# Glue Networks Deployment Guide for the Cisco Next-Generation WAN

Last Updated: May 1, 2013

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Glue Networks Deployment Guide for the Cisco Next-Generation WAN

# Glue Networks Deployment Guide for the Cisco Next-Generation WAN

## Introduction

Global networks are the foundation of business processes and customer transactions. The Cisco Next-Generation WAN (NGWAN) for Enterprises is an end-to-end architectural framework that provides foundational building blocks for next-generation enterprise networks to deliver critical business services such as voice, video, and real-time data. This hierarchical design approach provides the agility and scalability required by enterprises to extend and replicate networks across the globe.

Network management plays an important role within the NGWAN architecture. This guide describes the Gluware® automation engine from Glue Networks. This guide also describes the ability of the Gluware engine to deliver software-defined network management within the context of the Cisco NGWAN architecture.

## Software-Defined NGWANs Enabled with the Gluware Engine

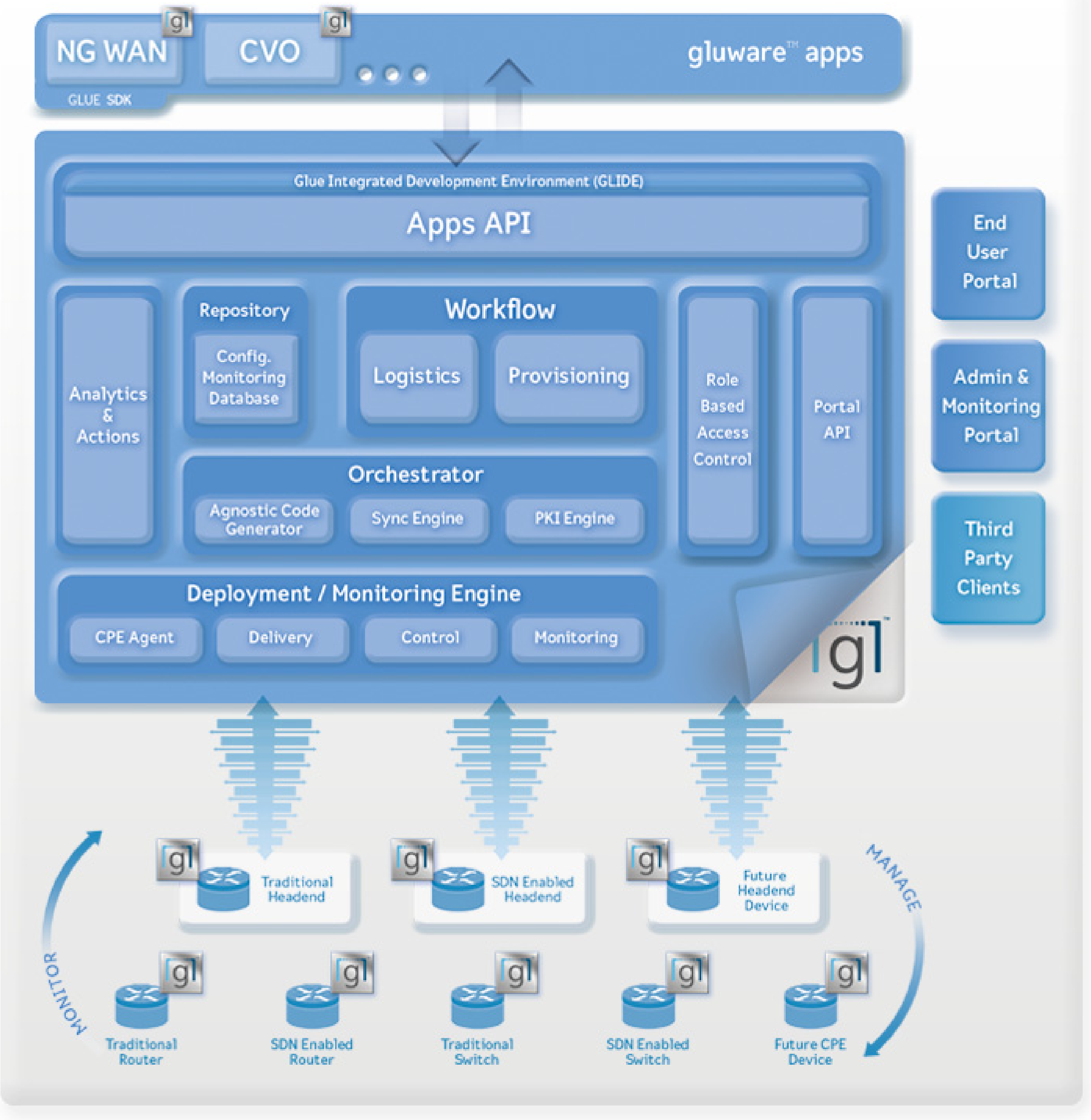
Software-defined networking (SDN) has received a lot of focus in the industry. However, the heavy emphasis that SDN places on configuring networks within the data center has not addressed the complexities of the WAN. The Gluware engine delivers feature-rich, software-defined WANs based on the Cisco NGWAN architecture. The Gluware automation engine integrates highly intelligent networking functions into an automated platform that allows the administrator to remotely build, monitor, and maintain networks with efficiency and precision.

The Gluware engine was designed to allow enterprises to code their network design standards into a management engine so that branch and teleworker networks are deployed in a rapid and repeatable fashion. Automating the deployment allows architecture and engineering organizations to refocus their efforts on higher-level tasks with assurance that configuration details are implemented with the desired standardization. This simplified management methodology allows the enterprise to move site-deployment activities from an ad hoc engineering effort to a consistent operational model that enables speed and agility.

**Corporate Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

Teleworker deployments leverage the same Gluware platform to deploy Cisco Virtual Office (CVO) solutions with remote user on-demand provisioning. The Glue Networks First Connect browser-based software allows remote users to leverage the Gluware engine to deploy a CVO router in about 12 minutes with integrated error-checking and self-healing.

*Figure 1 Gluware Architecture*



As shown in Figure 1 on page 5, the Gluware architecture has these critical components:

**Apps Application Programming Interface (API):** The Gluware engine can be configured through Gluware apps, which allow you to deploy Next Generation WANs quickly and with confidence. When the deployment of the WAN infrastructure and active monitoring of health and performance is automated, the basis for an application-aware, intelligent WAN is created.

**Analytics and Actions:** Integrated real-time tracking and monitoring of key performance indicators (KPIs) monitor the health of your network. Integrated alert generation allows the network administrator to define specific triggers and actions to be taken when user-defined KPI thresholds are reached.

**Logistics and Provisioning Workflow:** A streamlined workflow allows network administrators to seamlessly coordinate hardware ordering and logistics with Channel Partners, and provision headend and customer premise equipment (CPE) routers. The workflow can process individual end-user requests or link to Channel Partners who can utilize an API for batch uploads of user and hardware details for larger deployments.

**Portal API for End-User, Admin, and Monitoring Portals:** Interaction with the Gluware automation engine is enabled through the Glue Networks portal API. The API simplifies end-user interaction and provides admin access to advanced features. The End-User Portal guides end users to provision their own CPE routers by simply clicking a link in an email. The set-up wizard walks the user through a few simple steps to enable the device. The wizard also provides real-time progress updates that lead to successful configuration. Network administrators can configure network design parameters, manage user data, or initiate moves, adds, changes, and deletes (MACDs) through the Admin portal using an intuitive, RBAC-enabled Web 2.0 user interface.

**The Repository:** All network configurations, end-user data, monitoring, and reporting data are stored in a highly secure central database called the repository. The repository is accessible by the orchestrator, delivery engines, and utilities used for monitoring, reporting, and network troubleshooting.

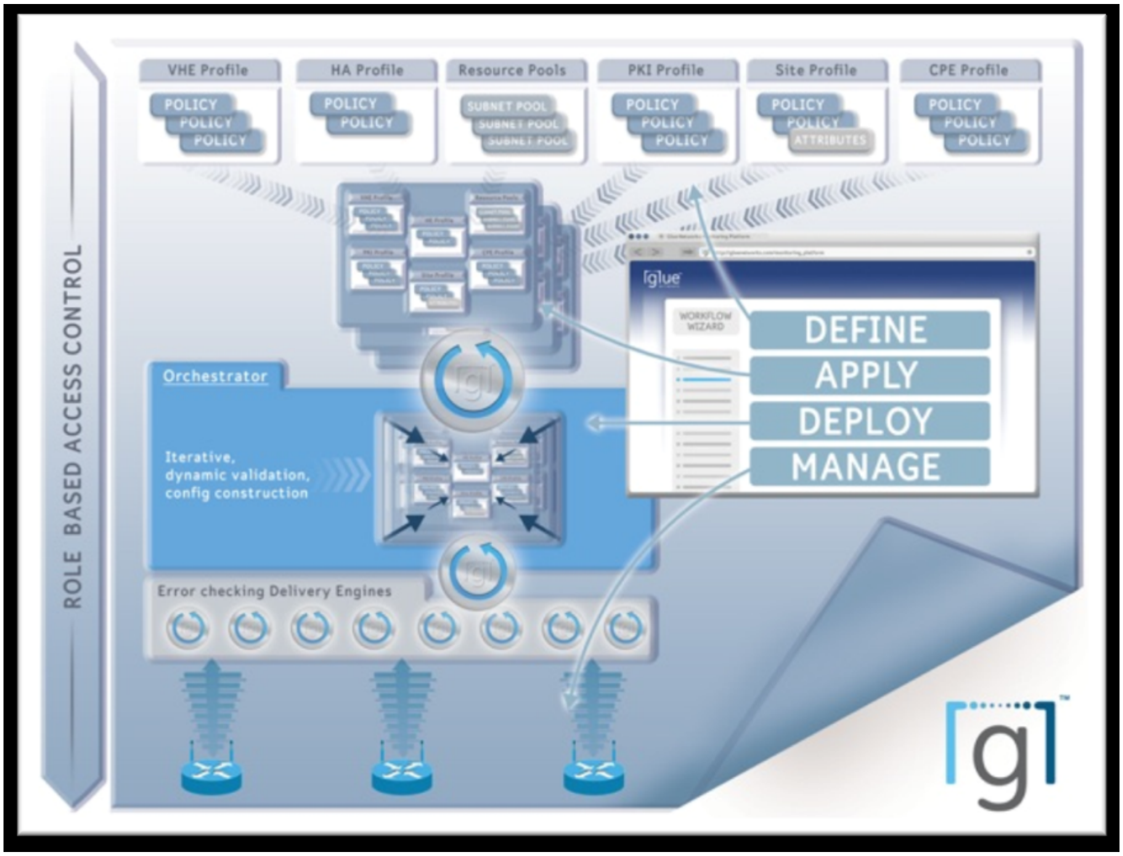
**The Orchestrator:** The heart of the Gluware engine is a central policy-based controller called the orchestrator, which oversees the entire lifecycle process. The orchestrator is a software component that generates hardware-agnostic network configurations based on best-practice templates. The orchestrator and delivery engine interact with each other and provide error checking and self-healing. This interaction allows the orchestrator to translate the agnostic network configurations into device-specific advanced configurations.

**Deployment and Monitoring Engine:** The Gluware deployment engine enables the provisioning, interaction, and monitoring of thousands of nodes. Scalable agents in the deployment engine run in parallel and configure routers automatically. The monitoring engine collects more than 20 head-end and CPE KPIs every 5 minutes. The monitoring engine uses this information to monitor the health of the network proactively. Everything from head-end CPU memory usage to CPE traffic is monitored.

# NGWAN Services Deployment Challenges

Network engineers can experience challenges when they deploy capabilities to new branch offices or teleworkers with associated router-based added services. Traditional provisioning models deploy configurations onto routers using prewritten text files. The configuration of the branch router is placed on the device at a staging facility and then the device is delivered physically to the final destination for installation. Many times only a partial configuration is placed on the branch router. A network engineer does the balance of the configuration manually after the router becomes remotely accessible. When the configuration is complex, this approach can be prone to errors and be time consuming, especially if the configuration contains an error and the device is not reachable.

