network Connect connection profile that you or an IVS administrator configures within each IVS is propagated to the standby node.
- **Network Connect in Active/Active cluster**—In an Active/Active cluster, the Network Connect IP address pool for each IVS is split across individual cluster nodes by way of role-level settings.
- **Role-based source IP aliasing**—The association of a role to a virtual port name is cluster-wide, but the association of a virtual port name to an IP address is node specific. As such, different cluster nodes can issue backend IP traffic with different source IP addresses even if the respective end-users map to the same role.
- **Failover behavior**—In the event of a failover, the VLAN interface does not disappear. Both Active and Passive nodes should contain the VLAN interface.

NOTE: When using Network Connect, you should always define virtual ports for each VLAN port you create. If you have defined a Network Connect IP address pool, and you are running in Active/Passive cluster mode, you must configure your routers to direct traffic to one of the VLAN's virtual ports as the next-hop gateway. Otherwise, Network Connect sessions may not recover gracefully from a failover.

For more information on clustering, see "Clustering" on page 699.

Configuring DNS for the IVS

This section contains the following topics:

- "Accessing a DNS server on the MSP network" on page 771
- "Accessing a DNS server on a subscriber company intranet" on page 772

Accessing a DNS server on the MSP network

In the root system, you can configure access so that any traffic destined for resources on the MSP network goes through the DNS server on the MSP network.

To access a DNS server on the MSP network:

1. In the admin console, choose **System > Network > Overview**.
2. Under DNS name resolution, provide the primary DNS address, secondary DNS address, and the DNS domains.

   When you add the DNS addresses, each one is added to the resolv.conf file on the IVE, in a nameserver directive.
3. If you are using WINS, provide the WINS server address.
4. Click **Save Changes**.
5. Follow the instructions in "Configuring the Network Connect connection profile" on page 773.

You can provide DNS services to non-Network Connect users by specifying a global DNS/WINS server in the MSP network. The global DNS/WINS server hosts DNS for all participating subscriber companies. As an alternative, you can configure a HOSTS file on the IVE with DNS entries for all participating subscriber companies.

When you configure a global DNS/WINS server in this way, it provides DNS services to any requesting entity, including from Network Connect users of participating subscriber companies that do not have DNS servers in their intranets.

Accessing a DNS server on a subscriber company intranet

In each IVS system, you can configure access so that any traffic destined for resources on the IVS subscriber's network goes through the DNS server on their internal company network.

Accessing a DNS server on a subscriber intranet

To access a DNS server on a subscriber intranet:

1. If you did not add a valid Network Connect IP address pool to the IVS profile when you created the virtual system, modify the IVS profile to include the Network Connect IP addresses. For more information, see "Provisioning an IVS" on page 753.
2. In the admin console, select the name of the subscriber IVS from the drop down menu in the console header bar.
3. Click **Go**.
4. On the subscriber IVS admin console page, choose **System > Network > Overview**.
5. Under DNS name resolution, provide the primary DNS address, secondary DNS address, and the DNS domains.

6. If you are using WINS, provide the WINS server address.
7. Click **Save Changes**.
8. Configure the Network Connect Connection Profiles as described in “Configuring the Network Connect connection profile” on page 773.

NOTE: You must perform this task for every IVS.

Configuring Network Connect Connection Profiles

To configure the Network Connect Connection Profiles:

1. Choose **Users > Resource Policies > Network Connect > Network Connect Connection Profiles**.
2. Click **New Profile**.
3. Provide a name for the **Connection Profile**.
4. In the **IP Address Pool** field, enter the range of IP addresses available for use by Network Connect users.
5. Select any other connection settings, or take the defaults.
6. Choose a role to which to apply the settings, if necessary. By default, if you do not choose a role, the policy applies to all roles.
7. Click **Save Changes**.
8. Click the **DNS** tab.
9. Select the **Use Custom Settings** checkbox.
10. Add the Primary DNS, Secondary DNS (optional), the DNS domain name, and WINS server IP addresses.
11. Select the DNS search order. When you enter custom settings for the IVS, the root system searches the subscriber DNS server first, then the MSP DNS server, by default.
12. Click **Save Changes**.

Configuring Network Connect for use on a virtualized IVE

You, as the root administrator, must work with the IVS administrator to configure Network Connect so that end-users can send traffic to the subscriber intranet and receive traffic back from the subscriber intranet.

NOTE: If you want to use Network Connect on a subscriber company's IVS (rather than just by way of Network Connect running on the MSP network) you must configure a DNS server on the IVS.

Configuring the Network Connect connection profile

Configure the Network Connect connection profile using the IP addresses from the range specified in the Network Connect IP pool in the IVS profile.

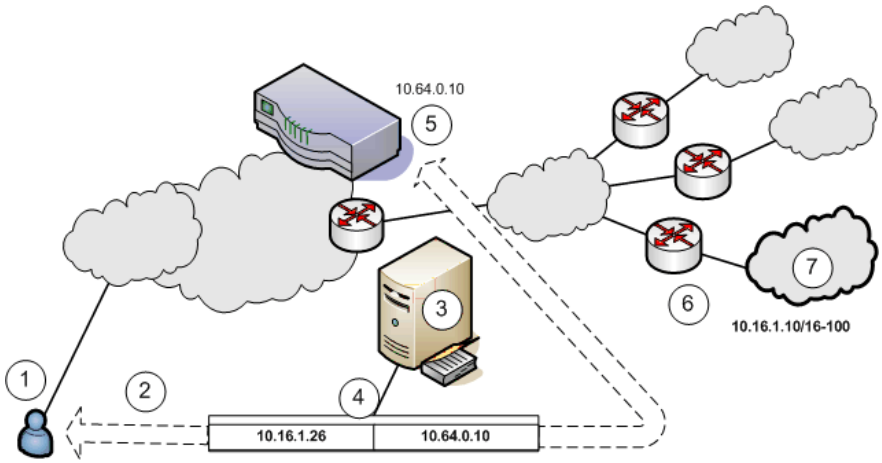
1. Select **Users > Resource Policies > Network Connect > Network Connect Connection Profiles**.
2. Click **New Profile**.
3. Enter the IP addresses in the **IP Address Pool** text box, one address per line. The Help text in the admin console shows examples of valid ranges.
4. Change the transport, encryption, and compression settings from the defaults, if necessary.
5. Add the appropriate role from the **Available roles** listbox to the **Selected roles** listbox.
6. Click **Save changes**.

