Chantry BeaconWorks User Guide

Chantry's next generation of wireless networking devices provide a truly scalable WLAN solution. Chantry's BeaconPoints are thin access points that are controlled through a sophisticated network device, the BeaconMaster. This solution provides the security and manageability required by enterprises and service providers alike.

BeaconMaster

BeaconPoint

BeaconWorks Release 2.0

In this document

The Chantry BeaconWorks Solution 4
What is the Chantry BeaconWorks System? 4
Conventional Wireless LANS 4
The Chantry BeaconWorks Solution 5
BeaconWorks and Your Enterprise Network 8
Network traffic flow in the BeaconWorks System 8
Network security 9
Interaction with Wired Networks: Virtual Network Services 10
Static Routing and Routing Protocols 10
Policy: Packet Filtering 10
Mobility and Roaming 11
Availability 11
BeaconWorks Release 2.0 Features: Overview 12
Backwards compatibility with Release 1.1 on the BeaconPoint 12
Backwards compatibility with Release 1.1 on the BeaconMaster 12
Multi-SSID: BeaconPoint radios on more than one VNS 12
Privacy using Wi-Fi Protected Access (WPA) 13
BeaconPoint software: Dual image capability 13
BeaconPoint software: Dynamic reconfiguration (without reboot) 13
BeaconPoint Statistics 13
Event reporting using Syslog 13
Capacity for Redundant RADIUS servers 14
Detection of Rogue APs 14
Quality of Service (QoS) on a VNS: Spectralink Voice Protocol (SVP) 14
BeaconPoint static configuration: Branch Office, Phase 1 14
BeaconMaster: Startup 15
BeaconMaster Features and Installation 15
First-Time Setup of BeaconMaster 16
Management Port First-Time Set Up 16
The Graphical User Interface (GUI): Overview 20
BeaconWorks Configuration Steps: Overview 22
BeaconWorks Configuration: Data Port and Routing Setup 23
Setting Up the Data Ports 23
Port Type or Function 24
Port-Level Filtering of Unauthorized Traffic 25
Setting up Static Routes 26
Setting up OSPF Routing 27
BeaconPoint: Startup 30
BeaconPoint (BP200) Features 30
Installing the BeaconPoints 32
BeaconPoint: Registering 33
Setting Parameters for BeaconPoint Registration 33
Discovery and Registration: The DHCP and SLP Solution 34
The BeaconPoint's Discovery Process and LED Sequence 35
BeaconPoint: Configuring Properties and Radios 36
BeaconPoint: Adding Manually 40
BeaconPoint Radios on a VNS 41
BeaconPoint Static Configuration: Branch Office Deployment 41
Virtual Network Services (VNS): Overview 43
What is a VNS? 44
Topology of a VNS: Overview 44
Multi-SSID: BeaconPoint radios on more than one VNS 45
Other network parameters for the VNS topology 45
Network Assignment and Authentication for a VNS 45
RADIUS Server: Location and Redundancy 46
Filtering for a VNS: How it works 46
Privacy on a VNS: Overview of WEP and WPA 47
Setting up a new VNS 48

Virtual Network Configuration: A VNS for Captive Portal 50
Topology for a VNS for Captive Portal 50
Authentication for a VNS for Captive Portal 53
Filtering Rules for a VNS for Captive Portal 57
The Non-Authenticated Filter 57
Privacy using WEP for a VNS for Captive Portal 59
Virtual Network Configuration: A VNS with No Authentication 61
Virtual Network Configuration: A VNS for Voice Traffic (QoS with SVP) 62
Voice Data Traffic on a Wireless Network: Overview..... 62
Setting up a VNS for Voice Traffic..... 62
Virtual Network Configuration: A VNS for AAA..... 65
Topology for a VNS for AAA..... 65
Authentication for a VNS for AAA..... 68
VNS Topology for an AAA group..... 71
Filtering Rules for a Filter ID group..... 72
Filtering Rules for a Default Filter 74
Filtering Rules for an AAA Group VNS..... 75
Filtering Rules between two wireless devices..... 76
Privacy for a VNS for AAA..... 76
Privacy for a VNS for AAA: WEP 76
Privacy for a VNS for AAA: Wi-Fi Protected Access (WPA) 77
BeaconMaster Configuration: Availability 80
BeaconMaster Configuration: Mobility and the VN Manager..... 85
BeaconMaster Configuration: Management Users..... 88
BeaconMaster Configuration: Network Time..... 89
Setting up Third-Party Access Points 90
BeaconKeeper Mitigator: Detecting Rogue Access Points..... 93
BeaconKeeper Mitigator: Overview..... 93
BeaconKeeper Mitigator: Enabling the Analysis and RFDC Engines ... 94
BeaconKeeper Mitigator: Running Scans 95
BeaconKeeper Mitigator: How the Analysis Engine works 97
BeaconKeeper Mitigator: Viewing the Scanner Status Report 100
Ongoing Operation: BeaconPoint Maintenance – Software..... 101
BeaconPoint software: Dynamic reconfiguration (without reboot) 101
BeaconPoint software: Dual image backup 101
Ongoing Operation: BeaconPoint Access Approval 104
Ongoing Operation: BeaconPoint Disassociate a Client 105
Ongoing Operation: BeaconMaster System Maintenance 106
Event Messages relayed to a Syslog server 107
Ongoing Operation: BeaconWorks Logs and Traces 109
Logs and Alarms..... 109
Traces..... 111
Audits..... 111
Ongoing Operation: BeaconWorks Reports and Displays..... 112
View Displays 112
View Statistics for BeaconPoints 113
View Reports 114
BeaconMaster Configuration: Setting up SNMP 115
Appendix 1: BeaconWorks System States and LEDs 118
Appendix 2: Glossary of Terms and Acronyms 120
Appendix 3: Index of Procedures, Screens and Figures 131

The Chantry BeaconWorks Solution

The BeaconWorks system is a highly scalable wireless local area network (WLAN) solution developed by Chantry Networks Inc. Based on a third generation WLAN topology, the BeaconWorks system makes wireless practical for medium and large-scale enterprises and for service providers.

The BeaconWorks system provides a secure, highly scalable, cost-effective solution based on the IEEE 802.11standard. The solution is intended for enterprise networks operating on many floors in more than one building, as well as in public environments such as airports and convention centers that require more than two access points.

This section provides an overview of the fundamental principles of the Chantry BeaconWorks system: what it is, how it works, and its advantages.

What is the Chantry BeaconWorks System?

The BeaconWorks system replaces the conventional access points used in wireless networking with two network devices that work as a system:

BeaconMaster A network device that provides smart centralized control over the elements (BeaconPoints) in the wireless network.

BeaconPoints The access points for 802.11 clients (wireless devices) in the network, controlled by the BeaconMaster. The BeaconPoint is a “thin access point” because its wireless control is handled by the BeaconMaster. The BeaconPoint (BP200 model) is a dual-band access point, with both 802.11a and 802.11b/g radios.

Together, the BeaconWorks products enable a radically simplified new approach to setting up, administering and maintaining a WLAN. BeaconWorks provides a Layer 3 IP routed WLAN architecture. This architecture can be implemented over several subnets without requiring the configuration of virtual local area networks (VLANs).

Conventional Wireless LANS

At its simplest, wireless communication between two or more computers requires that each one is equipped with a receiver/transmitter – a WLAN Network Interface Card (NIC) – capable of exchanging digital information over a common radio frequency. This is called an *ad hoc* configuration. An *ad hoc* network allows wireless devices to communicate together. This is an independent basic service set (IBSS).

An alternative to the ad hoc configuration is the use of an *access point*. This may be a dedicated hardware router or a computer running special software. Computers and other wireless devices communicate with each other through this access point. The 802.11 standard defines Access Point communications as devices that allow wireless devices to communicate with a “distribution system”. This is a basic service set (BSS) or infrastructure network.

For the wireless devices to communicate with computers on a wired network, the access points must be connected into the wired network, and provide access to the networked computers. This is called *bridging*. Clearly, there are security issues and management scalability issues in this arrangement.

Chantry Networks Inc. Copyright 2004. All rights reserved.

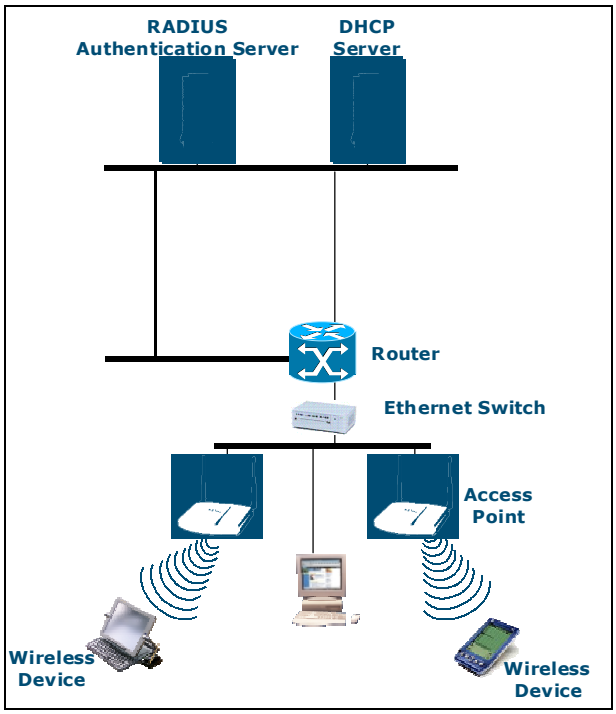


Figure 1: Standard wireless network solution

The wireless devices and the wired networks communicate with each other using standard networking protocols and addressing schemes. Most commonly, Internet Protocol (IP) addressing is used.

While this topology works well enough for small installations, as the network grows the difficulty of setting up and administering all the individual access points expands as well. When the expanding network has to cope with a large number of wireless users all signing on and off at random times, the complexity grows rapidly. Imagine, for example, a university library filled with professors and students – all equipped with laptops. Or a conference full of delegates and exhibitors.

Clearly, there must be a better way than setting up each access point individually.

The Chantry BeaconWorks Solution

The Chantry Networks BeaconWorks solution consists of two devices:

The **BeaconMaster** controller is a rack-mountable network device designed to be integrated into an existing wired Local Area Network (LAN). It provides centralized control over all access points (both BeaconPoints and third-party access points) and manages the network assignment of wireless device clients associating through access points.

The **BeaconPoint** is a wireless LAN *thin access point* (IEEE 802.11) provided with unique software that allows it to communicate only with a BeaconMaster. (A *thin access point* handles the radio frequency (RF) communication but relies on a controller to handle WLAN elements such as authentication.) The BeaconPoint also provides local processing such as encryption.

This architecture allows a single BeaconMaster to control many BeaconPoints, making the administration and management of large networks much easier.

Chantry Networks Inc. Copyright 2004. All rights reserved.

There can be several BeaconMasters in the network, each with its set of registered BeaconPoints. The BeaconMasters can also act as backups to each other, providing stable network availability.

In addition to the BeaconMasters and BeaconPoints, the solution requires two other components, which are standard for enterprise and service provider networks:

- **RADIUS Server** (Remote Access Dial-In User Service) (RFC2865 and RFC2866), or other authentication server. Assigns and manages ID and Password protection throughout the network. Used for authentication of the wireless users.
- **DHCP Server** (Dynamic Host Configuration Protocol) (RFC2131). Assigns IP addresses, gateways and subnet masks dynamically. Also used by the BeaconPoints to discover the location of the BeaconMaster during the initial registration process.

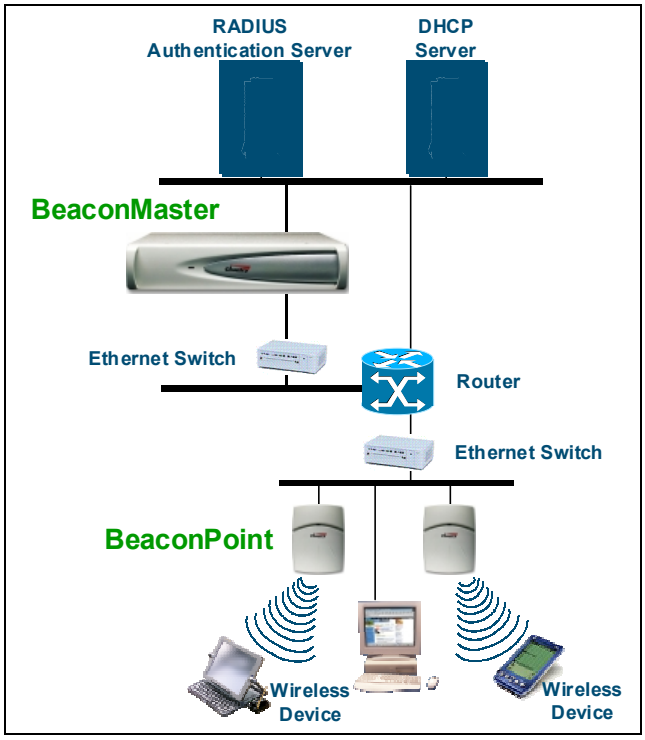


Figure 2: Chantry BeaconWorks Solution

The BeaconMaster appears to the existing network as if it were an access point, but in fact one BeaconMaster controls many BeaconPoints.

The BeaconMaster has built-in capabilities to recognize and manage the BeaconPoints. The BeaconMaster activates the BeaconPoints, enables them to receive wireless traffic from wireless devices, processes the data traffic from the BeaconPoints and forwards or routes that data traffic out to the network. This processing includes authenticating requests and applying access policies.

Simplifying the BeaconPoints make them:

- cost-effective
- easy to manage
- easy to deploy.

Chantry Networks Inc. Copyright 2004. All rights reserved.

Putting control on an intelligent centralized BeaconMaster enables:

- centralized configuration, management, reporting, maintenance
- high security
- flexibility to suit enterprise
- scalable and resilient deployments with a few BeaconMasters controlling hundreds of BeaconPoints.

Here are some of the BeaconWorks system advantages:

Scales up to Enterprise capacity	One BeaconMaster controls as many as 200 BeaconPoints. In turn each BeaconPoint can handle up to 254 wireless devices. With additional BeaconMasters, the number of wireless devices the Chantry system can support is in the thousands.
Integrates in existing network	A BeaconMaster can be added to an existing enterprise network as a new network device, greatly enhancing its capability without interfering with its existing functionality. Integration of the BeaconMasters and BeaconPoints does not require any reconfiguration of the existing infrastructure (e.g. VLANs).
Offers centralized management and control	An administrator accesses the BeaconMaster in its centralized location and uses its user interface to monitor and administer the entire wireless network. The BeaconMaster has functionality to recognize, configure and manage the BeaconPoints and distribute new software releases.
Provides easy deployment of BeaconPoints	The initial configuration of the BeaconPoints on the centralized BeaconMaster can be done with an automatic “discovery” technique.
Provides security via user authentication	BeaconWorks uses existing authentication (AAA) servers to authenticate and authorize users.
Provides security via filters and privileges	BeaconWorks uses virtual networking techniques to create separate virtual networks with defined authentication and billing services, as well as access policies and privileges.
Supports seamless mobility and roaming	BeaconWorks supports seamless roaming of a wireless device from one BeaconPoint to another on the same BeaconMaster or on a different BeaconMaster.
Integrates third-party access points	BeaconWorks can integrate legacy third-party access points, using a combination of network routing and authentication techniques.
Prevents rogue devices	Rogue devices will not be authenticated by the BeaconMaster, preventing unproved devices from masquerading as valid BeaconPoints.
Provides accounting services	The BeaconMaster has software to track and log wireless user sessions, user group activity, and other activity reporting, enabling the generation of consolidated billing records.
Offers troubleshooting capability	The BeaconMaster software logs system and session activity and provides reports to aid in troubleshooting analysis.

Chantry Networks Inc. Copyright 2004. All rights reserved.

BeaconWorks and Your Enterprise Network

Network traffic flow in the BeaconWorks System

The diagram below shows a simple configuration with a single BeaconMaster and two BeaconPoints, each supporting a wireless device. A RADIUS server on the network provides authentication, and a DHCP server is used by the BeaconPoints to discover the location of the BeaconMaster during the initial registration process. Also present in the network are routers and ethernet switches.

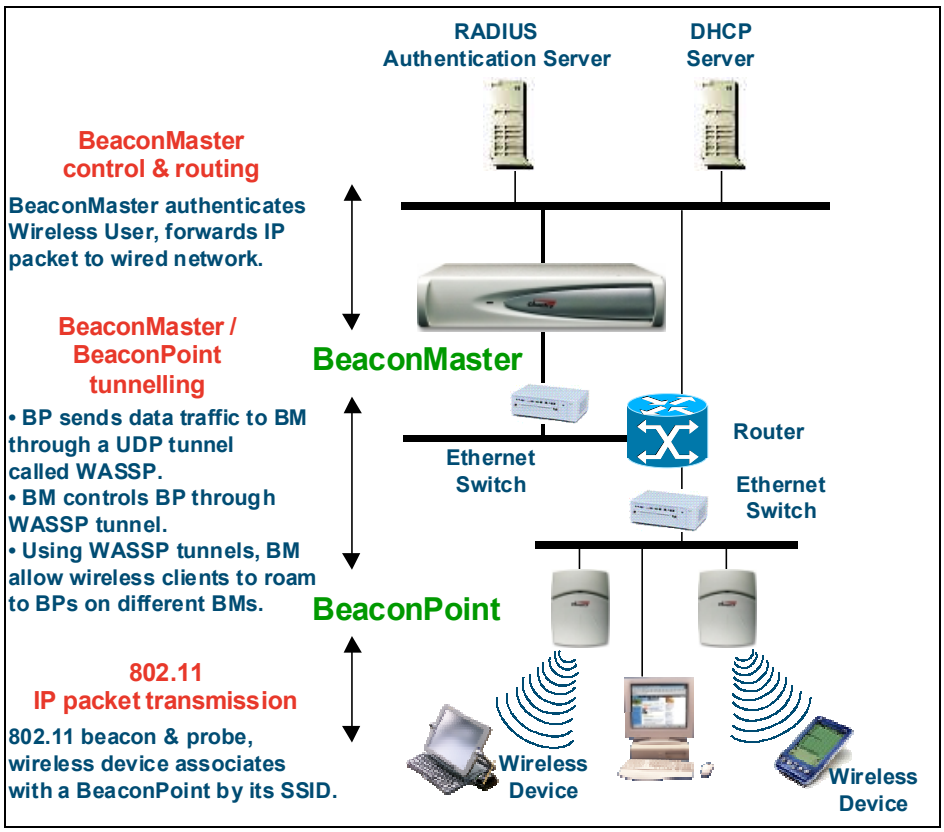


Figure 3: BeaconWorks Traffic Flow diagram

Each wireless device sends IP packets in the 802.11 standard to the BeaconPoint. The BeaconPoint uses a UDP (User Datagram Protocol) based tunnelling protocol called CAPWAP Tunnelling Protocol (CTP) to encapsulate the packets and forward them to the BeaconMaster.

Note: The CTP protocol defines a mechanism for the control and provisioning of wireless access points (CAPWAP) through centralized access controllers. In addition, it provides a mechanism providing the option to tunnel the mobile client data between the access point and the access controller.

The BeaconMaster decapsulates the packets, and routes these to destinations on the network, after authentication by the RADIUS server.

The BeaconMaster functions like a standard router, except that it is configured to route only between its ingress ports (incoming wireless device traffic via BeaconPoints) and egress ports (traffic out to the wired network). The BeaconMaster

can also be configured to simply forward traffic to a default or static route if dynamic routing is not preferred.

Network security

The Chantry BeaconWorks system provides features and functionality to control network access. These are based on standard wireless network security practices.

Current wireless network security methods provide a degree of protection. These methods include:

- Shared Key authentication, that relies on Wired Equivalent Privacy (WEP) keys
- Open System, that relies on Service Set Identifiers (SSIDs)
- 802.1x that is compliant with Wi-Fi Protected Access (WPA)
- Captive Portal based on Secure Sockets Layer (SSL) protocol

The Chantry BeaconWorks system supports these encryption approaches:

- Wired Equivalent Privacy (WEP), a security protocol for wireless local area networks defined in the 802.11b standard.
- Wi-Fi Protected Access (WPA) with Temporal Key Integrity Protocol (TKIP), also known as WPA version 1. (BeaconWorks Release 2.0)
- Advanced Encryption Standard (AES).

Authentication

The Chantry BeaconMaster relies on a RADIUS server, or authentication server, on the enterprise network to provide the authentication information (whether the user is to be allowed or denied access to the network).

The BeaconMaster provides authentication using:

- Captive Portal, a browser-based mechanism that forces users to a web page.
- RADIUS (using IEEE 802.1x)

The *802.1x mechanism* is a standard for authentication developed within the 802.11 standard. This mechanism is implemented at the port, blocking all data traffic between the wireless device and the network until authentication is complete. Authentication by 802.1x standard uses Extensible Authentication Protocol (EAP) for the message exchange between the BeaconMaster and the RADIUS server.

When 802.1x is used for authentication, the BeaconMaster provides the capability to dynamically assign per-wireless-device WEP keys (called per-station WEP keys in 802.11).

Note: In BeaconWorks Release 2.0, a RADIUS redundancy feature is provided, where you can define a failover RADIUS server (up to 2 servers) in the event that the active RADIUS server fails.

Privacy

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques.

Chantry Networks Inc. Copyright 2004. All rights reserved.

Chantry supports the Wired Equivalent Privacy (WEP) standard common to conventional access points.

It also provides Wi-Fi Protected Access (WPA) encryption, based on Pairwise Master Key (PMK) and Temporal Key Integrity Protocol (TKIP). This second option is available when the AAA (802.1x) authentication technique is used.

Interaction with Wired Networks: Virtual Network Services

BeaconWorks provides a versatile means of mapping wireless networks to the topology of an existing wired network. This is accomplished through the assignment of *Virtual Network Services*.

When you set up Virtual Network Services (VNS) on the BeaconMaster, you are defining subnets for groups of wireless users. This VNS definition creates a virtual IP subnet where the BeaconMaster acts as a default gateway for wireless devices.

This technique enables policies and authentication to be applied to the groups of wireless users on a VNS, as well as the collecting of accounting information on user sessions that can be used for billing.

When a VNS is set up on the BeaconMaster:

- one or more BeaconPoints (by radio) are associated with it
- a range of IP addresses is set aside for the BeaconMaster's DHCP server to assign to wireless devices.

If routing protocol is enabled, the BeaconMaster advertises the VNS as a routable network segment to the wired network, and routes traffic between the wireless devices and the wired network.

Note: In BeaconWorks Release 2.0, each radio on a BeaconPoint can participate in up to four VNSs, via the multi-SSID function.

Static Routing and Routing Protocols

Routing can be used on the BeaconMaster to support the VNS definitions.

In the User Interface on the BeaconMaster, you can configure routing on the BeaconMaster to use one of the following routing techniques:

- Static routes: Use static routes to set the default route of a BeaconMaster so that legitimate wireless device traffic can be forwarded to the default gateway.
- Open Shortest Path First (OSPF) (RFC2328): Use OSPF to specify the next best hop (route) of a BeaconMaster.

Open Shortest Path First (OSPF) is a protocol designed for medium and large IP networks, with the ability to segment routers into different routing areas for routing information summarization and propagation.

Policy: Packet Filtering

Policy refers to the rules that allow different network access to different groups of users. The BeaconWorks system can link authorized users to user groups. These user groups then can be confined to predefined portions of the network.

Chantry Networks Inc. Copyright 2004. All rights reserved.

In the BeaconWorks system, policy is carried out by means of packet filtering, within a VNS.

In the BeaconMaster user interface, you set up a filtering policy by defining a set of hierarchical rules that allow (or deny) traffic to specific IP addresses, IP address ranges, or services (ports). The sequence and hierarchy of these filtering rules must be carefully designed, based on your enterprise's user access plan.

The authentication technique selected determines how filtering is carried out:

- If authentication is by SSID and captive portal, a global filter will allow all users to get as far as the Captive Portal web page, where login occurs. When authentication is returned, then filters are applied, based on user ID and permissions.
- If authentication is by AAA (802.1x), there is no need for a global filter. Users will already have logged in and have been authenticated before being assigned an IP address. At this point, filters are applied, based on user ID and permissions.

Mobility and Roaming

The 802.11 standard allows a wireless device to preserve its IP connection when it roams from one access point to another on the same subnet. However, if a user roams to an access point on a different subnet, the user is disconnected.

Chantry BeaconWorks has functionality that supports mobility on any subnet in the network. Wireless device users can roam between BeaconPoints on any subnet without having to renew the IP connection

The BeaconMaster stores the wireless device's current session information, such as IP address and MAC address. If the wireless device has not disassociated, then when it requests network access on a different BeaconPoint, the BeaconMaster can match its session information and recognize it as still in a current session.

In addition, a BeaconMaster can learn about other BeaconMasters on the network, and then exchange client session information. This enables a wireless device user to roam seamlessly between different BeaconPoints on different BeaconMasters.

Availability

BeaconWorks provides seamless availability against BeaconPoint outages, BeaconMaster outages, and even network outages.

For example, if one BeaconPoint fails, coverage for the wireless device is automatically provided by the next nearest BeaconPoint.

If a BeaconMaster fails, all of its associated BeaconPoints, or access points, can automatically migrate to another BeaconMaster that has been defined as the secondary or backup BeaconMaster. When the original BeaconMaster returns to the network, the BeaconPoints automatically re-establish their normal connection with their original BeaconMaster.

Chantry Networks Inc. Copyright 2004. All rights reserved.

BeaconWorks Release 2.0 Features: Overview

Backwards compatibility with Release 1.1 on the BeaconPoint

In Release 2.0, the upgrading of software on the BeaconPoint is no longer automatic. You can schedule the upgrade and select the image to be used. Use the *BeaconPoint Maintenance* screen to select and schedule an upgrade.

One result of this feature is that you can continue to use BeaconPoints that still have Release 1.1 software. However, there are certain limitations to the functions supported. In Release 1.1, a BeaconPoint appeared as a single entity in a VNS, and could be assigned to only one VNS. Both radios had the same properties. Privacy by WPA was not supported. The default privacy mechanism was dynamic WEP.

A BeaconPoint that is still running a Release 1.1 software image will therefore retain these parameters, and these parameters are not modifiable. The new capability will only be available when the BeaconPoint is upgraded from Release 1.1 to Release 2.0 software.

Backwards compatibility with Release 1.1 on the BeaconMaster

Upgrading to BeaconWorks 2.0 requires a migration of the database on the BeaconMaster. In order to preserve the BeaconMaster network configurations that you defined in Release 1.1 software, the new release provides scripts that migrate the configuration data into the new data format.

Details of the software upgrade procedure, and the appropriate script to run are available in Technical Release Notes.

Multi-SSID: BeaconPoint radios on more than one VNS

In Release 1.1, a BeaconPoint appeared as a single entity in a VNS, and could be assigned to only one VNS.

In Release 2.0, each radio on a BeaconPoint BP200 can participate in up to four VNSs, for a total of eight VNSs per BeaconPoint. This provides greater flexibility in defining VNSs and providing support to a wide range of wireless devices.

This flexibility enables the network to support wireless devices with either:

- 802.11g radios on the 2.4 GHz band, and legacy support to 802.11b on the same band
- 802.11a radios on the 5 GHz band.

Furthermore, a VNS can be set up to support only one type of radio, for specific types of wireless traffic such as voice-over-internet traffic,

Use the *Virtual Network Configuration: Topology* screen to assign the BeaconPoint radios to a VNS. The *Virtual Network Configuration: Privacy* screen will allow only one WEP key to be set up. After a VNS definition has been saved, you can view (in the *BeaconPoint Configuration* screen) the properties for each radio for a selected BeaconPoint, including a list of the VNSs to which the radio has been assigned.

Chantry Networks Inc. Copyright 2004. All rights reserved.

Privacy using Wi-Fi Protected Access (WPA)

The VNS Privacy configuration function now includes Wi-Fi Protected Access (WPA) privacy, a new security solution that adds authentication and enhanced WEP encryption with key management. . WPA specifies IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).

WPA uses the Temporal Key Integrity Protocol (TKIP) mechanism, which shares a starting key between devices, and then changes their encryption key for every packet.

Configure the WPA option and define the initial shared key in the *Virtual Network Configuration: Privacy* screen

BeaconPoint software: Dual image capability

The BeaconPoint in Release 2.0 keeps a backup copy of its software image. When a software upgrade is sent to the BeaconPoint, the upgrade becomes the BeaconPoint's current image and the previous image becomes the backup. In the event of failure of the current image, the BeaconPoint will run the backup image.

BeaconPoint software: Dynamic reconfiguration (without reboot)

In Release 2.0, a number of the properties of each radio on a BeaconPoint can be modified (in the *BeaconPoint Configuration* screen) without requiring a reboot of the BeaconPoint. However, modifying the following properties does require a reboot:

- enabling or disabling either radio
- changing the radio channel.

In addition, the BeaconPoint must be rebooted after it has been added to a VNS, or the radio assignment in a VNS has been changed. Any changes to security also require a reboot of the BeaconPoint.

BeaconPoint Statistics

Radio statistics are available from a BeaconPoint running Release 2.0 software. On the BeaconMaster user interface, two displays (in the *Reports and Displays* area of the user interface) show information about activity on a selected BeaconPoint:

- Wired Ethernet Statistics by BeaconPoints
- Wireless Statistics by BeaconPoints, plus a subscreen that displays transmission and association information by wireless client.

These displays are snapshots of the BeaconPoint activity at the current point in time. The statistics displayed are those defined in the 802.11 MIB, defined in the IEEE 802.11 standard (in Section 11.4 and Annex D).

The BeaconMaster can also be configured to send these radio statistics as SNMP messages to the SNMP monitoring machine on a network.

Event reporting using Syslog

In addition to viewing BeaconWorks event messages in the BeaconWorks Reports and Displays area of the user interface, you can also set up the BeaconMaster to relay event messages on to a centralized Event Server on your enterprise network. The relay is done using the syslog protocol.

Use the *BeaconMaster System Maintenance* screen to enable the syslog function and to define the location of one or more centralized Event Servers.

Chantry Networks Inc. Copyright 2004. All rights reserved.

Capacity for Redundant RADIUS servers

BeaconWorks Release 2.0 provides the capability to define more than one RADIUS server for authentication, and to provide the priority of use during a failover situation.

Use the *Virtual Network Configuration: Authentication* screen to define the RADIUS server location and priority.

Detection of Rogue APs

BeaconWorks Release 2.0 provides a new mechanism that recognizes rogue access points. The mechanism scans radio frequency (RF) activity on the BeaconPoints and builds a data log of this activity. This data is then analyzed through various algorithms that assist in distinguishing rogue access points from legitimate activity.

Use the *BeaconKeeper* function in the user interface to enable this mechanism. Once enabled, you can configure and schedule the RF scan mechanism, maintain a list of "friendly AP" access points, and view the detected access points for which a match is not found in the "friendly AP" list.

Quality of Service (QoS) on a VNS: Spectralink Voice Protocol (SVP)

A VNS can be configured to handle voice-over internet traffic using SpectraLink Voice Protocol (SVP), a protocol developed by SpectraLink for implementation on an access point. The SVP protocol facilitates voice prioritization over an 802.11 wireless LAN that will carry voice packets from SpectraLink wireless telephones.

Use the *Virtual Network Configuration: Topology* screen to set up a VNS for voice-over-internet traffic with SVP prioritization. A number of conditions apply to a VNS for voice-over-internet.

BeaconPoint static configuration: Branch Office, Phase 1

The BeaconPoint static configuration feature provides BeaconWorks capability for a network with the central office / branch office model.

In the branch office scenario, BeaconPoints are installed in a remote site. The BeaconPoints require the capability to interact both in the local site network and in the central headquarters network. To achieve this, the BeaconPoint's automatic process of discovery and registration with the BeaconMaster is disabled, and a static configuration is used instead.

Chantry Networks Inc. Copyright 2004. All rights reserved.