***Figure 2 Gluware Policy-Based Networking***



As shown in Figure 2, the Gluware engine automated approach to deployment of network services increases efficiency and reduces provisioning time by using predefined policies, objects, and resources. The Gluware automation engine has an end-to-end understanding of the network before it generates a single line of configuration. Additionally, the orchestration engine delivers the configuration to the branch office router with a step-by-step approach and performs error checking and validation as each service is configured.

The Gluware automation engine helps IT organizations:

- Simplify network operations
- Reduce time-to-value
- Lower operating costs
- Ensure architectural integrity
- Improve business agility

# Capabilities of the Gluware Engine

An ever-increasing breadth of networking features is available on Cisco routers. The complexity and overhead that are associated with adding these features has caused enterprises to avoid or delay implementation to keep their network simple. The Gluware automation engine offers an opportunity to implement these advanced features with a standard, repeatable, and consistent methodology. This methodology allows the enterprise to extract the full value from network hardware resources. Table 1 lists the Cisco devices that are supported by the Gluware engine.

*Table 1 Cisco Devices Supported by the Gluware Engine*

| Devices | Model Numbers |
|---|---|
| **ISRs** | All 881s (1st and 2nd generation)<br>All 891s<br>All 892s<br>1921<br>All 1941s<br>All 2900-series<br>All 3900-series<br>All 3900E-series<br>Options supported: switchport HWICs and switching service module (ISR-side)<br>The Gluware engine also supports legacy 871s, 1800s, 2800s, and 3800s. |
| **ASRs** | ASR 1001<br>ASR 1002 |

Table 2 lists the Cisco device features that are supported by the Gluware engine.

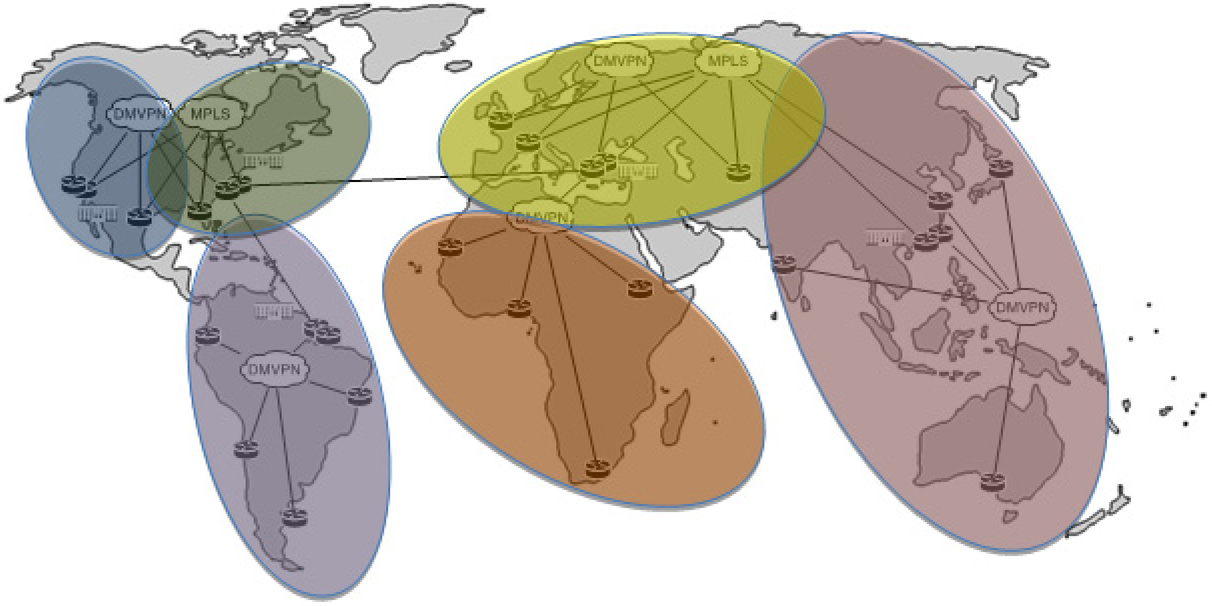
*Table 2 Cisco Device Features Supported by the Gluware Engine*

| Category | Features |
|---|---|
| **WAN** | Frame Relay and ATM<br>Ethernet 802.1q VLAN tags<br>DHCP, static IP<br>VPN NAT-T<br>PPP, PPoE, PPoA, RFC 1483 bridging<br>Dynamic Multipoint Virtual Private Network (DMVPN)<br>Dual DMVPN (Active/Active and Active/Passive)<br>Multicast support |
| **LAN** | Automatic assignment of IP address<br>Data VLAN, voice VLAN, and auxiliary VLAN<br>Per VLAN DHCP server<br>Multicast support<br>Routing<br>Static routes<br>Dynamic protocol handoff (that is, EIGRP)<br>Redistribution into dynamic protocols |
| **Security** | Public key infrastructure (PKI)<br>802.1x<br>Web authentication proxy<br>Stateful firewall (Context-Based Access Control [CBAC]) |
| **Wireless LAN** | Autonomous AP<br>Dual-band radio configuration<br>802.1 a/b/g/n<br>WEP, WPA, and WPS2<br>Cisco LEAP w/ local RADIUS |
| **QoS** | Voice and video<br>SCCP/SIP/H.323<br>Tandberg, Cisco CTS support |
| **Router Services** | Management<br>Simple Network Management Protocol (SNMP)<br>Syslog<br>Network Time Protocol (NTP) |

# Deploying Dynamic Multipoint VPN Using the Gluware Engine

The Gluware solution addresses the complexities of deploying and managing an extended enterprise network. The cost of deploying services on broadband circuits is 50–80 percent lower as compared to Multiprotocol Label Switching (MPLS) circuits. Cisco recommends Dynamic Multipoint Virtual Private Network (DMVPN) for cost-effective, direct, any-to-any, site-to-site connectivity because it provides a functional equivalent to MPLS technology. DMVPN also provides a cost-effective, redundant solution to an existing MPLS VPN network. Figure 3 represents a large-scale enterprise network that can be deployed and managed by the Gluware engine.

***Figure 3 Typical Enterprise Global WAN***



Whether DMVPN site designs are used for primary or backup WAN connectivity, they can incorporate one or more routers, depending on the size of the branch. Designs with two routers (or more) with one or more WAN circuits attached can leverage either MPLS VPN or DMVPN (broadband) to provide services to the site. You must run an interior routing protocol between the devices to provide the desired redundancy. DMVPN site designs can be used to enable each of these four branch office categories:

- Mobile branch office: Third- and fourth-generation (3G and 4G, respectively) wireless WAN as a primary connection in a mobile environment
- Standard branch office: Most typical remote branch offices that are connected to headquarters or regional sites
- High-end branch office: Large branch offices that have many users, services, and high-availability requirements
- Ultra-high-end branch office: Extremely large branch offices that combine the features of a remote office, campus environment, and even remote-office aggregation capabilities

The next sections describe how to leverage the Gluware engine to deploy a DMVPN-based standard site. In the first section, a VPN Head End (VHE) is deployed to provide spoke-to-spoke connectivity services for branch offices. In the second section, a spoke, or CPE, is deployed to offer services to branch employees.

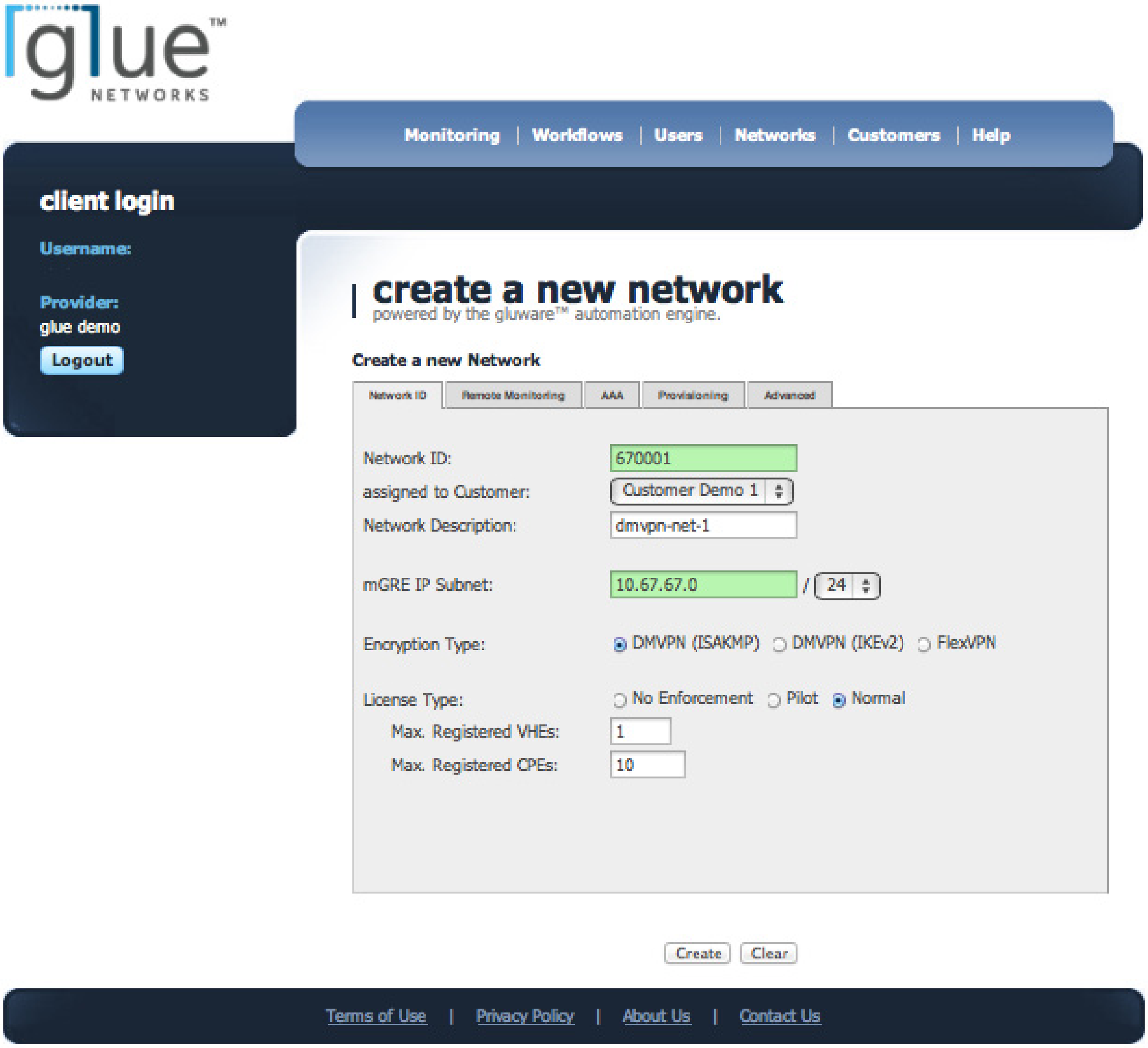
## Deploying a NGWAN VHE Using the Gluware Engine

**Step 1** Create a DMVPN Network

The first step to deploy a DMVPN network is to provision a VHE. Within the Gluware interface, configure a network and assign a network ID. DMVPN networks leverage a multipoint generic routing encapsulation (mGRE) interface to allow dynamic creation of spoke-to-spoke tunnels. The network used to assign mGRE interface IP addresses is configured on the network ID screen in Figure 4.

From the main menu, go to **Networks > Manage Network IDs > Create a new Network ID** and complete the form as shown in Figure 4. The network ID can be any 6-digit number and the subnet for mGRE tunnel interfaces must be large enough to accommodate the required number of spoke devices.

***Figure 4 Create a DMVPN Network***



create a new network

powered by the gluware™ automation engine.