Configuring Network Connect on backend routers

Both you, as the root administrator, and the IVS administrator must configure static routes on the backend to ensure that each Network Connect end-user can be reached from the subscriber intranet, and if needed, the MSP network.

If you want Network Connect users to be able to access the MSP network's DNS server, configure a static route in the route table of each application server or DNS server to the end-user's Network Connect IP pool address. Set the next-hop gateway to the IP address of the root system's internal interface. Figure 60 illustrates this operation.

Figure 60: Setting a static route in MSP network DNS or application servers



1. End-users sign in over an Internet connection, using an IP address from a Network Connect IP address pool, to reach the DNS server on the MSP network.

2. The root administrator specifies a static route in the DNS server route table to point to an IP address from the Network Connect IP address pool. The subscriber company must define the Network Connect IP address pool in its intranet.

3. The DNS server resides on the MSP network and serves all end-users of all subscriber companies.

4. The DNS server's route table contains a static route to the Network Connect IP address pool and the next-hop gateway IP address.

5. The IVE appliance's internal interface is the DNS server's next-hop gateway address.

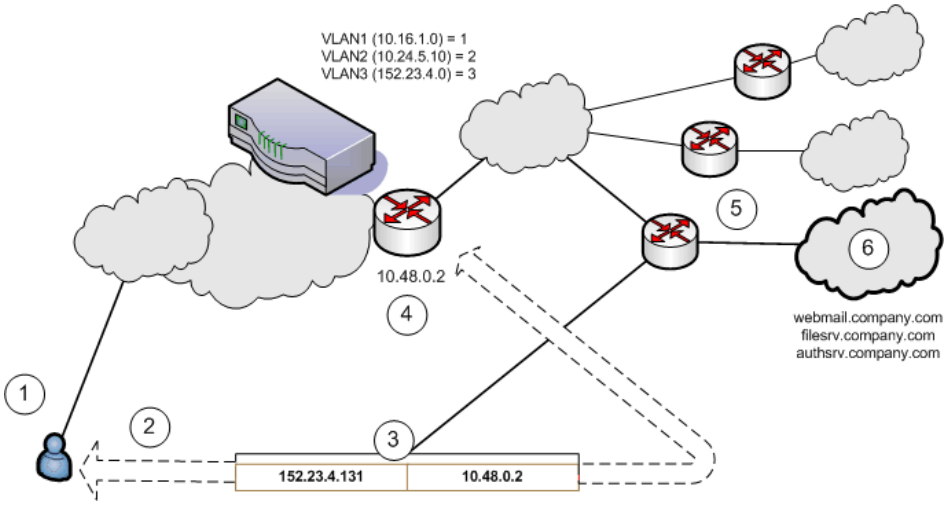
6. The subscribers' CPE routers perform the proper traffic routing to the subscriber company intranets.

7. Each subscriber company that intends its users to pass through the MSP DNS or application servers must define a corresponding Network Connect IP address pool.

As shown in Figure 61, the IVS administrator can configure the subscriber CPE router with a static route to the end-user's IP address, with the next-hop gateway set to the IP address of the corresponding CE router on the MSP network.

NOTE: Alternately, the subscriber can configure a default route on the CPE router to point to the MSP CE router as the next-hop gateway. In this case, you do not need to add individual static routes to the Network Connect IP pool addresses.

Figure 61: Setting a static route to Network Connect end-user IP address in CPE router



1. End-users sign in over an Internet connection using an IP address agreed upon by the MSP and the subscriber company.

2. Specify a static route in the subscriber company's CPE router's route table to point to the end-user sign-in IP addresses.

3. You must also specify the next-hop gateway in the CPE router's route table.

4. You use the MSP CE router's IP address as the next-hop IP in the CPE router's route table.

5. The CPE router resides on the subscriber company's intranet. Using this arrangement, each subscriber company must specify the static route to their own end-user sign-in address and must specify the MSP's CE router IP as the next-hop gateway in the CPE route table.

6. Once the MSP VLAN termination point (in this example, a CE router) determines the intended subscriber intranet, the termination point directs the traffic to the appropriate CPE router, which sends the traffic to the proper resource in the subscriber intranet.

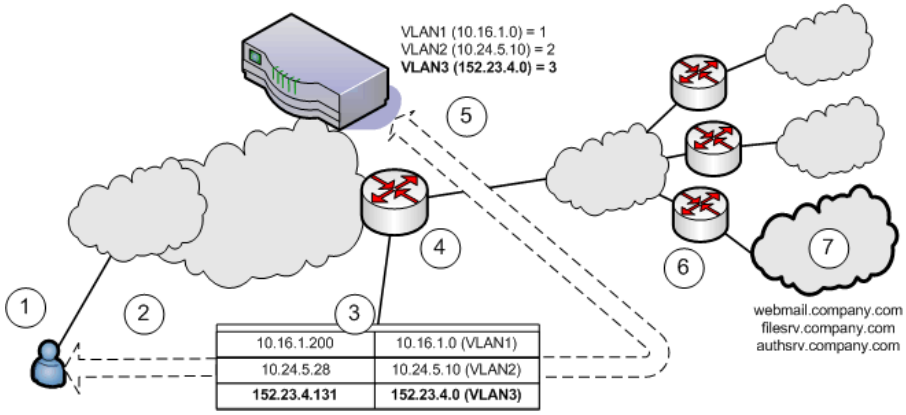
As shown in Figure 62, you can configure a static route in the CE router to point to the end-user's IP address, with the next-hop gateway set to the IP address of the subscriber's VLAN port.