BeaconMaster: Startup

BeaconMaster Features and Installation

The Chantry BeaconMaster is a network device designed to be integrated into an existing wired Local Area Network (LAN).

Figure 4: The Chantry BeaconMaster

The BeaconMaster provides centralized management, network access and routing to wireless devices that are using BeaconPoints to access the network. It can also be configured to handle data traffic from third-party access points.

The BeaconMaster performs the following functions:

- Controls and configures BeaconPoints, providing centralized management
- Authenticates wireless devices that contact a BeaconPoint
- Assigns each wireless device to a VNS when it connects
- Routes traffic from wireless devices, using VNSs, to the wired network
- Applies filtering policies to the wireless device session
- Provides session logging and accounting capability.

The BeaconMaster is rack-mountable and comes in two models:

- **BeaconMaster 100 (BM100)**:
  - Four Fast-Ethernet ports, (10/100 BaseT), supporting up to 60 BeaconPoints
  - One management port, (10/100 BaseT)
  - One console port (DB9 serial)
  - Power supply, either standard (S), or redundant (R)
- **BeaconMaster 1000 (BM1000)**:
  - Two GigE ports (dual 1GB SX network interfaces), supporting up to 200 BeaconPoints
  - One management port, (10/100 BaseT)
  - One console port (DB9 serial)
  - Power supply, either standard (S), or redundant (R)

Installing the BeaconMaster

Before you begin installation, make sure that a site survey has been done, to determine the number and location of BeaconPoints and BeaconMasters required. The site survey should take a number of factors into consideration, including:

Chantry Networks Inc. Copyright 2004. All rights reserved.

- coverage areas
- number of users
- architectural features that affect transmission
- existing wired network and access to ethernet cabling
- type of mount (wall, ceiling, plenum) for BeaconPoints
- type of power (Power-over-Ethernet or AC adaptor) for BeaconPoints
- physical security of the BeaconMaster, including access control.

Installing the BeaconMaster

1. Unpack the BeaconMaster from its shipment carton. Follow the instructions in the *Installation Guide* included with the unit to:
   - Check that all parts are present, including the ethernet cross-over cable
   - Install the BeaconMaster, using its rack mounts, or stand-alone table mount
   - Plug in the BeaconMaster power supply (single or dual).

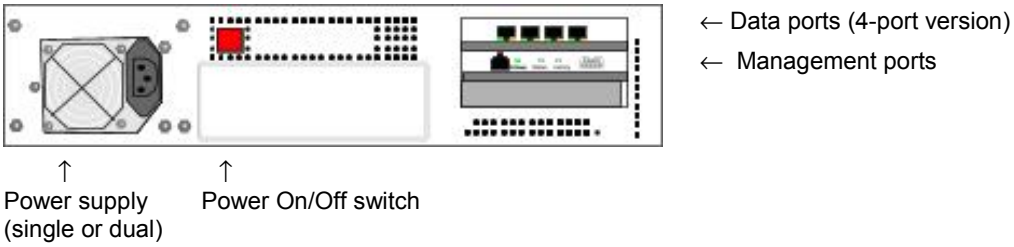
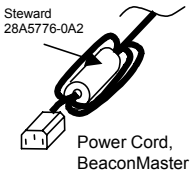
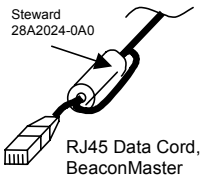


Figure 5: The Chantry BeaconMaster – back view diagram

2. Perform the First-Time Setup of the BeaconMaster, to change its factory default IP address (see next topic)
3. After that, connect the BeaconMaster to the enterprise LAN.



Note: Install ferrite beads as shown in the two diagrams:
← on the BeaconMaster power supply cord, and on the BeaconMaster ethernet cable →



First-Time Setup of BeaconMaster

Management Port First-Time Set Up

Before you can connect the BeaconMaster to the enterprise network, you must change the IP address of the BeaconMaster management port from its factory default to the IP address suitable for your enterprise network.

To access the BeaconMaster for this initial setup, use a laptop computer, running Internet Explorer 6.0 (or higher) web browser, attached to the BeaconMaster's ethernet Management Port (RJ45 port) via an ethernet cross-over cable (cable provided with the BeaconMaster).

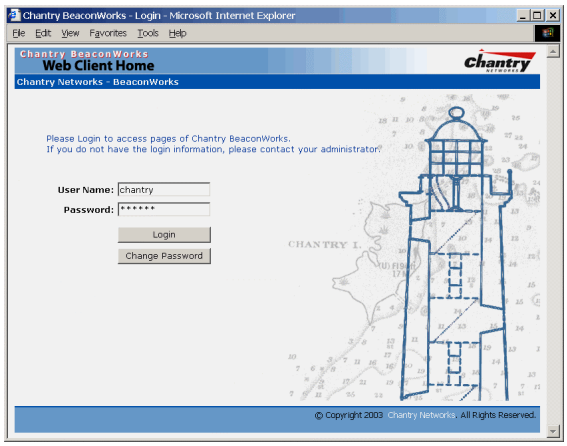
Chantry Networks Inc. Copyright 2004. All rights reserved.

The factory default management port setup of the BeaconMaster is:

Host Name:	BM0001
Management Port IP address:	192.168.10.1:5825
Management Network Mask:	255.255.255.0

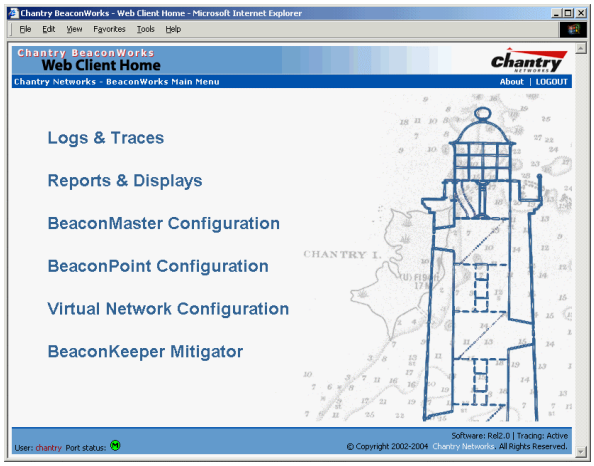
Changing the Management Port IP address web browser, ethernet port method

1. Connect a cross-over ethernet cable between the ethernet port of the laptop and ethernet Management Port of the BeaconMaster.
2. Statically assign an unused IP address in the 192.168.10.0/24 subnet for the ethernet port of the PC (for example, 192.168.10.205).
3. Run Internet Explorer (version 6.0 or above) on the laptop.
4. Point the browser to the URL https://192.168.10.1:5825. This URL launches the web-based GUI on the BeaconMaster.
   The Chantry BeaconWorks system login screen appears.



Screen 1: Chantry BeaconWorks User Interface Login

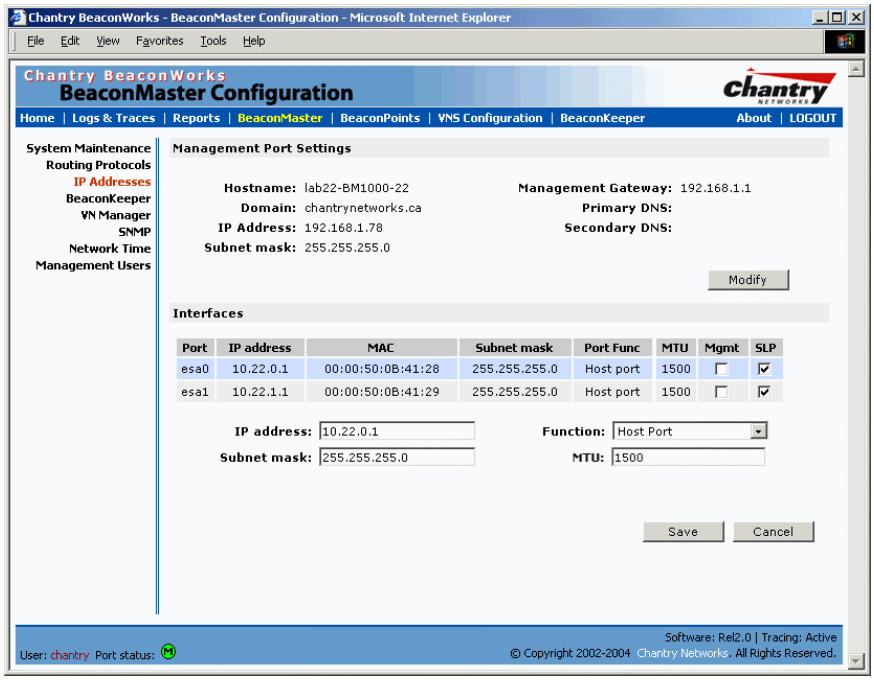
5. Key in the factory default **User Name** (“chantry”) and **Password** (“abc123”) . Click on the **Login** button. The main menu screen appears.



Screen 2: Chantry BeaconWorks User Interface Main Menu

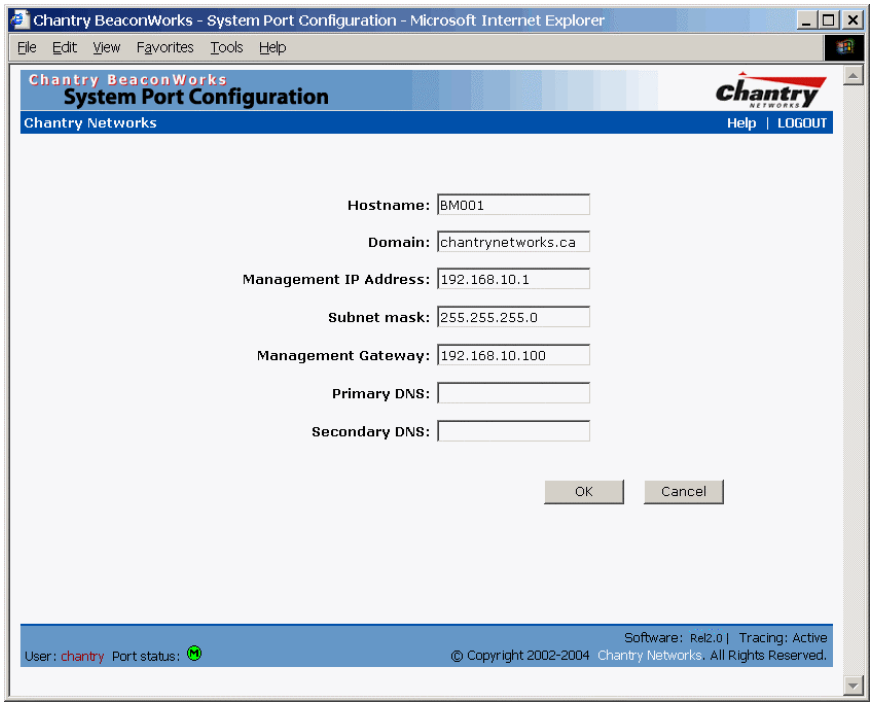
6. Click on the BeaconMaster Configuration menu option to navigate to the *BeaconMaster Configuration* screen.

7. In the left-hand list, click on the **IP Addresses** option. The Management Port Settings area (top portion of the screen) displays the factory settings for the BeaconMaster.



Screen 3: BeaconMaster Configuration – IP Addresses – Management Port

8. To modify Management Port Settings, click the **Modify** button. The *System Port Configuration* screen appears.



Screen 4: Modify Management Port Settings (System Port Configuration)

9. Key in:

Hostname	The name of the BeaconMaster.
Domain	The IP domain name of the enterprise network
Management IP Address	The new IP address for the BeaconMaster's management port (change this as appropriate to the enterprise network).
Subnet mask	For the IP address, the appropriate subnet mask to separate the network portion from the host portion of the address (typically 255.255.255.0)
Management Gateway	The default gateway of the network.
Primary DNS	The primary name server used by the network.
Secondary DNS	The secondary name server used by the network.

10. Click **OK** to return to the *BeaconMaster Configuration* screen.
11. Click on the **Save** button, to save the port changes.

The web connection between the laptop and the BeaconMaster is now lost, because their IP addresses are now on different networks.

Add the BeaconMaster to your enterprise network

1. Disconnect the laptop from the BeaconMaster Management Port.
2. Connect the BeaconMaster Management Port to the enterprise ethernet LAN.

Now you will be able to launch the BeaconWorks GUI again, with the system visible to the enterprise network.

The remaining steps in initial configuration of the BeaconWorks system are described in the next topic, after an overview of the GUI.

Chantry Networks Inc. Copyright 2004. All rights reserved.

The Graphical User Interface (GUI): Overview

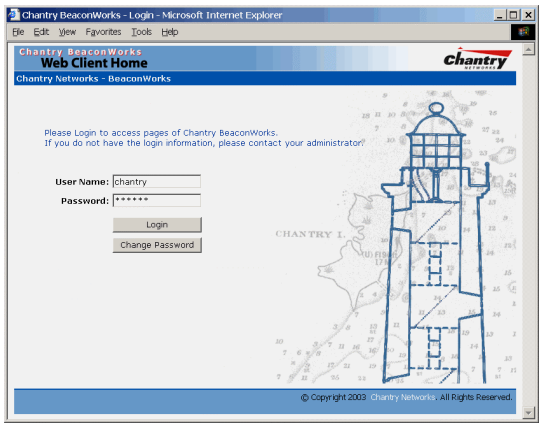
Note: The Chantry Graphical User Interface is web-based. The only browser it supports is Microsoft Internet Explorer 6.0 or above.

The administrator can configure and administer the BeaconWorks system using the web-based Graphical User Interface.

To run the Graphical User interface

1. Launch Microsoft Internet Explorer (version 6.0 or above).
2. In the address bar, key in the URL https://x.x.x.x:5825
   (your management gateway as defined in initial setup plus port 5825, formerly factory default 192.168.10.1:5825)

   The Chantry BeaconWorks system login screen appears.

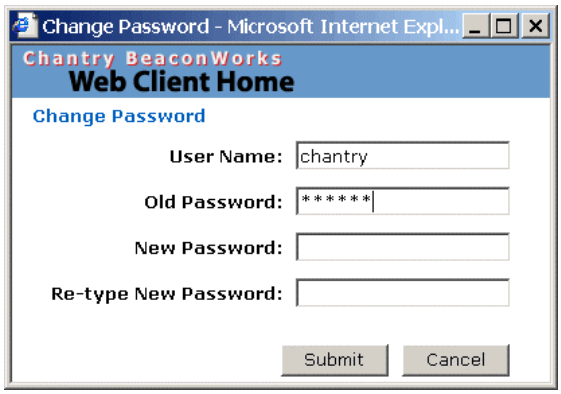


Screen 5: Chantry BeaconWorks User Interface Login

3. Key in the factory default **User Name** ("chantry") and **Password** ("abc123").

Note: In the *BeaconMaster Configuration: Management Users* screen, you can define which user names have full read/write access to the user interface ("Admin" users) and which users have "read-only" privileges. This is described in a later topic.

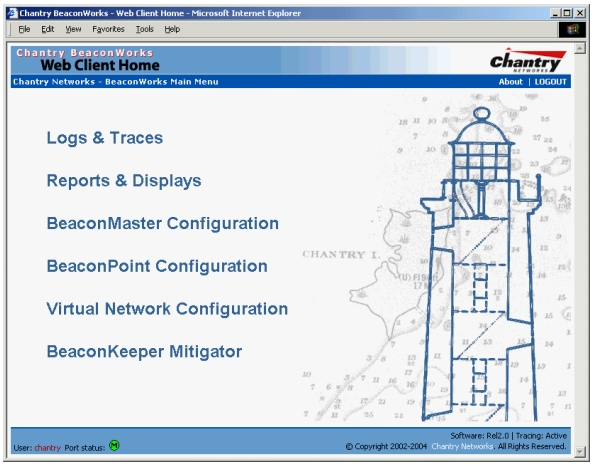
4. To change the password, click on the **Password** button. The *Change Password* popup screen appears.



Screen 6: Change Password popup

5. Enter the new password and click on the **Submit** button.

6. In the Login screen, click on the **Login** button. The main menu screen appears.



Screen 7: Chantry BeaconWorks Main Menu

The five areas in the BeaconWorks user interface are accessed from the main menu (above) or, in each area, by clicking on the tab across the top of each screen. Within each area, you access the associated subscreens by clicking on an item in the left-hand list in each screen. A few subscreens are popups from buttons on the parent screen.

Tab	Screen	Function
Logs & Traces		Logs normal events and alarm events. Trace logs are by component.
Reports & Displays		Access to various on-screen reports
BeaconMaster Configuration	System Maintenance Routing Protocols IP Addresses BeaconKeeper VN Manager SNMP Network Time Management Users	Various: shutdown, enable syslog. Define static routes, configure OSPF. Set up management port (Modify screen) Set up the data ports. Enable “detect rogue APs” mechanism. Manage multiple BeaconMasters. Enable SNMP messages to be sent. Configure synchronized time. Define user level.
BeaconPoint Configuration	Highlight a BP Access Approval BP Maintenance BP Registration BP Failover Client Disassociate	Modify properties, radios, static config. Modify the status of a BeaconPoint. View and set up BP software upgrade. Define registration mode, pairing of BPs. View failover VNS, part of VN Manager. Force a wireless device to disassociate
Virtual Network Configuration	Add a subnet VNS Topology VNS Authentication VNS Filtering VNS Privacy	Left-hand list. Enter name. Click to add. Define the VNS Define Filter IDs Define filtering rules to control access Set up WEP keys or WPA privacy.
BeaconKeeper Mitigator		Configure and view reports for the BeaconKeeper Mitigator (rogue access point detection)

BeaconWorks Configuration Steps: Overview

To set up and configure the BeaconMaster and BeaconPoints, follow these steps:

1. *First-Time Setup*: Perform "First-Time Setup" of the BeaconMaster on the physical network by configuring the Management Port (as described earlier):
   - modify the Management Port IP address to suit the enterprise network.
2. *Data Port Setup*: Set up the BeaconMaster on the physical network by configuring the physical data ports. Determine whether the data ports will be:
   - "host port"
   - "router port"
   - "3rd party AP port"
3. *Routing Setup*: For any port defined as a "router port", configure:
   - static routes
   - OSPF parameters, if appropriate to the network
4. *BeaconPoint Initial Setup*: Connect the BeaconPoints to the BeaconMaster:
   - first determine their Registration mode (in the BeaconPoint Registration screen)
   - then power on the BeaconPoints (they will perform an automatic discovery and registration process described in this User Guide)
5. *BeaconPoint Configuration*: Modify properties or settings of the BeaconPoint, if desired.
6. *Virtual Network Services (VNS) Setup*: Set up one or more virtual subnetworks, on the BeaconMaster. For each VNS:
   - select radios on the BeaconPoints that the VNS will use.
   - select and configure the authentication method for the wireless device user.
   - select and configure the privacy method on the VNS.
7. *Filtering Rules Setup*: For each VNS, define the filtering rules that will control network access:
   - define global and default filtering rules, depending on network assignment and authentication method
   - define specific filtering rules for the Filter IDs (defined user groups in your enterprise) that you want on this VNS.

Each of these steps is described in detail in the relevant section of this User Guide.

Chantry Networks Inc. Copyright 2004. All rights reserved.

BeaconWorks Configuration: Data Port and Routing Setup

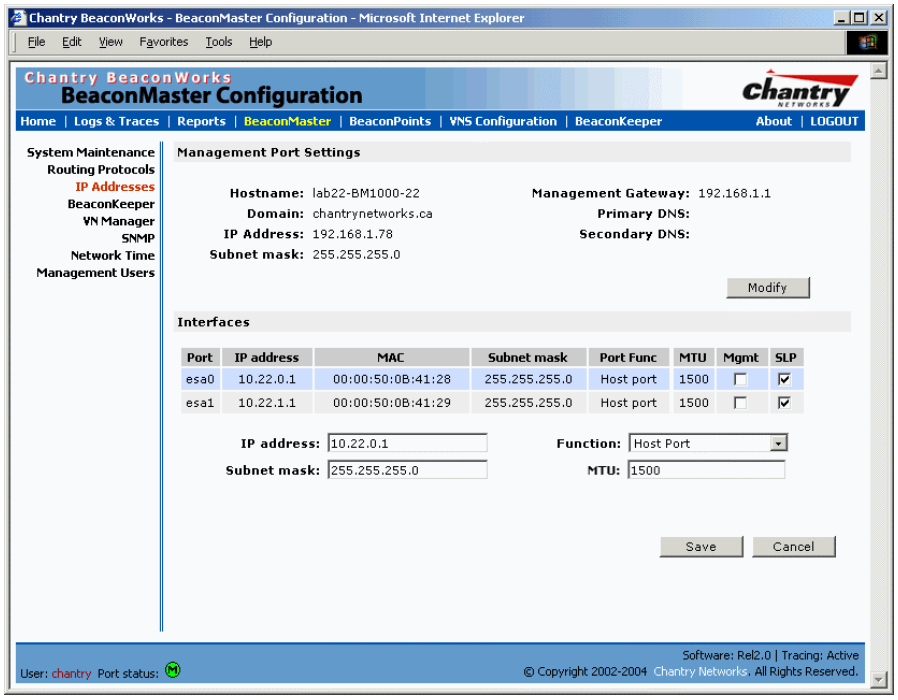
Once the "First-Time Setup" described above is complete, the next step in the initial setup of the BeaconMaster is to configure the data ports. Next, you can define routing on a data port, if appropriate.

Setting Up the Data Ports

Configuring the data ports on the BeaconMaster

1. Click on the **BeaconMaster** tab in any screen. The *BeaconMaster Configuration* screen appears.
2. In the left-hand portion of the screen, click on the **IP Address** option. The *Management Port Settings and Interfaces* screen appears.

   The lower portion of the *BeaconMaster Configuration* screen displays the **Interfaces**, either the four ethernet ports (for the BM100), or the two ports (for the BM1000). For each port, the MAC address is displayed automatically.



Screen 8: BeaconMaster Configuration – IP Addresses / Interfaces

3. Click in a port row to highlight it.
4. For the highlighted port, key in the:

IP address	IP Address of the physical ethernet port.
Subnet mask	For the IP address, the appropriate subnet mask to separate the network portion from the host portion of the address (typically 255.255.255.0)
MTU	Maximum Transmission Unit (maximum packet size for this port). Default setting is **1500**. *Do not change this setting.*

Note: In a "Branch Office" scenario, where the BeaconPoint is configured statically to function on a local network whose MTU is lower than 1500, a mechanism on the BeaconMaster automatically adjusts the MTU size to prevent packet fragmentation.

5. For the highlighted port, select its **Function** from the drop-down list: Host Port, 3rd Party AP, Router (*see "Port Type" explanation below*)

Note: It is recommended that one port be configured as a "Router" Port, so that static routes and/or OSPF routing can be defined for the BeaconMaster. See next topic.

6. For the highlighted port, click the **Mgmt** checkbox on to allow *Management Traffic* on this port.
7. For the highlighted port, click the **SLP** checkbox on to allow SLP protocol on this port for BeaconPoint discovery and registration.

Note: For the implications of these two options, see Port-Level Filtering (after the next topic).

8. To save the port configuration, click **Save**.
   To cancel the entries without saving, click **Cancel**.

Port Type or Function

A new BeaconMaster is shipped from the factory with all its data ports set up as "Host ports", and support of management traffic disabled on all data ports.

In the user interface, you can redefine the data ports to function as one of three types:

- **Host Port**

  Define as "Host Port" any port to which *only* BeaconPoints are connected, in a typical installation. When BeaconPoints are attached to a host port and assigned to a VNS (see later in this guide*)*, a virtual VNS port is created and wireless device traffic is directed to the virtual VNS port, allowing the BeaconMaster to forward traffic. IP forwarding and routing are disabled for third-party hosts attached to a "Host Port".

- **Third-Party Access Point Port**

  Define as "3rd-Party AP" any port to which you will connect *only* third-party access points, in order for the BeaconMaster to manage these access points. The BeaconMaster uses a combination of network routing and authentication techniques to forward traffic on this port. BeaconPoints must not be attached to a "3rd-Party AP" port.

- **Router Port**

  Define as "Router Port" a port that you wish to connect to an upstream next-hop router in the network. Dynamic routing protocol such as OSPF can be turned on for this port type.

  BeaconPoints can be attached to a "Router" port. The BeaconMaster will create a virtual VNS port and handle wireless device traffic in the same manner as a "Host port". Third-party access points must not be directly connected to a "Router" port (unless the BeaconMaster is not required to manage these access points).

There is a fourth port type that is not configurable in the user interface:

- **Virtual Network Services (VNS) Interface**

  A VNS port is a virtual port created automatically on the BeaconMaster when a new VNS is defined (see later in this guide.) The VNS port becomes the default gateway for wireless devices on this VNS. No BeaconPoints can be associated with a VNS port and no routing is permitted on this port.

Note: The **Management Port** is always a Host port, with management traffic support enabled.

The chart below summarizes the port types and their functions:

Port Type	IP Forwarding	BeaconPoint support	Management traffic support (SNMP, HTTP, TELNET, SLP, RADIUS, DHCP)	Routing protocol support (IP, OSPF and PIM)
Host	*No*	*Yes*	*Selectable*	*No*
Third-Party AP	*No*	*No*	*Selectable*	*No*
Router	*Selectable* *Route wireless device traffic only*	*Yes*	*Selectable*	*Selectable*
VNS	*No*	*No*	*Selectable*	*No*

Port-Level Filtering of Unauthorized Traffic

Port-based filters on the BeaconMaster are built in to protect it from unauthorized access to system management functions and services via the ports.

When you select a port type, you automatically activate a set of filtering rules that allow or deny traffic seeking access to specific services. For example:

- Router and Host interfaces allow access to specific management applications (SSH, HTTPS, SNMP) and to BeaconPoint registration mechanisms.
- Third Party AP and VNS interfaces deny access to management and BP registration mechanisms, but allow access to captive portal (HTTP, HTTPS) and IP assignment infrastructure (DHCP).

Only traffic allowed by the interface's filter are allowed to reach the BeaconMaster itself. All other traffic is dropped.

The physical Management Port that you configured in "First-Time Set-up" has a restricted set of *Management Traffic* filtering rules that apply automatically. These rules allow incoming traffic for SSH, HTTPS, FTP, SNMP, and outgoing traffic for Syslog, NTP, and RADIUS, both directions for ICMP, and then deny all other traffic.

When you enable Management Traffic on one of the data ports (clicking the checkbox on), you will activate the Management Traffic filter on that port. There is a second way to enable Management Traffic, and invoke this implicit filter – in the VNS Configuration: Topology, you can allow Management Traffic on a VNS by clicking a checkbox on. (See later in this Guide.)

Note: These implicit or built-in filtering rules work in conjunction with the VNS filtering rules that you can define in a VNS Configuration (described later in this Guide). The implicit rules on a port always override the administrator-defined rules, unless specific access is defined and allowed, as in a filter for Captive Portal.

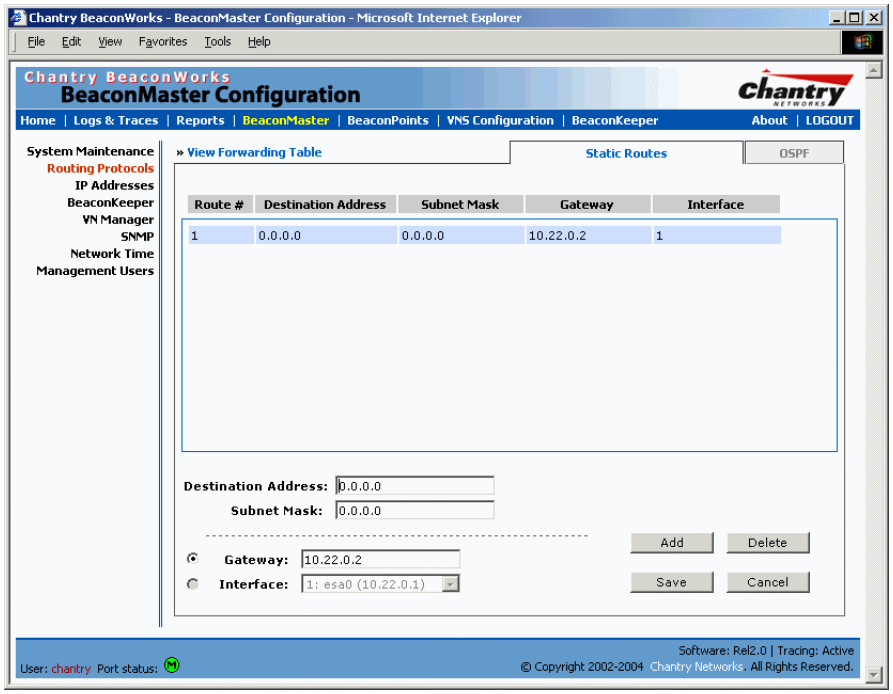
Chantry Networks Inc. Copyright 2004. All rights reserved.

Setting up Static Routes

It is recommended that one of the data ports be configured as a "Router" port. Then you can define a default route to your enterprise network, either with a static route or by using OSPF protocol. This will enable the BeaconMaster to forward wireless packets to the remainder of the network.

Setting up a Static Route on the BeaconMaster

1. Click on the **BeaconMaster** tab in any screen. The *BeaconMaster Configuration* screen appears.
2. In the left-hand portion of the screen, click on the **Routing Protocols** option. Then click the **Static Routes** tab. The *Static Routes* screen appears.



Screen 9: BeaconMaster Configuration – Static Routes

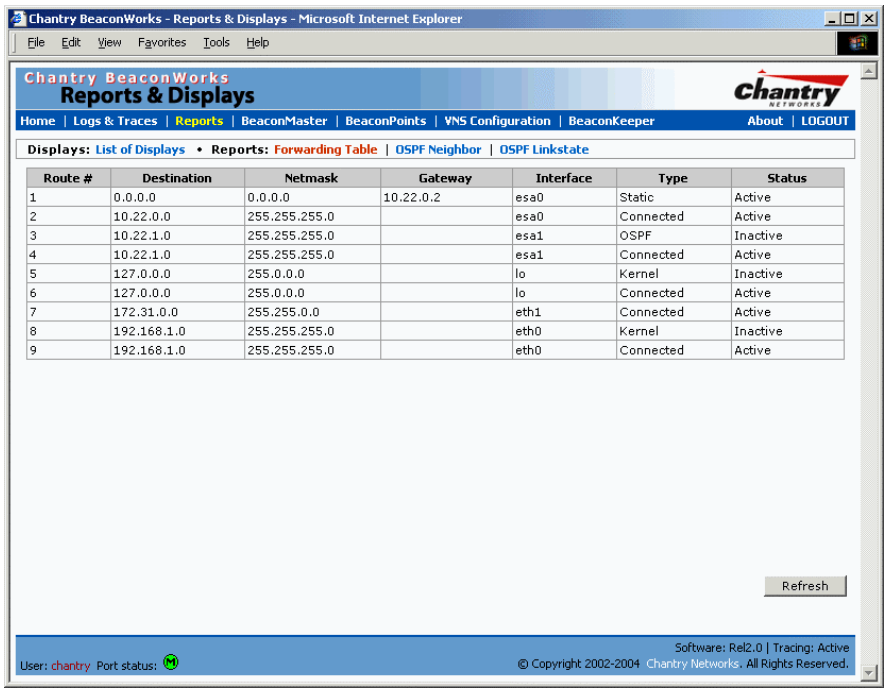
3. To add a new route, click in the **Destination Address** field, and key in the destination IP address of a packet.
   [The destination network IP address that this static route applies to. Packets with this destination address will be sent to the Destination below.]
   To define a *default static route* for any unknown address not in the routing table, key in 0.0.0.0
4. Key in the **Subnet Mask**. For the IP address, the appropriate subnet mask to separate the network portion from the host portion of the address (typically 255.255.255.0)
   For the *default static route* for any unknown address, key in 0.0.0.0.
5. Select an outbound destination for the packets, either:
   Click on the radio button in the **Gateway** field, and key in the IP address of the gateway (the IP address of the specific router port or gateway, on the same subnet as the BeaconMaster, to which to route these packets; that is, the IP address of the next hop between the BeaconMaster and the packet's ultimate destination) ,

or
Click on the **Interface** button, and select a port from the drop-down list.