Create a new Network

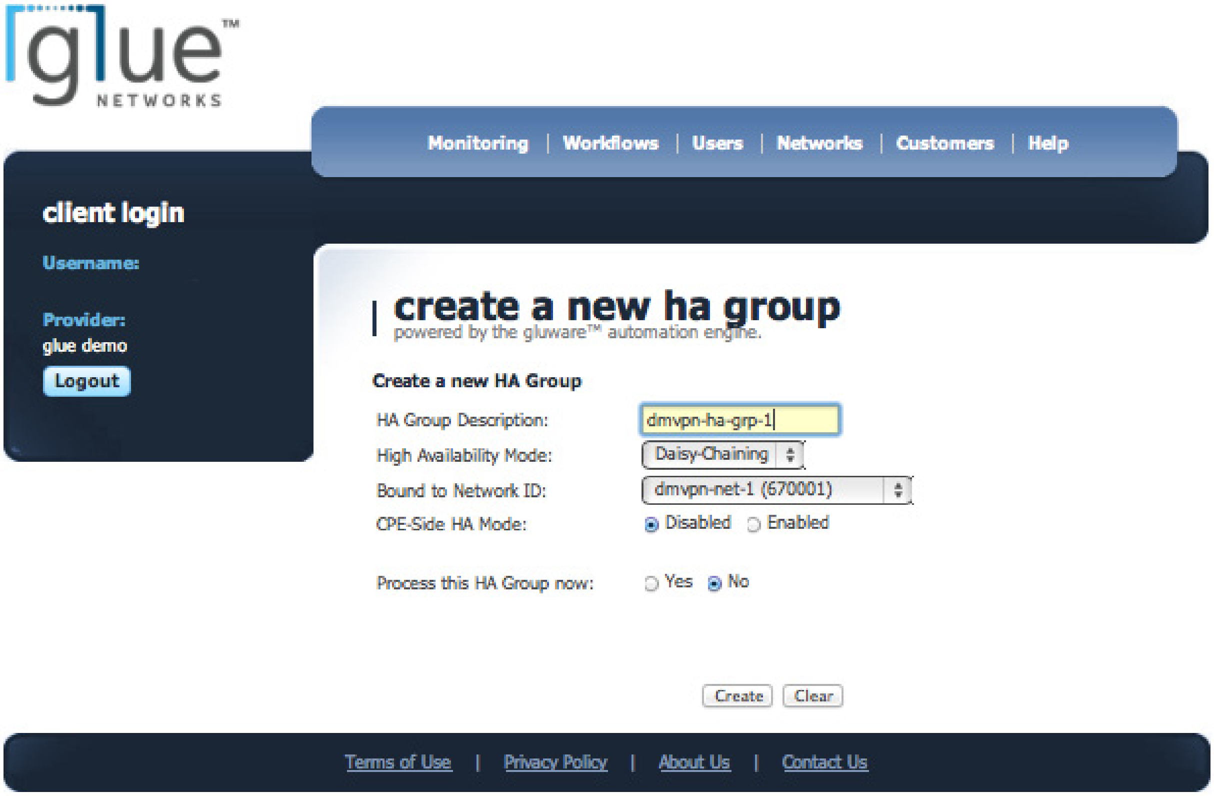
| | |
|---|---|
| Network ID: | 670001 |
| assigned to Customer: | Customer Demo 1 |
| Network Description: | dmvpn-net-1 |
| mGRE IP Subnet: | 10.67.67.0 / 24 |
| Encryption Type: | ● DMVPN (ISAKMP) ○ DMVPN (IKEv2) ○ FlexVPN |
| License Type: | ○ No Enforcement ○ Pilot ● Normal |
| Max. Registered VHEs: | 1 |
| Max. Registered CPEs: | 10 |

**Step 2** Create a HA Group

Create a high availability (HA) group to enable multiple VHE routers at a single site to resolve the public IP addresses of spoke routers. The HA group allows scalability and redundancy beyond the number of branches that can be provided by a single head-end router.

From the main menu, go to **Networks > Manage High Availability > Create a new HA Group**. Assign a HA Group name, use the network ID configured in the previous step, and assign the Daisy-Chaining high availability mode as shown in Figure 5.

***Figure 5*** ***Create a HA Group***


glue NETWORKS
Monitoring | Workflows | Users | Networks | Customers | Help
client login
Username:
Provider:
glue demo
Logout
create a new ha group
powered by the gluware™ automation engine.
Create
Clear
Terms of Use | Privacy Policy | About Us | Contact Us

Create a new HA Group

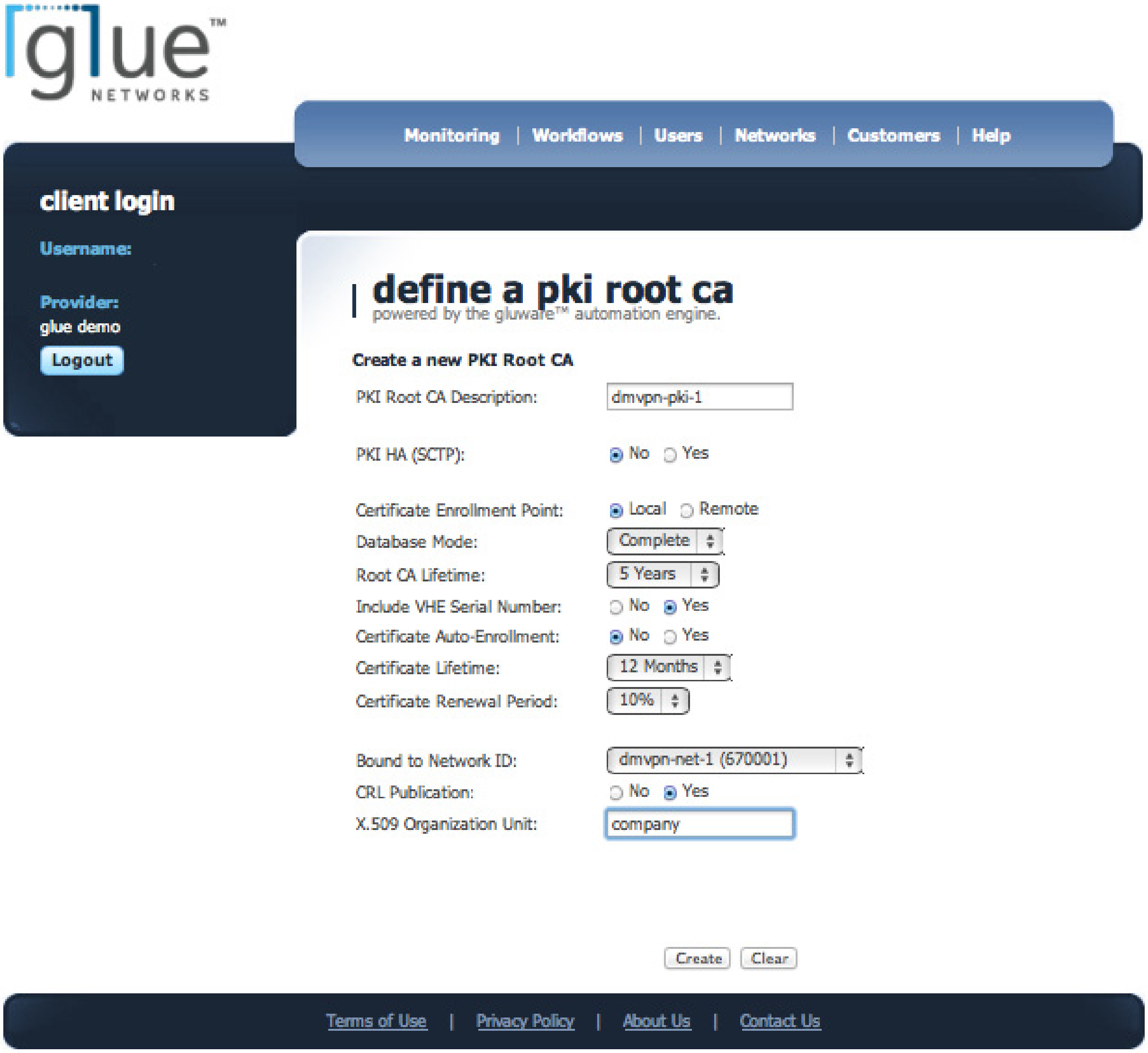
| | |
|---|---|
| HA Group Description: | dmvpn-ha-grp-1 |
| High Availability Mode: | Daisy-Chaining |
| Bound to Network ID: | dmvpn-net-1 (670001) |
| CPE-Side HA Mode: | ● Disabled ○ Enabled |
| Process this HA Group now: | ○ Yes ● No |

**Step 3** Define a PKI Root CA

Public key infrastructure (PKI) provides secure authentication services for a DMVPN network. The Gluware engine configures a Cisco router to act as a certificate authority (CA) and authenticates spokes to each other.

From the main menu, go to **Networks > Manage PKI and Certificates > Define a PKI Root CA** and configure the VHE to act as a PKI certificate server as shown in Figure 6.

***Figure 6*** ***Define a PKI Root CA***



glue™
NETWORKS
Monitoring | Workflows | Users | Networks | Customers | Help
client login
Username:
Provider:
glue demo
Logout

define a pki root ca

powered by the gluware™ automation engine.

**Create a new PKI Root CA**

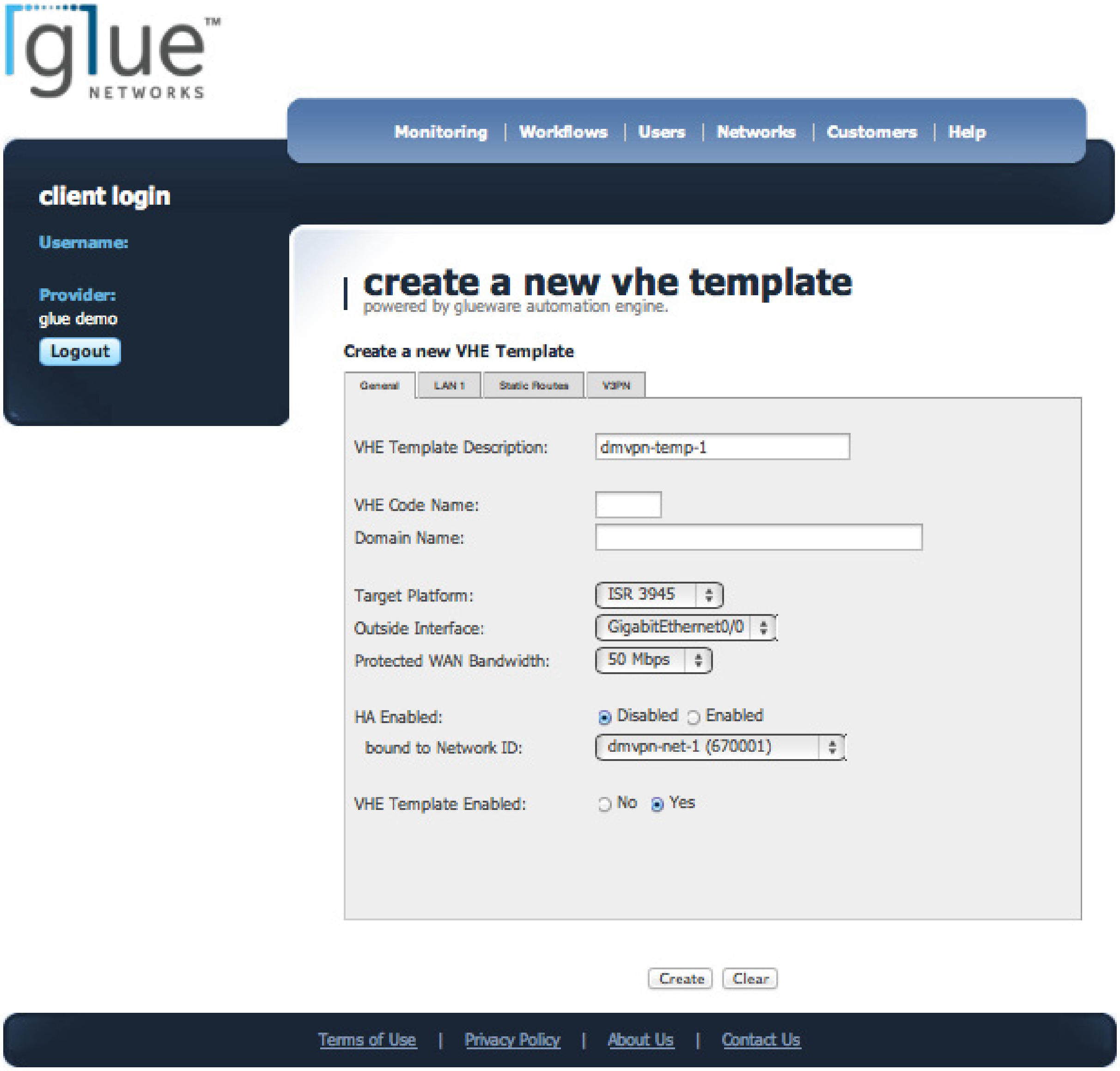
| | |
|---|---|
| PKI Root CA Description: | dmvpn-pki-1 |
| PKI HA (SCTP): | ● No ○ Yes |
| Certificate Enrollment Point: | ● Local ○ Remote |
| Database Mode: | Complete |
| Root CA Lifetime: | 5 Years |
| Include VHE Serial Number: | ○ No ● Yes |
| Certificate Auto-Enrollment: | ● No ○ Yes |
| Certificate Lifetime: | 12 Months |
| Certificate Renewal Period: | 10% |
| Bound to Network ID: | dmvpn-net-1 (670001) |
| CRL Publication: | ○ No ● Yes |
| X.509 Organization Unit: | company |

**Step 4** Create a VHE Template

The policies and resources shown in earlier steps were created for assignment to the VHE. The VHE template aggregates these resources into a device profile that can be assigned to a specific router.