NOTE:

- Alternately, you can configure a default route on the CE router with the next-hope gateway set to the IP address of the subscriber VLAN port. In this case, you do not need to add individual static routes to the Network Connect IP pool addresses.

- You can also allocate an entire network to an Network Connect IP address pool.

Figure 62: Setting a static route to Network Connect end-user's IP address in CE router



1. End-users sign in over an Internet connection using an IP address agreed upon by the MSP and the subscriber company.
2. Specify a static route in the MSP's VLAN termination point (in this example, a CE router) route table to point to the end-user sign-in IP addresses for each subscriber company.
3. You must also specify the next-hop gateway in the CE router's route table.
4. In the CE route table, specify all end-user sign-in IP addresses as static routes, and all corresponding VLAN port IP addresses as defined in the virtualized IVE.
5. Define at least one unique VLAN ID for each subscriber company. Use the IP addresses of each VLAN as the next-hop gateway addresses in the CE router's route table.
6. The subscribers' CPE routers perform the proper traffic routing to the subscriber company intranets.
7. Each subscriber company must provide sign-in pages for the IP addresses defined as static routes for end-user sign-in.

Once the MSP VLAN termination point (in this example, a CE router) determines the intended subscriber intranet, the termination point directs the traffic to the appropriate CPE router, which sends the traffic to the proper resource in the subscriber intranet.

Configuring a centralized DHCP server

You can configure one or more centralized DHCP servers if you want to provide Network Connect IVS users with dynamic IP addressing, without requiring each IVS subscriber to support an IVS-specific DHCP server.

The DHCP server maintains separate IP address pools for each IVS, using the **IVS name** property, defined in the IVS profile, to uniquely identify the IVS-specific pools.

Upon receiving a request from an IVS, the DHCP server selects an IP address based on the IVS name and the IP address of the node from which the request originated, which is delivered in the *giaddr* field of the request. Using this combination of data points, the DHCP server picks an available IP address from the appropriate pool and returns the address in the DHCP offer.

To configure your system to support a centralized DHCP server

1. Configure the DHCP server entry in the Network Connect Connection Profile, for each Network Connect role that will acquire IP addresses by way of DHCP.

NOTE: The following notes apply to the use of a centralized DHCP server in an IVS configuration:

- You can configure the same DHCP server IP address for Network Connect roles in multiple IVS systems.
- Within a Network Connect role, if you configure both an NC IP pool and a DHCP server for the same role, the DHCP server takes precedence.
- DHCP IP address assignment can co-exist with IP address assignment by way of NC IP pools within an IVS.
- You can employ multiple DHCP servers in the service provider network, with different groups of IVS systems pointing to different central servers.

2. Configure the DHCP server itself, by configuring classes and subclasses on the DHCP server to distinguish between requests from different IVS systems and to provide IP addresses from IVS-specific IP address pools.

To configure the DHCP server entry in the Network Connect Connection Profile

1. In the Root context, choose **Users > Resource Policies > Network Connect**.
2. Click the **NC Connection Profiles** tab.
3. Click **New Profile**.
4. Enter a name for the profile.
5. Under **IP address assignment**, select the **DHCP Server** radio button.
6. Enter the DHCP server name or IP address.
7. Under **Roles**, select the applicable roles in the **Available roles** list box and click **Add** to move them to the **Selected roles** list box.
8. Click **Save Changes**.
9. Repeat the procedure for each IVS that should use the DHCP server., making sure to enter the same DHCP server name or IP address that you entered for the Root.

Configuring authentication servers

You can configure authentication servers, such as RADIUS and Active Directory, on both the MSP network and the subscriber company intranets. The authentication server authenticates the incoming traffic differently depending on whether the traffic is authenticated when it comes into the MSP network or when it reaches the customer intranet.

NOTE: If you connect an authentication server to the internal port, you must set the default VLAN to the internal port when configuring the IVS.

The following authentication servers are supported on a subscriber IVS:

- Local Authentication
- LDAP Server
- RADIUS Server
- Active Directory/Windows NT
- Anonymous Server
- Certificate Server

The following authentication servers are supported on the root system:

- Local Authentication
- LDAP Server
- NIS Server
- ACE Server
- RADIUS Server
- Active Directory/Windows NT
- Anonymous Server
- SiteMinder Server
- Certificate Server

Rules governing access to authentication servers

The following rules apply to the access of authentication servers on the MSP network or on the subscriber company network. Each IVS profile must include settings for:

- The default VLAN, which can also be the internal port, if provisioned as the default VLAN.
- The default VLAN interface IP is the source IP address used to contact the authentication server.
- Static routes in the VLAN that point to the appropriate authentication servers, which can reside in the MSP network (with an assigned VLAN ID or untagged on the internal port), or on the subscriber company network.

Configuring authentication on a RADIUS server

You must configure the RADIUS server in each IVS. If you have a RADIUS server on the MSP network as well, all of the IVS RADIUS servers can point to the same MSP RADIUS IP address.

To configure the RADIUS server:

1. Select the context:
   - If you are in an IVS context, and you want to define a RADIUS server on the MSP network, select Root from the context drop down menu in the admin console header bar and click Go.
   - If you are in the root context, and you want to define a RADIUS server on a subscriber intranet, select the IVS name from the context drop down menu in the admin console header bar and click Go.
2. Refer to the instructions in “Configuring a RADIUS server instance” on page 122.