6. Click on the **Add** button. The new route appears in the list, numbered sequentially.
7. Click on **Save** to update the routing table on the BeaconMaster.

Viewing the Routing Table on the BeaconMaster

To view the static routes that have been defined for the BeaconMaster, click on the **View Forwarding Table** tab. This displays the *Forwarding Table Screen* from the **Reports & Displays** area of the user interface.



Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	10.22.0.2	esa0	Static	Active
2	10.22.0.0	255.255.255.0		esa0	Connected	Active
3	10.22.1.0	255.255.255.0		esa1	OSPF	Inactive
4	10.22.1.0	255.255.255.0		esa1	Connected	Active
5	127.0.0.0	255.0.0.0		lo	Kernel	Inactive
6	127.0.0.0	255.0.0.0		lo	Connected	Active
7	172.31.0.0	255.255.0.0		eth1	Connected	Active
8	192.168.1.0	255.255.255.0		eth0	Kernel	Inactive
9	192.168.1.0	255.255.255.0		eth0	Connected	Active

Screen 10: Report – Forwarding Table

This report displays all defined routes, whether static or OSPF, and their current status. To update the display, click on the **Refresh** button.

Setting up OSPF Routing

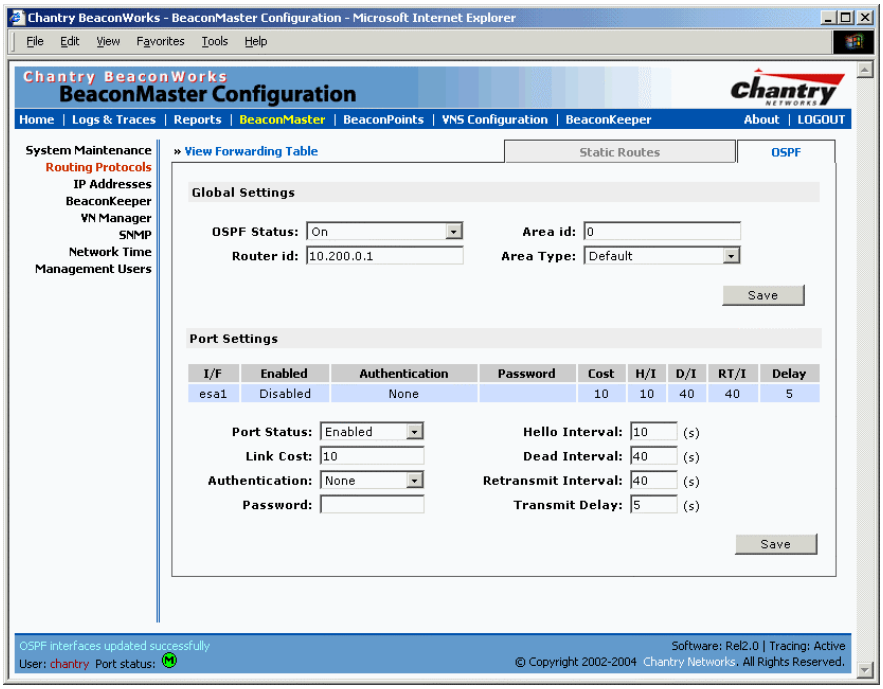
For each data port defined as a "Router Port", you can enable OSPF (as well as, or instead of, defining static routes). First, you enable OSPF on the BeaconMaster, and define the global OSPF parameters. Then you enable (or disable) OSPF on each port that you defined as a "Router Port" in the data port setup.

Note: Ensure that the OSPF parameters defined here for the BeaconMaster are consistent with the adjacent routers in the OSPF area. For example:

- If the peer router has different timer settings, the protocol timer settings in the BeaconMaster must be changed to match, in order to achieve OSPF adjacency.
- The MTU of the ports on either end of an OSPF link must match. The MTU for ports on the BeaconMaster is defined as 1500, in the Interfaces area of the IP Addresses screen, during data port setup. This matches the default MTU in standard routers.

Setting up OSPF Routing on the BeaconMaster

1. Click on the **OSPF** tab in *Routing Protocols* screen. The *OSPF Settings* screen appears.



Screen 11: BeaconMaster Configuration – Routing, OSPF tab

2. In the *Global Settings* area, enable OSPF on the BeaconMaster by filling in the following fields:

OSPF Status:	To enable OSPF, select **ON** from the drop-down list.
Router ID:	If left blank, the OSPF daemon will automatically pick a router ID from one of the BeaconMaster's interface IP addresses. If filled in here with the IP address of the BeaconMaster, this ID must be unique across the OSPF area.
Area ID:	0 is the main area in OSPF (**Note:** The Area ID must be the same for all ports on the BeaconMaster defined as router ports, to avoid creating an area boundary in the BeaconMaster.)
Area Type:	Select Default (Normal), Stub or Not-so-stubby (OSPF area types) from the drop-down list.

3. To save these settings, click on the **Save** button.

4. In the *Port Settings* area, for each data port defined as a "Router Port", you can enable (or disable) OSPF by filling in the following fields:

Port Status:	To enable OSPF on the port, select **Enabled** from the drop-down list.
Link Cost:	Key in the OSPF standard for your network for this port. Default displayed is 10. (The cost of sending a data packet on the interface. The lower the cost, the more likely the interface is to be used to forward data traffic.)

Note: If more than one port on the BeaconMaster is enabled for OSPF, it is desirable to prevent the BeaconMaster from serving as a router for other network traffic (other than the traffic from wireless device users controlled by the BeaconMaster). One solution is to set the **Link Cost** to its maximum value of 65535. This will ensure that the BeaconMaster is never the preferred OSPF route. Filters should also be defined in the *Virtual Network Configuration – Filtering* screen that will drop routed packets.

Authentication: From the drop-down list, select the authentication type set up for the OSPF on your network: **None** or **Password**.

Password: If "Password" was selected above, key it in here. This password must match on either end of the OSPF connection.

Dead-Interval: Time in seconds (displays OSPF default).

Hello-Interval: Time in seconds (displays OSPF default).

Retransmit-Interval: Time in seconds (displays OSPF default).

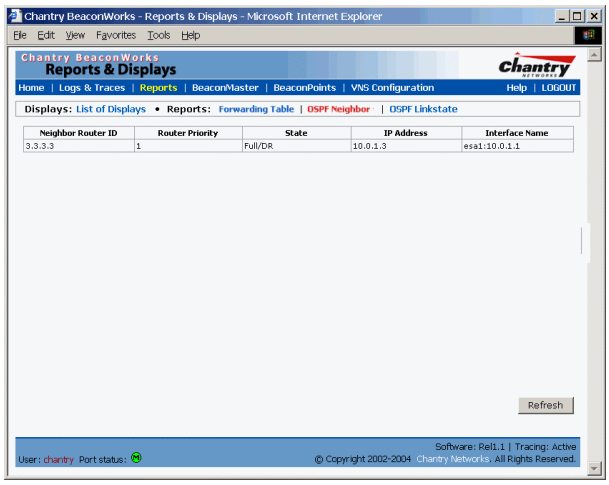
Transmit delay: Time in seconds (displays OSPF default).

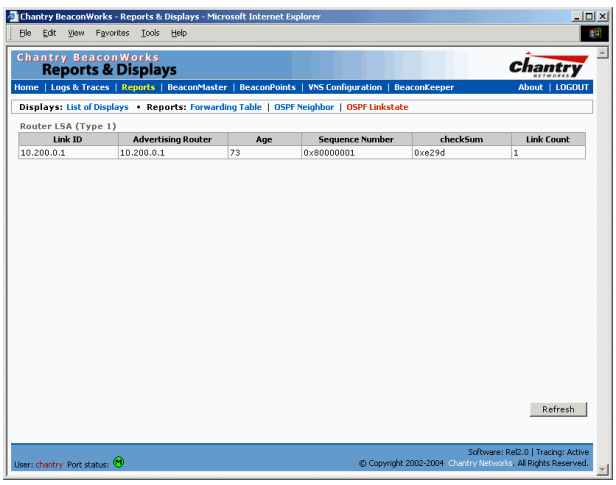
5. To save these settings, click on the **Save** button.

To confirm that the ports are set up for OSPF, and that advertised routes from the upstream router are recognized, view the *Forwarding Table* report (described above for static routes) by clicking the tab. This display shows the current routing table, displaying the default, connected, static and OSPF routes.

Two additional reports in the Reports and Displays area of the GUI display OSPF information when the protocol is in operation:

- *OSPF Neighbor* report displays the current neighbors for OSPF (routers that have interfaces to a common network)
- *OSPF Linkstate* report shows the Link State Advertisements (LSAs) received by the currently running OSPF process. The LSAs describe the local state of a router or network, including the state of the router's interfaces and adjacencies.





Screen 12: Reports – OSPF Neighbor and Linkstate

BeaconPoint: Startup

You are now ready to add the BeaconPoints to the BeaconWorks system and register them with the BeaconMaster. Before the BeaconPoints can handle wireless traffic, you will also need to assign the BeaconPoints to a VNS (see later in this Guide).

BeaconPoint (BP200) Features

The Chantry BeaconPoint is a wireless LAN access point using the 802.11 wireless standards that allow wireless functionality comparable to ethernet (802.11a, 802.11b and 802.11g).

The BeaconPoint is provided with proprietary software that allows it to communicate only with the BeaconMaster.

The BeaconPoint is physically connected to a LAN infrastructure with an IP connection to a BeaconMaster. The BeaconPoint has no user interface. The only way to communicate with a BeaconPoint is through the BeaconMaster.

All communication with the BeaconMaster is carried out using a UDP-based protocol called CAPWAP Tunnelling Protocol (CTP) to encapsulate IP traffic from the BeaconPoints and direct it to the BeaconMaster. The BeaconMaster decapsulates the packets and routes them to the appropriate destinations, while managing sessions and applying policy.

Figure 6: The Chantry BeaconPoint

The BeaconPoint BP200 has two radios:

- a radio that supports the 802.11a standard.
  The *802.11a standard* is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5-GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
- a radio that supports the 802.11g standard (and 802.11b).
  The *802.11g standard* applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band. Because 802.11g uses the same communication frequency range as 802.11b (2.4 GHz), it is backwards compatible with 802.11b.

  The *802.11b (High Rate)* standard is an extension to 802.11 that specifies a transmission rate of 11 Mbps (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 to 2.4835 GHz frequency band. The 802.11b standard uses direct-sequence spread spectrum (DSSS).

Either radio on the BP200 can be enabled or disabled in the user interface.

Chantry Networks Inc. Copyright 2004. All rights reserved.

The BP200 supports the full range of 802.11a:

5.15 to 5.25 GHz	U-NII Low Band
5.25 to 5.35 GHz	U-NII Middle Band
5.725 to 5.825 GHz	U-NII High Band
New 5.470 GHz to 5.725 GHz Band (when approved by FCC)	

The U-NII bands (Unlicensed National Information Infrastructure) are three frequency bands of 100 MHz each in the 5 GHz band designated for short-range, high-speed wireless networking communication.

The BeaconPoint BP200 has two models:

- internal antenna (Model BP200s), internal dual (multimode) diversity antennas
- external antenna (Model BP200e) (dual external antennas) RP-SMA

The BeaconPoint are powered in one of three ways:

- **Power Over Ethernet (PoE)**

  If your network is already set up with PoE, attach the LAN ethernet cable to the RJ45 ethernet connector in the top of the BeaconPoint.

- **Power Over Ethernet: Adding PoE Injector**

  If your network is not set up with PoE, you can provide power to the ethernet cable with a PoE injector. The PoE injector must be 802.3af compliant. The PoE injector is not provided with the BeaconPoint.

- **Power by AC Adaptor**

  An AC adaptor is not provided with the BeaconPoint. If you wish to use one, the specifications are: *BP200* – Input: 120-240 VAC, Output Voltage DC +6V, max amps 1.50, max watts 10.

  To use an adaptor, install the BeaconPoint within six feet of a wall outlet, attach the adaptor to the BeaconPoint and then plug the adaptor into the wall outlet.

Note: For a list of recommended and tested devices (PoE Injectors or AC adaptors) for use with the BeaconPoint, contact Chantry Networks Customer Service, or go to www.chantrynetworks.com/site/support.html.

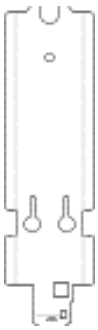
The BeaconPoint has a mounting bracket for wall, ceiling or plenum mount, and security hardware (an allen key and a spreading rivet with screw, described later).

Chantry Networks Inc. Copyright 2004. All rights reserved.

Installing the BeaconPoints

The steps to install the BeaconPoints are repeated here from the *Installation Guide* packed with the units. Keep the security instructions for future reference (along with the allen key needed to remove the BeaconPoint from its mounting bracket).

1. Unpack the BeaconPoint from its shipment carton. Check that all parts are present, using the *Installation Guide* packed with the unit.

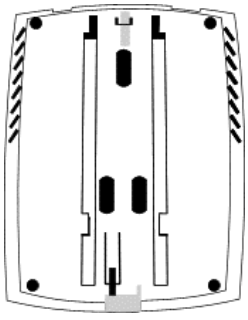


BeaconPoint wall bracket

2. Mount the BeaconPoint wall bracket, using 3 screws. Make sure the top of the bracket is near the LAN ethernet cable plug coming from the wall.

3. Press the back of the BeaconPoint onto the bracket, aligning it with the open notches in the bracket.

Then slide it downwards until it clicks into place.

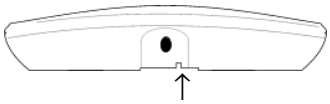


↑
Channel for allen key to spring clip

> **Security Note #1:** A small spring clip on the BeaconPoint case has now snapped into the bracket. To remove the BeaconPoint from the bracket, insert the allen key (provided) into the small hole at the bottom of the bracket. Use the allen key to depress the spring clip. Then slide the case up the bracket and lift off the BeaconPoint.

4. Insert the *plastic spreading rivet* through the hole at the bottom of the bracket and into the BeaconPoint case. Then screw in the plastic screw. This spreads the rivet and locks the case to the bracket.

Opening for rivet
↓



↑
Opening for allen key

> **Security Note #2:** The spreading rivet prevents casual removal of the BeaconPoint. You will need a screwdriver to remove it.

5. Attach the LAN ethernet cable to the ethernet port of the BeaconPoint.
6. If you are using the optional power adaptor (rather that Power-over-Ethernet), plug in the unit.

> **Note:** Before you power up the BeaconPoint (steps 5 or 6), you should first power up the BeaconMaster, and then define the Registration Mode in the User Interface of the BeaconMaster (**BeaconPoint Configuration**, *BP Registration* screen).
> Powering up the BeaconPoint initiates its automatic discovery and registration process described below. The parameters for this process should be set first. See next topic.

BeaconPoint: Registering

Setting Parameters for BeaconPoint Registration

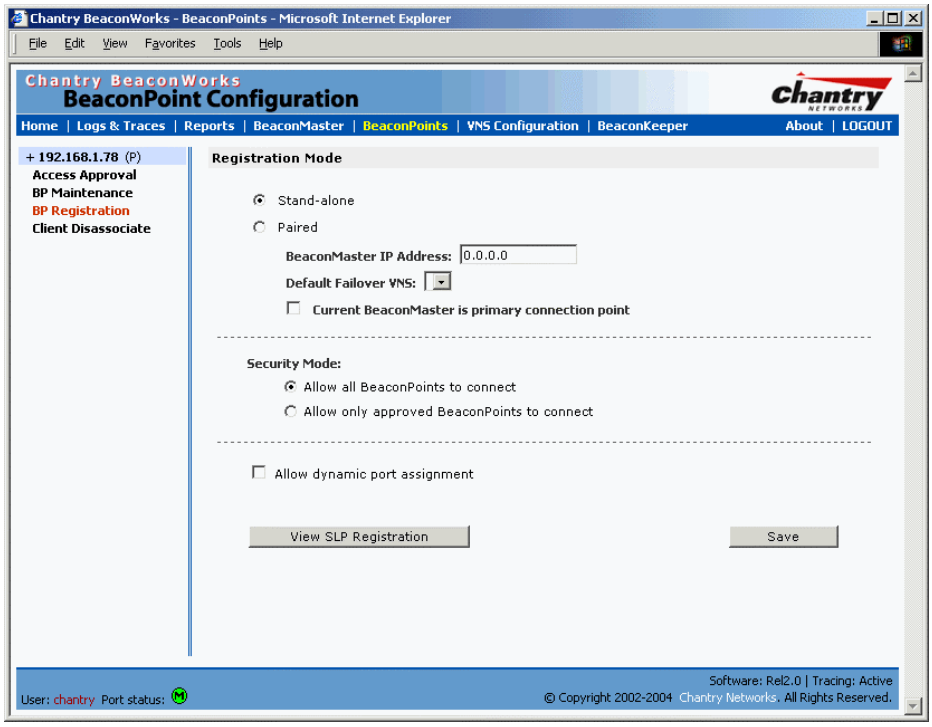
Before the BeaconPoints are powered and begin their automatic process of "Discovery" and "Registration", you should define the parameters of this process. This is done in the *BeaconPoint Registration Mode* screen.

In this screen you define the Security Mode: whether the BeaconMaster should automatically allow all BeaconPoints to register, or whether only approved BeaconPoints should be allowed.

This screen also controls the "Availability" function, whether this BeaconMaster is paired with another BeaconMaster. If they are paired, then they share information about BeaconPoints and if one BeaconMaster fails, the other can continue to provide service availability. This is discussed in detail later in this Guide (BeaconMaster Configuration: Availability).

Define the Security Mode for registering BeaconPoints

1. Select **BeaconPoints** tab in any screen.
2. In the left-hand list, click on **BP Registration**. The *BeaconPoint Registration Mode* screen appears.



Screen 13: BeaconPoint Configuration – BP Registration Mode

3. To **allow all** BeaconPoints to connect, click this radio button. (The screen is in this mode by default.)

   To **allow approved** BeaconPoints *only* to connect, click on this radio button

   During the "Registration" process, the BeaconMaster's approval of the serial number of the BeaconPoint depends on the security mode that has been set:

- **Allow all**
  If the BeaconMaster does not recognize the serial number, it sends a default configuration to the BeaconPoint.
  If it recognizes the serial number, it sends the specific configuration (port and binding key) set for that BeaconPoint.
- **Allow approved**
  If the BeaconMaster does not recognize the serial number, the operator is prompted to create a configuration.
  If it recognizes the serial number, it sends the configuration for that BeaconPoint.

Note: It may be advisable, for the initial set up of the network, to select the "Allow All" option here. This is the most efficient way to get a large number of BeaconPoints registered with the BeaconMaster.
However, after that, you may want to reset this option to "Allow Approved", so that no unapproved BeaconPoints would be able to connect. You can modify the status of an unapproved BeaconPoint in the *BeaconPoint Configuration: BP Maintenance* screen described later in this Guide.

4. To save the above parameters, click the **Save** button.

Note: The remaining functions in this screen are part of the "Availability" feature, described later in this Guide. Whether this BeaconMaster is **Stand-alone** (the default) or is **Paired** with another BeaconMaster, and whether it is the Primary or Secondary connection, is part of the "Availability" feature. The **Allow dynamic port assignment** checkbox is also used as part of the "Availability" feature.

Now you can go back to the BeaconPoints and power them on. They will begin the automatic Discovery and Registration sequence.

Discovery and Registration: The DHCP and SLP Solution

Before you can begin to register the BeaconPoints with the BeaconMaster, you must ensure that the DHCP server on your network supports Option 78. The BeaconPoints rely on these to locate the BeaconMaster during the discovery process, as explained below.

The solution to centrally configuring BeaconPoints, and to mass deployment, is to take advantage of two services that are present on most networks: DHCP and SLP.

DHCP (Dynamic Host Configuration Protocol), is the standard means of providing IP addresses dynamically to devices on a network.

SLP (Service Location Protocol) is a means of allowing client applications to *discover* network services without knowing their location beforehand. Devices advertise their services, using a *Service Agent*. In larger installations, a *Directory Agent* collects information from Service Agents and creates a central repository.

A device that is searching for a service makes use of the SLP *User Agent* to retrieve information from Service Agents or Directory Agents. DHCP Option 78 returns a list of IP addresses of Directory Agents.

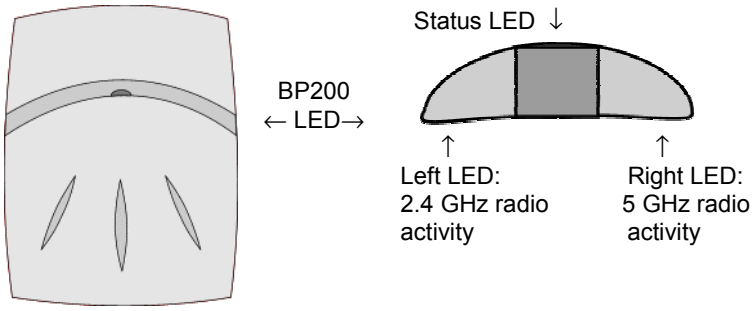
Meanwhile, the active BeaconMaster has management software that has registered itself as a service. When a BeaconMaster starts up, it queries the DHCP server for Option 78. It registers with the Directory Agents as service type "Chantry".

This information enables the BeaconPoint to discover the location of the BeaconMaster.

The BeaconPoint's Discovery Process and LED Sequence

As soon as the BeaconPoint is powered and connected to the LAN, it begins its automatic process to discover and register with the BeaconMaster.

For the BP200 the Status LED in the centre also indicates power. The Status LED is dark when unit is off and is green (solid) when the BP has completed discovery and is operational.



The BeaconPoint boot sequence is described below:

1. When powered on, the BeaconPoint status LED turns from dark to green briefly.
   Status LED: green (solid) then to dark before beginning boot sequence.
2. [available in Release 2.0 only] The BeaconPoint performs a self-test.
   [available in Release 2.0 only] *Status LED: red (solid) if POST failed.*
3. The "Discovery" mode: the BeaconPoint sends a request to the DHCP server on the enterprise network for the location of the BeaconMaster. (This is accomplished through a combination of Service Location Protocol (SLP) and DHCP, as described above.)
   Status LED: orange (solid) while searching ("Discovery")
   Status LED: red-orange (alternate blink) if DHCP server not found on network
   Status LED: green-orange (alternate blink) if SLP issues in failed discovery.
4. The BeaconPoint "learns" the IP address of the BeaconMaster,
   Status LED: orange (blink) when IP address successfully obtained ("Registration" process underway)
   Status LED: red (blink) if "Registration" fails
5. The BeaconPoint sends its serial number (a unique identifier that is hard coded during manufacture) to the BeaconMaster.
   Status LED: green (blink) when BeaconPoint finds BeaconMaster ("Standby" status)
6. The BeaconMaster sends the BeaconPoint a port IP address and a binding key, as follows:
   - If the BeaconMaster does not recognize the serial number, it sends a default configuration to the BeaconPoint.

Chantry Networks Inc. Copyright 2004. All rights reserved.

- If it does recognize the serial number, it sends the specific configuration (port and binding key) set for that BeaconPoint.

The BeaconMaster also adds the BeaconPoint to its database.

Status LED: green (blink) when BeaconPoint finds BeaconMaster ("Standby" status)

7. When the binding key is received, the BeaconPoint's status changes from "Standby" to "Active". It becomes active and is enabled to transmit data traffic. *LED: green steady ("Active")*

When the BeaconPoint has wireless traffic, you will see a green blink on the traffic LED. On the BP200, the left LED indicates the traffic LED for activity on the 2.4 GHz radio, while the right LED indicates activity on the 5 GHz radio.

Once a BeaconPoint is registered with a BeaconMaster:

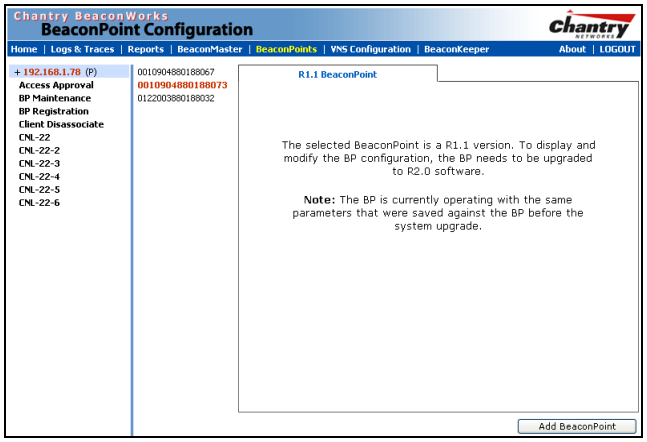
- it appears in the side list in the *BeaconPoint Configuration: Properties* screen, where you can modify the properties and radio parameters.
- its two radios appear as available choices in the *Virtual Network Configuration: Topology* screen, when you are setting up a VNS (for up to four VNS for each radio).

Note: Before a registered BeaconPoint can handle wireless traffic, you must set up a VNS definition, and assign the BeaconPoint's radios to a VNS. See *Virtual Network Configuration*.

BeaconPoint: Configuring Properties and Radios

View and modify properties of registered BeaconPoints

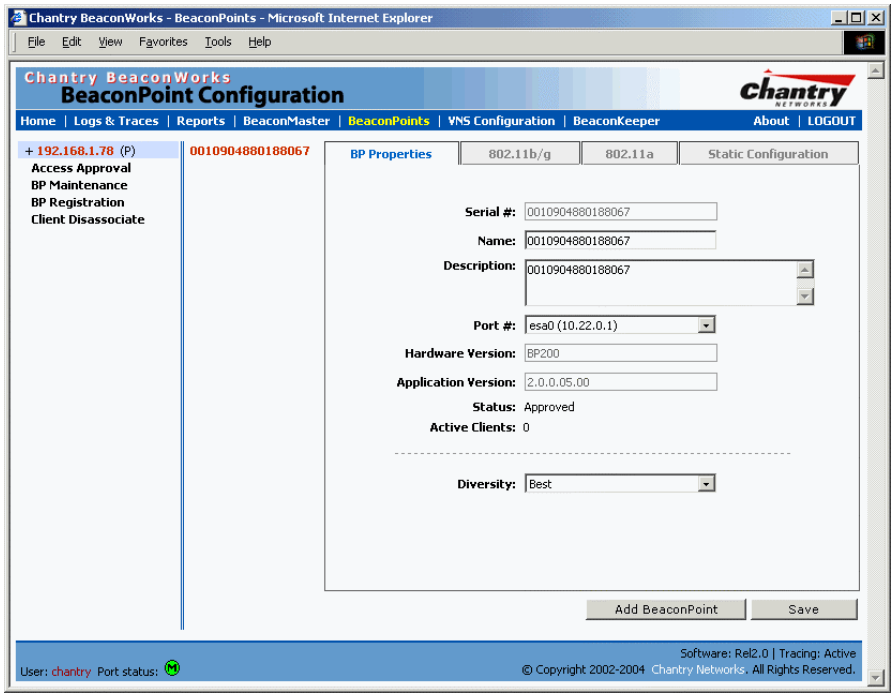
1. Select the **BeaconPoints** tab in any screen. The *BeaconPoint Configuration* screen appears, with a list of registered BeaconPoints.
2. Highlight the appropriate BeaconPoint in the list.
3. If the selected BeaconPoint is running Release 1.1 software, the properties cannot be modified. You will see the following message:



Screen 14: BeaconPoint Configuration: Message R1.1 version of BP software

To schedule a software upgrade for the BeaconPoint, use the *BeaconPoint Configuration: BP Maintenance* screen, described later in this guide.

4. For a BeaconPoint running Release 2.0 software, click on the **BP Properties** tab to view basic information about the highlighted BeaconPoint.



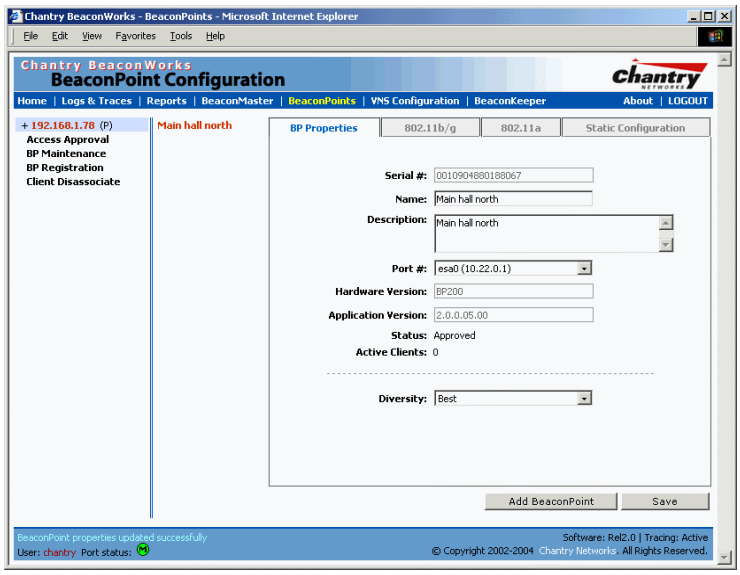
Screen 15: BeaconPoint Configuration – Properties

5. To modify the default information about a selected BeaconPoint, key in information in the following fields (where appropriate):

Serial #	(Display only) A unique identifier set during manufacture.
Name	Change the serial number to a unique descriptive name that more easily identifies the BeaconPoint.
Description	Available for descriptive comments (optional).
Port #	From the drop-down list, select the ethernet port through which the BeaconPoint can be reached.
Hardware Version	(Display only) Current version of the BeaconPoint hardware.
Application Version	(Display only) Current version of the BeaconPoint software.
Status	(Display only) "Approved" = BeaconPoint has received its binding key from the BeaconMaster after the Discovery process. "Pending" = binding key not yet received.
Active Clients	(Display only) The number of wireless devices currently active on the BeaconPoint.
Diversity	From the drop-down list, select "Best," for the best signal from both antennas, or "Left" or "Right" to choose either of the two diversity antennas.

Note: You can modify the status of a BeaconPoint (for example from "Pending" to "Approved") in the *Access Approval* screen.

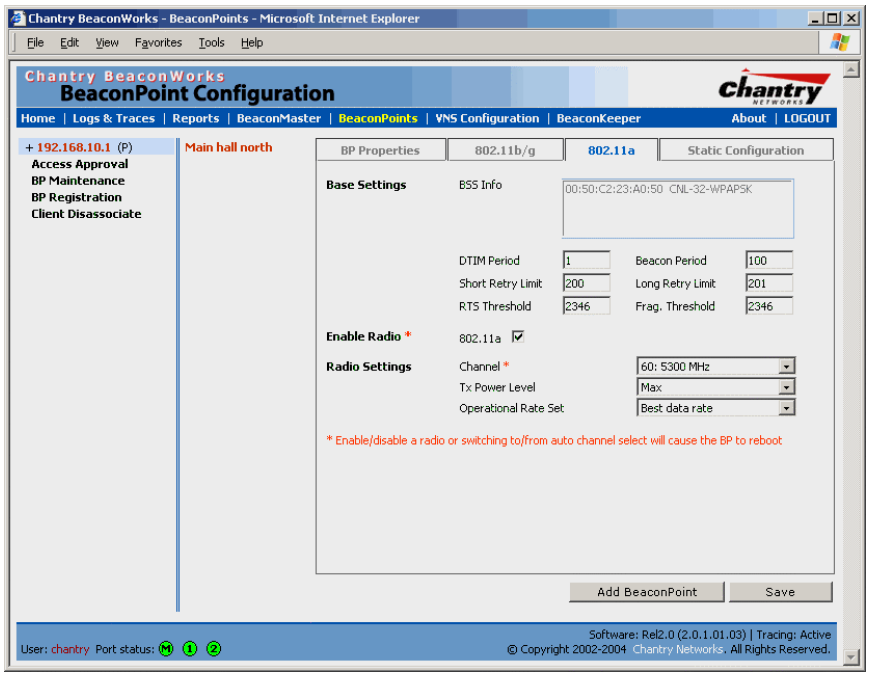
3. To save the modified information, click on the **Save** button.