From the main menu, go to **Networks > Manage VPN Head-Ends > Manage VHE Templates > Create a new VHE Template**. Choose the type of platform that the template will be assigned to, the interface that will be Internet facing, and the DMVPN network ID that was previously created as shown in Figure 7. The LAN interface is also configured in this step to provide IP service to the branch office as shown in Figure 8 on page 15.

*Figure 7 Create a VHE Template – WAN Interface*


glue NETWORKS
Monitoring | Workflows | Users | Networks | Customers | Help
client login
Username:
Provider:
glue demo
Logout
General
LAN 1
Static Routes
V3PN
Create
Clear
Terms of Use | Privacy Policy | About Us | Contact Us

create a new vhe template

powered by glueware automation engine.

Create a new VHE Template

VHE Template Description: dmvpn-temp-1

VHE Code Name:

Domain Name:

Target Platform: ISR 3945

Outside Interface: GigabitEthernet0/0

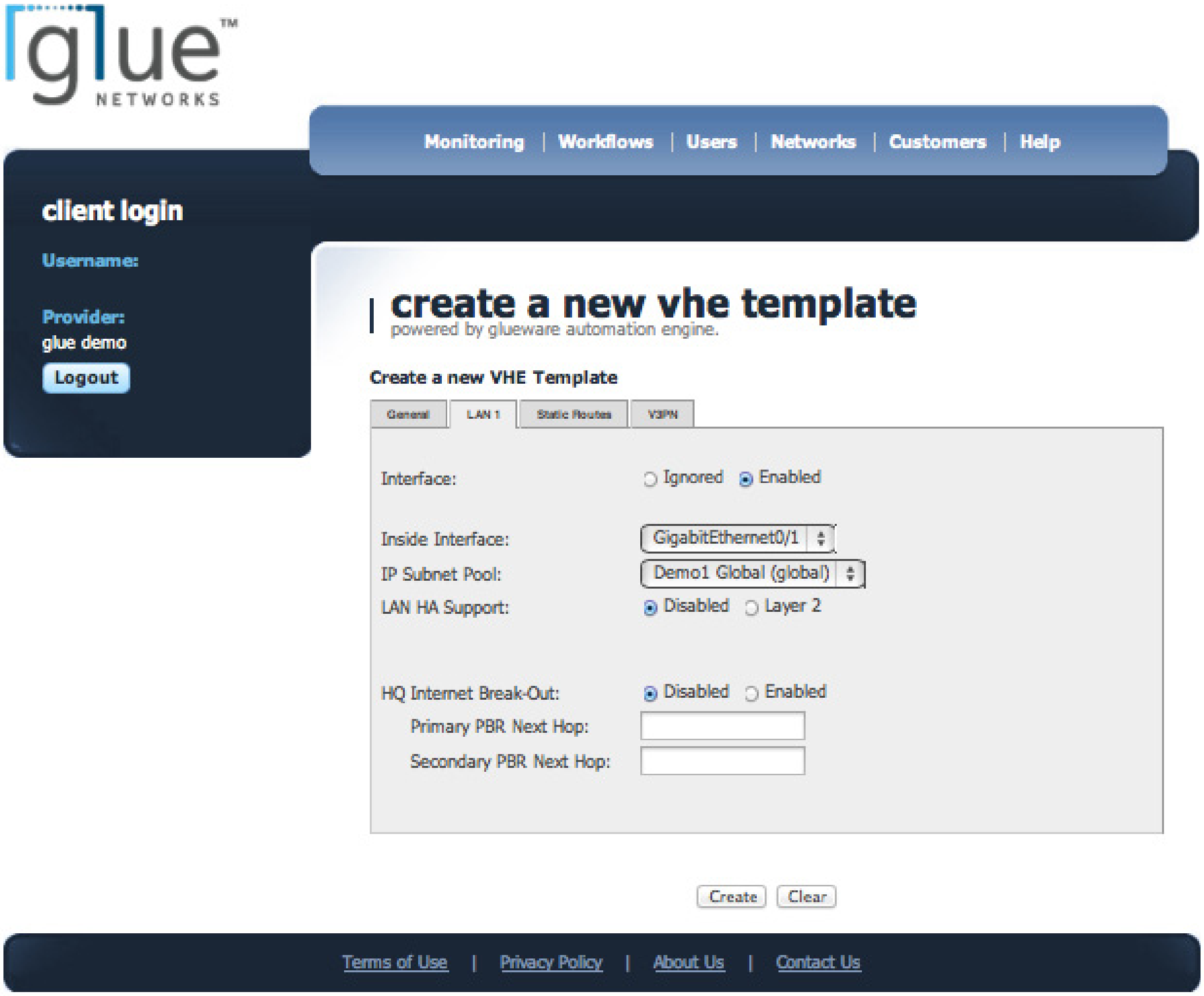
Protected WAN Bandwidth: 50 Mbps

HA Enabled: ● Disabled ○ Enabled

bound to Network ID: dmvpn-net-1 (670001)

VHE Template Enabled: ○ No ● Yes

***Figure 8 Create a VHE Template – LAN Interface***


glue™ NETWORKS
Monitoring | Workflows | Users | Networks | Customers | Help
client login
Username:
Provider:
glue demo
Logout
General
LAN 1
Static Routes
V3PN
Create
Clear
Terms of Use | Privacy Policy | About Us | Contact Us

create a new vhe template
powered by glueware automation engine.

Create a new VHE Template

Interface: ○ Ignored ● Enabled

Inside Interface: GigabitEthernet0/1

IP Subnet Pool: Demo1 Global (global)

LAN HA Support: ● Disabled ○ Layer 2

HQ Internet Break-Out: ● Disabled ○ Enabled

Primary PBR Next Hop:

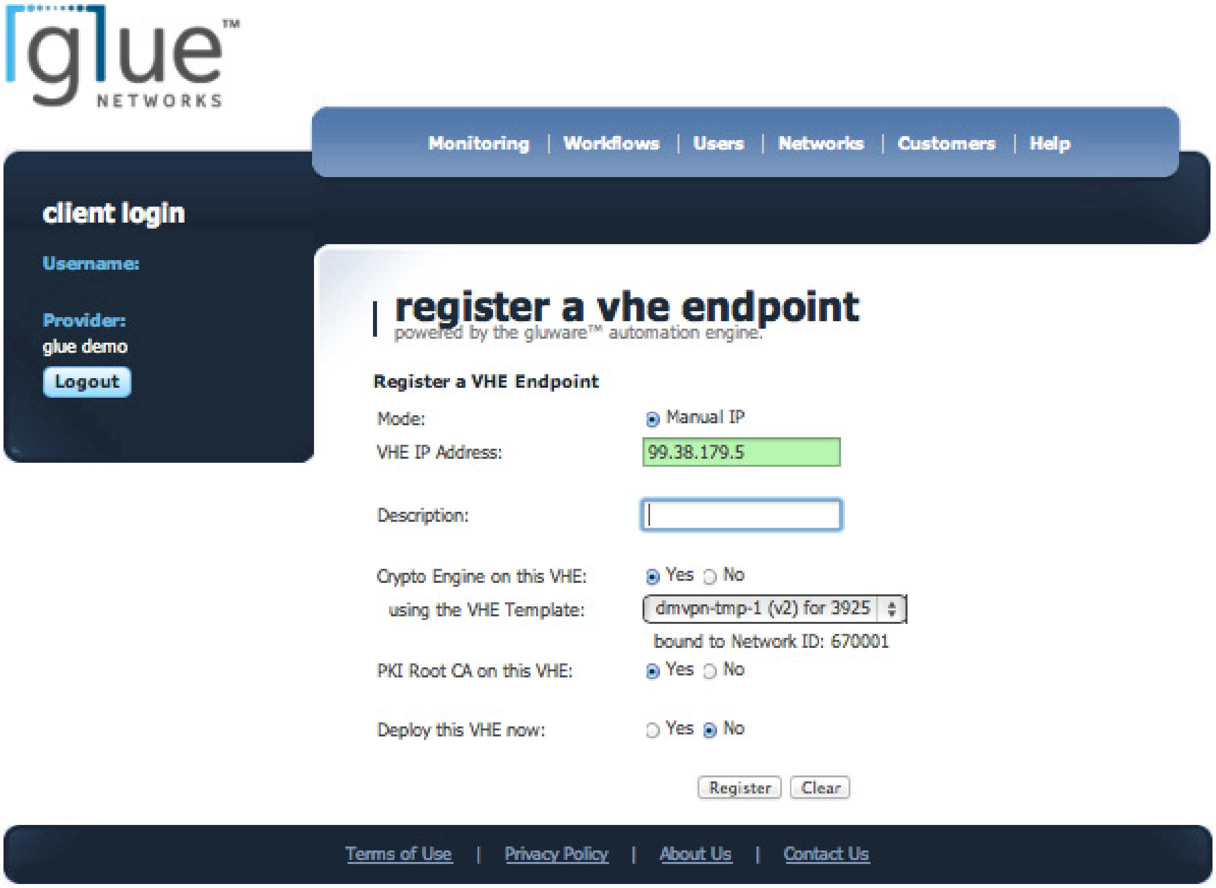
Secondary PBR Next Hop:

**Step 5** Register the Public IP Address of the VHE

The last step is to deploy the VHE. To deploy the VHE, register the device and assign the site identifier to the physical resource.

From the main menu, go to **Networks > Manage VPN Head-Ends > Manage VHE Endpoints > Register a VHE**. Register the public IP address of the VHE and apply the previously created VHE template as shown in Figure 9. Then the router is completely configured.

***Figure 9*** ***Register a VHE Endpoint***



glue™ NETWORKS
Monitoring | Workflows | Users | Networks | Customers | Help
client login
Username:
Logout
Register
Clear
Terms of Use | Privacy Policy | About Us | Contact Us

Provider: glue demo

register a vhe endpoint

powered by the gluware™ automation engine.