NOTE: In the current release, ACE authentication is not available for individual IVS systems. If you want to use RSA 2 factor token-based authentication, you should use RADIUS from the IVS to access RSA ACE.

Configuring authentication on Active Directory

You must configure the AD/NT server in each IVS. If you have an AD/NT server on the MSP network as well, all of the IVS AD/NT servers can point to the same MSP AD/NT IP address.

To configure the Active Directory server:

1. Select the context:
   - If you are in an IVS context, and you want to define an AD/NT server on the MSP network, select Root from the context drop down menu in the admin console header bar and click Go.
   - If you are in the root context, and you want to define an AD/NT server on a subscriber intranet, select the IVS name from the context drop down menu in the admin console header bar and click Go.

2. Refer to the instructions in "Configuring an Active Directory or NT Domain instance" on page 101.

Delegating administrative access to IVS systems

As the root administrator, you can delegate administrative access and responsibilities to specific IVS systems. You can delegate read/write access or read-only access to all IVS systems, or to selected IVS systems.

To delegate administrative access to IVS systems

1. Select **Administrators > Admin Roles >** *SelectRole* where *SelectRole* indicates one of the listed administrator roles. You can also create a new administrator role, if you prefer.
2. Click the IVS tab.
3. If you want to give the administrator read/write access to the IVS, select one of the following:
   - If you want to give the administrator read/write access to all IVS systems, select the **Administrator can manage ALL IVSs** checkbox.
   - If you want to limit the administrator's access to specific IVS systems, select the **Administrator can manage SELECTED IVSs** checkbox, then select the IVS systems from the **Available IVSs** list and click **Add** to move them to the **Selected IVSs** list.
4. If you want to give the administrator read only access to the IVS, select one of the following:
   - If you want to give the administrator read only access to all IVS systems, select the **Administrator can view (but not modify) ALL IVSs** checkbox.
   - If you want to limit the administrator's access to specific IVS systems, select the **Administrator can view (but not modify) SELECTED IVSs** checkbox, then select the IVS systems from the **Available IVSs** list and click **Add** to move them to the **Selected IVSs** list.
5. Click **Save Changes**.

By adding these access rights to a given role, you can exercise different levels of control over different MSP administrators.

Accessing standalone installers

The IVS administrator might need to access the Host Checker, WSAM, or other standalone installers. To give IVS administrators access to the installers, which are located on the **Maintenance > System > Installers** page, you can delegate the access to them by way of the **Administrators > Admin Roles >** *SelectRole* **> IVS** page. Once you have delegated access, the IVS administrator can see the Installers page from within the context of the IVS admin console.

For more information about the installers, see **"Downloading application installers" on page 573**.

Performing export and import of IVS configuration files

Use the IVE binary import/export feature to export and import root system and user settings, and also to export and import subscriber IVS settings and profiles. The two types of operations are mutually exclusive: if exporting IVS settings, the exported configuration file does not contain root system settings; if exporting root system settings, the exported configuration file does not contain subscriber IVS settings.

You perform export and import operations from the context of the root system. On the **Maintenance > Import/Export > Import/Export Configuration** page and on the **Maintenance > Import/Export > Import/Export Users** page, you can find the standard controls for exporting root system and user configuration. A subscriber IVS administrator cannot export or import data from or to a subscriber IVS. Only you, as the root administrator, can perform these tasks.

NOTE:

- You can only import/export all IVS systems in a single operation. You cannot import/export an individual IVS system's configuration.
- You can also use the IVE binary archiving feature to perform local backups of your IVS system. For more information, see "Archiving IVE binary configuration files" on page 622.

Exporting and importing the root system configuration

To export and import the root system configuration, navigate to the **Maintenance > Import/Export > Import/Export Configuration** page, and refer to the instructions in "Importing and exporting IVE configuration files" on page 626.

Exporting IVS configurations

To export IVS configurations, perform the following steps:

1. Select the **Maintenance > Import/Export > Import/Export IVS** page.
2. To password protect the configuration file, enter a password in the **Password for configuration file:** text box.
3. Click **Save Config As**.
4. Click **Save**.
5. Provide a file name and target location for the file.
6. Click **Save** and **Close**, if necessary.

The saved configuration file contains the following settings for all IVS systems:

- IVS Profiles
- IVS System Settings
- IVS Signing In Settings
- IVS Administrators
- IVS Users
- IVS Resource Policies
- IVS Maintenance Settings

Importing IVS configurations

To import IVS configurations, perform the following steps:

1. Select the **Maintenance > Import/Export > Import/Export IVS** page.
2. Click **Browse**.
3. Locate and select the file and click **Open**.
4. If you password protected the configuration file, enter the password in the **Password:** text box.
5. To import the network settings in the IVS profile, such as VLAN ports and virtual ports, select the **Import IVS Profile Network Settings** checkbox.

NOTE:

- Importing network settings as described in above only works if you export the system and IVS configurations from the same system.
- The network settings themselves do not get imported; only the references to the network settings get imported. Network settings are only imported/exported when importing/exporting the root system settings.

6. Click **Import Config**.

The IVS provides a confirmation message if the import operation succeeds. The IVS then restarts certain services, which may require several minutes.

NOTE:

- You can use the XML Import/Export feature to export and import XML-based configuration files on the root IVS. You cannot use the XML Import/Export feature for subscriber IVS systems. Instead, use the binary configuration file import/export.
- You can use Push Config to copy one root IVS configuration to another root IVS. You cannot use Push Config to copy configuration data between subscriber IVS systems or from a root IVS to a subscriber IVS.

Monitoring subscribers

Log files contain detailed information about events, user access, administrator access and more. The log entries specify the context of each entry, whether the entry was caused by a root action or an action on one of the IVS systems. The root entries contain the word Root. For example, the following entries show access by two administrators, the first being Root and the second, an administrator called Test:

ADM20716 2005-05-10 10:52:19 - ive - [10.11.254.160] Root::administrator(administrator Users)[.Administrators] - User Accounts modified. Added Unspecified Name with username testuser1 to authentication server System Local.