Screen 16: BeaconPoint Configuration – Properties (after modifications)

View and modify the radio settings of registered BeaconPoints

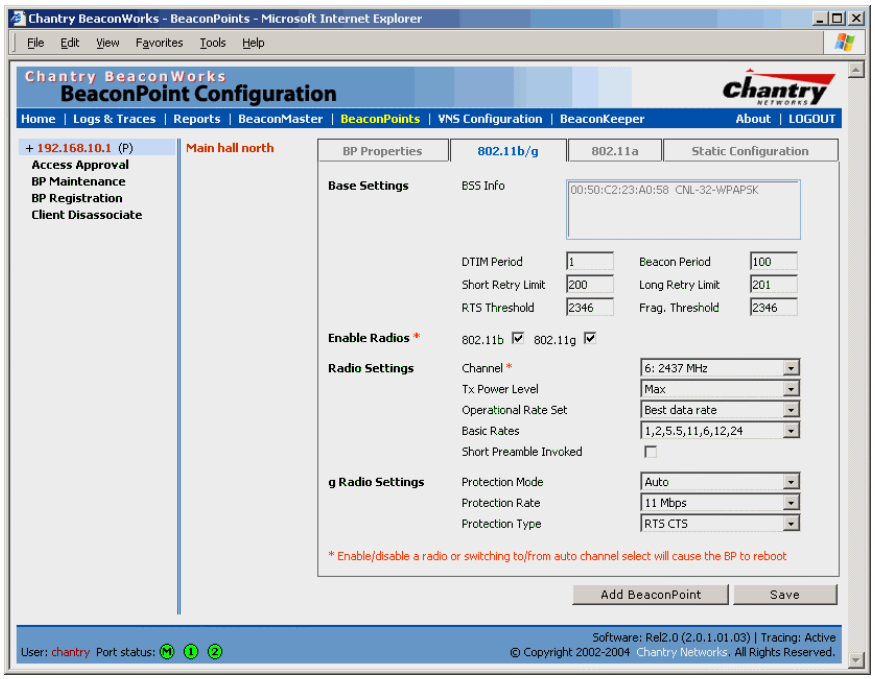
1. Select the **BeaconPoints** tab in any screen. The *BeaconPoint Configuration* screen appears, with a list of registered BeaconPoints.
2. Highlight the appropriate BeaconPoint in the list. Then click on the appropriate radio tab:
   - **802.11a** (5 GHz radio)
   - **802.11 b/g** (2.4 GHz radio)



Screen 17: BeaconPoint Configuration – Radio 802.11a (5 GHz)

The screen displays the default radio settings for each radio on the BeaconPoint.

> **Note:** If this radio has been assigned to a VNS (or up to four VNSs), the VNS names and MAC addresses will be displayed in the Base Settings area. (See *Virtual Network Configuration*.)



Screen 18: BeaconPoint Configuration – Radio 802.11b/g (2.4 GHz)

3. Modify these **Base Settings** where appropriate.

BSS Info	(Display only) After VNS configuration, the Basic Service Set (BSS) area displays the MAC address on the BeaconPoint for each VNS and the SSIDs of the VNSs to which this radio has been assigned.
DTIM	Delivery Traffic Indication Message period. Default is 1.
Beacon Period	The time units between beacon transmissions. Default is 100.
Short Retry Limit	The maximum number of transmission attempts of a frame that is less than or equal to the RTS Threshold, before a failure condition is indicated. Default is 200.
Long Retry Limit	The maximum number of transmission attempts of a frame that is greater than the RTS Threshold, before a failure condition is indicated. Default is 201.
RTS Threshold	Request To Send Threshold, the size of a data unit below which an RTS/CTS (RTS/Clear to Send) handshake is not performed. Default is 2346.
Frag. Threshold	The Fragmentation Threshold, the maximum size of a packet or data unit that can be delivered. Default is 2346.
Enable Radios	Click checkbox on for each radio.

Radio Settings:

Channel (Drop-down list) The wireless channel that the BeaconPoint should use to communicate with wireless devices.

802.11a	802.11b/g
Auto	Auto
36: 5180 MHz	1: 2412 MHz
40: 5200 MHz	2: 2417 MHz
44: 5220 MHz	3: 2422 MHz
48: 5240 MHz	4: 2437 MHz
52: 5260 MHz	5: 2432 MHz
56: 5280 MHz	6: 2437 MHz
60: 5300 MHz	7: 2442 MHz
64. 5320 MHz	8: 2447 MHz
149: 5745 MHz	9: 2452 MHz
153: 5765 MHz	10: 2457 MHz
157: 5785 MHz	11: 2462 MHz
161: 5805 MHz	
165: 5825 MHz	

Tx Power Level (Drop-down list) Min, 13%, 25%, 50%, Max.

Operational Rate Set (Drop-down list) in Mbps
A: Best data rate, 6, 9 12,18, 24, 36, 48, 54
B/G: Best data rate, 1, 2, 5.5, 11, 6, 9 12,18, 24, 36, 48, 54

Basic Rates (for b radio only) Select a set of basic rates from the drop-down list. The best data rate from the set will be used for current conditions (power vs range)

Short Preamble Invoked Click checkbox on to enable.

g Radio Settings:

Protection Mode (Drop-down list) None, Auto (default), Always

Protection Rate (Drop-down list) in Mbps: 1, 2, 5.5, 11 (default)

Protection Type (Drop-down list) CTS (Clear To Send),
RTS CTS (Request To Send, Clear To Send) – default.

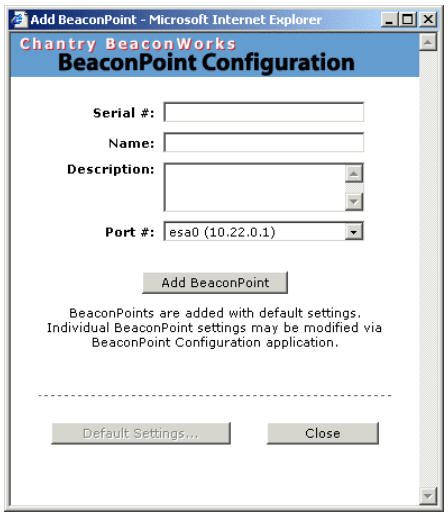
4. To save the modified information, click on the **Save** button.

Note: In Release 2.0, a number of the properties of each radio on a BeaconPoint can be modified (in the *BeaconPoint Configuration* screen) without requiring a reboot of the BeaconPoint.
However, modifying the following properties will trigger a reboot of the BeaconPoint:
- enabling or disabling either radio
- changing the radio channel between "Auto" and any fixed channel number.

BeaconPoint: Adding Manually

Add and register a BeaconPoint manually

1. Select the **BeaconPoint** tab. In the *BeaconPoint Properties* screen, click on the **Add BeaconPoint** button. The *BeaconPoint Configuration* subscreen appears.



Screen 19: BeaconPoint Configuration – Add BeaconPoint

3. Key in, or select from the drop-down list, information in the following fields:

Serial #	A unique identifier set during manufacture.
Name	A unique name for the BeaconPoint.
Description	Available for descriptive comments (optional).
Port #	The ethernet port through which the BeaconPoint can be reached

4. To add the BeaconPoint, click the **Add BeaconPoint** button.
   To return to the previous screen, click **Close**.

The BeaconPoint is added with default settings. To modify these settings, use the *BeaconPoint Configuration* screens described earlier. You can modify the properties and the settings for each radio on the BeaconPoint.

BeaconPoint Radios on a VNS

Before a registered BeaconPoint can handle wireless traffic, you must set up a VNS definition, and assign one or both of the BeaconPoint's radios to a VNS. See *Virtual Network Configuration* section for details.

After you have set up *Virtual Network Configuration* definitions and assigned the BeaconPoint radios to a VNS (or up to four VNSs), the VNS names and the MAC addresses are displayed in the Base Settings: "BSS Info" area.

BeaconPoint Static Configuration: Branch Office Deployment

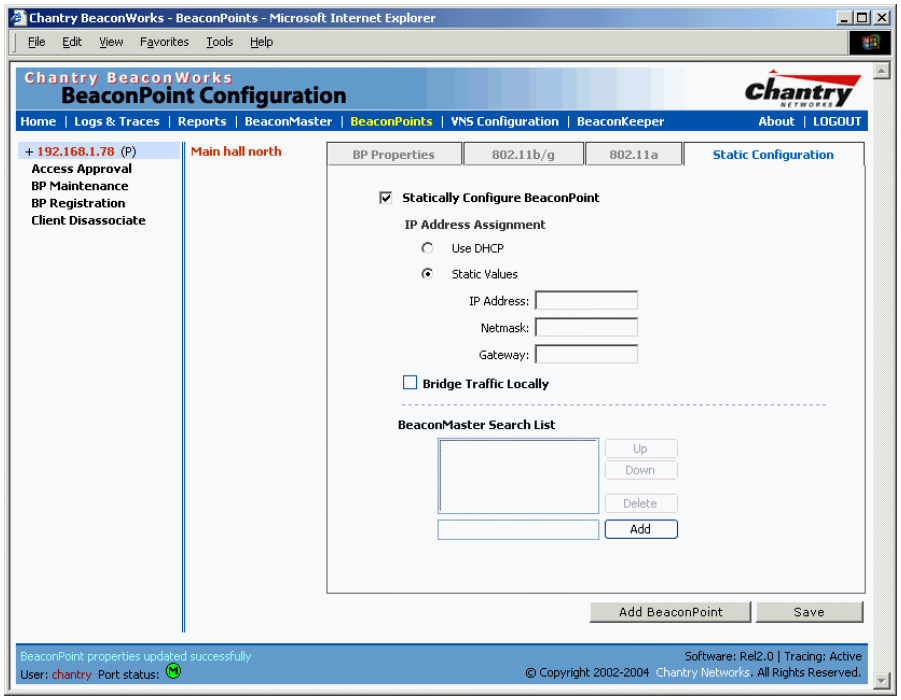
The BeaconPoint static configuration feature provides BeaconWorks capability for a network with the central office / branch office model.

In the branch office scenario, BeaconPoints are installed in remote sites, while the BeaconMaster is in the central office. The BeaconPoints require the capability to interact both in the local site network and in the central network.

To achieve this, the BeaconPoint's automatic process of discovery and registration with the BeaconMaster is disabled, and a static configuration is used instead.

Set up a BeaconPoint with static configuration

1. Select the **BeaconPoint** tab in any screen. In the *BeaconPoint Properties* screen, click on the **Static Configuration** tab. The *Static Configuration* screen appears.



Screen 20: BeaconPoint Configuration: Static Configuration

2. To enable static configuration of the BeaconPoint, click the **Statically Configure BeaconPoint** checkbox on.
3. Select one of the two methods of IP address assignment for the BeaconPoint:
   - to enable **DHCP**, click the radio button on (default), *or*
   - to specify the IP address of the BeaconPoint, click the **Static Values** radio button on and fill in the IP Address, Subnet Mask, and Gateway.

Note: For first time deployment of the BeaconPoint for a Branch Office scenario, it is recommended that you use DHCP initially on the central office network to obtain an IP address for the BeaconPoint.
Then enter these values in the *Static Configuration* screen for this BeaconPoint and save the configuration.

4. Add a BeaconMaster IP address to the list of BeaconMasters. Click in the entry field and key in the address of the BeaconMaster that will control this BeaconPoint. This allows the BeaconPoint to bypass the discovery process. If this field is not filled in, the BeaconPoint will use SLP to discover a BeaconMaster.
5. To save the static configuration, click on the **Save** button.

Note: In a "Branch Office" scenario, where the BeaconPoint is configured statically to function on a local network whose MTU is lower than 1500, a mechanism on the BeaconMaster automatically adjusts the MTU size to prevent packet fragmentation. The MTU is set in the *BeaconMaster Configuration – IP Addresses / Interfaces* screen and should not be changed.

Virtual Network Services (VNS): Overview

Virtual Network Services (VNS) are the key to the advantages that the Chantry BeaconWorks system has to offer. This technique provides a versatile means of mapping wireless networks to the topology of an existing wired network.

When you set up a VNS on the BeaconMaster, you are defining a subnet for a group of wireless device users. This VNS definition creates a virtual IP subnet where the BeaconMaster acts as a default gateway to wireless devices.

Before you begin to define a VNS, you should have determined:

- a *user access plan* for both individual users and user groups
- the RADIUS attributes that support the user access plan
- the location and identity of the BeaconPoints that will be used on the VNS
- the routing mechanism to be used on the VNS
- the network addresses that the VNS will use
- the type of authentication for wireless device users on the VNS
- the specific filters to be applied to the defined users and user groups to control network access
- what privacy mechanisms should be employed between the BeaconPoints and the wireless devices.
- whether the VNS is to be used for voice traffic.

The *user access plan* should analyze the enterprise network and identify which users should have access to which areas of the network. What areas of the network should be separated? Which users can go out the World Wide Web?

The BeaconWorks system relies on authenticating users via a RADIUS server (or other authentication server). To make use of this feature, you will, of course, require such an authentication server on the network. Make sure that the server's database of registered users, with login identification and passwords, is current.

Note: It is possible to deploy BeaconWorks without a RADIUS server (and without the authentication of users on the network). In that scenario, select **SSID** as the network assignment (in the *Topology* screen described later in this section) and then, in the *Authentication* screen, click on the **None** radio button. That means there is no authentication of users, but BeaconWorks is otherwise operational.

The user access plan should also identify the user groups in your enterprise, and the business structure of the enterprise network. You could identify users for various purposes, as in these examples:

- department (such as Engineering, Sales, Finance)
- role (such as student, teacher, library user)
- status (such as guest, administration, technician).

For each user group, you should set up a Filter ID attribute in the RADIUS server, and then associate each user in the RADIUS server to at least one Filter ID name.

Chantry Networks Inc. Copyright 2004. All rights reserved.

Chantry enables you to define specific filtering rules, by Filter ID attribute, that will be applied to user groups to control network access.

What is a VNS?

A VNS is an IP subnet that is especially designed to enable Chantry BeaconPoints to interact with wireless devices.

In many ways, a VNS is very similar to a regular IP subnet. However, it has the following required features:

1. Each VNS is assigned a unique identifier.
2. Each VNS is assigned an SSID. These do not have to be unique.
3. Each VNS is assigned a range of IP addresses for wireless devices. All the wireless devices share the same IP address prefix (the part of the IP address that identifies the network and subnet).

   The IP addresses of the wireless devices are assigned dynamically by the BeaconMaster's DHCP server within the assigned range.

   (These IP addresses are not "virtual". They are regular IP addresses, and are unique over the network. These IP addresses are *advertised* to other hosts on the network so that they can exchange traffic with the wireless devices in the VNS.)

Note: Alternatively, you can allow the enterprise network's DHCP server to provide the IP addresses for the VNS, by enabling *DHCP Relay* in the Topology screen.

4. A single overall filtering policy applies to all the wireless devices within the VNS. However, further filtering can be applied when the wireless user is authenticated by the RADIUS server.
5. When the BeaconMaster creates the VNS, it also creates a *virtual IP subnet* for that VNS.

Topology of a VNS: Overview

The first step in setting up a VNS is configuring the topology in the *Topology* screen. The type of network assignment determines all the other factors of the VNS. The options for network assignment are:

- **SSID**:
  - has Captive Portal authentication, or no authentication.
  - requires restricted filtering rules before authentication and, after authentication, filtering rules for group Filter IDs.
  - is used for a VNS supporting wireless voice traffic (QoS).
  - is used for a VNS supporting third-party APs.
  - has WEP privacy.
- **AAA** (Authentication, Authorization and Accounting).
  - has 802.1x authentication
  - requires filtering rules for group Filter IDs and default filter.
  - has WEP and WPA privacy.

Chantry Networks Inc. Copyright 2004. All rights reserved.

The next step to assign the available BeaconPoints (by radio) to the VNS.

Multi-SSID: BeaconPoint radios on more than one VNS

In Release 2.0, each radio on a BeaconPoint BP200 can participate in up to four VNSs, for a total of eight VNSs per BeaconPoint. The *Topology* screen displays a list of registered BeaconPoints with a checkbox for each radio. A BeaconPoint radio will appear in the list as available for VNS assignment until it has been assigned to four VNSs. After that, it will no longer appear in the list.

After a VNS definition has been saved, the BeaconMaster updates this information on the BeaconPoint. Each radio acquires up to four SSIDs (one for each VNS it is part of), and broadcasts these during beacon transmission (unless the beacon is suppressed in the VNS topology screen).

You can view (in the *BeaconPoint Configuration* screen) a list of defined VNSs to which each radio has been assigned.

Other network parameters for the VNS topology

In the *Topology* area of VNS configuration, you also define other aspects of the VNS, such as the parameters for DHCP for IP address assignment. You might also configure this VNS for management traffic only, or for Third-Party Access Points, or for Voice Traffic. (These are described in detail later in this Guide.)

Network Assignment and Authentication for a VNS

The second step is to configure the authentication mechanism for the VNS. The authentication mechanism depends on the network assignment.

Authentication with SSID Network Assignment

If **SSID** was selected, there are two authentication options:

- *None*: The wireless device connects to the network, but can only access specified network destinations (those defined in the **Non-Authenticated Filter** described in *Filtering*). No authentication is performed.
- *Captive Portal*: The wireless device connects to the network, but can only access specified network destinations (those defined in the **Non-Authenticated Filter** described in *Filtering*). One of those destinations is a web page logon screen (the portal in which he is captive), where the user must input an ID and a password. This identification is sent by the BeaconMaster to the RADIUS server for authentication. Four authentication types are supported by BeaconWorks for Captive Portal:
  - PAP (Password Authentication Protocol)
  - CHAP (Challenge Handshake Authentication Protocol)
  - MS CHAP (Windows-specific version of CHAP)
  - MS CHAP v2 (Windows-specific version of CHAP, version 2)

Note: For Captive Portal, the RADIUS server must support the selected authentication type: PAP, CHAP (RFC2484), MS-CHAP (RFC2433), MS-CHAPv2 (RFC2759).

Authentication with AAA (802.1x) Network Assignment

If **AAA (802.1x)** was selected, the wireless device user requesting network access via BeaconWorks must first be authenticated. The wireless device's client utility must support 802.1x. The user's request for network access along with login identification or user profile will be forwarded by the BeaconMaster to a RADIUS server. BeaconWorks supports these authentication types:

- EAP-TLS Extensible Authentication Protocol - Transport Layer Security that relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.
- EAP-TTLS (EAP with Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
- PEAP (Protected Extensible Authentication Protocol) is a standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user.

Note: For 802.1x, the RADIUS server must support RADIUS extensions (RFC2869).

If the RADIUS servers sends an "access-accept" message to the BeaconMaster, the BeaconMaster's DHCP server assigns the device its IP address and allows network access controlled by the filtering rules defined for the specific Filter ID associated with the wireless device user.

RADIUS Server: Location and Redundancy

Both Captive Portal and AAA (802.1x) authentication mechanisms in BeaconWorks rely on a RADIUS server on the enterprise network.

In BeaconWorks Release 2.0, up to three RADIUS servers can be identified and prioritized on the BeaconMaster. This means that in the event of a failover of the active RADIUS server, the BeaconMaster will poll the other servers in the list for a response.

Filtering for a VNS: How it works

The Chantry VNS capability provides a technique to apply policy, to allow different network access to different groups of users. This is done by packet filtering.

After setting up the authentication, the next step is to define the filtering rules for the filters that apply to your network and the VNS you are setting up.

Three types of filters are applied by the BeaconMaster in the following order:

1. Non-Authenticated filter, with filtering rules that apply before authentication, to control network access and to direct users to a Captive Portal web page for login.
2. Group filters (by Filter ID) for designated user groups, to control access to certain areas of the network, with names that match defined RADIUS Filter ID attributes.
3. Default filter, to control access if there is no matching Filter ID for a user.

Chantry Networks Inc. Copyright 2004. All rights reserved.

Within each type of filter, you define a sequence of filtering rules. This sequence must be carefully planned and arranged in the order that you want them to take effect. You define each rule to either *allow* or *deny* traffic in either direction:

- "In": from a wireless device in to the network
- "Out": from the network out to the wireless unit.

Note: The final rule in any filter should be a catch-all for any traffic that did not match a filter. This final rule should either "allow all" or "deny all" traffic, depending on the requirements for network access. For example, the final rule in a *Non-Authenticated Filter* for Captive Portal is typically "deny all". A final "allow all" rule in a Default Filter will ensure that a packet is not dropped entirely if no other match can be found.

Each rule can be based on any *one* of the following:

- destination IP address, or any IP address within a specified range that is on the network subnet (as a wildcard)
- ports, by number and range
- protocols (UDP, TCP, etc.)

This is how the BeaconMaster software filters traffic:

1. The BeaconMaster software attempts to match each packet of a VNS to the filtering rules that apply to the wireless device user.
2. If a filtering rule is matched, the operation (allow or deny) is executed.
3. The next packet is fetched for filtering.

The filtering sequence depends on the type of authentication:

- **No authentication (network assignment by SSID)**
  Only the Non-Authenticated filter will apply. Specific network access can be defined. Since there will be no authentication, the final rule should be "deny all".
- **Authentication by Captive Portal (network assignment by SSID)**
  The Non-Authenticated filter will apply before authentication. Specific network access can be defined. The filter should also include a rule to allow all users to get as far as the Captive Portal webpage where the user can enter login identification for authentication. When authentication is returned, then the Filter ID group filters are applied. If no Filter ID matches are found, then the Default filter is applied.
- **Authentication by AAA (802.1x)**
  Since users have already logged in and have been authenticated, there is no need for a Non-Authenticated filter. When authentication is returned, then the Filter ID group filters are applied. For AAA, a VNS can have a subgoup with Login-LAT-group ID that has its own filtering rules. If no Filter ID matches are found, then the Default filter is applied.

Privacy on a VNS: Overview of WEP and WPA

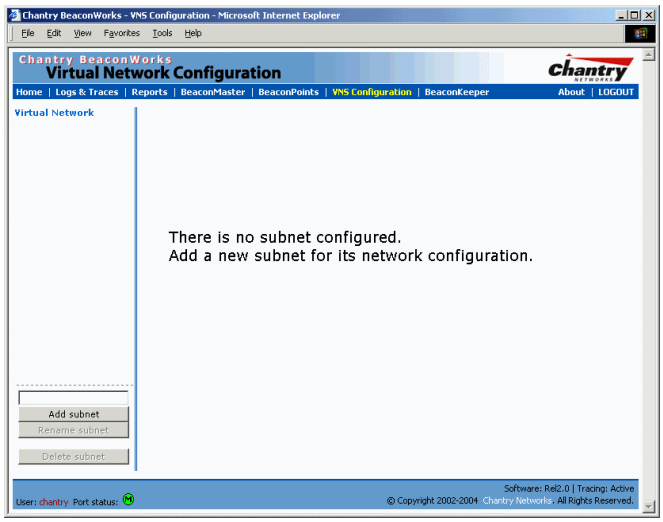
Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques.

BeaconWorks supports the Wired Equivalent Privacy (WEP) standard common to conventional access points. WEP provides data confidentiality services by encrypting the data sent between wireless nodes. Each node must use the same encryption key.

For a VNS with AAA network assignment, BeaconWorks also provides Wi-Fi Protected Access (WPA) privacy, a solution that adds authentication and enhanced WEP encryption with key management. WPA is available in Enterprise Mode (which specifies 802.1x authentication and requires an authentication server) or in Pre-Shared Key mode (which relies on a shared secret). Encryption is by Temporal Key Integrity Protocol (TKIP), which changes the encryption key after a specified interval.

Setting up a new VNS

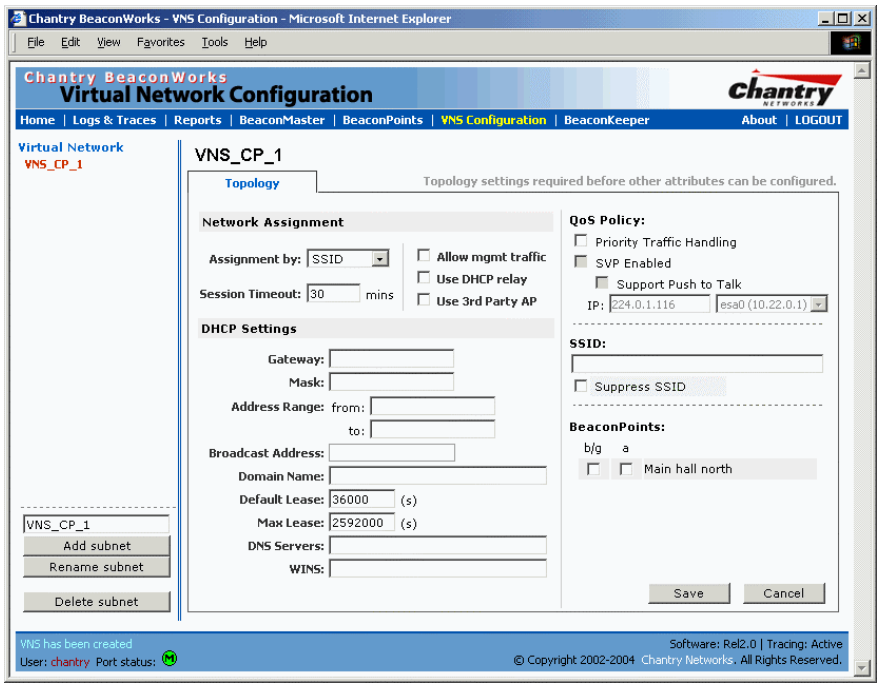
Click on the **Virtual Network Configuration** tab in any screen. The *Virtual Network Configuration* screen appears. For a new BeaconWorks installation, where no VNS has yet been defined, the screen is blank, except for the **Add subnet** function.



Screen 21: Virtual Network Configuration: Before any VNS definitions

Create a subnet (VNS)

1. In the entry field above the **Add subnet** button, key in a name that will uniquely identify the new VNS.
2. Click on the **Add subnet** button. The name appears in the left-hand list. The *Topology* screen appears.
3. Highlight the name of the subnet you wish to configure. Its parameters can be configured now in the *Topology* screen.



Screen 22: Virtual Network Configuration: Topology for a new VNS Subnet

Configure the new VNS (overview of basic steps)

1. Select the network assignment mechanism from the **Assignment by** drop-down list:
   - **SSID**
   - **AAA**
2. In the **SSID** box at the right, key in the SSID that the wireless devices will use to access the BeaconPoint.
3. Select the **BeaconPoints** (by radio) to be assigned to this VNS. The displayed list of available **BeaconPoints** has a checkbox for each radio on the BeaconPoint. Each radio on a BeaconPoint can be assigned to a maximum of four VNSs. When this maximum is reached, the radio will no longer be available in this list.
4. Configure other options for this VNS: Allow Management Traffic, Use DHCP Relay, Use 3rd Party APs, or Enable Priority Traffic Handling.
5. Define the DHCP settings for this VNS.
6. To save the new VNS Topology, click on the **Save** button.

When the new Topology has been saved, the screen changes to display tabs for *Authentication*, *Filtering* and *Privacy*, for configuring these aspects of the new VNS.

The next sections explain several scenarios for possible VNS configurations:

- VNS for Captive Portal: Network Assignment by SSID and Authentication by Captive Portal
- VNS with no Authentication: Network Assignment by SSID and no Authentication
- VNS for Voice Traffic
- VNS with 802.1x Authentication: Network Assignment by AAA (802.1x)

Virtual Network Configuration: A VNS for Captive Portal

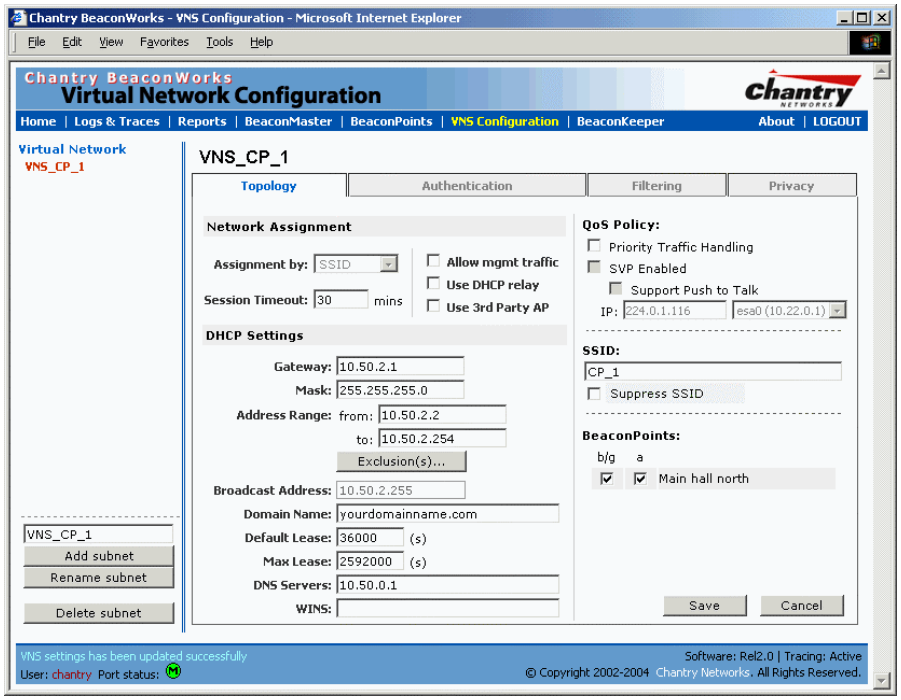
This section describes how to set up a VNS for Captive Portal: its Topology, Authentication, Filtering and Privacy.

If the authentication technique for network assignment is by Captive Portal, the process is as follows. The wireless device requesting network access via BeaconWorks first gets its IP network assignment from the DHCP server, but can access only the specific IP addresses defined in the **Non-Authenticated Filter**. Typically, one of these addresses is a *Captive Portal web page*, where the wireless device user can log in and become authenticated.

Topology for a VNS for Captive Portal

For a VNS with Captive Portal authentication, select Network Assignment by SSID in the *Topology* screen.

In the *Virtual Network Configuration* screen, highlight the VNS name in the left-hand list and click on the **Topology** tab.



Screen 23: Virtual Network Configuration – Topology – SSID Assignment

Create an SSID for Captive Portal VNS

1. Using the **Assignment by** drop-down list, select **SSID**.
2. In the **SSID** box at the right, key in the SSID that the wireless devices will use to access the BeaconPoint.
3. Click the **Suppress SSID** checkbox on to prevent this SSID from appearing in the beacon message sent by the BeaconPoint. The wireless device user seeking network access will not see this SSID as an available choice, and will need to specify it.

4. In the **Session Timeout** box, key in the number of minutes that a wireless device can be inactive before the BeaconMaster closes the session.

Identify the BeaconPoint radios that will be assigned to this VNS

5. From the displayed list of **BeaconPoint Radios** that are available throughout the network, check the ones to be assigned to this VNS.
   Once you have assigned a BeaconPoint radio to four VNSs, it will not appear in the list for another VNS setup.

Note: You can view the VNSs that each radio is participating in by clicking on the appropriate tab for each radio in the *BeaconPoint Configuration* screen

Enable Management Traffic on this VNS

6. To allow Management Traffic on this VNS, click the **Allow management traffic** checkbox on.

Note: This choice invokes the built-in port-based filtering rules for Management Traffic, as described earlier in the "Port Type or Function" topic.

Enable Third Party Access Points on this VNS

7. If this VNS is to be used for third-party access points, click the **Use 3rd Party AP** checkbox on. The screen changes to include fields to enter the IP Address and MAC Address of the third-party access point.

Note: Use this function as part of the process defined in the topic "Setting up a Third-Party Access Point". For further information, see that section in this Guide.

Enable QoS Policy for voice-over-internet traffic on this VNS

8. To set up this VNS to prioritize voice-over-internet traffic, click on the **Priority Traffic Handling** checkbox. Enable **SVP** by clicking on the checkbox.