**Register a VHE Endpoint**

| | |
|---|---|
| Mode: | ● Manual IP |
| VHE IP Address: | 99.38.179.5 |
| Description: | |
| Crypto Engine on this VHE: | ● Yes ○ No |
| using the VHE Template: | dmvpn-tmp-1 (v2) for 3925<br>bound to Network ID: 670001 |
| PKI Root CA on this VHE: | ● Yes ○ No |
| Deploy this VHE now: | ○ Yes ● No |

## Deploying NGWAN CPEs Using the Gluware Engine

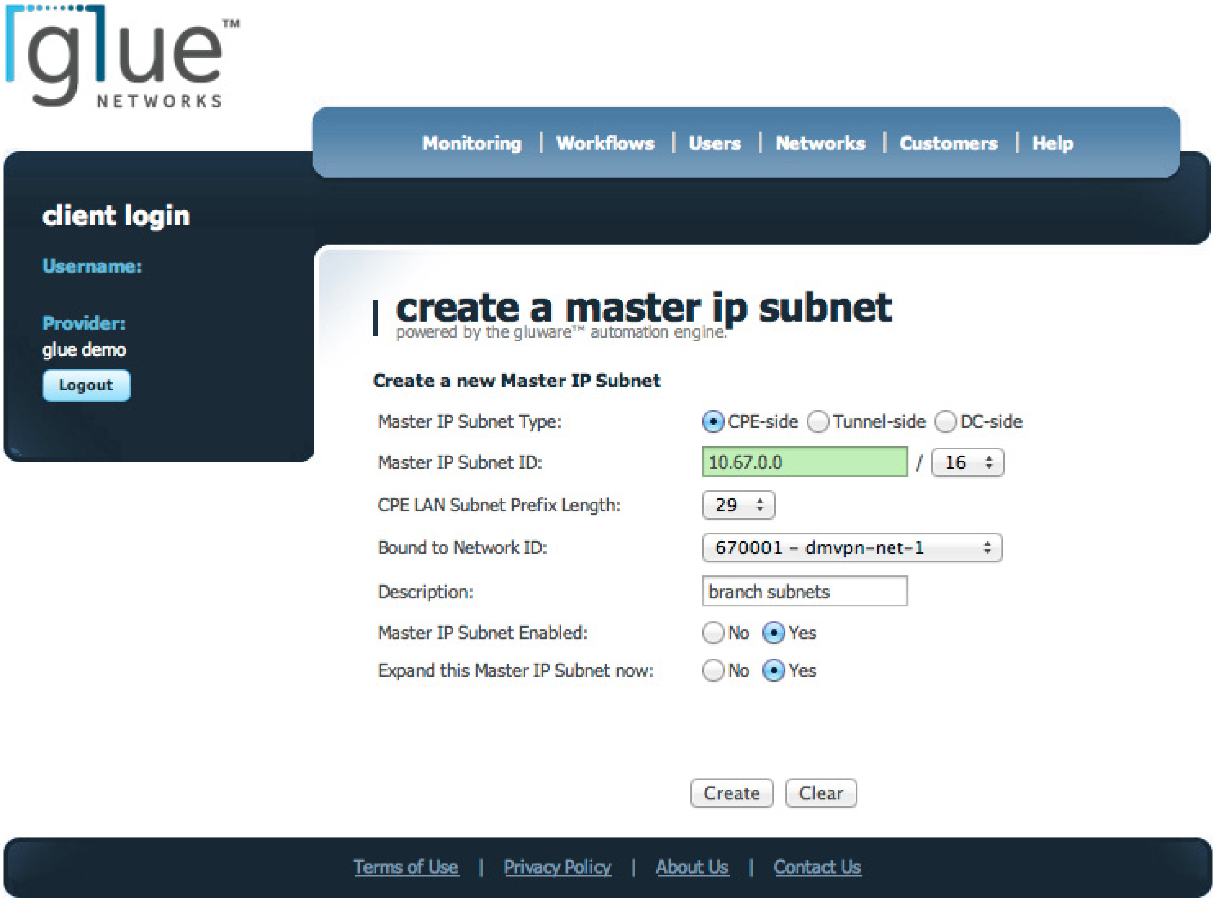
Now that the VHE has been deployed, CPEs must be associated with the network ID so that branch routers can join the DMVPN network.

**Step 1** Create Master IP Subnet

The master IP subnet is a pool of addresses (a resource) that is available to deploy LANs at remote branches.

From the main menu, go to **Networks > Manage Master IP Subnets > Add Master IP Subnet**. Allocate a supernet (pool of subnets) that is large enough to accommodate the internal networks required across all the branch networks as shown in Figure 10.

***Figure 10*** ***Create a Master IP Subnet***


glue™ NETWORKS
Monitoring | Workflows | Users | Networks | Customers | Help
Logout
Create
Clear
Terms of Use | Privacy Policy | About Us | Contact Us

client login

Username:

Provider:
glue demo

create a master ip subnet
powered by the gluware™ automation engine.

**Create a new Master IP Subnet**

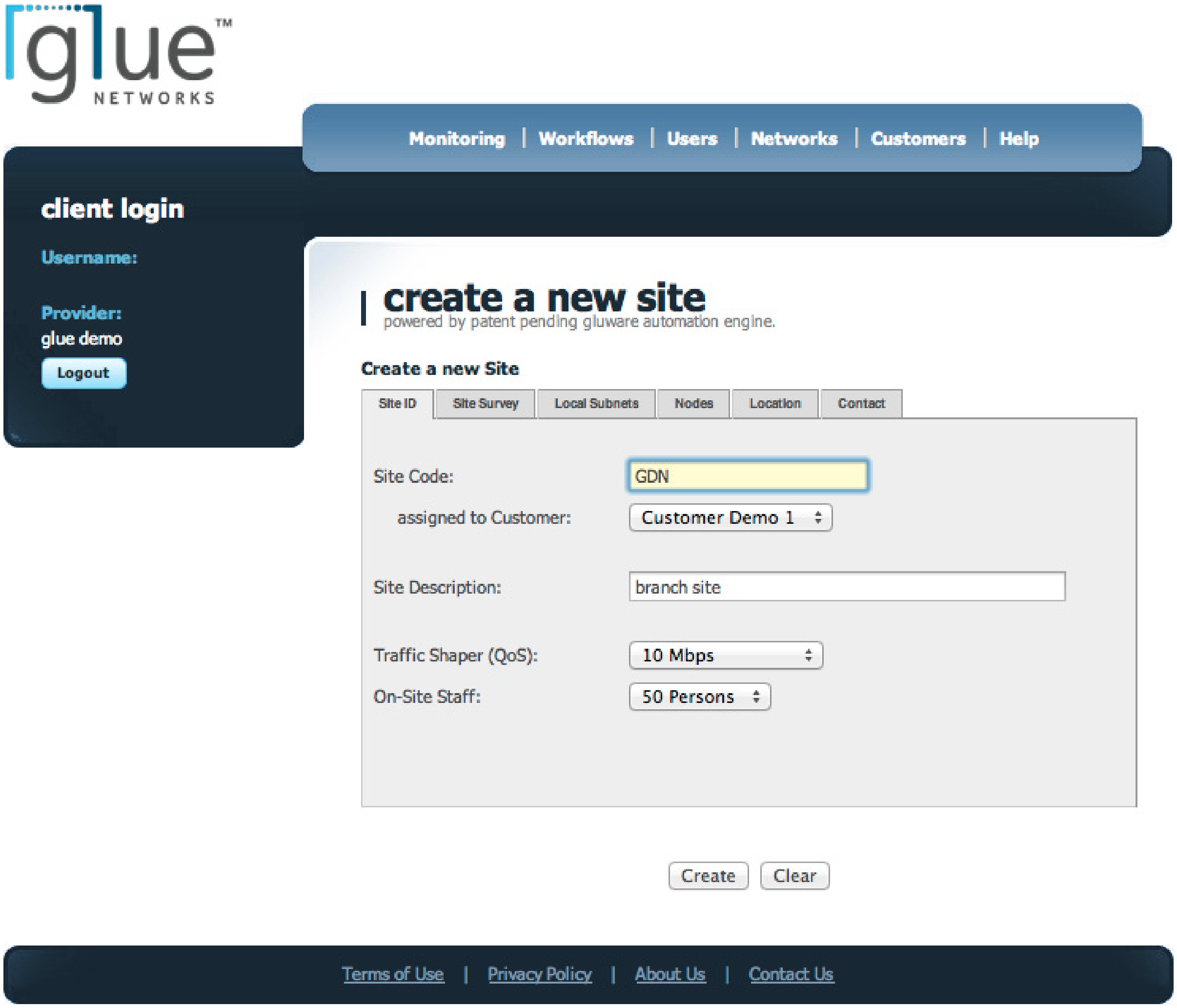
| | |
|---|---|
| Master IP Subnet Type: | ● CPE-side ○ Tunnel-side ○ DC-side |
| Master IP Subnet ID: | 10.67.0.0 / 16 |
| CPE LAN Subnet Prefix Length: | 29 |
| Bound to Network ID: | 670001 - dmvpn-net-1 |
| Description: | branch subnets |
| Master IP Subnet Enabled: | ○ No ● Yes |
| Expand this Master IP Subnet now: | ○ No ● Yes |

**Step 2** Create a New Site

Create a site and attach it to the previously configured DMVPN network ID.

From the main menu, go to **Networks > Manage Remote Locations > Manage Sites > Create a New Site**. Enter a 3-letter site identifier and configure the site-specific configurations (LAN side) as required as shown in Figure 11. The site configuration supports First Hop Redundancy Protocols (such as HSRP) for flat VLAN topologies as well as routing protocols to support multiple routing hops at a site as shown in Figure 12 on page 19.

***Figure 11*** ***Create a New Site***


glue™ NETWORKS
Monitoring | Workflows | Users | Networks | Customers | Help
client login
Username:
Provider:
glue demo
Logout
create a new site
powered by patent pending gluware automation engine.
Create a new Site
Site ID
Site Survey
Local Subnets
Nodes
Location
Contact
Create
Clear
Terms of Use | Privacy Policy | About Us | Contact Us

Site Code: GDN

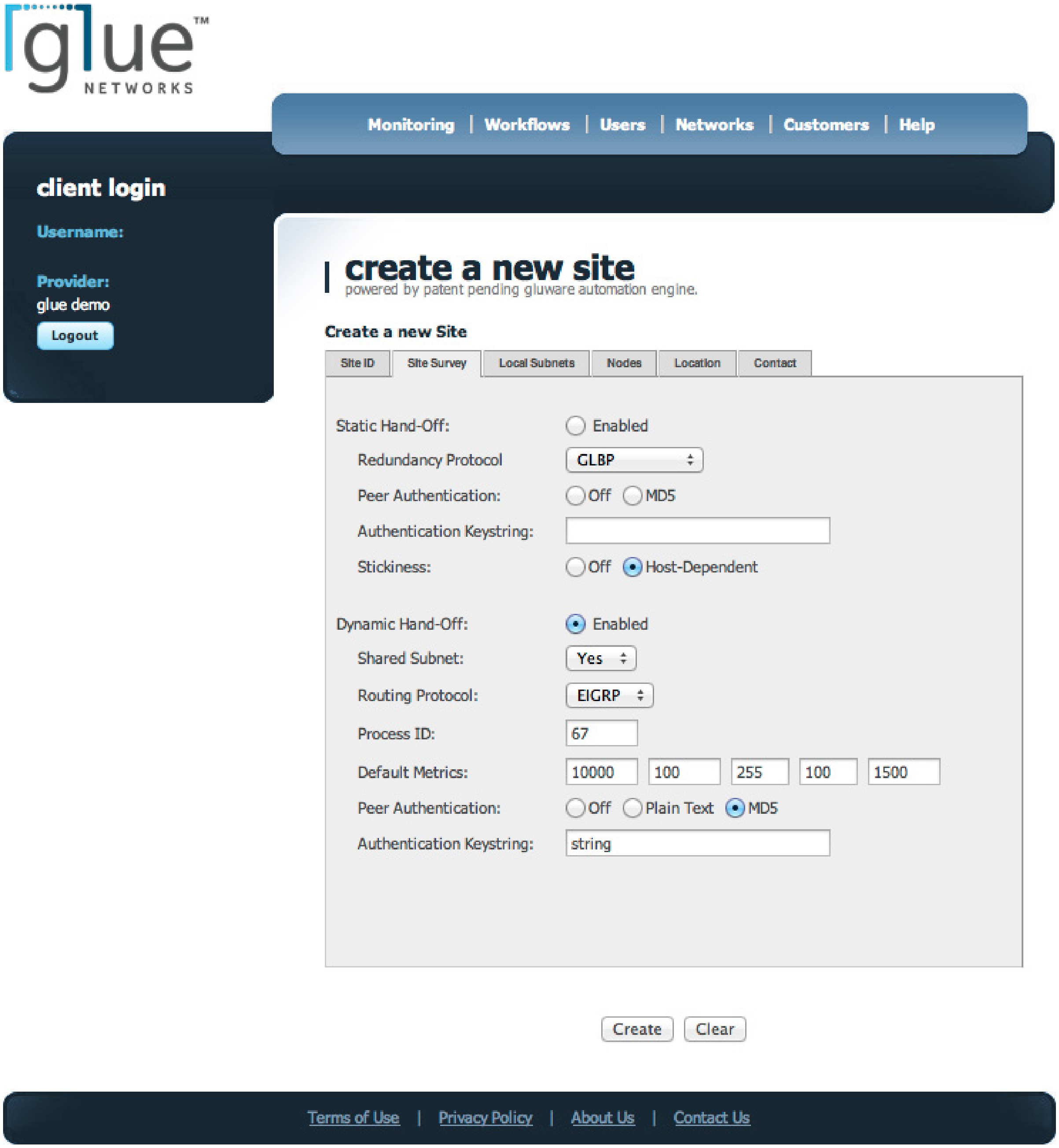
assigned to Customer: Customer Demo 1

Site Description: branch site

Traffic Shaper (QoS): 10 Mbps

On-Site Staff: 50 Persons

*Figure 12 Create a New Site – LAN Handoff*



glue NETWORKS
Monitoring | Workflows | Users | Networks | Customers | Help
client login
Username:
Provider:
glue demo
Logout
create a new site
powered by patent pending gluware automation engine.
Site ID
Site Survey
Local Subnets
Nodes
Location
Contact
Create
Clear
Terms of Use | Privacy Policy | About Us | Contact Us