Info ADM20716 2005-05-10 10:35:26 - ive - [10.11.254.160] Test::administrator(administrator Users)[.Administrators]!Root - User Accounts modified. Added IVE Platform Administrator with username omiadmin to authentication server Administrators.

Suspending subscriber access to the IVS

To suspend subscriber access to the IVS:

1. Select **System > Virtual Systems**.
2. Click the **Disabled** radio button.

By performing this step, you make the IVS unavailable to any user of the IVS, including the IVS administrator. To provide access to the IVS, set the radio button to the Enabled state.

Troubleshooting VLANs

In addition to the standard troubleshooting features provided by the IVE, the virtualized IVE provides several enhancements, specifically for managing IVS systems. You can use the following troubleshooting features on either the root system or each IVS, separately:

- Policy simulation
- Policy tracing
- Session recording

Functionally, these utilities are the same as the standard IVE capabilities. The key difference is a matter of context. If you initiate one of these three utilities from the root system context, you get results for users, policies, and sessions on the root system or from the MSP network. If you initiate the utilities from a subscriber IVS context, you get results for users, policies, and sessions on the IVS or the subscriber intranet. For more information about user sessions, policy tracing, and session recording, see "Troubleshooting" on page 683.

The TCPDump, Ping, Traceroute, NSLookup, and ARP commands are enhanced for use in virtualized IVE systems. You can initiate these commands on the internal and external ports, as well as on selected VLAN ports, which you might do if you want to troubleshoot traffic on a subscriber VLAN. The basic functionality of the commands is unchanged, except for the ability to specify a VLAN port

Performing TCPDump on a VLAN

1. If you are not in the root system context, select **Root** from the **IVS** drop down menu in the admin console header, and then click **Go**.
2. Choose **Troubleshooting > TCP Dump**.
3. With **Internal Port** selected, select the VLAN from the **VLAN Port** drop down menu.
4. Add a filter to the **Filter** text box (Optional).
5. Click **Start Sniffing**.
6. To retrieve the results, click **Stop Sniffing**.
7. Choose the type of Dump file from the **Dump File** drop down menu.
8. Click **Get**.
9. Open the file with the appropriate editor.

For more information on using TCP Dump, see "Creating TCP dump files" on page 689.

Using commands on a VLAN (Ping, traceroute, NSLookup, ARP)

1. If you are not in the root system context, select **Root** from the **IVS** drop down menu in the admin console header, and then click **Go**.
2. Choose **Troubleshooting > Commands**.
3. Select a command from the Command drop down menu.
4. Enter the target server.
5. Select the VLAN from the **VLAN Port** drop down menu.
6. Enter the other settings, depending on the command you choose.
7. Click OK.

For more information on using TCP Dump, see "Creating TCP dump files" on page 689.

IVS use cases

The following use cases illustrate some common tasks you might want to perform while configuring your IVS system.

- "Policy routing rules resolution use case for IVS" on page 786
- "Configuring a global authentication server for multiple subscribers" on page 791
- "Configuring a DNS/WINS server IP address per subscriber" on page 791
- "Configuring access to Web applications and Web browsing for each subscriber" on page 792
- "Configuring file browsing access for each subscriber" on page 793
- "Setting up multiple subnet IP addresses for a subscriber's end-users" on page 794
- "Configuring multiple IVS systems to allow access to shared server" on page 795.
- "Configuring Network Connect for use on a virtualized IVE" on page 773

Policy routing rules resolution use case for IVS

This use case illustrates how policy routing takes place in an MSP deployment. The first part of the use case details two subscriber company configurations and how end-users access their respective subscriber company networks. The second part of the use case describes what happens when you create a VLAN on the MSP network to provide shared services to the subscriber companies' end-users.

Company 1 and Company 2 are hosted companies on the MSP network. Table 47 shows the VLANs, VLAN IDs, interfaces and roles defined for each company. Company 1 has defined two VLANs, one for Sales and one for Human Resources. Each company has an associated role defined for each VLAN. The root administrator creates each VLAN, providing a unique VLAN ID for each, and indicating a given port. In this case, the root administrator has created all four VLANs on the internal interface.

Table 47: Deployments in MSP and subscriber company networks

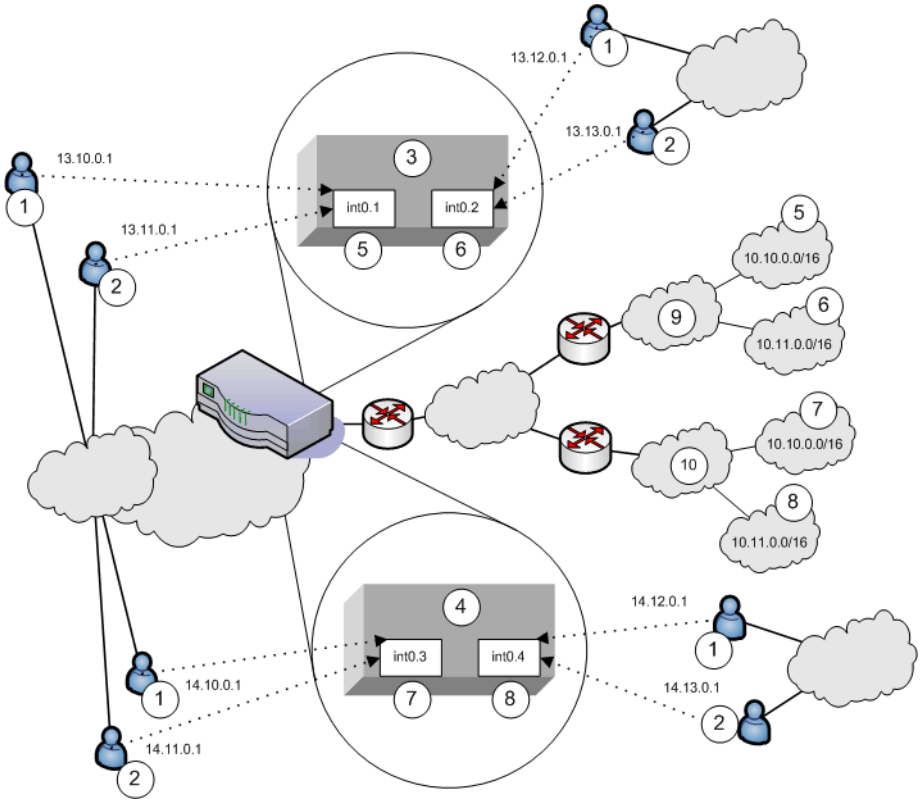
	VLAN	VLAN ID	Interface	Role
Company 1	Sales	1	int0.1	SALES
	HR	2	int0.2	HR
Company 2	Employee	3	int0.3	EMPLOYEE
	Partner	4	int0.4	PARTNER