Note: There is no authentication on a voice traffic VNS. For more information about a voice traffic VNS, see the "Quality of Service (QoS) on a VNS" in this Guide.

Set the IP address for the VNS (for the DHCP server on the BeaconMaster)

9. In the **Network Address** box, key in the network IP address for the VNS.

   This IP address is the *default gateway* for the VNS. The BeaconMaster advertises this address to the wireless devices when they sign on.

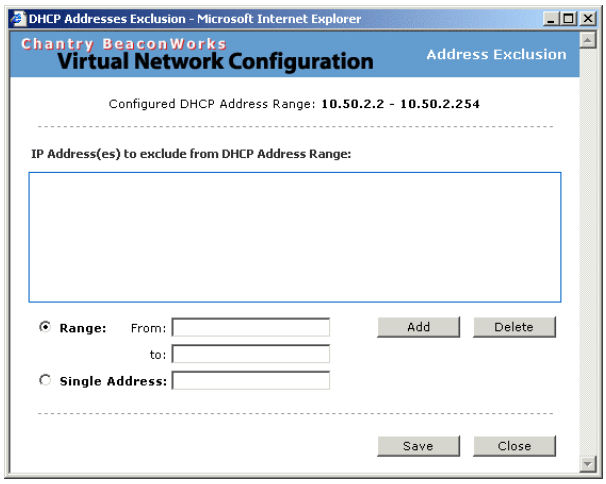
10. In the **Mask** box, key in the appropriate subnet mask for this IP address, to separate the network portion from the host portion of the address (typically 255.255.255.0)

    The **Address Ranges** fields populate automatically (based on the IP address you keyed in) with the range of IP addresses to be assigned to wireless devices using this VNS.

11. To modify the **Address Ranges,** key the first available address in the **from** box. Key the last available address in the **to** box.

12. If there are specific IP addresses to be excluded from this range, click on the **Exclusions** field. The *Exclusions* subscreen appears.

Chantry Networks Inc. Copyright 2004. All rights reserved.



Screen 24: Virtual Network Configuration – Exclusions subscreen

13. In the *Exclusions* subscreen, key in the IP addresses or address ranges to exclude. Click on the **Add** button after each entry. Click on the **Save** button to save the changes and return to the *Topology* screen.
14. The **Broadcast Address** field populates automatically, based on the IP address and subnet mask of the VNS. Modify this if appropriate..
15. In the **Domain Name** box, key in the external enterprise domain name.

Set time limits for IP assignments

16. In the **Default Lease** box, accept the default value of 3600 seconds (1 hour), or modify. This is the default time limit that an IP address would be assigned by the DHCP server to a wireless device.

    In the **Max Lease** box, accept the default value is 24000 seconds (40 hours), or modify. This is the maximum time that an IP address can be assigned.

Set the name server configuration

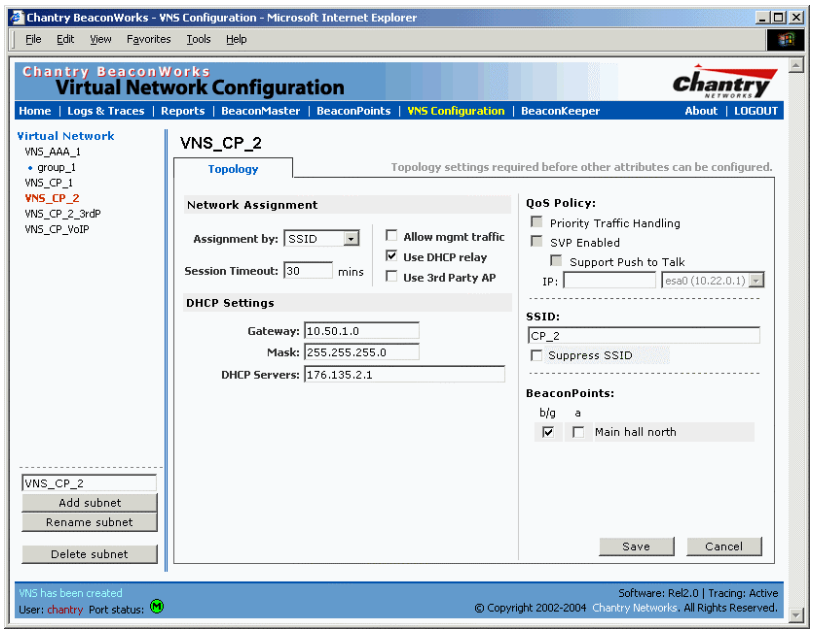
17. In the **DNS Servers** box, key in the IP Address of the Domain Name Server(s) to be used.
18. If the DHCP server uses WINS (Windows Internet Naming Service), key in the IP address in the **WINS** box. If not, leave it blank.

Use DHCP Relay for the VNS

Use **DHCP Relay** to force the BeaconMaster to forward DHCP requests to an external DHCP server on the enterprise network. This function will bypass the local DHCP server on BeaconMaster (to bypass steps 9 to 18 above). This function allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure.

19. To use an external DHCP server, click the **Use DHCP Relay** checkbox on. The *DHCP Settings* area of the screen changes to display only the **Gateway IP**, **Mask** and **DHCP Server** fields. Key in the appropriate IP addresses and mask to reach the enterprise's external DHCP server.

Note: The range of IP addresses to be assigned to the wireless device users on this VNS should also be designated on the external DHCP server.



Screen 25: Virtual Network Configuration – Topology – DHCP Relay

Save the new VNS

20. To save this VNS configuration, click on the **Save** button.

When the new Topology has been saved, the screen changes to display tabs for *Authentication*, *Filtering* and *Privacy*.

Authentication for a VNS for Captive Portal

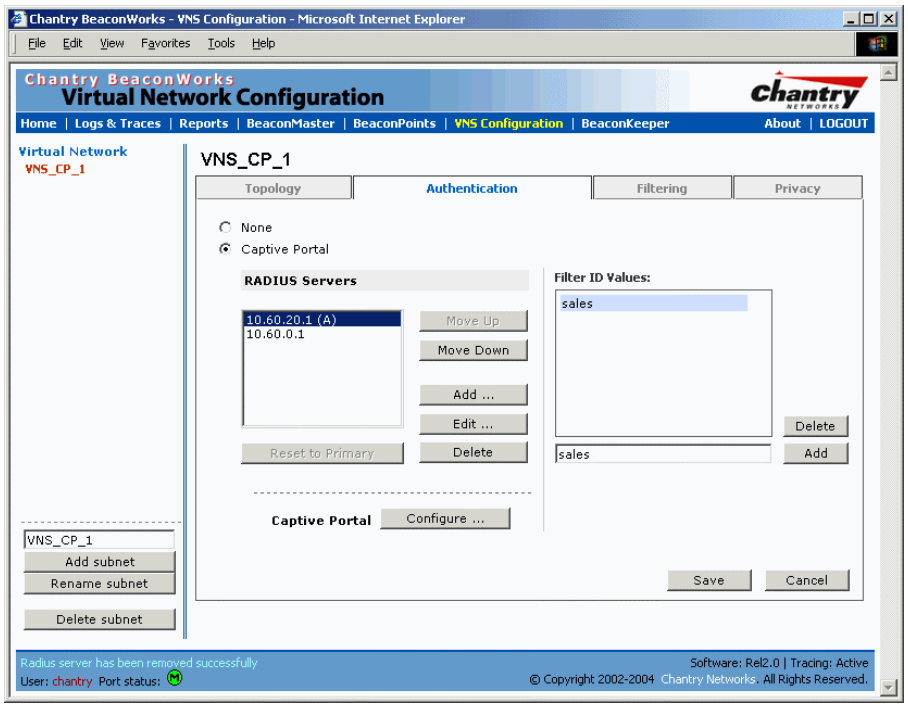
The next step is to set up the Authentication mechanism for Captive Portal.

For Captive Portal, the wireless device connects to the network, but can only access the specific network destinations defined in the Non-Authenticated Filter (see *Filtering*). One of these destinations should be a web page logon screen (the Captive Portal). The user must input an ID and a Password. This request for authentication is sent by the BeaconMaster to a RADIUS server.

Captive Portal authentication relies on a RADIUS server on the enterprise network. You can define more than one RADIUS server for authentication and define the priority of use in the event of a failover situation.

Set up authentication by Captive Portal

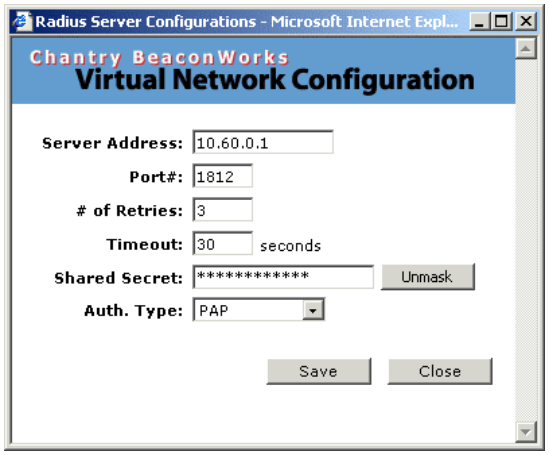
1. Highlight the VNS name. Click on the **Authentication** tab. In the *Authentication* configuration screen, click the **Captive Portal** radio button. The Captive Portal portion of the screen appears.



Screen 26: Virtual Network Configuration – Authentication – Captive Portal

Define how the BeaconMaster will access the RADIUS server.

2. For each RADIUS server to be defined, click on the **Add** button. The *RADIUS Server Configuration* popup window appears.



Screen 27: Virtual Network Configuration – Authentication CP – Add RADIUS Server

3. For each server, fill in the following fields:

Server Address	The IP address of the RADIUS server.
Port #	The port used to access the RADIUS server (default: 1812)
# of Retries	Number of times the BeaconMaster will attempt to access the RADIUS server
Timeout	The maximum time that a BeaconMaster will wait for a response from the RADIUS server, before attempting again (up to the maximum number of retries).

4. Key in the **Shared Secret** (a password that is required in both directions) that is set up on the RADIUS Server. This password is used to validate the connection between the BeaconMaster and the RADIUS Server.

   To display the shared secret (in order to proofread your entry before saving the configuration), click on the **Unmask** button. To mask the shared secret again, click on the button again (the button toggles between **Mask** and **Unmask**).

Note: This precautionary step is recommended at this point in order to avoid an error later when the BeaconMaster attempts to communicate with the RADIUS server.

5. Select the authentication protocol to be used by the RADIUS server to authenticate the users of the wireless devices (for Captive Portal authentication).

PAP	(Password Authentication Protocol)
CHAP	(Challenge Handshake Authentication Protocol)
MS CHAP	(Windows-specific version of CHAP)
MS CHAP v2	(Windows-specific version of CHAP, version 2)

6. To save these settings and return to the main *Authentication* screen, click on the **Save** button.
   To return to the main *Authentication* screen without saving, click on the **Close** button.

Define the RADIUS server priority for RADIUS Redundancy

After setting up a RADIUS server, its IP address will appear in the **RADIUS Servers** box. To allow for RADIUS server redundancy, set up one or two additional server, as described above (three is the maximum).

7. To define the priority of the servers, highlight a RADIUS server in the list and use the **Move Up** or **Move Down** key to change the order.

   The first server in the list is the active one.

   In the event of a failover of the main RADIUS server (if no response after the set number of retries), then the other servers in the list will be polled on a round-robin basis until one responds.

   If one of the other servers becomes the active one during a failover, an “A” will appear after that server name.

Note: If all defined RADIUS servers fail to respond, a critical message will be generated in the logs.

8. To remove a defined server from the list, highlight it and click on the **Delete** button.
9. To modify the parameters of a defined server, highlight it and click on the **Edit** button. In the RADIUS Server popup screen, follow steps 2 to 6 described above.

Note: It is recommended that the RADIUS databases with names, logins, and attributes be kept synchronous on all RADIUS servers.

Chantry Networks Inc. Copyright 2004. All rights reserved.

Define the Filter ID Values on this VNS.

10. In the **Filter ID Values** entry field, key in the name of a group that you want to define specific filtering rules for, to control network access. Click on the **Add** button. The Filter ID name appears in the list above.

    Repeat for additional Filter ID names.

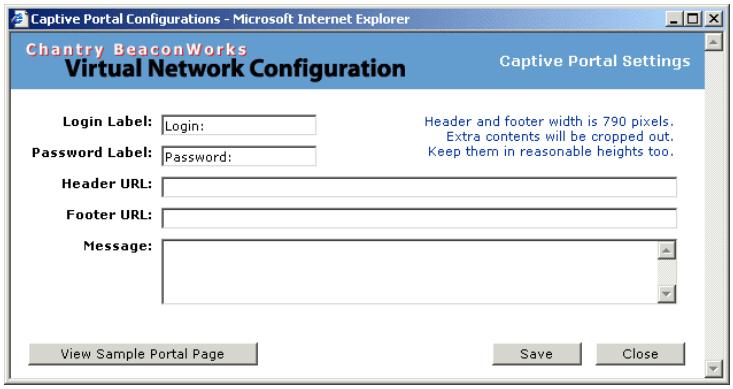
These Filter ID names will appear in the Filter ID list in the *Filtering* screen.

Note: These names must match the Filter ID attribute names in the RADIUS server.

11. To save the authentication parameters for this VNS, click on the **Save** button.

Configure the appearance of the Captive Portal page

1. To design how the Captive Portal authentication page will display for Captive Portal, click on the **Configure** button in the *Authentication* screen. The *Captive Portal Configuration* subscreen appears.



Screen 28: Captive Portal login configuration

2. Key in the text that will appear on the Captive Portal page.

Login Label	The text that will appear as a label for the user login field in the Captive Portal screen.
Password Label	The text that will appear as a label for the user password field

3. Key in the locations of the header and footers.

Header URL	The location of the file to be displayed in the Header portion of the Captive Portal screen. This page can be customized to suit your company, with logos or other graphics. (Caution: Ensure that such graphics in the header are not so large that they push the login area out of view.)
Footer URL	The location of the file to be displayed in the Footer portion of the Captive Portal screen.

Note: You can also add URLs in the header and footer that link to other websites, to allow the wireless device user to access to some specific areas of your enterprise, or to the World Wide Web, before authentication.

4. In the **Message** field, key in the message that will appear above the login field to greet the user. For example, this could explain why this Captive Portal page is appearing, and what the user should do.
5. To save this configuration, click on **Save**.
6. To see how the Captive Portal page you have designed will look (after saving the configuration), click on the **View Sample Portal Page** button.

Filtering Rules for a VNS for Captive Portal

The next step is to configure the filtering rules for a Captive Portal VNS. Three types of filters are required:

- Non-Authenticated Filter, with restrictive filtering rules that apply to all wireless device users *before authentication*.
- Filter ID filtering rules that apply *after authentication*, when the RADIUS server returns the "access-accept" message along with associated Filter ID for the user.
- Default filtering rules that apply *after authentication*, to control network access if there are no Filter ID matches for the user.

The Non-Authenticated Filter

The Non-Authenticated Filter should allow access to the Captive Portal page IP address, as well as to any URLs for the header and footer of the Captive Portal page. The filter should also allow network access to the IP address of the DNS server and to the Network Address, the Gateway, of the VNS (the VNS Gateway is used as the IP for the Captive Portal page).

You can also set up filtering rules to allow access, before authentication, to explicitly defined areas of the network. Then you must deny all other access.

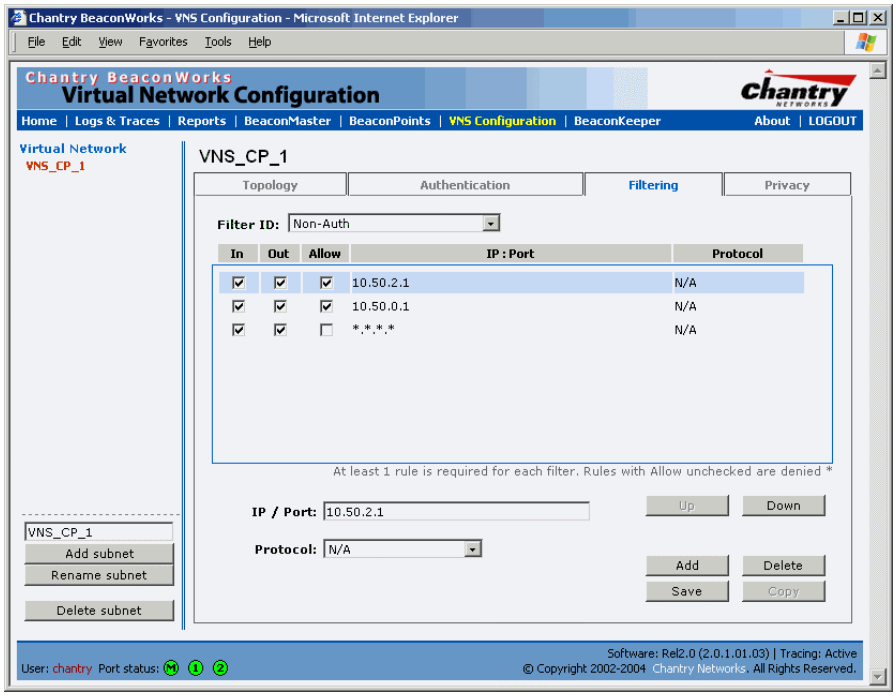
Redirection and captive portal credentials only apply to HTML traffic, that is, if a wireless device user is attempting to reach websites other than those specifically allowed in the Non-Authenticated Filter, they will be redirected to the allowed destinations.

All other network access will be controlled after the user is authenticated, when the Filter ID or Default filtering rules are applied. The wireless device user who does not authenticate will not get a wireless session.

Define filtering rules for a Non-Authenticated Filter

1. In the *Virtual Network Configuration* screen, click on the **Filtering** tab. The *Filtering* screen appears. Click on the subnet name in the left-hand list. The right portion of the screen displays the filtering screen for the selected subnet.
2. Using the **Filter ID** drop-down list, select **Non-Authenticated**.

Note: If you defined specific Filter ID Values in the *Authentication* screen, these Filter IDs will appear in **Filter ID** drop-down list.



Screen 29: Virtual Network Configuration – Non-Authenticated Filter for Captive Portal

The *Filtering* screen automatically provides a "Deny All" rule already in place. Use this rule as the final rule in the Non-Authenticated Filter for Captive Portal.

3. For each filtering rule you are defining:

   IP / Port: Type in the destination IP address. You can also specify an IP range, a port designation or a port range on that IP address.

   Protocol: Default is N/A. To specify a protocol, select from the drop-down list (may include UDP, TCP, IPsec-ESP, IPsec-AH, ICMP).

> **Note**: For Captive Portal, select **IP / Port** and key in the IP address you defined as the Network Address in the *Topology* screen for this VNS (its default gateway)

4. Click on the **Add** button.
   The information appears in a new line in the **Filter Rules** area of the screen.
5. Highlight the new filtering rule and fill in (or leave unchecked) the three checkboxes in the combinations that define the traffic access:

   In: Click checkbox *on* to refer to traffic from the wireless device that is trying to get on the network ("going to" the network)

   Out: Click checkbox *on* to refer to traffic from the network host that is trying to get to a wireless device. ("coming from" the network)

   Allow Click checkbox on to *allow*. Leave unchecked to *disallow*.

> **Note**: For Captive Portal, to allow access to the IP address, check all three boxes on.

6. Edit the order of a filtering rule by highlighting the line and clicking on the **Up** and **Down** button. The filtering rules are executed in the order defined here.
7. To save the filtering rules, click on the **Save** button.

Non-Authenticated Filters: Examples

A basic Non-Authenticated Filter for Captive Portal should have three rules in the following order:

In	Out	Allow	IP / Port	Description
x	x	x	IP address of the Default Gateway	Allow all incoming wireless devices access to the default gateway of the VNS.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the VNS.
x	x		*.*.*.*	Deny everything else.

Note: If you put URLs in the header and footer of the Captive Portal page, you must include a filtering rule to allow traffic to each of these URLs. Put this rule above the "deny everything" rule.

Here is another example of a Non-Authenticated Filter that adds two more filtering rules: one denies access to a specific IP address, and the next rule allows only HTML traffic, before denying all other access:

In	Out	Allow	IP / Port	Description
x	x	x	IP address of the Default Gateway	Allow all incoming wireless devices access to the default gateway of the VNS.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the VNS.
x	x		[a specific IP address, or address plus range]	Deny all traffic to a specific IP address, or to a specific range within an IP address (such as :0/24)
x	x	x	*.*.*.*:80	Allow all port 80 (HTML) traffic.
x	x		*.*.*.*.	Deny everything else.

Once a wireless device user has logged in on the Captive Portal page, and has been authenticated by the RADIUS server, then the following filters will apply:

- Filter ID Filter, if a Filter ID associated with this user was returned the authentication server
- Default Filter, if no matching Filter ID was returned from the authentication server.

These filters are described in detail in the *Filtering for an AAA VNS*.

Privacy using WEP for a VNS for Captive Portal

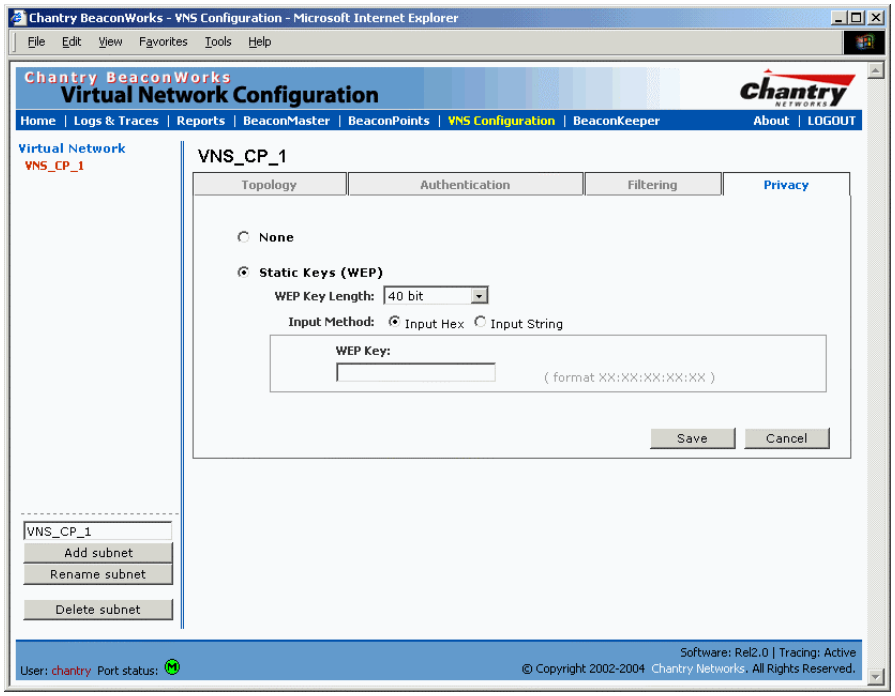
Use the *Privacy* screen to set up the static Wired Equivalent Privacy (WEP) keys for a selected VNS, so that it matches the WEP mechanism used on the rest of the network.

In BeaconWorks Release 2.0, you can assign each radio on a BeaconPoint to up to four VNSs by SSID. For each VNS, only one WEP key can be specified. BeaconWorks always uses the first key (key index 0).

Set up a Static WEP key for a selected VNS

1. In the *Virtual Network Configuration* screen, click on the **Privacy** tab. The *Privacy* screen appears.

2. Click on the VNS subnet name in the left-hand list. The right portion of the screen displays the privacy parameters for the selected subnet.
3. For no privacy mechanism on this VNS, click on the **None** radio button.
4. To configure static keys for WEP, click on the **Static Keys (WEP)** radio button.



Screen 30: Virtual Network Configuration – Privacy – Captive Portal VNS

5. From the drop-down list, select the **WEP Key Length:** 40-bit, 104-bit, 128-bit
6. Click on the appropriate radio button to select the **Input Method**: Input Hex, Input String.
7. Type in the WEP key input, as appropriate to the technique selected. The key is generated automatically, based on the input.
8. To save these settings, click on the **Save** button.

Virtual Network Configuration: A VNS with No Authentication

You can choose to set up a VNS that will bypass all Chantry authentication mechanisms and run BeaconWorks with no authentication of a wireless device user.

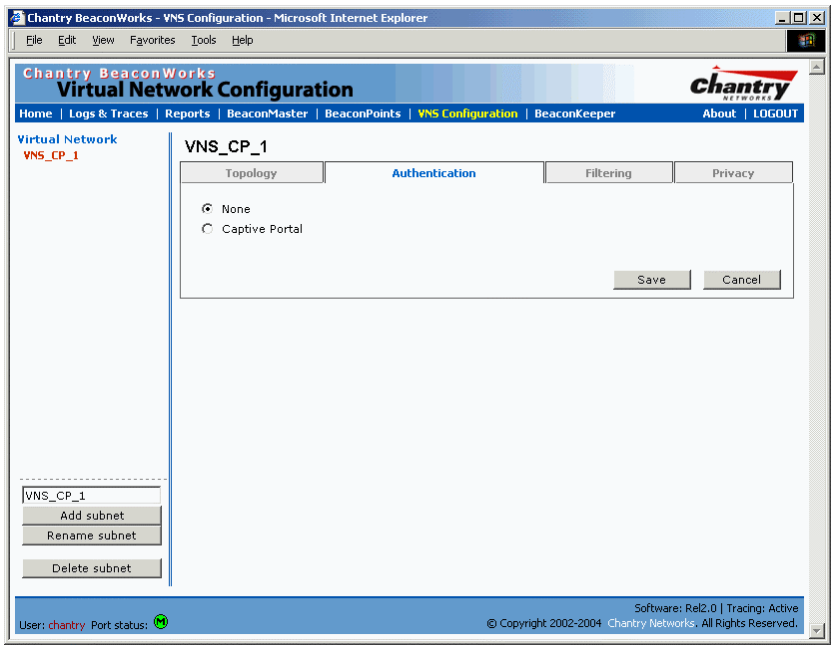
On such a VNS, however, you can still control network access with filtering rules. See the *Filtering Rules: Non-Authenticated Filter for Captive Portal* topic for information on how to set up filtering rules that allow access only to specified IP addresses and ports.

Set up a VNS with no authentication

1. In the *Virtual Network Configuration* screen, highlight the VNS name in the left-hand list and click on the **Topology** tab.
2. In the *Topology* screen, select Network Assignment by **SSID**.

   For the remaining Topology parameters, follow the steps described above for a VNS for Captive Portal.

   Save the new VNS Topology by clicking on the **Save** button..
3. Then click on the **Authentication** tab for this VNS.



Screen 31: Virtual Network Configuration – Authentication – None

4. Select the **None** radio button, for no authentication on this VNS. Click on the **Save** button.
5. In the *Filtering* screen, define a Non-Authenticated Filter that will control specific network access for any wireless device users on this VNS. These rules should be very restrictive. The final rule should be a “Deny All” rule.

   See “Filtering Rules for a VNS for Captive Portal” for more information.

   The Non-Authenticated Filter for a VNS with no authentication will not have a Captive Portal page for login.

Virtual Network Configuration: A VNS for Voice Traffic (QoS with SVP)

Voice Data Traffic on a Wireless Network: Overview

New developments are enabling the integration of internet telephony technology on wireless networks – Voice over Internet Protocol (VoIP) using 802.11 wireless local area networks (WLANs).

VoIP over 802.11 WLANs raises various issues including quality-of-service (QoS), call control, network capacity, and network architecture.

Wireless voice data requires a constant transmission rate and must be delivered within a time limit. This type of data is called *isochronous* data. This requirement for isochronous data is in contradiction to the concepts in the 802.11 standard that allow for data packets to wait their turn, to avoid data collisions. (Regular traffic on a wireless network is an *asynchronous* process in which data streams are broken up by random intervals.)

The solution is to add mechanisms to the network that give voice data traffic priority over all other traffic, and allow for continuous transmission of voice traffic.

One such mechanism is SpectraLink Voice Protocol (SVP), a protocol developed by SpectraLink for implementation on an access point. The SVP protocol facilitates voice prioritization over an 802.11 wireless LAN that will carry voice packets from SpectraLink wireless telephones.

In BeaconWorks Release 2.0, you can configure a VNS that supports wireless voice-over-internet devices. Specifically, you can enable SpectraLink Voice Protocol (SVP) on the VNS in order to provide priority queuing on the BeaconPoint.

This feature is part of the development of Quality of Service (QoS) mechanisms in BeaconWorks. Such techniques match the needs of specific applications to the network resources available, in order to provide better network traffic flow.

Setting up a VNS for Voice Traffic

In order to set up a VNS for voice-over-internet traffic, a number of factors should be taken into account, on the enterprise network and in the BeaconWorks system.

On the enterprise network, the wireless telephone users will require access to:

- a private branch exchange (PBX), a private telephone system within an enterprise, with such features as voicemail.
- a Telephony Gateway, for access to an external standard telephone network, such as the wireless cellular network or the public switched telephone network (PSTN).

Note: The Telephony Gateway should be located on the same subnet as the BeaconMaster.

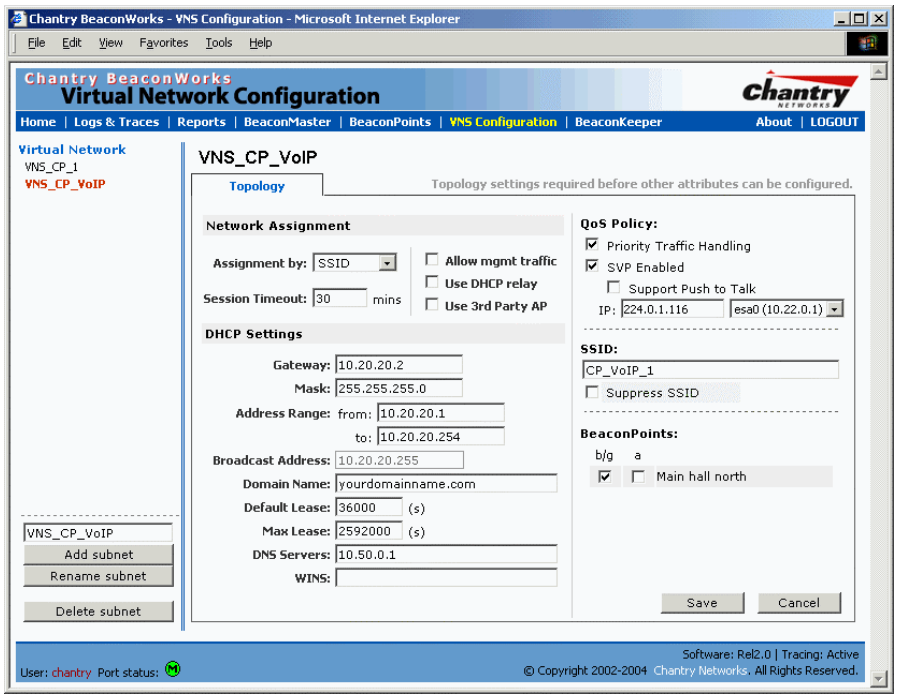
For large deployments, an SVP server is required on the enterprise network.

In BeaconWorks, the VNS that is dedicated voice-over-internet traffic should be configured as follows:

- Network assignment by **SSID**
- Authentication set to **None**, since wireless telephone users do not have a user interface in which they can enter authentication identification
- Filtering rules that allow access to the DNS server, to the Telephony Gateway, and then deny all other traffic.
- Privacy using 104-bit WEP key (recommended for greater security).

Set up a VNS for voice traffic

1. In the *Virtual Network Configuration* screen, add a new VNS, as described earlier. Then configure the VNS as described below.



Screen 32: Virtual Network Configuration: Topology – QoS for Voice Traffic

2. In the *Topology* screen, in the **Assignment by** field, select **SSID** from the drop-down list.
3. In the **QoS Policy** area of the screen, enable **Priority Traffic Handling** by clicking the checkbox on.