Create a new Site

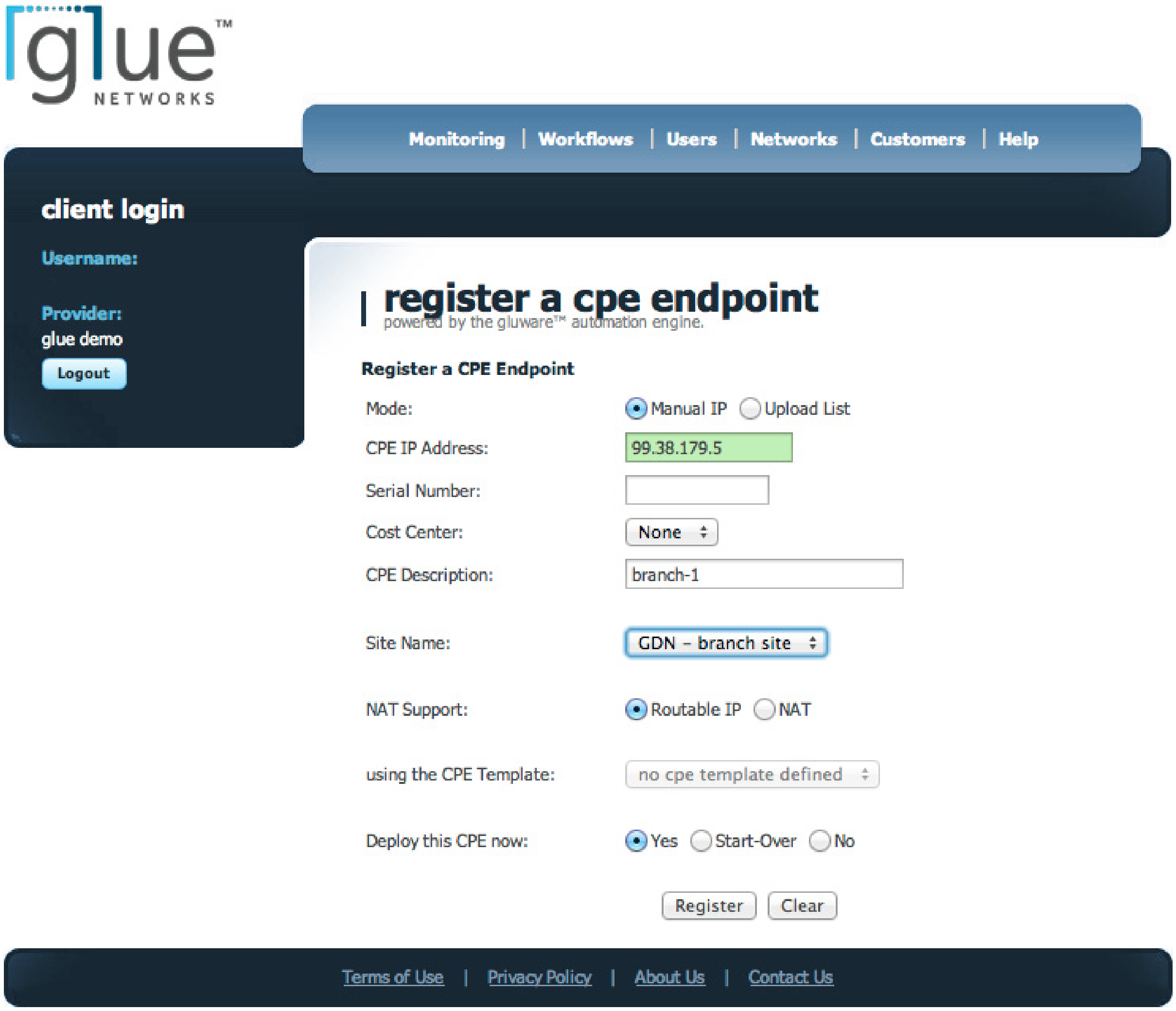
|  |  |
|---|---|
| Static Hand-Off: | ○ Enabled |
| Redundancy Protocol | GLBP |
| Peer Authentication: | ○ Off ○ MD5 |
| Authentication Keystring: | |
| Stickiness: | ○ Off ● Host-Dependent |
| Dynamic Hand-Off: | ● Enabled |
| Shared Subnet: | Yes |
| Routing Protocol: | EIGRP |
| Process ID: | 67 |
| Default Metrics: | 10000 100 255 100 1500 |
| Peer Authentication: | ○ Off ○ Plain Text ● MD5 |
| Authentication Keystring: | string |

**Step 3** Register a CPE Endpoint

The last step in the process is to register a physical device to the site and deploy the router with the required configurations.

From the main menu, go to **Networks > Manage Remote Locations > Manage CPE Endpoints > Register a CPE**. Configure the public IP address of the branch router and associate the site identifier as shown in Figure 13. Then the router is deployed and integrated into the DMVPN network.

***Figure 13 Register a CPE Endpoint***


glue™ NETWORKS
Monitoring | Workflows | Users | Networks | Customers | Help
client login
Username:
Provider:
glue demo
Logout
register a cpe endpoint
powered by the gluware™ automation engine.
Register
Clear
Terms of Use | Privacy Policy | About Us | Contact Us

**Register a CPE Endpoint**

|   |   |
|---|---|
| Mode: | ● Manual IP ○ Upload List |
| CPE IP Address: | 99.38.179.5 |
| Serial Number: | |
| Cost Center: | None |
| CPE Description: | branch-1 |
| Site Name: | GDN – branch site |
| NAT Support: | ● Routable IP ○ NAT |
| using the CPE Template: | no cpe template defined |
| Deploy this CPE now: | ● Yes ○ Start-Over ○ No |

# Operating a Network Defined by the Gluware Engine

The Gluware automation engine enables enterprises to unlock the full feature set available on Cisco networking hardware. Services that can be provisioned by the Gluware engine are discussed in the next section. For example, transport services provide enhanced features for packet forwarding. Security services support the ability of the enterprise to extend the network edge to remote locations.

The Gluware engine provides full lifecycle management for NGWAN deployments. Service provisioning, security, and change management are key components of delivering consistent, always-available services. Monitoring and troubleshooting network issues are integral parts of the Gluware change management feature set.

## Provisioning Services

Cisco routers are feature-rich platforms that offer many network-based features. Many organizations purchase these platforms, but do not deploy all the services available to them in an effort to keep the configuration simple.

The Gluware automation engine is designed to simplify the deployment of router features and allow scalable, consistent configurations across networks aligned with the Cisco NGWAN architecture.

### Network Transport Services

Cisco routers offer many options for providing WAN and LAN connectivity. Whether your enterprise needs to terminate private circuits, support MPLS VPN endpoints, or leverage broadband circuits for cost savings, the Gluware engine provides a scalable, simple solution to manage network infrastructure easily.

### Private Circuit / MPLS VPN

The Gluware automation engine can support routers as endpoints on both private circuits and MPLS VPN connections. Common routing protocols (such as BGP) can be leveraged to allow routers to communicate across the WAN. The Gluware engine supports MPLS VPN when the router is used as a Customer Edge (CE) functional node.

### Dynamic Multipoint Virtual Private Network

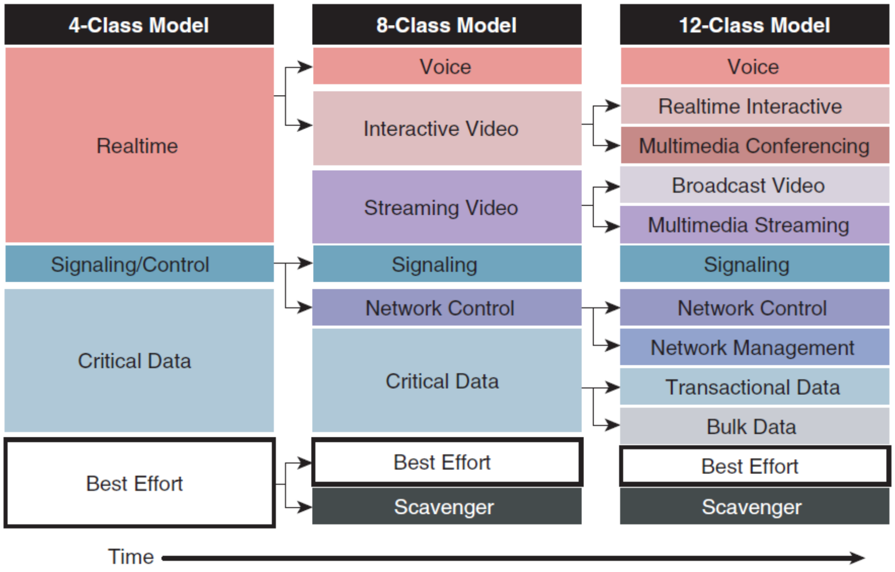
DMVPN is a Cisco IOS Software solution for building scalable IPsec virtual private networks (VPNs). DMVPN allows branch locations to communicate directly with each other over the public WAN (Internet) and reduces latency and jitter. At the same time, DMVPN optimizes head office bandwidth utilization. This technology is particularly useful for applications that require delivery of voice and video content or when performance routing overlays are leveraged as a cost-saving measure.

The Gluware automation engine reduces the complexity of deploying DMVPN by enabling zero-touch deployment and integration of sites into the wider WAN infrastructure. The Gluware engine can also load-balance traffic across VHEs, which provides a significant savings over traditional load-balanced solutions.