NOTE:

- The labels for ports have been changed. The port name eth0 (internal port) is now called int0 and eth1 (external port) is now ext0.
- You can only see the route table device names (such as int0.1) from the serial console. You can view the route table by selecting menu item 1, then menu item 2 from the serial console.

Figure 63 illustrates the MSP and subscriber company deployments.

Figure 63: MSP and subscriber company deployment



NOTE: IVS VLANs are not explicitly tied to subscriber intranets by configuration on the IVE. The association of a VLAN to a subscriber intranet is accomplished by mapping VLAN interfaces to private tunnels in the subscriber intranet within the CE-> CPE router framework. For more information, refer to the discussion on static routes in “Adding static routes to the VLAN route table” on page 761.

In Figure 63, Network Connect end-users get their source IP addresses from configured Network Connect IP address pools that the root administrator has defined for the IVS. Also, in the figure, non-Network Connect users can still access specified realms based on their roles and on role-based source IP (VIP sourcing) addresses that you define as virtual ports on the VLAN.

The following list describes each item that is marked with a numbered label in Figure 63.

1. Network Connect end-users get IP addresses from Network Connect IP pools. Traffic from these users is routed through the appropriate subscriber VLAN, which you define on the internal port.

2. Non-Network Connect end-users get IP addresses from virtual IP (VIP) pools. Traffic from these users is sourced through the appropriate subscriber VLAN.

3. In Figure 63, this numbered box represents a subscriber IVS, which contains two VLANs that are defined on ports int0.1 and int0.2.

4. In Figure 63, this numbered box represents a second subscriber IVS, which contains two VLANs that are defined on ports int0.3 and int0.4.

5. The subscriber defines a role for “Sales” on VLAN1. End-users signing in to IP 13.10.0.1 over the Internet are routed to the Company 1 intranet, to the appropriate backend resources located in the “Sales” realm at 10.10.0.0/16. End-users signing in on IP 13.11.0.1 are VIP sourced to the Company 1 intranet, also to the appropriate backend resources located in the “Sales” realm at 10.10.0.0/16.

6. The subscriber defines a role for “HR” on VLAN2. End-users signing in on IP 13.12.0.1 over the Internet are routed to the Company 1 intranet, to the appropriate backend resources located in the “HR” realm at 10.11.0.0/16. End-users signing in on IP 13.13.0.1 are VIP sourced to the Company 1 intranet, also to the appropriate backend resources located in the “HR” realm at 10.11.0.0/16.

7. The subscriber defines a role for “Employee” on VLAN3. End-users signing in on IP 14.10.0.1 over the Internet are routed to the Company 2 intranet, to the appropriate backend resources located in the “Employee” realm at 10.10.0.0/16. End-users signing in on IP 14.11.0.1 are VIP sourced to the Company 2 intranet, also to the appropriate backend resources located in the “Employee” realm at 10.10.0.0/16.

8. The subscriber defines a role for “Partner” on VLAN4. End-users signing in on IP 14.12.0.1 over the Internet are routed to the Company 2 intranet, to the appropriate backend resources located in the “Partner” realm at 10.11.0.0/16. End-users signing in on IP 14.13.0.1 are VIP sourced to the Company 2 intranet, also to the appropriate backend resources located in the “Partner” realm at 10.11.0.0/16.

9. The Company 1 intranet supports two realms: “Sales” at 10.10.0.0/16 and “HR” at 10.11.0.0/16. These realms correspond to the roles defined on VLAN1 and VLAN2/

10. The Company 2 intranet supports two realms: “Employee” at 10.10.0.0/16 and “Partner” at 10.11.0.0/16.

NOTE: The realms are valid even though they contain overlapping IP addresses. Because the roles are defined for different VLANs, the VLAN IDs provide the separation that allows them to overlap without danger of mixed traffic.