> **Note:** It is possible to enable only the Priority Traffic Handling on a VNS without using SVP. The Priority Traffic Handling mode sets the BeaconPoint to give priority to traffic on this VNS. There is no multicast on with this feature.
> However, this mode is usually used together with SVP enabled (the next feature)

4. To enable SVP on the VNS, click the **SVP Enabled** checkbox on.

   When SVP is enabled, multicast traffic is also automatically enabled.

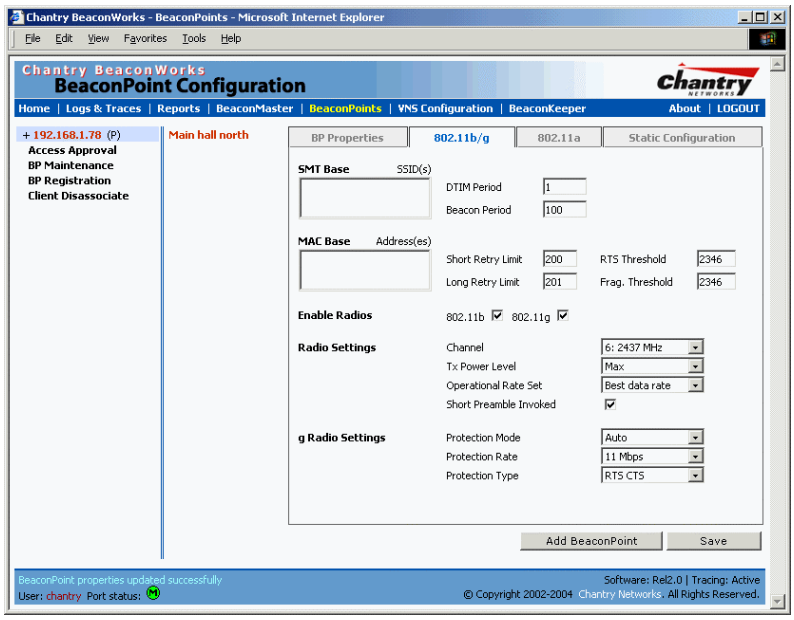
5. Define parameters for multicast. The **IP** entry field displays an IP address that SVP can use for multicast. The next field displays one of the BeaconMaster physical data ports for multicast. You can modify these if required.
6. To allow this VNS to handle Push-To-Talk wireless communication, click the **Support Push-To-Talk** checkbox on.

Note: The Push-To-Talk feature on wireless telephones allows direct communication between any devices open on the same handset channel (like a walkie-talkie).

7. Define the remaining parameters of the VNS topology as described earlier for network assignment by SSID.
8. To save this VNS configuration, click on the **Save** button.
9. In the *Authentication* screen, set the Authentication method for this VNS to **None**. Click on the **Save** button.
10. In the *Filtering* screen, define filtering rules in the Non-Authenticated Filter that allow access to the DNS server, to the Telephony Gateway, and then deny all other traffic. Click on the **Save** button.
11 In the *Privacy* screen, set up Privacy using a 104-bit WEP key. Click on the **Save** button.

Configure the BeaconPoint radio for a voice traffic VNS

In the *BeaconPoint Configuration* screen, make the following changes on the BeaconPoint radio for this VNS, to support SVP requirements:



Screen 33: BeaconPoint Configuration for QoS VNS (need screen with correct settings)

1. Set the 2.4 Ghz radio to support only B mode (G mode not supported)
2. Set the operational radio rate to **Best data rate**.
3. The save these modifications, click on the **Save** button.

Virtual Network Configuration: A VNS for AAA

This section describes how to set up a VNS for AAA (802.1x): its Topology, Authentication, Filtering and Privacy.

If network assignment is by **AAA (802.1x)** with 802.1x authentication, the process is as follows. The wireless device user requesting network access via BeaconWorks must first be authenticated. The wireless device's client utility must support 802.1x. The user's request for network access along with login identification or user profile will be forwarded by the BeaconMaster to a RADIUS server. BeaconWorks supports these authentication types:

- EAP-TLS Extensible Authentication Protocol - Transport Layer Security that relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.
- EAP-TTLS (EAP with Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
- PEAP (Protected Extensible Authentication Protocol) is a standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user.

Note: For 802.1x, the RADIUS server must support RADIUS extensions (RFC2869).

If the RADIUS servers sends an "access-accept" message to the BeaconMaster, the BeaconMaster's DHCP server assigns the wireless device its IP address.

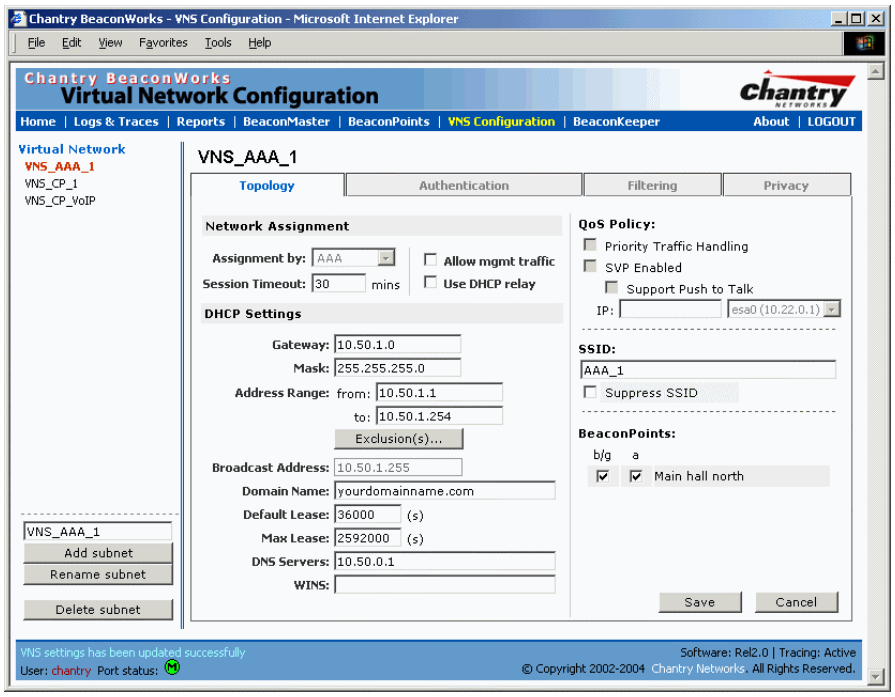
The BeaconMaster controls network access by means of the filtering rules defined for the specific Filter ID associated with the wireless device user, as defined in the *Filtering* screen.

For a VNS with AAA (802.1x), privacy by Wi-Fi Protected Access (WPA) is available.

Topology for a VNS for AAA

For a VNS with 802.1x authentication, select Network Assignment by AAA (Authentication, Authorization, Accounting) in the *Topology* screen.

In the *Virtual Network Configuration* screen, highlight the VNS name in the left-hand list and click on the **Topology** tab.



Screen 34: Virtual Network Configuration – Topology – AAA Assignment

Create an AAA topology

1. Using the **Assignment by** drop-down list, select **AAA**.
2. In the **SSID** box at the right, key in the SSID that the wireless devices will use to access the BeaconPoint.
3. Click the **Suppress SSID** checkbox on to prevent this SSID from appearing in the beacon message sent by the BeaconPoint. The wireless device user seeking network access will not see this SSID as an available choice, and will need to specify it.
4. In the **Session Timeout** box, key in the number of minutes that a wireless device can be inactive before the BeaconMaster closes the session.

Identify the BeaconPoint radios that will be assigned to this VNS

5. From the displayed list of **BeaconPoint Radios** that are available throughout the network, check the ones to be assigned to this VNS.
   Once you have assigned a BeaconPoint radio to four VNSs, it will not appear in the list for another VNS setup.

Note: You can view the VNSs that each radio is participating in by clicking on the appropriate tab for each radio in the *BeaconPoint Configuration* screen

Enable Management Traffic on this VNS

6. To allow Management Traffic on this VNS, click the **Allow management traffic** checkbox on.

Note: This choice invokes the built-in port-based filtering rules for Management Traffic, as described earlier in the "Port Type or Function" topic.

Set the IP address for the VNS (for the DHCP server on the BeaconMaster)

7. In the **Network Address** box, key in the network IP address for the VNS.

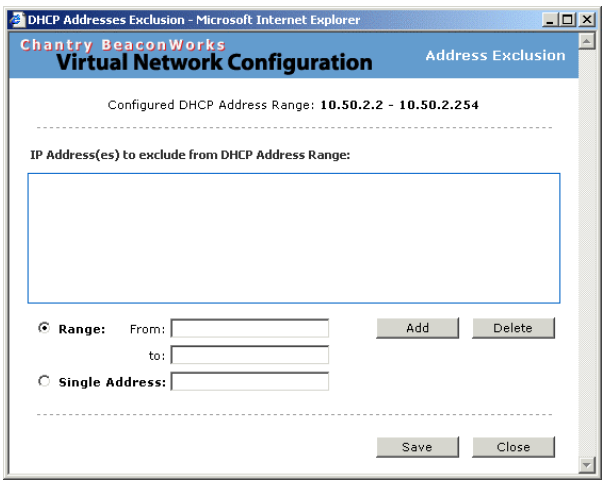
   This IP address is the *default gateway* for the VNS. The BeaconMaster advertises this address to the wireless devices when they sign on.

8. In the **Mask** box, key in the appropriate subnet mask for this IP address, to separate the network portion from the host portion of the address (typically 255.255.255.0)

   The **Address Ranges** fields populate automatically (based on the IP address you keyed in) with the range of IP addresses to be assigned to wireless devices using this VNS.

9. To modify the **Address Ranges,** key the first available address in the **from** box. Key the last available address in the **to** box.

10. If there are specific IP addresses to be excluded from this range, click on the **Exclusions** field. The *Exclusions* subscreen appears.



Screen 35: Virtual Network Configuration – Exclusions subscreen

11. In the *Exclusions* subscreen, key in the IP addresses or address ranges to exclude. Click on the **Add** button after each entry. Click on the **Save** button to save the changes and return to the *Topology* screen.

12. The **Broadcast Address** field populates automatically, based on the IP address of the VNS. Modify this if appropriate..

13. In the **Domain Name** box, key in the external enterprise domain name.

Set time limits for IP assignments

14. In the **Default Lease** box, accept the default value of 3600 seconds (1 hour), or modify. This is the default time limit that an IP address would be assigned by the DHCP server to a wireless device.

    In the **Max Lease** box, accept the default value is 24000 seconds (40 hours), or modify. This is the maximum time that an IP address can be assigned.

Set the name server configuration

15. In the **DNS Servers** box, key in the IP Address of the Domain Name Server(s) to be used.

Chantry Networks Inc. Copyright 2004. All rights reserved.

16. If the DHCP server uses WINS (Windows Internet Naming Service), key in the IP address in the **WINS** box. If not, leave it blank.

Use DHCP Relay for the VNS

Use **DHCP Relay** to force the BeaconMaster to forward DHCP requests to an external DHCP server on the enterprise network. This function will bypass the local DHCP server on BeaconMaster (to bypass steps 9 to 18 above). This function allows the enterprise to manage IP address allocation to a VNS from its existing infrastructure.

17. To use an external DHCP server, click the **Use DHCP Relay** checkbox on. The *DHCP Settings* area of the screen changes to display only the **Gateway IP**, **Mask** and **DHCP Server** fields. Key in the appropriate IP addresses and mask to reach the enterprise's external DHCP server.

Note: The range of IP addresses to be assigned to the wireless device users on this VNS should also be designated on the external DHCP server.

Save the new VNS for AAA

18. To save this VNS configuration, click on the **Save** button.

When the new Topology has been saved, the screen changes to display tabs for *Authentication*, *Filtering* and *Privacy*.

Authentication for a VNS for AAA

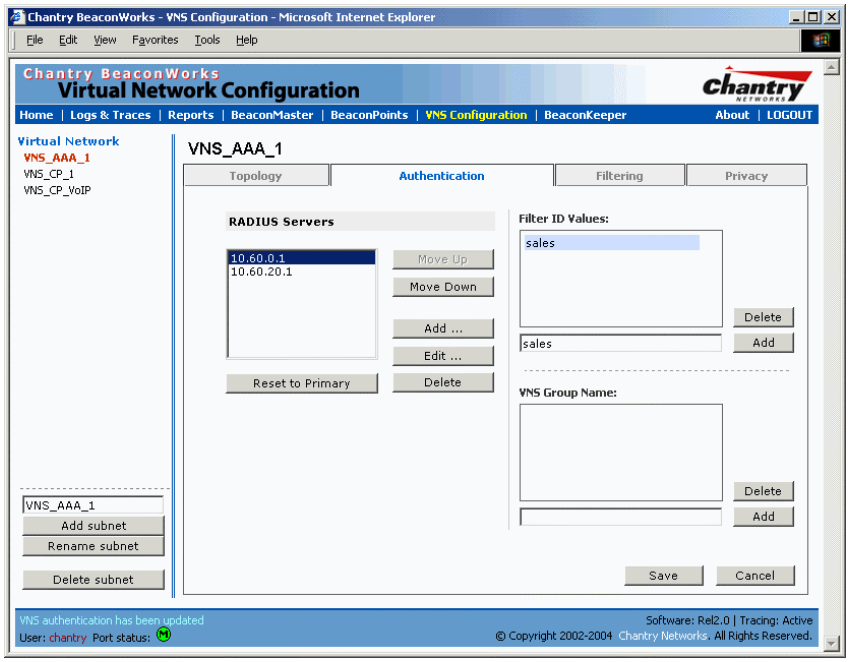
The next step is to set up the Authentication mechanism for **AAA (802.1x)**.

This type of authentication relies on a RADIUS server on the enterprise network. You can define more than one RADIUS server for authentication and define the priority of use in the event of a failover situation.

Set up authentication by AAA (802.1x) method

1. Highlight the VNS name. Click on the **Authentication** tab. For an AAA VNS, the AAA version of the *Authentication* screen appears.

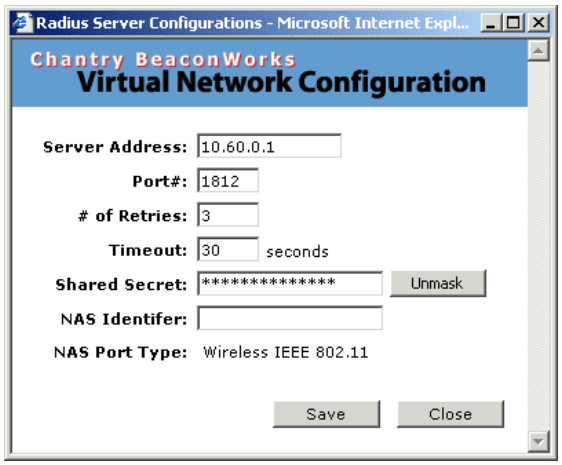
Chantry Networks Inc. Copyright 2004. All rights reserved.



Screen 36: Virtual Network Configuration – Authentication – AAA

Define how the BeaconMaster will access the RADIUS Server.

2. For each RADIUS server to be defined, click on the **Add** button. The *RADIUS Server Configuration* popup window appears.



Screen 37: Virtual Network Configuration – Authentication AAA – RADIUS Server Configuration

3. For each server, fill in the following fields:

Server Address	The IP address of the RADIUS Server.
Port #	The port used to access the RADIUS Server (default: 1812)
# of Retries	Number of times the BeaconMaster will attempt to access the RADIUS Server
Timeout	The maximum time that a BeaconMaster will wait for a response from the RADIUS server, before attempting again (up to the maximum number of retries).

4. Key in the **Shared Secret** (a password that is required in both directions) that is set up on the RADIUS Server. This password is used to validate the connection between the BeaconMaster and the RADIUS Server.

   To display the shared secret (in order to proofread your entry before saving the configuration), click on the **Unmask** button. To mask the shared secret again, click on the button again (the button toggles between **Mask** and **Unmask**).

Note: This precautionary step is recommended at this point in order to avoid an error later when the BeaconMaster attempts to communicate with the RADIUS server.

5. In the **NAS Identifier** field, type in the Network Access Server (NAS) identifier, a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS Servers and then acting on the response returned. [Optional]
6. To save these settings and return to the main *Authentication* screen, click on the **Save** button. To return to the main *Authentication* screen without saving, click on the **Close** button.

Define the RADIUS server priority for RADIUS Redundancy

After setting up a RADIUS server, its IP address appears in the **RADIUS Servers** box. To allow for RADIUS server redundancy, set up a second server, as described above.

7. To define the priority of the servers, highlight a RADIUS server in the list and use the **Move Up** or **Move Down** key to change the order.

   The first server in the list is the active one.

   In the event of a failover of the main RADIUS server (if no response after the set number of retries), then the other servers in the list will be polled on a round-robin basis until one responds.

   If one of the other servers becomes the active one during a failover, an "A" will appear after that server name.

Note: If all defined RADIUS servers fail to respond, a critical message will be generated in the logs.

8. To remove a defined server from the list, highlight it and click on the **Delete** button.
9. To modify the parameters of a defined server, highlight it and click on the **Edit** button. In the RADIUS Server popup screen, follow steps 2 to 6 described above.

Note: It is recommended that the RADIUS databases with names, logins, and attributes be kept synchronous on all RADIUS servers.

Define the Filter ID Values on this VNS.

10. In the **Filter ID Values** entry field, key in the name of a group that you want to define specific filtering rules for, to control network access. Click on the **Add** button. The Filter ID name appears in the list above.

    Repeat for additional Filter ID names.

These Filter ID names will appear in the Filter ID list in the *Filtering* screen.

Chantry Networks Inc. Copyright 2004. All rights reserved.

Note: These names must match the Filter ID attribute names in the RADIUS server.

11. To save the authentication parameters for this VNS, click on the **Save** button.

VNS Topology for an AAA group

You can set up a group within a VNS that relies on the RADIUS attribute Login-LAT-Group (RFC2865). For each group, you can define filtering rules to control access to the network.

If you define a group within an AAA VNS, the group (or child) definition acquires the same authentication and privacy parameters as the parent VNS. However, you need to define a different topology and filtering rules for this group.

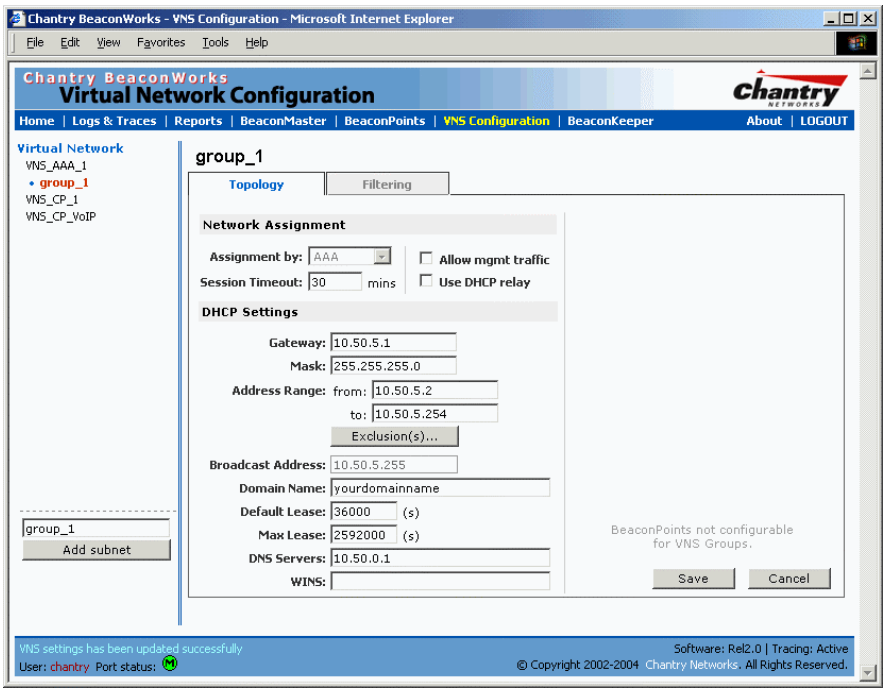
Set up an AAA Group

1. Highlight the VNS name for which you selected **AAA** as the Assignment method in the *Topology* screen. Click on the **Authentication** tab. For an AAA VNS, the AAA version of the *Authentication* screen appears.
2. To create and define a VNS Group within the selected parent VNS, key in the name in the **VNS Group Name** field. Then click on the **Add** button.

   The Group Name that you defined will appear as a child of the parent VNS in the left-hand list. (To configure the Topology of a group, see the next topic.)
3. To save these settings and create the group VNS definition, click on **Save**.

Configure the VNS Topology for an AAA Group

1. To configure the VNS topology for an AAA Group, click on its name in the left-hand list. The Group version of the *Topology* screen appears.



Screen 38: Virtual Network Configuration – Topology – AAA Group

2. Define the DHCP settings for this VNS, as described above for the parent VNS. The Gateway and DHCP Ranges must be different than those of the parent VNS.
3. To save the modifications, click on **Save**.

The filtering screen for an AAA Group is described at the end of the *Filtering* topic.

Filtering Rules for a Filter ID group

After setting up RADIUS parameters for Authentication and the Filter ID Values, the next step is to define the filtering rules for the Filter ID Values on the VNS for AAA.

When the wireless device user enters a login identification, that identification is sent by the BeaconMaster to the RADIUS server or other authentication server, through a sequence of exchanges depending on the type of authentication protocol used.

When the server allows this request for authentication (sends an "access-accept" message), the RADIUS server may also send back to the BeaconMaster a Filter ID attribute associated with the user, or a Login-LAT-Group identifier for the user.

If the Filter ID attribute (or Login-LAT-Group attribute) from the RADIUS server matches a Filter ID Value that you have set up on the BeaconMaster, the BeaconMaster applies to the wireless device user the filtering rules that you defined for that Filter ID Value.

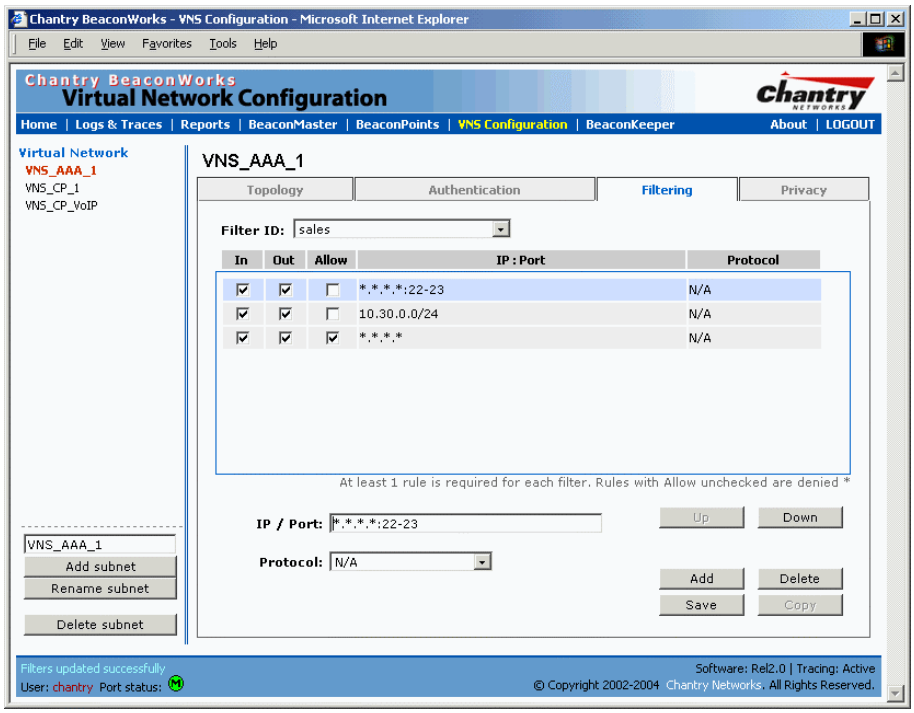
Note: The BeaconMaster's Filter ID Values must match the Filter ID attribute names in the RADIUS server.

If no Filter ID is returned by the authentication server, or no match is found on the BeaconMaster, then the Default Filter and its filtering rules will apply to the wireless device user.

Define filtering rules for a Filter ID group

1. In the *Virtual Network Configuration* screen, highlight the VNS name in the list and click on the **Filtering** tab. The *Filtering* screen for this VNS appears.
2. Using the **Filter ID** drop-down list, select one of the names you defined in the **Filter ID Values** field in the *Authentication* screen [one of your enterprise's user groups, such as Sales, Engineering, Teacher, Guest....]

Chantry Networks Inc. Copyright 2004. All rights reserved.



Screen 39: Virtual Network Configuration –Filter ID Value filtering rules

The screen automatically provides a "Deny All" rule already in place. This can be modified to "Allow All", if appropriate to the network access needs for this VNS.

3. Select one of the following as the basis for each filtering rule you are defining:

   IP / Port: Type in the destination IP address, and if desired, the port designation on that IP address.

   Protocol: Select from the drop-down list (may include UDP, TCP, IPsec-ESP, IPsec-AH, ICMP)

4. Click on the **Add** button.
   The information appears in a new line in the **Filter Rules** area of the screen.

5. Highlight the new filtering rule and fill in (or leave unchecked) the three checkboxes in the combinations that define the traffic access:

   In: Click checkbox *on* to refer to traffic from the wireless device that is trying to get on the network ("going to" to network)

   Out: Click checkbox *on* to refer to traffic from the network host that is trying to get to a wireless device. ("coming from" the network)

   Allow Click checkbox on to *allow*. Leave unchecked to *disallow*..

6. Edit the order of a filtering rule by highlighting the line and clicking on the **Up** and **Down** button. The filtering rules are executed in the order defined here

7. To save the filtering rules, click on the **Save** button.

Filtering Rules by Filter ID: Examples

Below are two examples of possible filtering rules for a Filter ID. The first disallows only some specific access before allowing everything else.

In	Out	Allow	IP / Port	Description
x	x		*.*.*.*:22-23	Deny all telnet sessions
x	x		[specific IP address, range]	Deny all traffic to a specific IP address, or address range
x	x	x	*.*.*.*.	Allow everything else.

The second example does the opposite of the first example. It allows only some specific access and denies everything else.

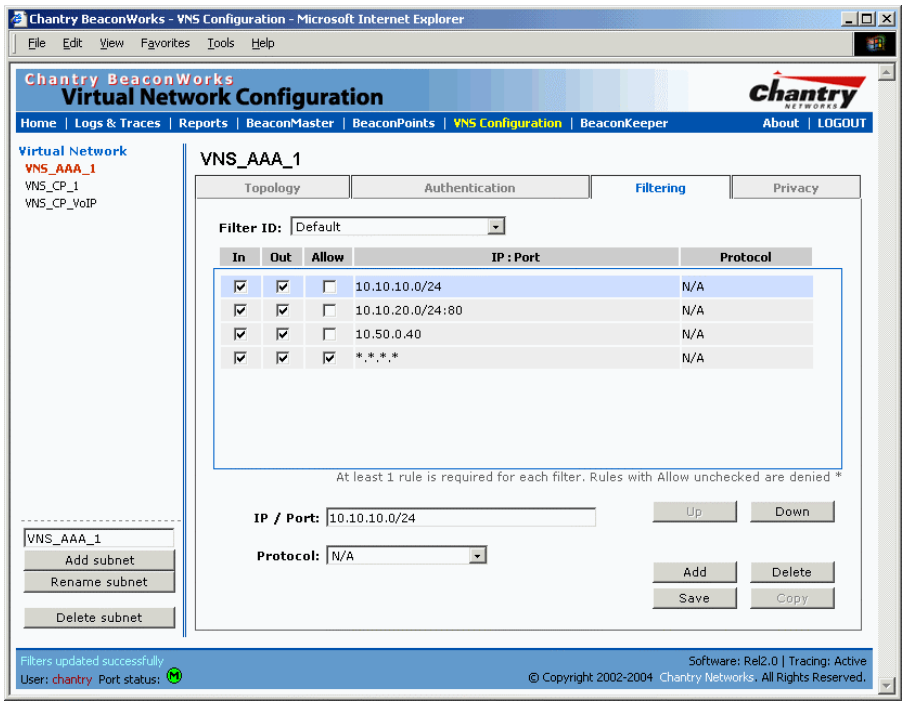
In	Out	Allow	IP / Port	Description
x	x	x	[specific IP address, range]	Allow all traffic to a specific IP address, or address range
x	x		*.*.*.*.	Deny everything else.

Filtering Rules for a Default Filter

If, after authentication of the wireless device user, no Filter ID attribute is returned by the authentication server for this user, or no match is found on the BeaconMaster for a Filter ID Value, then the Default Filter will apply.

Define the filtering rules for a Default Filter

1. In the *Virtual Network Configuration – Filtering* screen, using the **Filter ID** drop-down list, select **Default**.



Screen 40: Virtual Network Configuration – Default Filter

2. Follow Steps 2 to 5, as described above.
3. To save the filtering rules, click on the **Save** button.

Default Filter: Examples

Here is an example of filtering rules for a Default Filter:

In	Out	Allow	IP / Port	Description / Purpose
x	x		Intranet IP, range	Deny all access to an IP range
x	x		Port 80 (HTTP)	Deny all access to web browsing.
x	x		Intranet IP	Deny all access to a specific IP
x	x	x	*.*.*.*	Allow everything else.

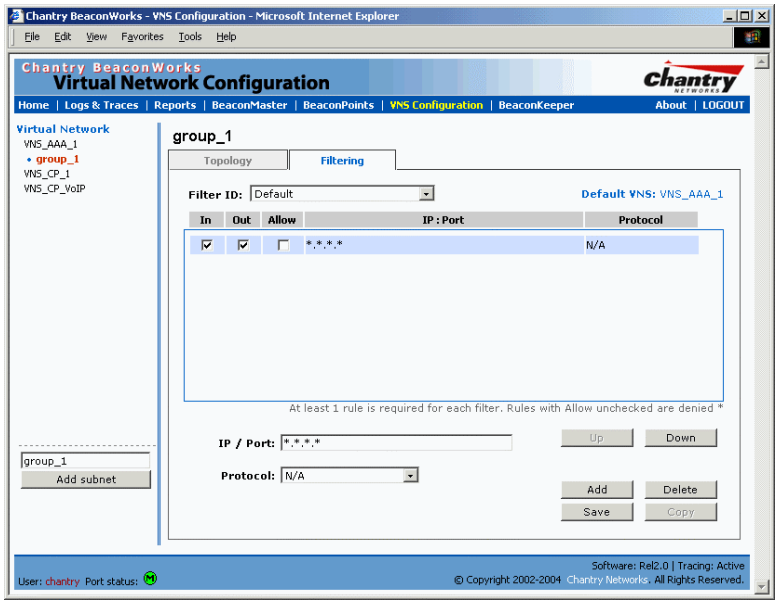
Here is another example of filtering rules for a Default Filter:

In	Out	Allow	IP / Port	Description / Purpose
x			Port 80 (HTTP) on host IP	Deny all incoming wireless devices access to web browsing the host.
	x		Intranet IP 10.3.0.20, ports 10-30	Deny all traffic from the network to the wireless devices on the port range, such as TELNET (port 23) or FTP (port 21).
x		x	Intranet IP 10.3.0.20	Allow all other traffic from the wireless devices to the Intranet network.
	x	x	Intranet IP 10.3.0.20	Allow all other traffic from Intranet network to wireless devices.
x	x	x	*.*.*.*	Allow everything else.

Filtering Rules for an AAA Group VNS

If you defined a child group for an AAA VNS, it will have the same authentication parameters and Filter IDs as the parent VNS. However, you can define different filtering rules for these Filters IDs in the child configuration than in the parent configuration.

1. In the *Virtual Network Configuration* screen, highlight the VNS group name in the list and click on the **Filtering** tab. The *Filtering* screen for this VNS group appears.



Screen 41: Virtual Network Configuration – Filtering – AAA Group

2. Follow Steps 2 to 5, as described above for a parent VNS.
3. To save the filtering rules, click on the **Save** button.

Filtering Rules between two wireless devices

Traffic from two wireless devices that are on the same VNS and are connected to the same BeaconPoint will pass through the BeaconMaster and therefore be subject to filtering policy.