## Quality of Service

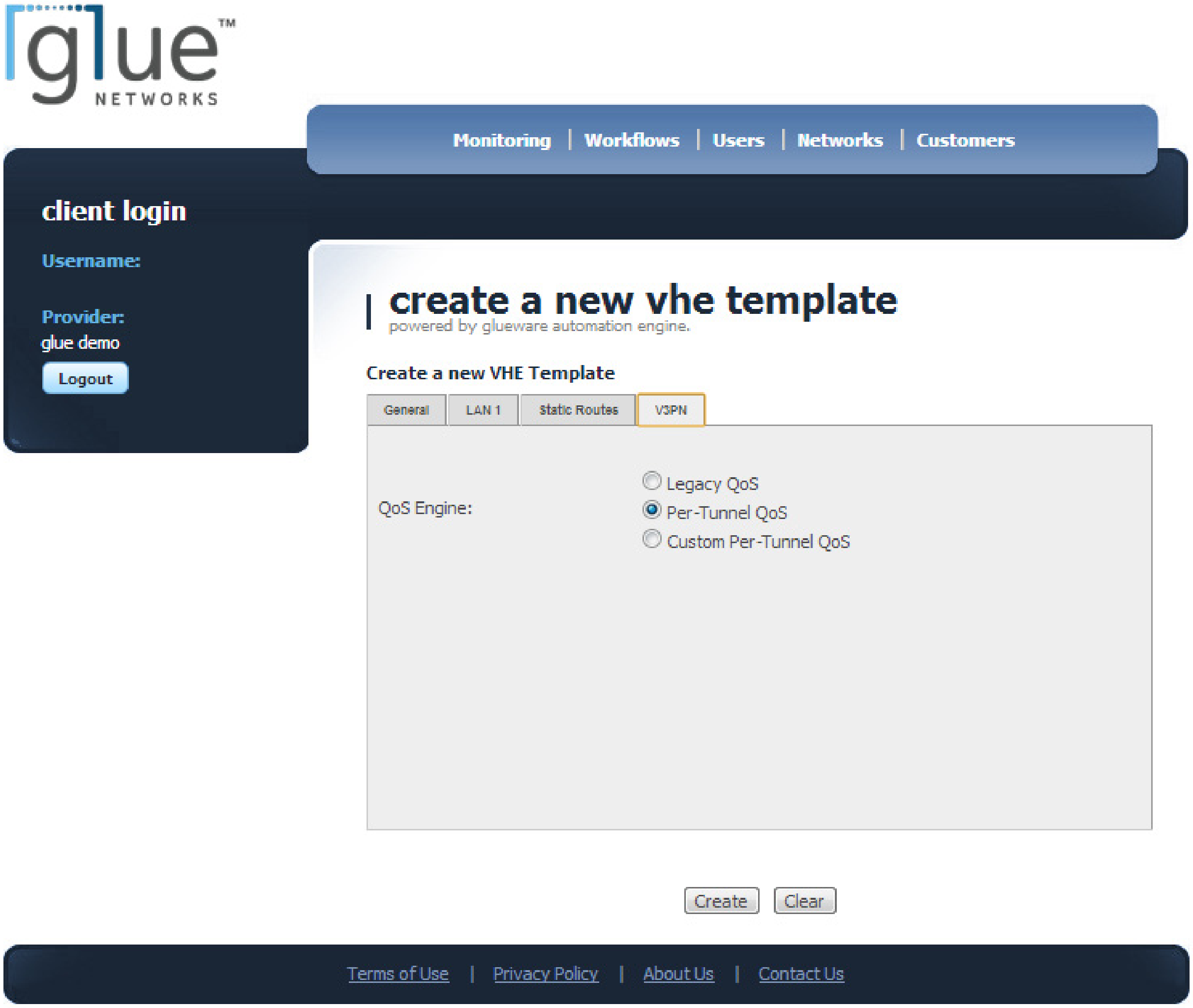
The Gluware automation engine provides full support of the RFC 4594 Medianet quality of service (QoS) framework. As the traffic mix on networks has evolved, the complexity of the QoS framework to support these diverse traffic types has also evolved. Traditional QoS models have leveraged four traffic classes to deliver services. Networks now require 8- and 12-class models to support the increase in types of network services as shown in Figure 14. The Gluware engine automates the deployment of these complex models over a large variety of Cisco platforms.

***Figure 14 QoS Model Evolution***



The Gluware engine can be used to configure QoS for VHE and CPE devices through the use of its template and site creation functions. Step 4 in Deploying a NGWAN VHE Using the Gluware Engine, page 11 outlines how to configure a VHE template. While you configure a VHE template, click the V3PN tab to set the QoS for the VHE as shown in Figure 15. (V3PN is Voice and Video Enabled IPsec VPN.)

***Figure 15 Create a VHE Template – V3PN QoS Settings***



Username:

Provider:
glue demo

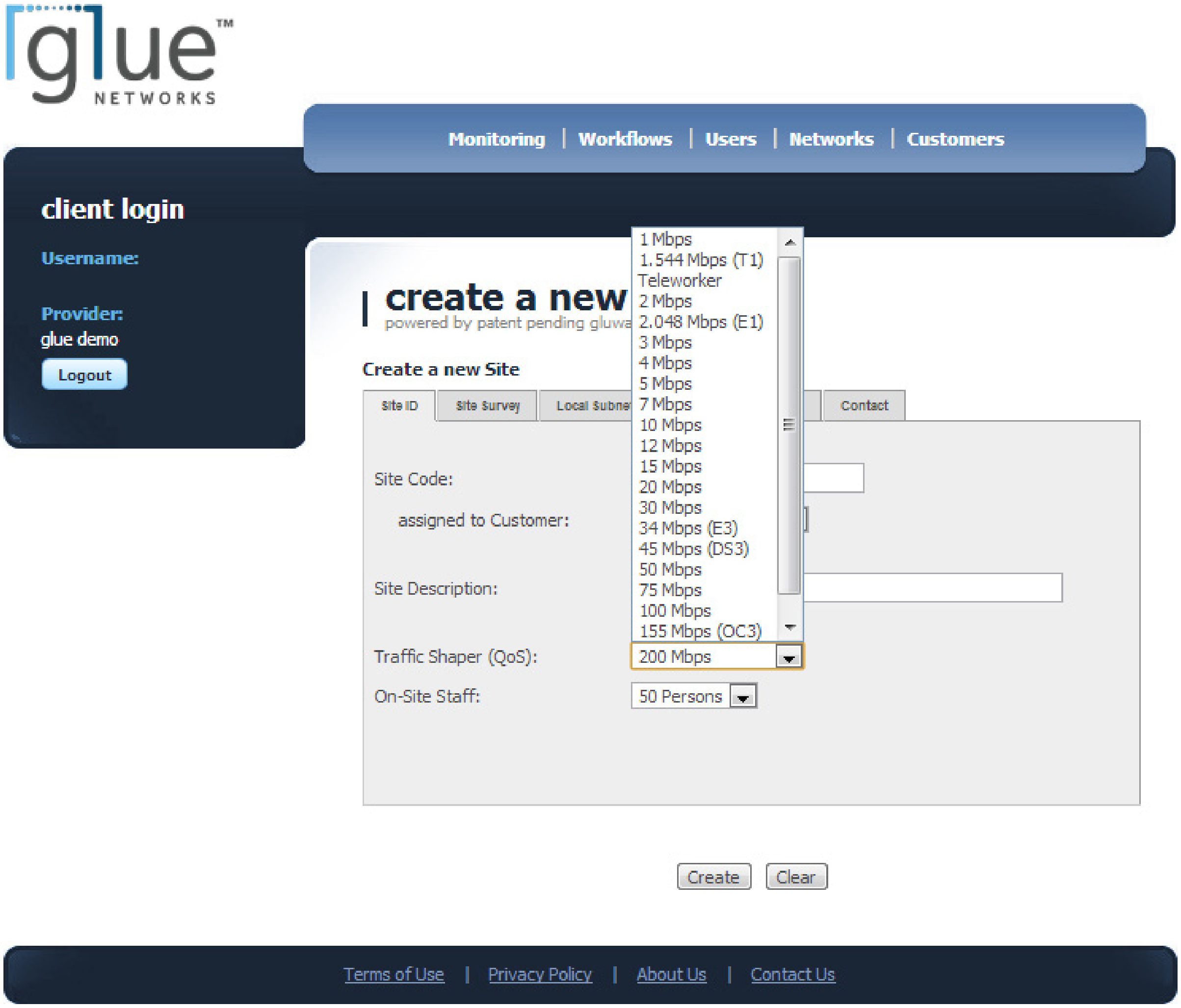
create a new vhe template
powered by glueware automation engine.

Create a new VHE Template

QoS Engine:
○ Legacy QoS
● Per-Tunnel QoS
○ Custom Per-Tunnel QoS

To configure QoS for the branch site and CPEs, you can use the site creation function. Step 2 in Deploying NGWAN CPEs Using the Gluware Engine, page 17 outlines how to create a site. Click the Traffic Shaper (QoS) option to set the QoS for the site between 1 Mbps and 200 Mbps as shown in Figure 16.

*Figure 16 Create a New Site – Traffic Shaper (QoS) Selection*



Traffic Shaper (QoS): 200 Mbps

On-Site Staff: 50 Persons

## Security Services

For highly distributed networks, the task of deploying and managing a consistent security policy across the organization is daunting. The level of effort that is needed to ensure that all devices in the infrastructure have a consistent policy can be burdensome when approached manually.

The Gluware automation engine allows enterprises to automate and orchestrate configurations across all of the managed devices, which greatly simplifies deployment. Architects and engineers can create a single design and deploy consistent configurations to each location without variance. The Gluware engine significantly increases the architectural integrity of the deployment and improves the security of the enterprise.

## PKI Management

Public key infrastructure (PKI) is an important component to provide secured communications across a WAN. PKI removes some of the vulnerabilities associated with older methods of encryption that left the enterprise open to security threats. Without PKI, static pre-shared keys must be used, which expose the enterprise to identity theft, eavesdropping, and man-in-the-middle attacks.

However, PKI is not without challenges. Many of the steps to distribute and verify certificates are manual and require human intervention. The Gluware engine establishes and manages the PKI certificate lifecycle, which automates a previously manual processes and increases security.

## Edge Security (802.1x)

Edge security allows the enterprise to control admission to their networks. Network access control is particularly important when the enterprise does not have physical control of their network edge, as in a home teleworker deployment.

The Gluware automation engine can configure network access control to authenticate devices from branch or teleworker locations before they access the corporate network. The engine authenticates users with web-based authentication-proxy capability or via the 802.1x protocol with device certificates.

## Intrusion Prevention Systems

While it is common practice to deploy intrusion prevention systems (IPSs) at the data center or central office, network-based attacks can come from anywhere. Blocking such malicious traffic at the branch and teleworker location is critical.

The Gluware engine enables the automated deployment of the Cisco IOS feature set using a scalable, consistent methodology. The deployment of this comprehensive threat protection capability increases network availability and reduces the time needed to remediate a security breach. When the capability is deployed as close to the source of the attack as possible, the effort needed to identify the attack source in forensic analysis is reduced significantly.

## Firewalling

Using Cisco IOS firewall helps ensure network availability and security by protecting the network infrastructure against attacks from the Internet. The router may be leveraged for firewall services at the branch to reduce costs by reducing the need for additional equipment.

The Gluware engine automates the provisioning and ongoing management of firewall services on routers. MACDs are all orchestrated by the Gluware automation engine. Granular policy control is often a requirement to meet regulatory requirements such as Payment Card Industry (PCI), Health Insurance Portability Act (HIPPA), and Sarbanes-Oxley (SOX). The router management that the Gluware engine provides is a key enabler of meeting these requirements cost effectively.

### Web Security (Cisco Cloud Web Security)

Cisco ISR web security with Cisco Cloud Web Security allows enterprises to intelligently redirect web traffic through a cloud-based policy engine that can protect branch networks from Trojan horses, back doors, rogue scanners, viruses and worms.

The Gluware engine automates the deployment of Cisco Cloud Web Security on branch and teleworker routers, which avoids the need to backhaul traffic through a central site for servicing. This distributed approach to web security increases performance while centralized policy control is maintained.

## Infrastructure Monitoring and Troubleshooting

Understanding the status of the network and quickly and efficiently identifying problems are critical to successful operations. The Gluware automation engine monitors network availability and provides features for inventory management and network troubleshooting.