The route tables for each VLAN appear as follows:

Table 48: VLAN1 route table

Destination IP	Gateway	Output port
0.0.0.0	Default gateway on VLAN1	int0.1
10.10.0.0/16	0.0.0.0	int0.1

Table 49: VLAN2 route table

Destination IP	Gateway	Output port
0.0.0.0	Default gateway on VLAN2	int0.2
10.10.0.0/16	0.0.0.0	int0.2

Table 50: VLAN3 route table

Destination IP	Gateway	Output port
0.0.0.0	Default gateway on VLAN3	int0.3
10.10.0.0/16	0.0.0.0	int0.3

Table 51: VLAN4 route table

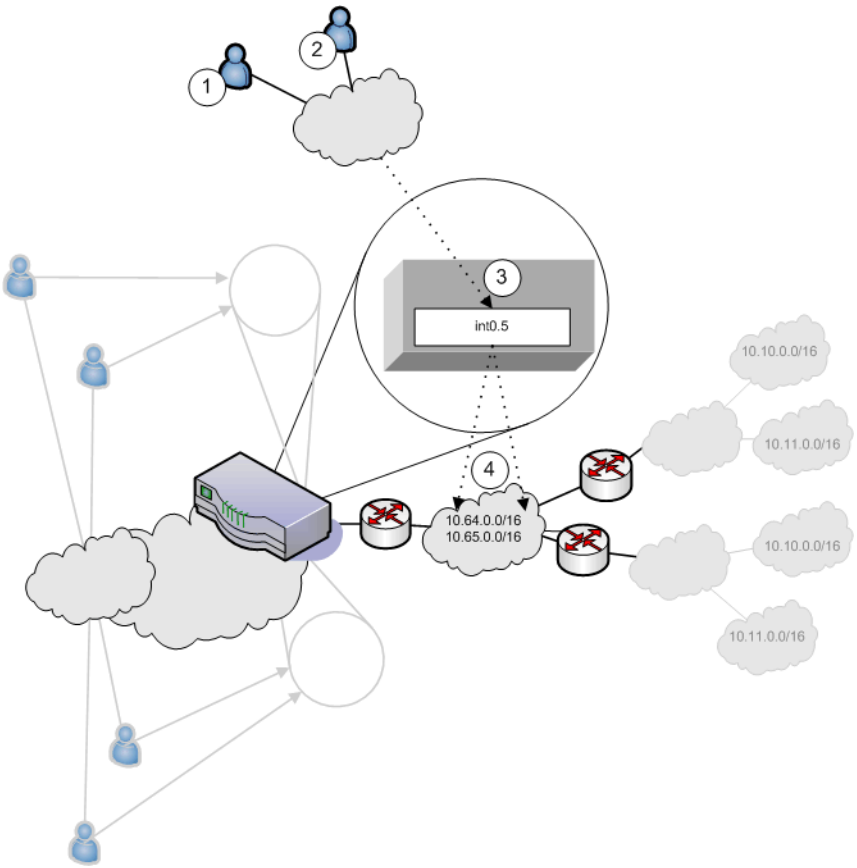
Destination IP	Gateway	Output port
0.0.0.0	Default gateway on VLAN4	int0.4
10.10.0.0/16	0.0.0.0	int0.4

Now consider the situation in which the MSP decides to provide shared services to end-users of Company 1 and Company 2. Assume the MSP network is also on a VLAN (VLAN5). If you want to provide services on 10.64.0.0/16 to both Company 1 and Company 2, and services on 10.65.0.0/16 to Company 2 only, you can configure either Network Connect pools or virtual ports for those addresses.

Figure 64 illustrates this situation.

NOTE: Some details from Figure have been removed or greyed out to improve readability of Figure 64.

Figure 64: MSP VLAN providing shared services



1. Company 1 end-users sign-in over the Internet to the MSP network and the MSP VLAN, VLAN5 (represented as number 3 in the illustration).

2. Company 2 end-users sign-in over the Internet to the MSP network and the MSP VLAN, VLAN5 (represented as number 3 in the illustration).

3. The MSP VLAN5 provides access to shared services on the MSP network.

4. You must define separate IP addresses for each subscriber company's end-users, even though they share MSP services.

Once you configure routes to support users who have access to shared services on the MSP network and to support users who also have access to restricted MSP network services, the VLAN route tables appear as follows:

Table 52: VLAN1 route table

Destination IP	Gateway	Output port
0.0.0.0	Default gateway on VLAN1	int0.1
10.64.0.0	Router on VLAN5	int0.5

Table 53: VLAN2 route table

Destination IP	Gateway	Output port
0.0.0.0	Default gateway on VLAN2	int0.2
10.64.0.0	Router on VLAN5	int0.5

Table 54: VLAN3 route table

Destination IP	Gateway	Output port
0.0.0.0	Default gateway on VLAN3	int0.1
10.64.0.0	Router on VLAN5	int0.5
10.65.0.0	Router on VLAN5	int0.5

Table 55: VLAN4 route table

Destination IP	Gateway	Output port
0.0.0.0	Default gateway on VLAN4	int0.2
10.64.0.0	Router on VLAN5	int0.5
10.65.0.0	Router on VLAN5	int0.5

NOTE: If the MSP network is connected to the untagged port (internal), the route entries are similar, but the output port is int0 only.

Configuring a global authentication server for multiple subscribers

If your subscriber companies prefer to lease or purchase authentication services from you, the service provider, you can configure a global authentication server on your network. In that case, you must perform several tasks:

1. Configure one or more authentication servers on your MSP network.
2. Configure path-based URLs or virtual ports for sign-in on your MSP network.
3. Configure VLANs and IVS systems to map to the authentication servers on the MSP network.

For more information, see “Configuring authentication servers” on page 778.

Configuring a DNS/WINS server IP address per subscriber

If you want to configure a particular DNS/WINS server IP address per subscriber, you can do so from within each IVS.

To configure a DNS/WINS server IP address:

1. Configure your IVS systems.
2. Select an IVS from the system drop down menu in the admin console header area and then click **Go**. Within the IVS context, the header color changes and displays the name of the subscriber.

3. Select **System > Network > Overview**.

4. Enter the DNS/WINS settings that correspond to the DNS/WINS server on the subscriber intranet.

5. Click **Save Changes**.

For more information, see "Configuring DNS for the IVS" on page 771. For an example of how to set up a global DNS/WINS server, see "Configuring Network Connect for use on a virtualized IVE" on page 773.

Configuring access to Web applications and Web browsing for each subscriber

The IVS administrator may want to configure specific Web browsing policies for the IVS end-users.