You can set up filtering rules that allow each wireless device access to the default gateway, but prevent each device from communicating each other. Add the following two rules to a Filter ID filter before allowing everything else:

In	Out	Allow	IP / Port	Description / Purpose
x	x	x	[Intranet IP]	Allow access to the Gateway IP address of the VNS only
x	x		[Intranet IP, range]	Deny all access to the VNS subnet range 0/24
x	x	x	*.*.*.*	Allow everything else.

Privacy for a VNS for AAA

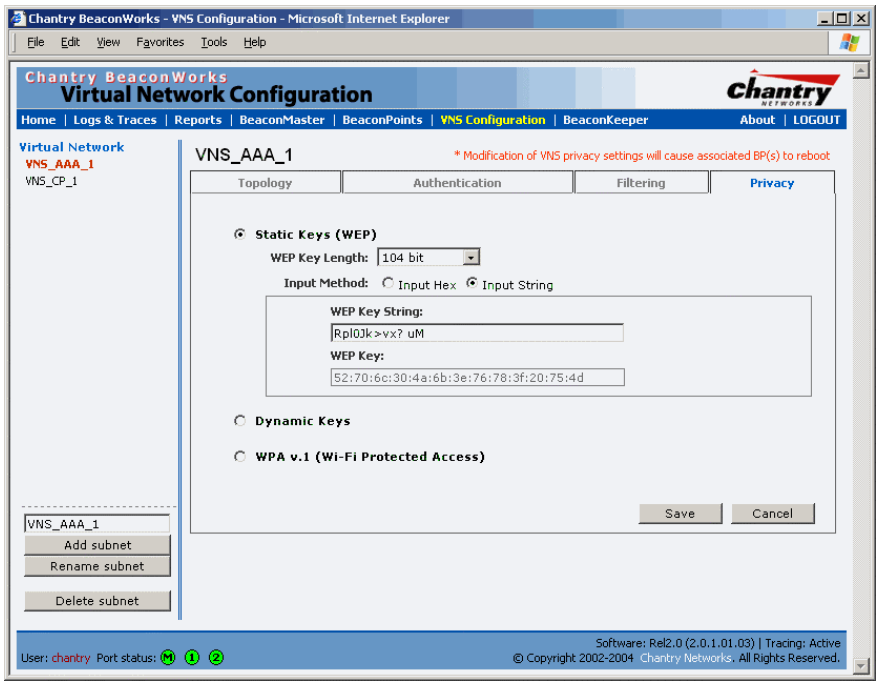
Use the *Privacy* screen to set up privacy mechanisms for a VNS with authentication by 802.1x (AAA). There are three options

- Static keys (WEP)
- Dynamic keys
- Wi-Fi Protected Access (WPA) version 1, with Temporal Key Integrity Protocol (TKIP).

Privacy for a VNS for AAA: WEP

Set up static WEP privacy for a selected AAA VNS

1. In the *Virtual Network Configuration* screen, highlight the VNS name in the list and click on the **Privacy** tab. The *Privacy* screen for the selected VNS appears.



Screen 42: Virtual Network Configuration – Privacy – AAA VNS: Static Keys

2. To use static keys, click on the **Static Keys (WEP)** radio button.
3. From the drop-down list, select the **WEP Key Length:** 40-bit, 104-bit, 128 bit
4. Click on the appropriate radio button to select the **Input Method**: Input Hex, Input String.
5. Type in the WEP key input, as appropriate to the technique selected. The key is generated automatically, based on the input.
6. To save these settings, click on the **Save** button.

Set up dynamic WEP privacy for a selected AAA VNS

The dynamic key WEP mechanism changes to key for each user and each session.

1. To use dynamic keys, click on the **Dynamic Keys** radio button.
2. To save these settings, click on the **Save** button.

Privacy for a VNS for AAA: Wi-Fi Protected Access (WPA)

The VNS Privacy configuration function now includes Wi-Fi Protected Access (WPA) privacy, a new security solution that adds authentication to enhanced WEP encryption and key management.

The authentication portion of WPA has two modes:

- Enterprise Mode:
  - Specifies 802.1x with Extensible Authentication Protocol (EAP)
  - Requires a RADIUS or other authentication server
  - Uses RADIUS protocols for authentication and key distribution
  - Centralizes management of user credentials
- Pre-Shared Key (PSK) Mode: Pre-Shared Key for authentication:
  - Does not require an authentication server (suitable for home or small office)
  - Uses a Pre-Shared Key (shared secret) used for authentication to the access point

The encryption portion of WPA is Temporal Key Integrity Protocol (TKIP). TKIP includes:

- a per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet or after the specified re-key time interval.
- a extended WEP key length of 256-bits
- an enhanced Initialization Vector (IV) of 48 bits, instead of 24 bits, making it more difficult to compromise.
- a Message Integrity Check or Code (MIC), an additional 8-byte code that is inserted before the standard WEP 4-byte Integrity Check Value (ICV). These integrity codes are used to calculate and compare, between sender and receiver, the value of all bits in a message, to ensure that the message has not been tampered with.

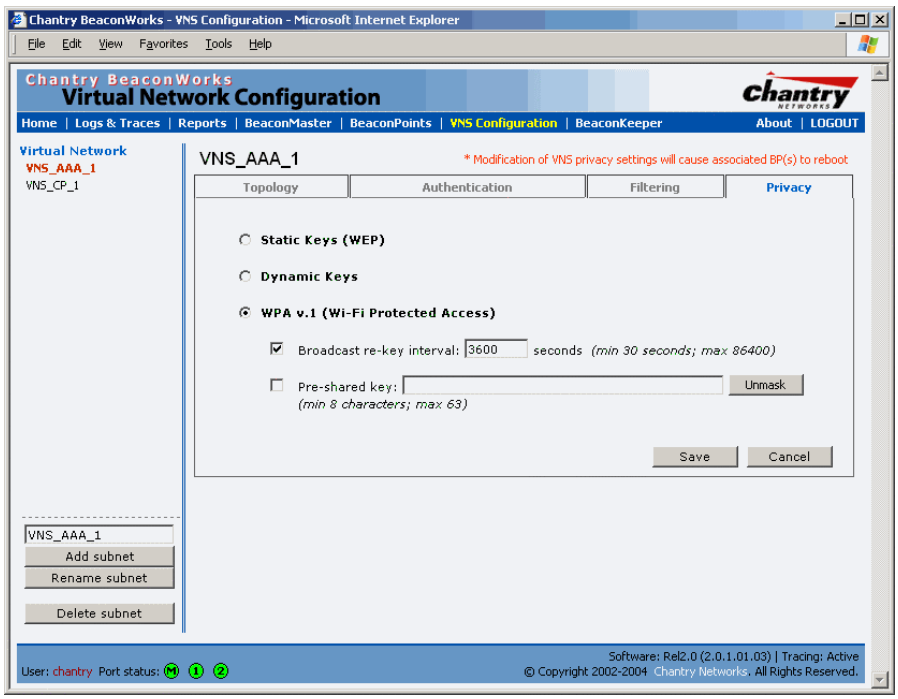
Chantry Networks Inc. Copyright 2004. All rights reserved.

The steps in the WPA authentication and encryption process are as follows:

1. The wireless device client associates with BeaconPoint.
2. BeaconPoint blocks the client's network access while the authentication process is carried out (the BeaconMaster sends the authentication request to the RADIUS authentication server)
3. The wireless client provides credentials that are forwarded by the BeaconMaster to the authentication server.
4. If the wireless device client is not authenticated, the wireless client stays blocked from network access.
5. If the wireless device client is authenticated, the BeaconMaster distributes encryption keys to the BeaconPoint and the wireless client.
6. The wireless device client gains network access via the BeaconPoint, sending and receiving encrypted data. The traffic is controlled with permissions and policy applied by the BeaconMaster.

Set up Wi-Fi Protected Access privacy (WPA) for an AAA VNS

1. To set up WPA privacy on the VNS, click on the **WPA** radio button.



Screen 43: Virtual Network Configuration – Privacy – AAA VNS: WPA

Specify a re-key interval for WPA Privacy

2. To enable re-keying after a time interval, click the **Broadcast re-key interval** checkbox on (the default is on). Type in the re-key time interval (the time after which the broadcast encryption key is changed automatically) in seconds.

   If the box is unchecked, the Broadcast encryption key is never changed and the BeaconPoint will always use the same broadcast key for Broadcast/Multicast transmissions. Note that this reduces the level of security for wireless communications.

Enable WPA in PSK mode if there is no authentication server

3. To enable WPA-PSK, for authentication on a network without an authentication server, click the **Pre-Shared Key** checkbox on.
4. Type in the **Pre-Shared Key** (PSK), or shared secret, to be used between the wireless device and BeaconPoint. The key should be between 8 and 63 characters. It is used to generate the 256-bit key.
5. To display the Pre-Shared Key (in order to proofread your entry before saving the configuration), click on the **Unmask** button. To mask the key again, click on the button again (the button toggles between **Mask** and **Unmask**).

Save the privacy parameters for this VNS

6. To save the privacy parameters for the new VNS, click on the **Save** button.

Chantry Networks Inc. Copyright 2004. All rights reserved.

BeaconMaster Configuration: Availability

The BeaconWorks system provides a feature that maintains service availability in the event of a BeaconMaster outage.

The Availability feature links two BeaconMasters as a pair, so that they share information about their BeaconPoints. If one BeaconMaster in a pair fails, then its BeaconPoints are allowed to connect instead to the second BeaconMaster. The second BeaconMaster provides the wireless network and a pre-assigned VNS for the BeaconPoint.

From the viewpoint of a BeaconPoint, if its home BeaconMaster fails, the BeaconPoint reboots and begins its discovery process. The BeaconPoint will be directed to the appropriate second BeaconMaster of the pair.

Note: The Availability feature relies on SLP and a DHCP server that supports Option 78, as described earlier in the BeaconPoint discovery and registration process. The Availability feature controls how the paired BeaconMasters register as services with SLP, in normal operations and in the event of an outage.

The wireless device users that were on the BeaconPoint must log in again and become authenticated on the second BeaconMaster.

The Availability feature is set up in the *BeaconPoint Registration Mode* screen.

Prepare for setting up the Availability feature

Before you begin, the following preparation should be done:

- choose which BeaconMaster is the primary and which is the secondary
- determine the physical communication link for the TCP/IP connection between the two BeaconMasters (this is done over TCP port 13907), and ensure that the interfaces used for this connection are routable
- set up DHCP to support Option 78 for SLP, so that it points to the IP addresses of both BeaconMasters

Now set up each BeaconMaster separately. One method is as follows:

1. In the *BP Registration* screen, set up each BeaconMaster in “Stand-alone Mode” and “Secure Mode” (allow only approved BeaconPoints to connect)
2. In the *VNS Configuration, Topology* screen, define a VNS on each BeaconMaster with the same SSID (but different IP addresses)
3. Associate the appropriate BeaconPoints to each BeaconMaster. The BeaconPoints will appear on each BeaconMaster as “Pending” in the *Access Approval* screen.
4. In the *BP Registration* screen, now enable the two BeaconMasters as a pair, as described below.
5. On each BeaconMaster in the *Access Approval* screen, change the status of the relevant BeaconPoints from “Pending” to “Approved”.

Chantry Networks Inc. Copyright 2004. All rights reserved.

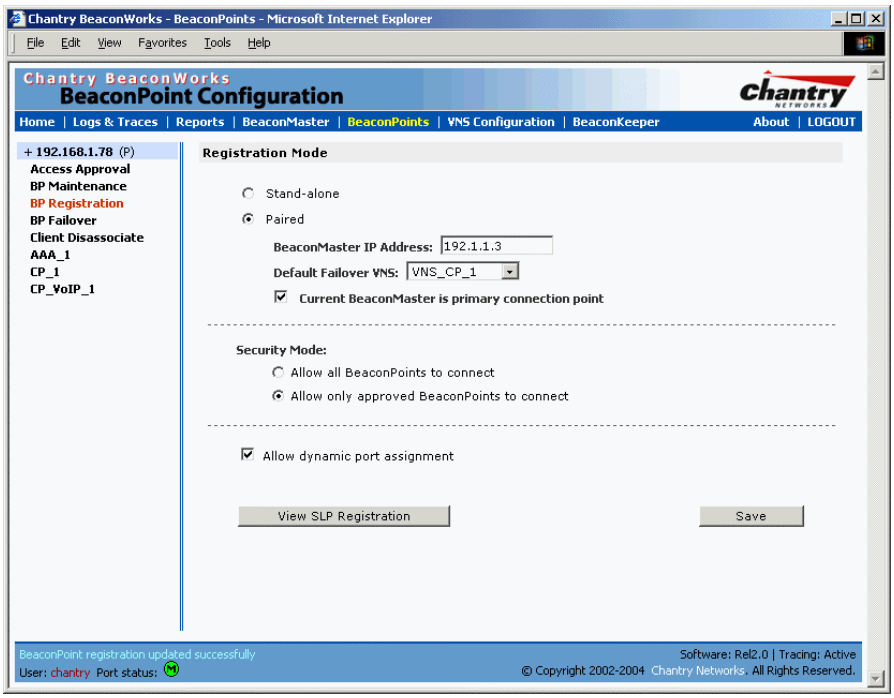
A second method to set up the BeaconMasters is as follows:

1. In the *BP Registration* screen, enable the two BeaconMasters as a pair, as described below.
2. Add each BeaconPoint manually to each BeaconMaster. (Select the **BeaconPoint** tab. In the *BeaconPoint Properties* screen, click on the **Add BeaconPoint** button. The *BeaconPoint Configuration* subscreen appears. Define the BeaconPoint and click on the **Add BeaconPoint** button.)

Note: *Caution:* If two Beacon Masters are paired and one BeaconMaster has the "Allow All" option set for BeaconPoint registration, all BeaconPoints will register with that BeaconMaster.

Set up two BeaconMasters as a pair, for availability

1. On the BeaconMaster that is to be the primary, select **BeaconPoints** tab in any screen. Then, in the left-hand list, click on **BP Registration**. The *BeaconPoint Registration Mode* screen appears.



Screen 44: BeaconPoint Configuration – Paired BeaconMasters for Availability

2. Click the **Paired** radio button.
3. Enter the **IP address** of the physical port of the secondary BeaconMaster.

Note: This IP must be on a routable subnet between the two BeaconMasters.

4. Select a **Default Failover VNS** on the other BeaconMaster from the drop-down list of VNS's (this list will be populated only after a VNS has been defined).
5. Since this BeaconMaster is to be the **primary connection point**, click the checkbox on.
6. Set the **Security Mode** to "Allow Approved" by clicking the radio button. [recommended after initial set up for paired BeaconMasters]

7. Click the **Allow dynamic port assignment** checkbox on. This ensures that the BeaconPoint will always find a port for the return connection to its home BeaconMaster after a failover.
8. To save these settings, click on the **Save** button.

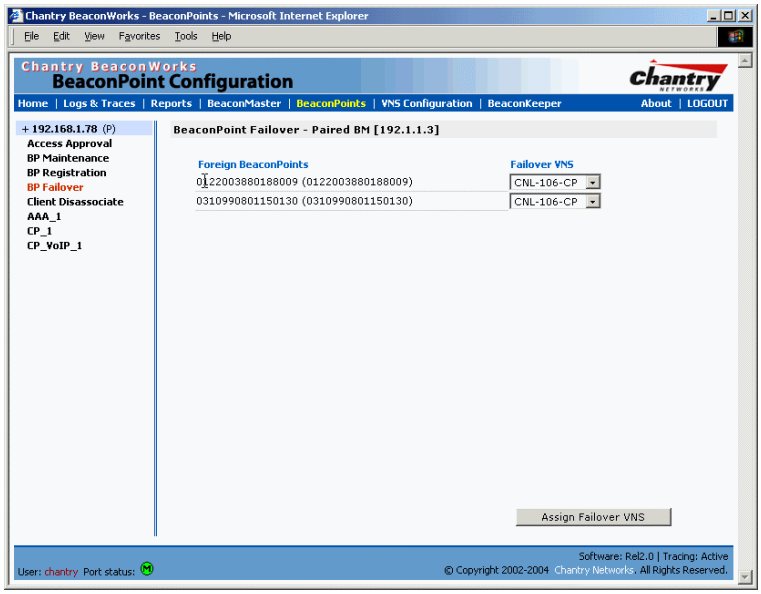
On the BeaconMaster that is to be the secondary one, repeat Steps 1 to 8, with these exceptions:

- In Step 3, enter the **IP address** of the Management port or physical port of the primary BeaconMaster.
- In Step 5, leave the **primary connection point** checkbox unchecked.

Modifying BP Failover selections for availability

When you have enabled a pair of BeaconMasters as described above, **BP Failover** is added as an option in the *BeaconPoint Configuration* left-hand list.

1. Click on **BP Failover** option. The *BeaconPoint Failover – Paired BM* screen appears.



Screen 45: BeaconPoint Configuration – BP Failover for Paired BM

This screen displays the BeaconPoints registered on the other BeaconMaster of the pair.

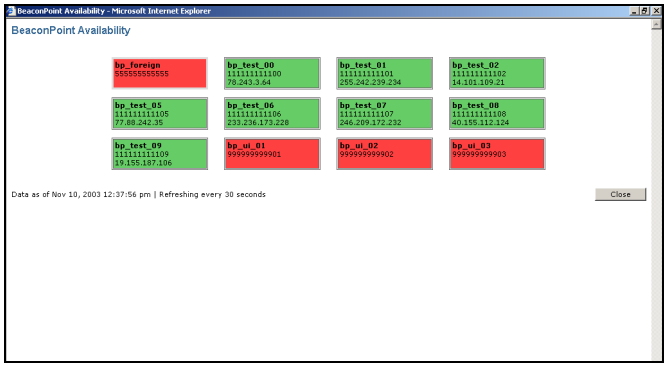
2. For each BeaconPoint, select a **Failover VNS** from the drop-down list.

   This selection overrides the Default Failover VNS selected in the *BeaconPoint Registration Mode* screen. If no VNS is assigned in here in the *BeaconPoint Failover – Paired BM* screen, then the Default Failover VNS will be used.

View the BeaconPoint Availability Report

When the *BeaconPoint Configuration: BP Registration Mode* screen has been saved for the BeaconMaster in Paired Mode, the *BeaconPoint Availability* report will show the status of both “local” and “foreign” BeaconPoints for that BeaconMaster.

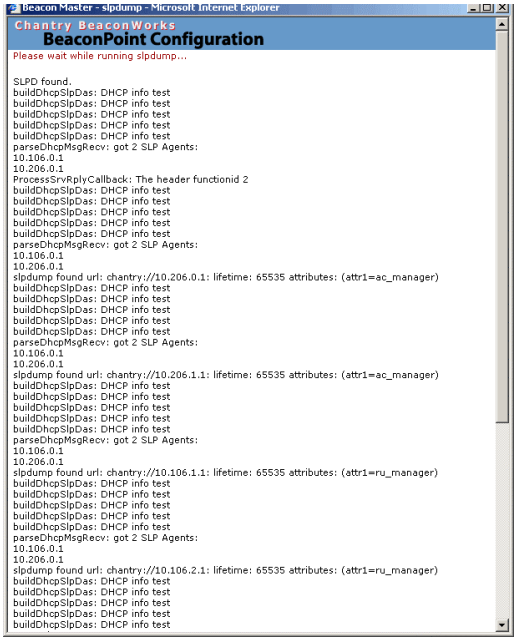
In normal operations, when Availability is enabled, the "local" BeaconPoints are green, and the "foreign" BeaconPoints are red. If the other BeaconMaster fails, and the "foreign" BeaconPoints connect to the current BeaconMaster, then the display will show all BeaconPoints as green. If the BeaconPoints are not attached they do not appear in the report.



Screen 46: Report – BeaconPoint Availability

View the SLP activity with the "slpdump tool"

1. Select **BeaconPoints** tab in any screen. Then, in the left-hand list, click on **BP Registration**. The *BeaconPoint Registration Mode* screen appears.
2. Click on the **View SLP Registration** button. A popup screen displays the results of the "slpdump tool", showing the recent SLP activity:



Screen 47: BeaconPoint configuration – View SLP Registration

In normal operations, the primary BeaconMaster registers as an SLP service called "ac_manager" and directs the BeaconPoints to the appropriate BeaconMaster of a pair. During an outage, if the remaining BeaconMaster is the secondary one, it will register as an SLP service "ru_manager".

Events and actions during a Failover

If one of the BeaconMasters in a pair fails, then the connection between the two BeaconMasters is lost. This triggers a "Failover mode" condition, and a critical message appears in the information log of the remaining BeaconMaster.

After the BeaconPoint on the failed BeaconMaster loses its connection, it will attempt a reboot. Because of the pairing of the two BeaconMasters, the BeaconPoint will then register with the other BeaconMaster.

Note: A BeaconPoint connects first to a BeaconMaster registered as "ac_manager" and, if not found, then seeks an "ru_manager". If the primary BeaconMaster fails, the secondary one registers as an SLP service "ru_manager". This enables the secondary BeaconMaster to be found by BeaconPoints after they reboot.

When the BeaconPoints connect to the second BeaconMaster, they will be assigned to the Failover VNS defined in setup in that BeaconMaster. The wireless device users will log in again and be authenticated on the second BeaconMaster.

When the failed BeaconMaster recovers, each BeaconMaster in the pair goes back to normal mode. They exchange information that includes the latest lists of registered BeaconPoints. The administrator will release the BeaconPoints on the second BeaconMaster, so that they may re-register with their home BeaconMaster.

To support the Availability feature during a "Failover" event, administrator will need to perform the following actions:

1. Monitor the critical messages in the information log of the remaining BeaconMaster for the "Failover mode" message (in the *Reports and Displays* area of the user interface).
2. After recovery, on the BeaconMaster that did not fail, select the "foreign" BeaconPoints and click on the **Release** button (in the *BeaconPoint Configuration – BP Maintenance* screen).

BeaconMaster Configuration: Mobility and the VN Manager

The BeaconWorks system has a technique by which multiple BeaconMasters on a network can discover each other and exchange information about a client session. This enables a wireless device user to roam seamlessly between different BeaconPoints on different BeaconMasters.

The solution introduces the concept of a "VN Manager". This means that one BeaconMaster on the network must be designated as the "VN Manager". All other BeaconMasters are designated as "VN Agents". To define whether the BeaconMaster is a Manager or an Agent, use the *VN Manager* screen in the BeaconMaster Configuration area.

The wireless device will keep the IP address, VNS assignment and filtering rules that it received from the BeaconMaster that it first connected to – its "home" BeaconMaster. (This information is collected in the *Active Clients by VNS* display on the home BeaconMaster.) The VNS on each BeaconMaster must have the same SSID. If the VNS has static WEP, it is recommended that the same key be used.

Note: The "VN Manager" concept relies on SLP and DHCP. Before you begin, you must ensure that the DHCP server on your network supports Option 78. These are also used during the BeaconPoint discovery process, and are explained in that topic earlier in this Guide.

VN Manager and VN Agent: Background

The BeaconMaster that is the "VN Manager":

- uses SLP to register itself as a service with the SLP Directory Agent
- listens for connection attempts from "VN Agents"
- if it receives a connection attempt from "VN Agent", it establishes connection and sends a message to the "VN Agent" specifying the Heartbeat interval, and the VN Manager's IP address.
- sends regular Heartbeat messages (which contain wireless device session changes and Agent changes) to the VN Agents and waits for an Update message back
- if it fails to receive an Update from the VN Agent after three Heartbeat messages, it sends a Disconnect message to the VN Agent, removes all wireless device users associated with that VN Agent BeaconMaster from its tables and closes down the connection.

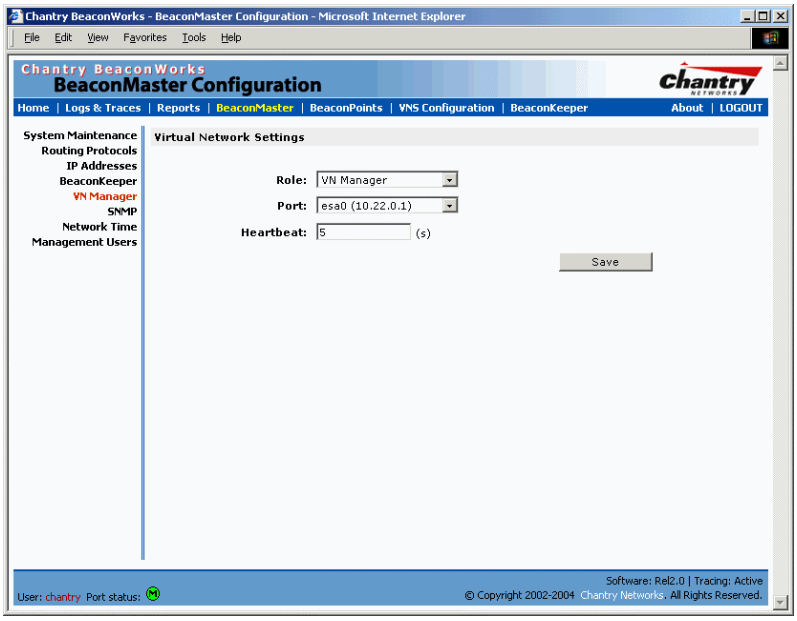
The BeaconMaster that is a "VN Agent":

- uses SLP to find the location of the VN Manager
- attempts to establish a TCP/IP connection with the VN Manager
- when it receives the connection-established message (see above), it updates its tables, and sets up data tunnels to and between all BeaconMasters it has been informed of
- after every Heartbeat massage received, it uses the information to update its own tables and then sends an Update message to the VN Manager, with updates on wireless device users and data tunnels it is managing.

Chantry Networks Inc. Copyright 2004. All rights reserved.

Set up a BeaconMaster as a VN Manager

1. In the *BeaconMaster Configuration* screen, click on the **VN Manager** option. The *Virtual Network Settings for VN Manager* screen appears.



Screen 48: BeaconMaster Configuration – VN Manager

2. From the **Role** drop-down list, select **VN Manager** (other options: None, Agent).
3. From the drop-down list, select the **Port** on the BeaconMaster to be used by the VN Manager process.

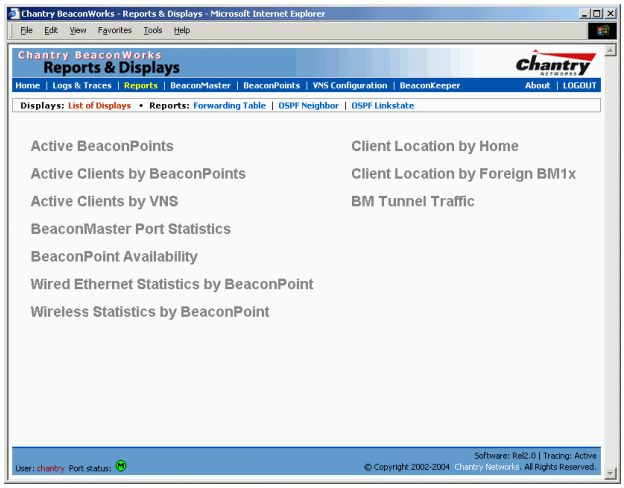
Note: Ensure that the port selected is routable on the network.

4. In the **Heartbeat** field, type in the time interval at which the VN Manager sends a Heartbeat message to a VN Agent. The default is 5 seconds.
5. To save these settings, click on the **Save** button.

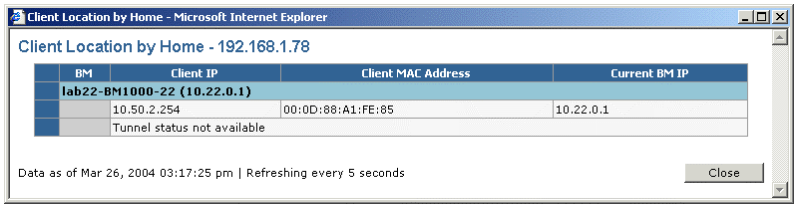
If you set up one BeaconMaster on the network as a "VN Manager", then all other BeaconMasters must be set up as "VN Agents". In the *VN Manager* screen, in the **Role** drop-down list, select **Agent**. The **Heartbeat** value, for a "VN Agent", is how long to wait for a connection establishment response before trying again.

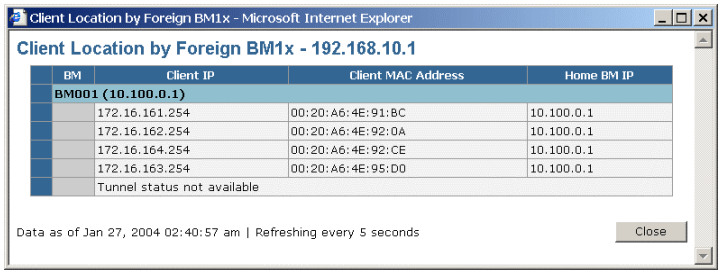
View displays when VN Managers is enabled

When a BeaconMaster has been configured as a VN Manager, three additional displays are available in the *List of Displays* screen:



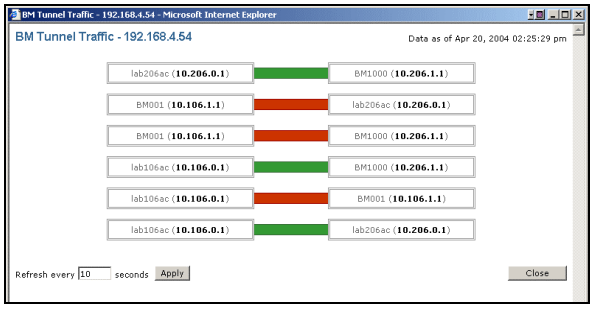
Screen 49: Reports and Displays for a VN Manager: Menu

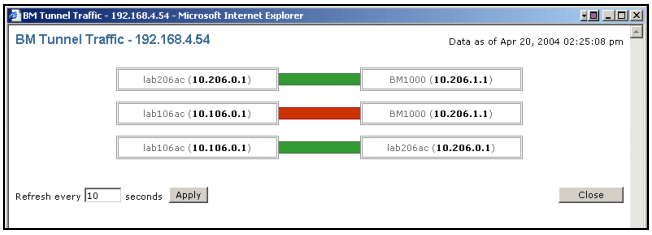




Screen 50: Reports and Displays for a VN Manager: Examples

To view the status of the tunnels between the BeaconMasters, click on the BM Tunnel Traffic display option. This screen displays the BeaconMasters known to the VN Manager. If a tunnel is active, a green band is displayed between BeaconMasters. A red band indicates that there is no traffic on the tunnel. If the BeaconMasters are not displayed, the tunnel is inactive.





Screen 51: Reports and Displays for a VN Manager: BM Tunnel Traffic

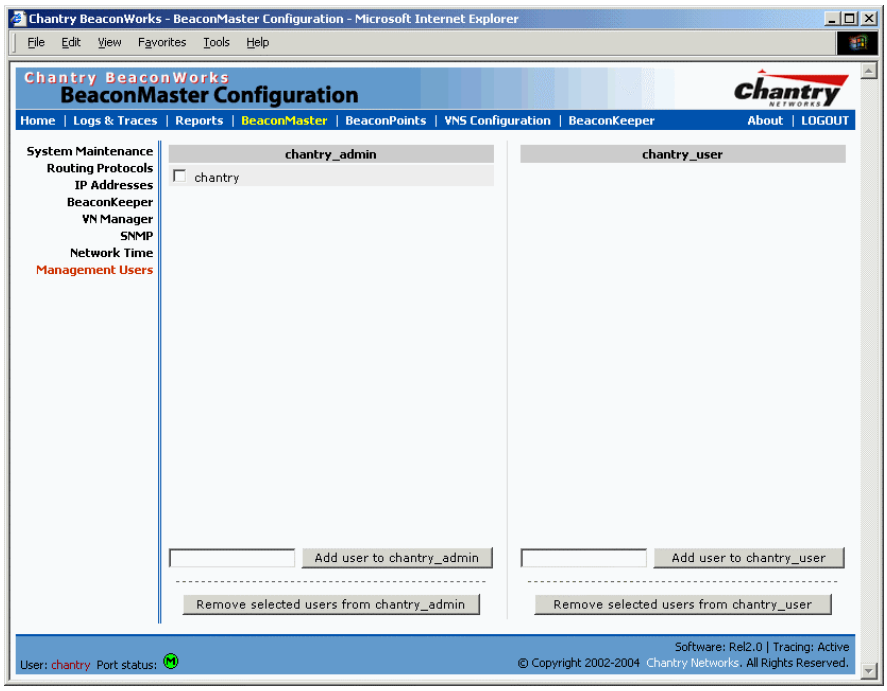
The *Active Clients by VNS* display also collects information on the VN Manager BeaconMasters of for all BeaconPoints, and for the wireless devices that travel, if they are on the same SSID.