### Change Management

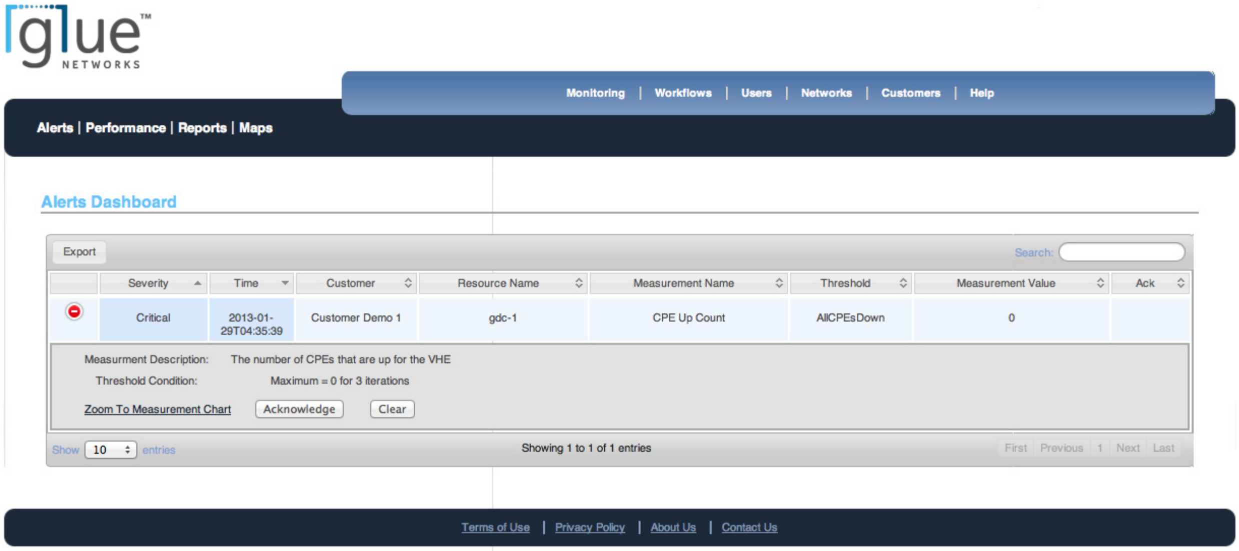
Change management is a key component of operating the network. Configuration changes and hardware and software inventory changes are driven by technology advances and changing business requirements. The Gluware automation engine can support virtually any change-control process. MACDs can be scheduled for all or a subset of managed devices. Day-to-day support events often drive out-of-process changes to routers. The Gluware engine identifies and reports these types of events, and reconciles the Gluware configuration database with out-of-process changes.

Devices can be upgraded with additional interface cards or other accessories, such as VPN accelerator cards. The Gluware automation engine monitors devices under management and reports all hardware changes so that device inventory data is relevant and up-to-date. Device firmware can also be changed or varied from the desired standard. The Gluware alerts dashboard notifies administrators about nonstandard firmware deployments and changes to firmware on managed devices.

## Monitoring and Troubleshooting

The monitoring service that the Gluware automation engine provides proactively monitors the availability and performance of the routers as shown in Figure 17 and Figure 18 on page 28, respectively. SNMP data is collected from each device and is summarized. Network status is monitored in real time through a simple dashboard. Network status can be viewed on an interactive map for continuous tracking of router status as shown in Figure 19.

*Figure 17* *Monitoring – Alerts Dashboard*


glue NETWORKS
Monitoring | Workflows | Users | Networks | Customers | Help
Alerts | Performance | Reports | Maps
Alerts Dashboard
Export
Search:
Zoom To Measurement Chart
Acknowledge
Clear
First Previous 1 Next Last
Terms of Use | Privacy Policy | About Us | Contact Us

| | Severity | Time | Customer | Resource Name | Measurement Name | Threshold | Measurement Value | Ack |
|---|---|---|---|---|---|---|---|---|
| ⊖ | Critical | 2013-01-29T04:35:39 | Customer Demo 1 | gdc-1 | CPE Up Count | AllCPEsDown | 0 | |

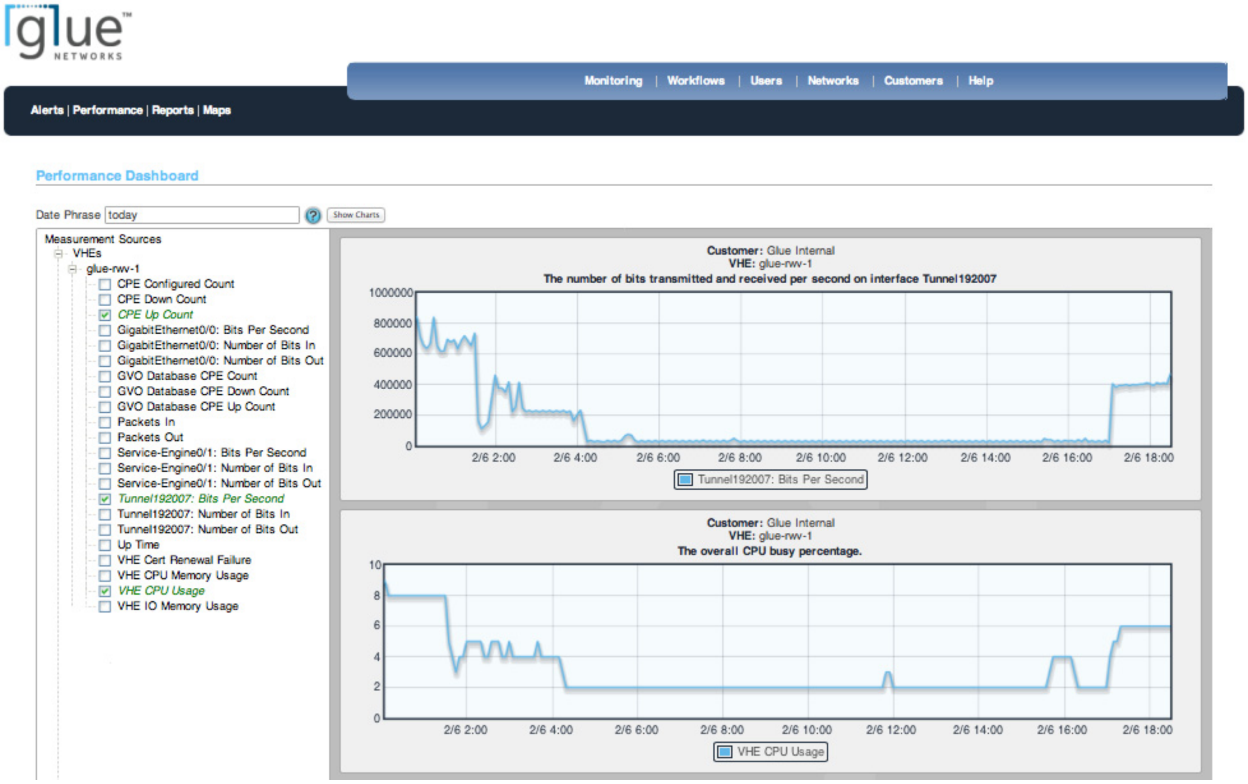
Measurment Description: The number of CPEs that are up for the VHE

Threshold Condition: Maximum = 0 for 3 iterations

Show 10 entries

Showing 1 to 1 of 1 entries

## *Figure 18 Monitoring – Device Statistics*



Performance Dashboard

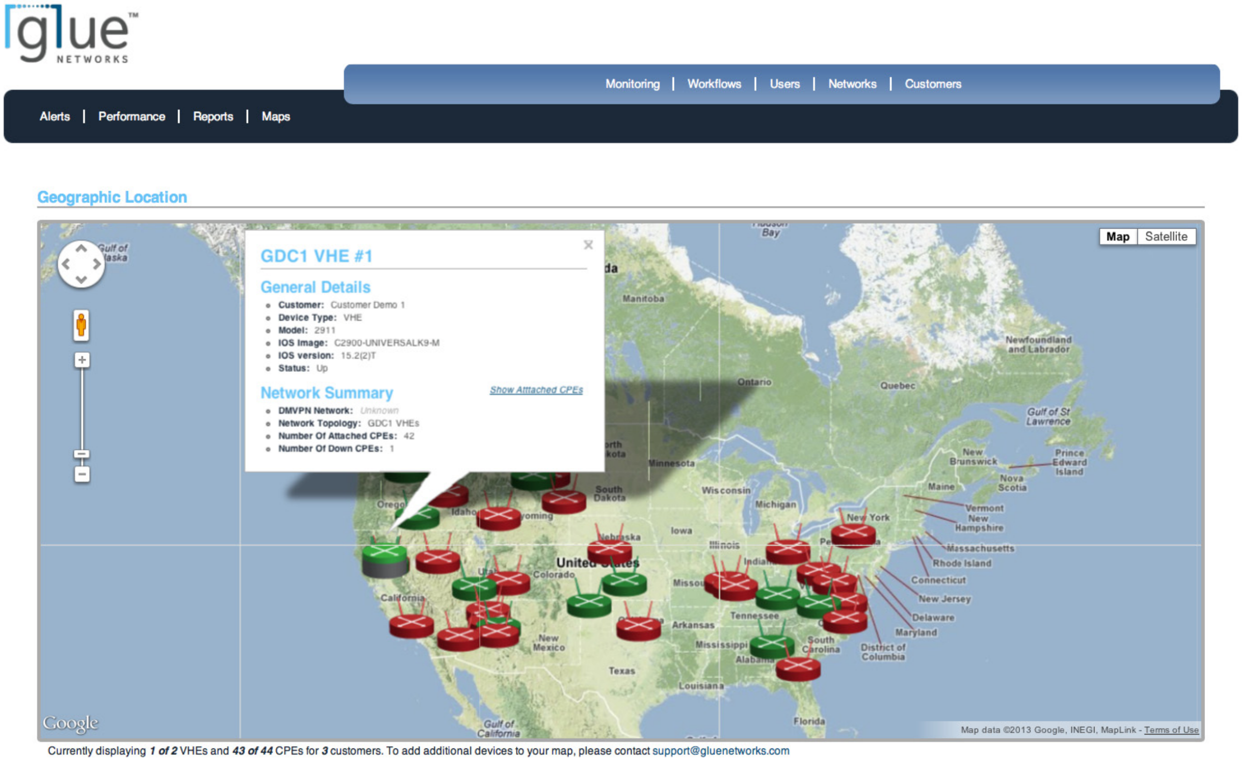
Date Phrase today

Measurement Sources
- VHEs
  - glue-rwv-1
    - □ CPE Configured Count
    - □ CPE Down Count
    - ☑ CPE Up Count
    - □ GigabitEthernet0/0: Bits Per Second
    - □ GigabitEthernet0/0: Number of Bits In
    - □ GigabitEthernet0/0: Number of Bits Out
    - □ GVO Database CPE Count
    - □ GVO Database CPE Down Count
    - □ GVO Database CPE Up Count
    - □ Packets In
    - □ Packets Out
    - □ Service-Engine0/1: Bits Per Second
    - □ Service-Engine0/1: Number of Bits In
    - □ Service-Engine0/1: Number of Bits Out
    - ☑ Tunnel192007: Bits Per Second
    - □ Tunnel192007: Number of Bits In
    - □ Tunnel192007: Number of Bits Out
    - □ Up Time
    - □ VHE Cert Renewal Failure
    - □ VHE CPU Memory Usage
    - ☑ VHE CPU Usage
    - □ VHE IO Memory Usage

**Customer:** Glue Internal
**VHE:** glue-rwv-1
**The number of bits transmitted and received per second on interface Tunnel192007**

**Customer:** Glue Internal
**VHE:** glue-rwv-1
**The overall CPU busy percentage.**

## *Figure 19 Interactive Maps*



Geographic Location

**GDC1 VHE #1**

**General Details**
- **Customer:** Customer Demo 1
- **Device Type:** VHE
- **Model:** 2911
- **IOS Image:** C2900-UNIVERSALK9-M
- **IOS version:** 15.2(2)T
- **Status:** Up

**Network Summary** Show Atttached CPEs
- **DMVPN Network:** Unknown
- **Network Topology:** GDC1 VHEs
- **Number Of Attached CPEs:** 42
- **Number Of Down CPEs:** 1

Currently displaying *1 of 2* VHEs and *43 of 44* CPEs for *3* customers. To add additional devices to your map, please contact support@gluenetworks.com

# Conclusion

The Glue Networks Gluware automation engine automates the deployment and management of networks. Automation accelerates time to value, which reduces cost and complexity and improves productivity. The Gluware engine allows IT organizations to implement design standards so that the network is deployed in a consistent and reliable way. The Gluware engine builds, monitors, and maintains highly complex network functionality with efficiency and precision. The Gluware engine brings agility and stability to enterprise networks and enables enterprises to take full advantage of the advanced feature sets on Cisco routers.

# For More Information

Read more about the Cisco Next-Generation Enterprise WAN at http://www.cisco.com/en/US/netsol/ns816/networking_solutions_program_home.html or contact your local account representative.

Read more about Glue Networks and the Gluware engine at http://www.gluenetworks.com/company/contact-us (Phone: 916-877-8224).