To configure Web browsing access, the IVS administrator needs to configure the following pages:

- **Users > User Roles >** *RoleName* **> Web**
- **Users > Resource Policies > Web**

Configuring Web browsing access

To configure Web browsing access:

1. Choose **Users > User Roles >** *RoleName* **> Web**.

2. Select the **Bookmarks** tab.

3. Click **New Bookmark**.

4. Supply settings to configure the bookmark to a given Web URL.

5. Click **Save Changes** or **Save + New** if you want to add multiple bookmarks.

   The bookmarks you define here appear in the Secure Access Web bookmarks section to which end-users have access.

6. Select the **Options** tab.

7. Select the Web browsing privileges you want to provide to your end-users.

8. Choose the other options you want, including setting the timeout value for the HTTP connection.

9. Click **Save Changes**.

Configuring Web browsing access policies

To configure Web browsing access policies:

1. Choose **Users > Resource Policies > Web**.

2. Supply the appropriate settings on each of the tabs.

For information on resource policies and how to configure Web resource policies, see both "Web rewriting" on page 281 and "Defining resource policies: Overview" on page 322.

Configuring file browsing access for each subscriber

The IVS administrator may want to configure specific file-browsing access policies for the IVS end-users. The IVS administrator can perform this type of operation based on roles.

To configure file browsing, the IVS administrator needs to configure the following pages:

- **Users > User Roles >** *RoleName* **> General**
- **Users > User Roles >** *RoleName* **> Files**
- **Users > Resource Policies > Files**

Configuring file browsing access

To configure file browsing access:

1. Choose **Users > User Roles >** *RoleName* **> General.**
2. Under **Access Features**, select the **Files** checkbox (for Windows).
3. Click **Save Changes**.
4. Select the **Files** tab.
5. Select the **Options** page.
6. Depending on the file system type, select the options that apply to the IVS end-user access.
7. Click **Save Changes**.

Configuring file system bookmarks

To configure file system bookmarks:

1. Make sure you are in the IVS context. If the IVS drop down menu in the admin console header bar displays Root, select the IVS name from the menu and click **Go**.
2. Select **Users > User Roles >** *RoleName* **> General > Files**.
3. Select either the **Windows Bookmarks** or the **UNIX Bookmarks** page.
4. Click **New Bookmark**.
5. Supply the appropriate settings.
6. Click **Save Changes**.

For more information on setting up bookmarks to file systems, see “File rewriting” on page 369.

Configuring file system access policies

To configure file system access policies:

1. Make sure you are in the IVS context. If the IVS drop down menu in the admin console header bar displays Root, select the IVS name from the menu and click **Go**.
2. Select **Users > Resource Policies > Files > Access > Windows**.
3. Choose the role from the **Show policies that apply to** drop down menu, and click **Update**.
4. Click **New Policy**.
5. Supply the appropriate settings.
6. Click **Save Changes**.
7. Select the **Credentials** tab.
8. Supply the appropriate settings.
9. Click **Save Changes**.
10. Repeat these steps for each role.
11. Select the Encoding tab to select the language encoding and click **Save Changes**.
12. Select the Options tab to set options, such as IP based matching for Hostname based policy resources and click **Save Changes**.

For more information on file policies, see “Defining resource policies: UNIX/NFS file resources” on page 387. For more information on encoding, see “Multi-language support” on page 839. For more information on access options, see “Writing UNIX/NFS resource policies” on page 389.

Setting up multiple subnet IP addresses for a subscriber’s end-users

Assume that the subscriber wants to create subnets within the intranet to support traffic separation between subscriber end-users from three different departments: Marketing, Finance, and Engineering. The procedures needed to accomplish this task are divided between those performed by the root administrator and those performed by the IVS administrator.

Tasks performed by the root administrator

1. Create subscriber VLAN. See“Configuring a Virtual Local Area Network (VLAN)” on page 759.
2. Create subscriber IVS. See “Creating a virtual system (IVS profile)” on page 763.

3. Create path-based URLs or virtual ports for sign-in. See“Signing-in using the sign-in URL prefix” on page 747 or “Configuring a virtual port for sign-in on the internal port” on page 758.

4. Create virtual ports for role-based source IP aliasing. See “Configuring role-based source IP aliasing” on page 766.

Tasks performed by the IVS administrator

1. Create users. Create roles for Marketing, Finance, and Engineering. See “Configuring user roles” on page 56.

2. Assign roles to VLAN/Source IP. See “Associating roles with source IP addresses in an IVS” on page 767.

3. Assign users to roles. See “Creating user accounts on a local authentication server” on page 119.

Configuring multiple IVS systems to allow access to shared server

There may be cases in which you want to provide end-users of multiple subscriber companies to access a shared server on the MSP network. For more information about accessing shared servers, see “Configuring Network Connect for use on a virtualized IVE” on page 773 and “Policy routing rules resolution use case for IVS” on page 786.

The following steps describe a simple use case and solutions.

Solution #1

To configure access to a shared server, assuming two IVS systems for two subscribers:

1. Add the internal port to the IVS1 list of selected VLANs.

2. Add the internal port to the IVS2 list of selected VLANs. For instructions on adding ports to the IVS system’s selected VLAN field, see “Provisioning an IVS” on page 753.

3. Edit the internal port’s route table and configure a static route pointing to the shared server, with the internal interface as the output port.

Solution #2

To configure access to a shared server, assuming two IVS systems for two subscribers:

1. Add VLAN1 to the IVS1 selected VLAN list and set it as the default VLAN.

2. Add VLAN2 to the IVS2 selected VLAN list and set it as the default VLAN. For instructions on adding VLANs to the IVS system’s selected VLAN field, see “Provisioning an IVS” on page 753.

3. Edit the route tables for both VLAN1 and VLAN2 and configure a static route in each that points to the shared server, with the internal interface as the output port.