BeaconMaster Configuration: Management Users

In this screen you define the login usernames that have access to the GUI, either for Administrators with "read/write" privileges, or other users with "read only" privileges.

Designate BeaconMaster management users

1. Click on the **BeaconMaster** tab in any screen. The *BeaconMaster Configuration* screen appears.
2. In the left-hand portion of the screen, click on the **Management Users** option. The *Management Users* screen appears. .



Screen 52: BeaconMaster Configuration – Management Users

The list on the left is for "Admin" users who have read/write privileges. The right-hand list is for users who have "read only" privileges.

To add a User ID, type it in the entry field (on the appropriate side) and click on the **Add user...** button.

To delete a User ID, click in its checkbox to select it, and then click on the **Remove selected user...** button.

Note: A User ID can only be used once, in only one of these two lists.

BeaconMaster Configuration: Network Time

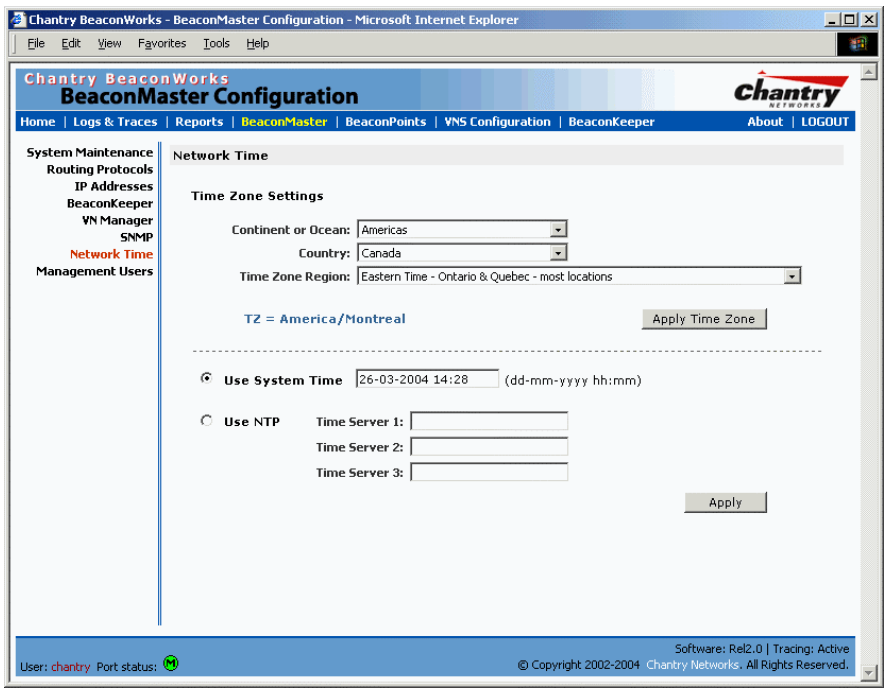
Use the Network Time screen to synchronize the elements on the network to a universal clock. This ensures accuracy in usage logs.

The Network Time screen synchronizes in one of two ways:

- using system time
- using Network Time Protocol (NTP), an Internet standard protocol that synchronizes client workstation clocks.

Set Network Time parameters

1. Click on the **BeaconMaster** tab in any screen. The *BeaconMaster Configuration* screen appears.
2. In the left-hand portion of the screen, click on the **Network Time** option. The *Network Time* screen appears.



Screen 53: BeaconMaster Configuration – Network Time

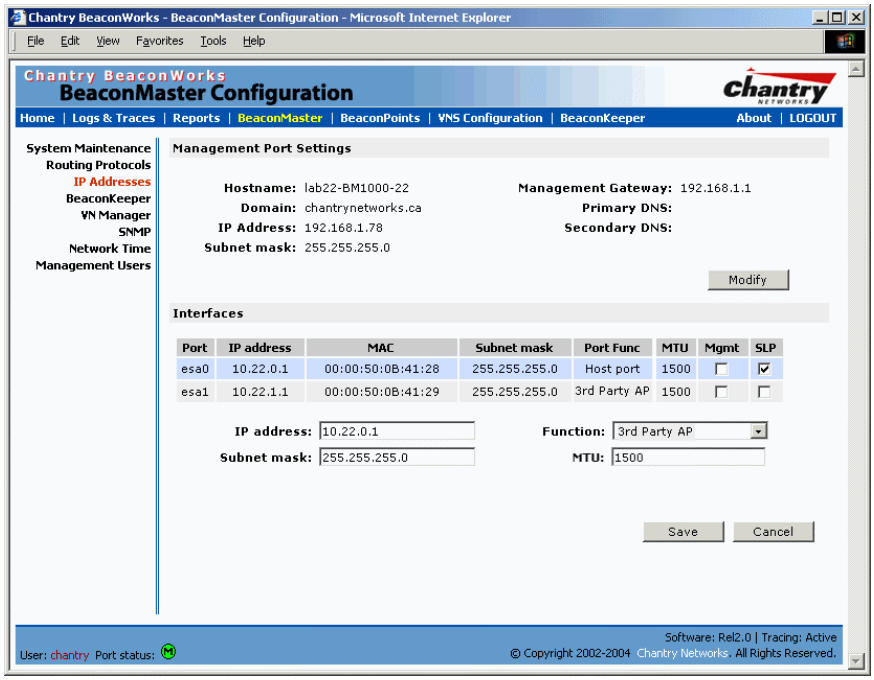
3. From the drop-down list, select the **Continent** or **Ocean**, the large-scale geographic grouping.
4. From the drop-down list, select the **Country**, within the previous group (the contents of the list will change based on the selection in the previous field).
5. From the drop-down list, select the **Time Zone Region** for the country selected.
6. To apply these time zone settings, click on the **Apply Time Zone** button.
7. To use System Time, click on its radio button. Type in the time setting.
8. To use Network Time Protocol, click on the **NTP** radio button. Then fill in the location (IP address) of up to three standard NTP Time Servers.
9. To apply these settings, click on the **Apply** button

Setting up Third-Party Access Points

Your enterprise's WLAN may have existing third-party access points that you would like to integrate into the Chantry WLAN solution. You can set up the BeaconMaster to handle wireless device traffic from third-party access points, providing the same policy and network access control.

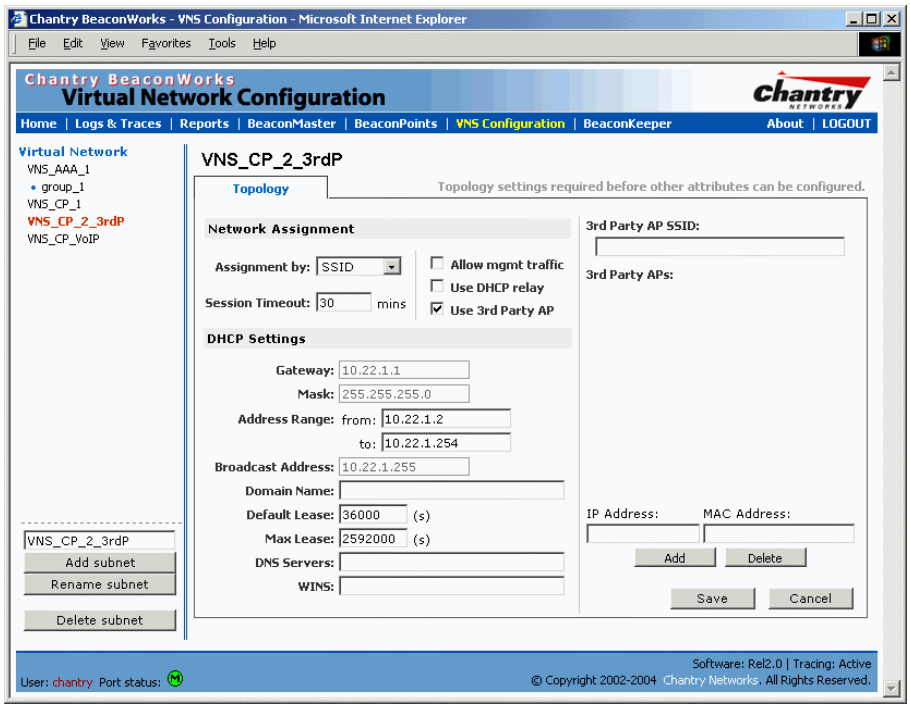
Set up third-party access points on the BeaconMaster

1. Define one data port as a "3rd-party AP" port:
   In the *BeaconMaster Configuration* screen, click on the **IP Address** option. The *Management Port Settings and Interfaces* screen appears. Highlight the appropriate port, and in the **Function** field, select "3rd-party AP" from the drop-down list. Make sure that Management Traffic and SLP are disabled for this port.



Screen 54: BeaconMaster Configuration – IP Addresses / Interfaces

2. Connect the third-party access point to this port, via a switch.
3. Define a static route to the access point:
   In the *BeaconMaster Configuration* screen, click on the **Routing Protocols** option. Then click the **Static Routes** tab. The *Static Routes* screen appears. Define a static route to the access point (see Routing topic earlier).
4. Set up a VNS for the "3rd-party AP" port:
   In the *Virtual Network Configuration* screen, add a new VNS. Then highlight the VNS name in the left-hand list and click on the **Topology** tab.



Screen 55: Virtual Network Configuration – Topology for Third-Party APs

In the Topology screen, select **Assignment by SSID**.
Click on the **Use 3rd Party AP** checkbox to select it.
Fill in the **IP Address** and **MAC Address** entry fields that appear on the right (the addresses of the third party access points, and click on the **Add** button. They will appear in the list of access points known to the BeaconMaster.
Follow the remaining steps described in the setting up a VNS for Captive Portal earlier in this Guide.

5. Set up Authentication by Captive Portal for the "3rd-party AP" VNS:
   Click on the **Authentication** tab. In the *Authentication* configuration screen, click the **Captive Portal** radio button. In the Captive Portal portion of the screen, define the RADIUS Attributes and the Filter IDs to match those in RADIUS..

Note: Alternatively, for third-party APs, you can define network assignment by AAA, and authentication by 802.1x. The RADIUS requests from the third-party access point will flow through the BeaconMaster.

6. Set up filtering rules for Filter IDs for the 3rd-Party APs:
   In the *Virtual Network Configuration* screen, click on the **Filtering** tab. The *Filtering* screen appears. Click on the subnet name in the left-hand list.
   Define filtering rules that allow access to other services and protocols on the network such as HTTP, FTP, Telnet, SNMP.

In addition, modify the following functions on the third-party access point:

- Disable the access point's DHCP server, so that the IP address assignment for any wireless device on the AP is from the DHCP server at the BeaconMaster with VNS information
- Disable the third-party access point's layer 3 IP routing capability and set the access point to work as a layer 2 bridge.

Here are the differences between third-party access points and BeaconPoints on the BeaconWorks system:

- An access point exchanges data with the BeaconMaster's data port using standard IP over ethernet protocol. The third-party access points do not support the CAPWAP Tunnelling Protocol (CTP) header for encapsulation.
- For third-party access points, the VNS is mapped to the physical data port and this is the default gateway for mobile units supported by the third-party access points.
- A BeaconMaster cannot directly control or manage the configuration of an access point.
- Access points are required to broadcast an SSID unique to their segment. This SSID cannot be used by any other VNS.
- Roaming from access points to BeaconPoints not supported.

Chantry Networks Inc. Copyright 2004. All rights reserved.

BeaconKeeper Mitigator: Detecting Rogue Access Points

BeaconKeeper Mitigator: Overview

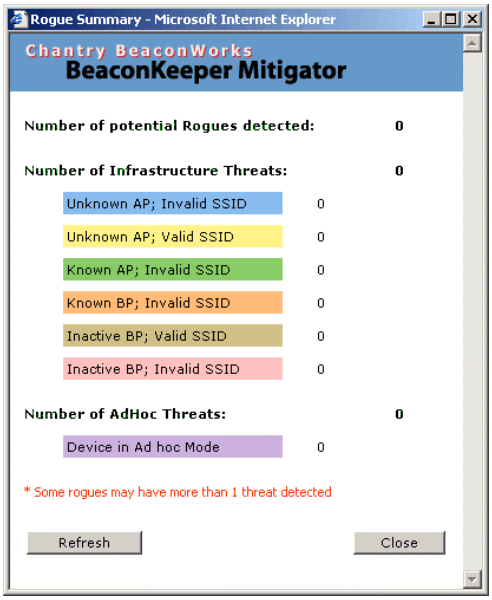
The BeaconWorks system (Release 2.0) includes a mechanism that assists in the detection of rogue access points. The function is called the BeaconKeeper Mitigator.

Th BeaconKeeper Mitigator feature has three components:

- a *radio frequency (RF) scanning task* that runs on the BeaconPoint. The BeaconPoint itself functions as a scan device. Its scan function alternates with providing its regular service the wireless devices on the network. You set up the scan parameters in the BeaconKeeper user interface.
- an application called the *RF Data Collector (RFDC)* on the BeaconMaster that receives and manages the RF scan messages sent by the BeaconPoint. The scan data includes lists of all connected BeaconPoints, third Party APs and other friendly APs and the RF scan information that has been collected from the BeaconPoints.
- an *Analysis Engine* on the BeaconMaster that processes the scan data from the RFDC through algorithms that make decisions about whether a detected access point is a rogue access point.

Note: In a network with more than one BeaconMaster, the analysis engine should be active on only one BeaconMaster that communicates with the RFDC applications running on itself and on the other BeaconMasters on the network.

The BeaconKeeper Mitigator function must be enabled in the user interface. Before it is enabled, the **BeaconKeeper** menu item in the main menu, or the **BeaconKeeper** tab in any screen will only access a popup *Rogue Summary* report screen:



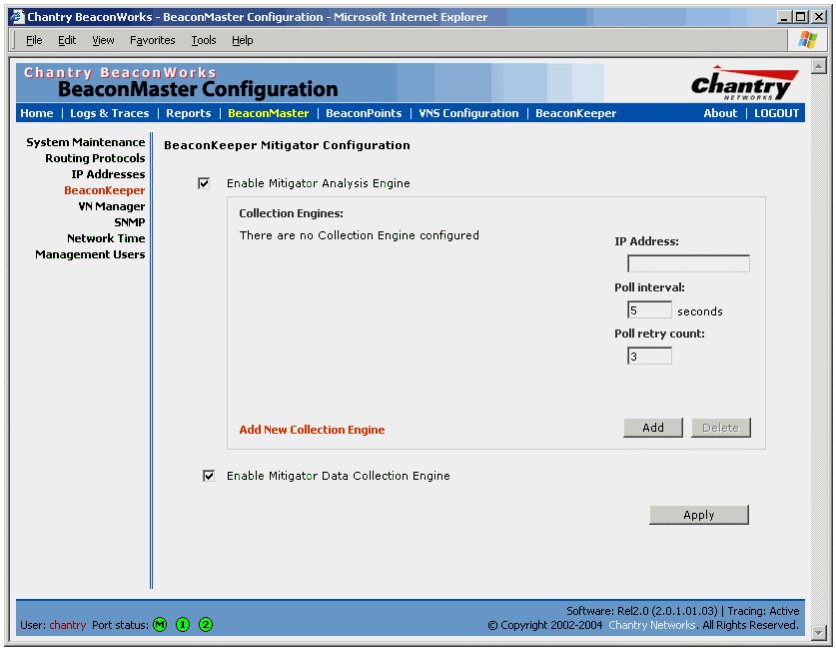
Screen 56: BeaconKeeper Mitigator – Rogue Summary Report

To enable the BeaconKeeper Mitigator, use the menu option in the *BeaconMaster Configuration* area of the user interface.

BeaconKeeper Mitigator: Enabling the Analysis and RFDC Engines

Enable and configure the BeaconKeeper Mitigator Analysis Engine

1. Click on **BeaconMaster** tab in any screen. The *BeaconMaster Configuration* area of the user interface appears. In the left-hand list, click on the **BeaconKeeper** option. The *BeaconKeeper Mitigator Configuration* screen appears.



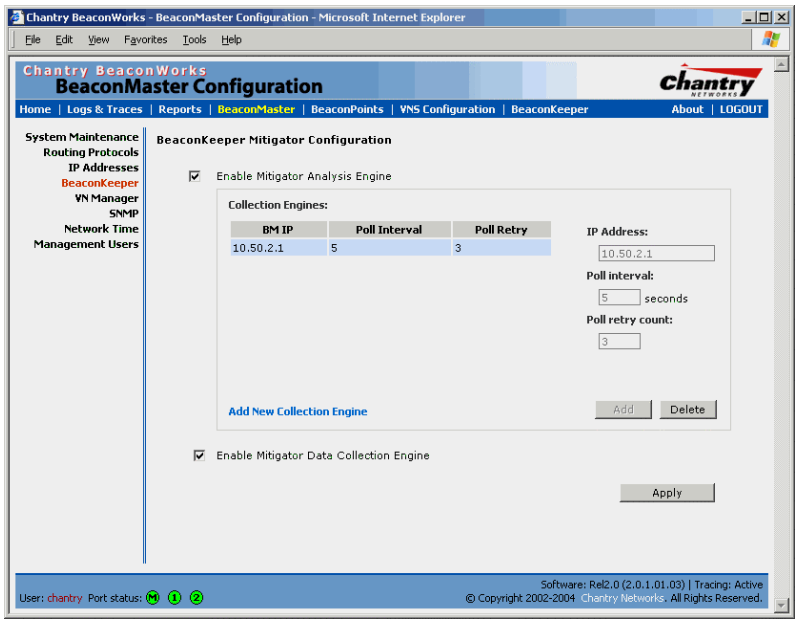
Screen 57: BeaconMaster Configuration – BeaconKeeper Mitigator Configuration

2. To enable the **Mitigator Analysis Engine**, click the checkbox on.

Define the BeaconKeeper Mitigator RF Data Collector Engines

3. To enable the **Mitigator Data Collection Engine** on this BeaconMaster click the checkbox on.
4. Identify the remote RF Data Collector Engines that the Analysis Engine will poll for data: In the **Collection Engine IPs** entry field, key in the IP address of the BeaconMaster on which the remote RFDC resides. (For this BeaconMaster, the local IP address is displayed by default.)
5. For each data collection engine, enter:
   - In the **Poll interval** field (he interval that the Analysis Engine polls the RF Data Collector for data), key in the time in seconds. Default is 30 seconds.
   - In the **Poll retry count** field, key in the number of times the Analysis Engine will attempt to poll the RF Data Collector for data before it stops sending requests. Default is 2 attempts.
6. Click on the **Add** button. The IP address of the Data Collection Engine, with its Poll Interval and Poll Retry parameters, appears in the list.

Note: For each remote RF Data Collection Engine you define here, you must also enable it (click the checkbox on) in the same screen on the remote BeaconMaster.



Screen 58: BeaconMaster Configuration – BeaconKeeper Mitigator: Collection Engines

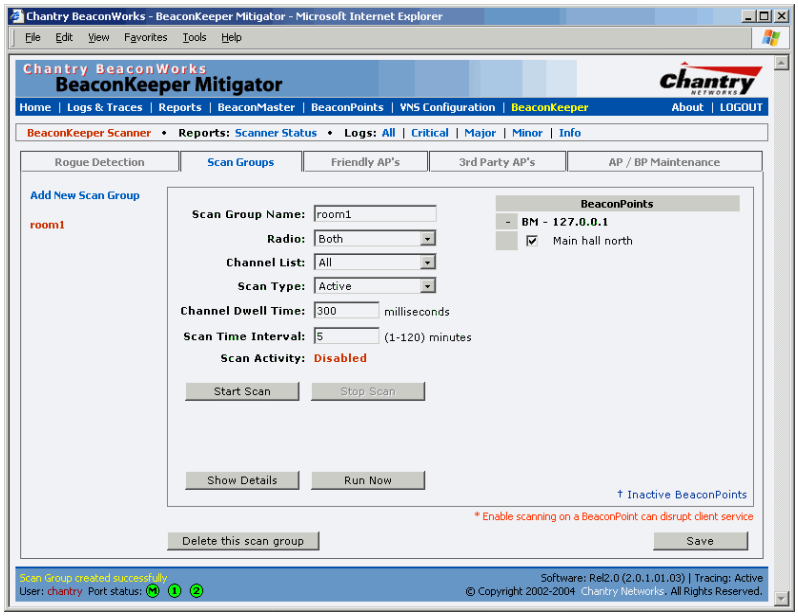
7. To clear the entry fields and add a new Collection Engine, click on the **Add Collection Engine** option. Repeat steps 4 to 6 above.
8. To save these settings, click on the **Apply** button.

BeaconKeeper Mitigator: Running Scans

After enabling the BeaconKeeper engines (as described above), click the **BeaconKeeper** menu item in the main menu, or the **BeaconKeeper** tab in any screen. The BeaconKeeper Scanner screen appears, with five tabs.

Set up and run the BeaconKeeper Mitigator scan task mechanism:

1. To set up the parameters of the scan task mechanism, click on the **Scan Groups** tab. The *Scan Groups* screen appears.

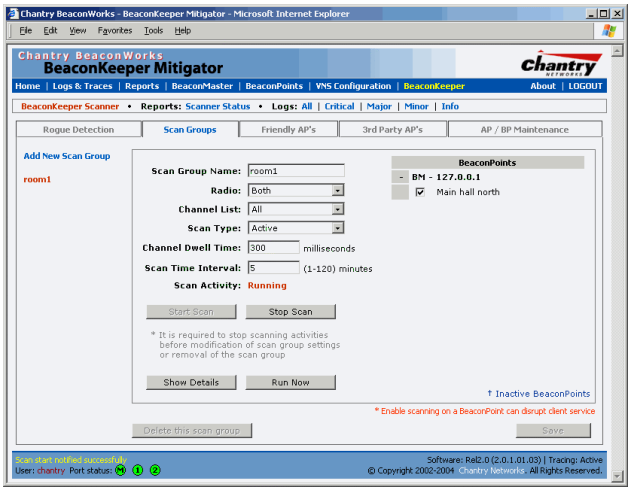


Screen 59: BeaconKeeper Mitigator Scanner – Scan Groups

3. In the **Scan Group Name** entry field, key in a name for this Scan Group.
4. In the **BeaconPoints** area, clicking the checkbox on to select the BeaconPoint (or BeaconPoints) that will be included in this Scan Group and will perform the scan function.

> **Note:** A BeaconPoint can participate in only one Scan Group at a time.
> It is recommended that the Scan Groups represent geographical groupings of BeaconPoints.

5. In the **Radio** field, from the drop-down list select which radios on the BeaconPoint are to perform the scan function Both, A only, B/G only.
6. In the **Channel List** field, from the drop-down list select the radio channels to scan on: **All**, or **Current**.
7. In the **Scan Type** field, from the drop-down list select either **Active** or **Passive**.
   - Active: the BeaconPoint sends out ProbeRequests and waits for ProbeResponse messages from any access points.
   - Passive: the BeaconPoint listens for 802.11 beacons
8. In the **Channel Dwell Time** field, key in the time in milliseconds that the scanner waits for a response (either for 802.11 beacons in passive scanning, or ProbeResponse in active scanning).
9. In the **Scan Time Interval** field, key in the time in minutes {1 to 120}, to define the frequency at which a BeaconPoint within the Scan Group will initiate a scan of the RF space.
10. To start a scan, using the periodic scanning parameters defined above, click on the **Start Scan** button
11. To initiate an immediate scan on request, click on the **Run Now** button.



12. To stop the scan, click on the **Stop Scan** button.

> **Note:** You must stop the scan before modifying any parameters of the Scan Group, or before adding or removing a BeaconPoint from a Scan Group.

13. The **Scan Activity** field displays the current state of the scan engine.

14. To view a popup report showing the timeline of scan activity and results, click on the **Show Details** button.

BeaconKeeper Mitigator: How the Analysis Engine works

The Analysis Engine relies on a database of known devices on the BeaconWorks system as follows:

- BeaconPoints registered with any BeaconMaster that has its RF Data Collector enables and has been associated with the Analysis Engine on this BeaconMaster.
- Third-Party Access Points that have been defined and assigned to a VNS (as described earlier in this Guide).
- Friendly APs, a list created in the BeaconKeeper Mitigator user interface as potential rogue access points are designated by the administrator as "Friendly".

The Analysis Engine compares the data from the RF Data Collector with the above database of known devices.

The Analysis Engine looks for access points with seven conditions:

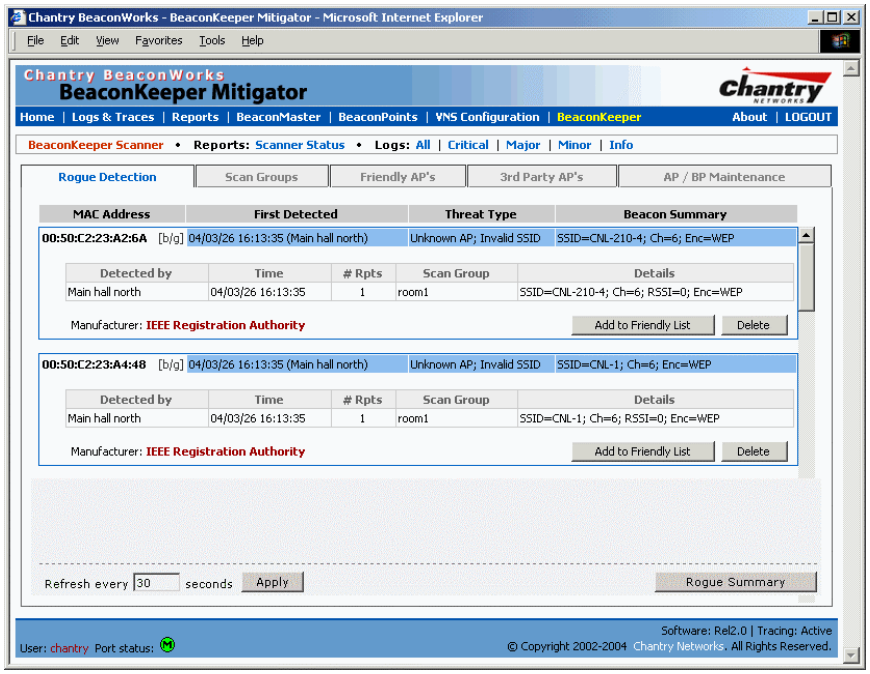
- unknown MAC address and unknown SSID (critical alarm)
- unknown MAC, with a valid SSID – a known SSID is being broadcast by the unknown access point (critical alarm)
- known MAC, with an unknown SSID – a rogue may be spoofing a MAC address (critical alarm)
- inactive BeaconPoint with valid SSID (critical alarm)
- inactive BeaconPoint with unknown SSID (critical alarm)
- known BeaconPoint with an unknown SSID (major alarm)
- in ad-hoc mode (major alarm).

Note: In Release 2.0, there is no capability to initiate a DoS attack on the detected rogue access point. Containment of a detected rogue will require an inspection of the geographical location of its Scan Group area (where its RF activity has been found).

View the BeaconKeeper scan results and build list of Friendly APs

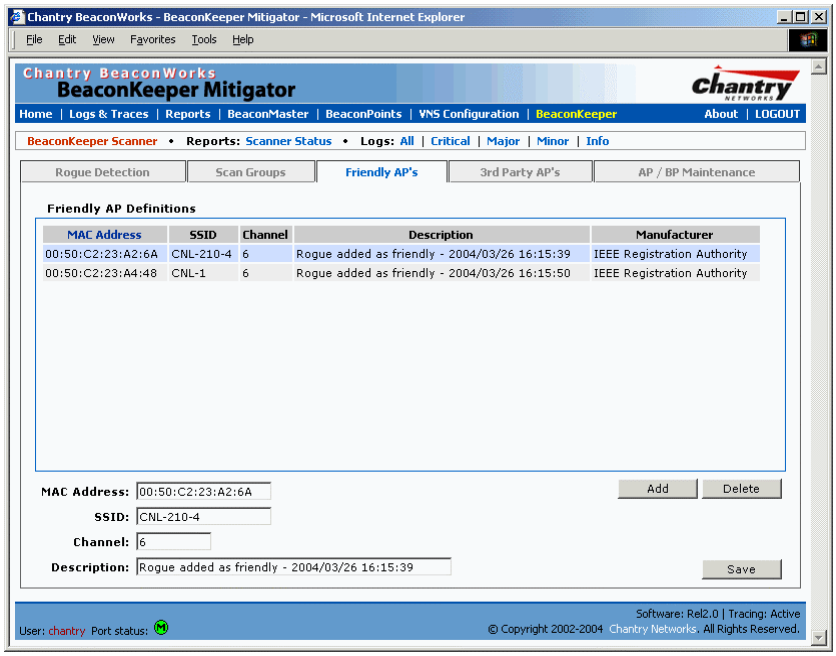
1. Click on the **BeaconKeeper** tab in any screen Then click on the **Rogue Detection** tab. The *Rogue Detection* screen appears displaying all access points and BeaconPoints that were found in the scan but are not in the database of known devices (as defined above).
2. To modify the rate that this information is refreshed, key in a time in seconds and click on the **Apply** button.

Note: The **Rogue Summary** button accesses the *Rogue Summary* popup report described earlier in this Guide.



Screen 60: BeaconKeeper Mitigator Scanner – Rogue Detection

3. To remove an access point from this list, click on the **Delete** button.
4. To add an access point or BeaconPoint to the *Friendly APs* list, click on the **Add to Friendly List** button. The access point item will be removed from this list and will appear in the *Friendly APs* list.
5. To view the Friendly list, click on the **Friendly APs** tab. The *Friendly AP Definitions* screen appears.



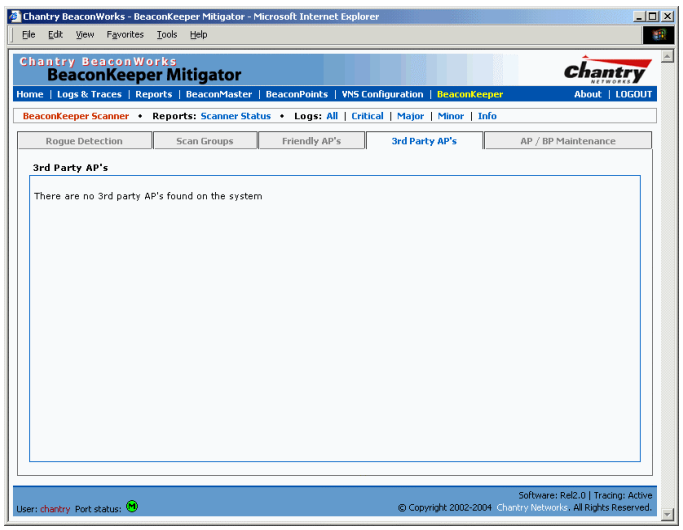
Screen 61: BeaconKeeper Mitigator Scanner – Friendly APs

6. To add friendly access points manually to the *Friendly AP Definitions* list, key in the **MAC Address**, **SSID**, **Channel** and a text description of the access point. Click on the **Add** button. The new access point appears in the list above.

7. To delete an access point from the list, highlight it and click on the **Delete** button.
8. To modify an access point in the list, highlight it and make the appropriate changes in the entry fields. Click on the **Save** button.

View the BeaconKeeper list of Third-Party APs

To view the list of the known third-party access points, click on the **3rd Party APs** tab. The *3rd Party APs* screen appears.

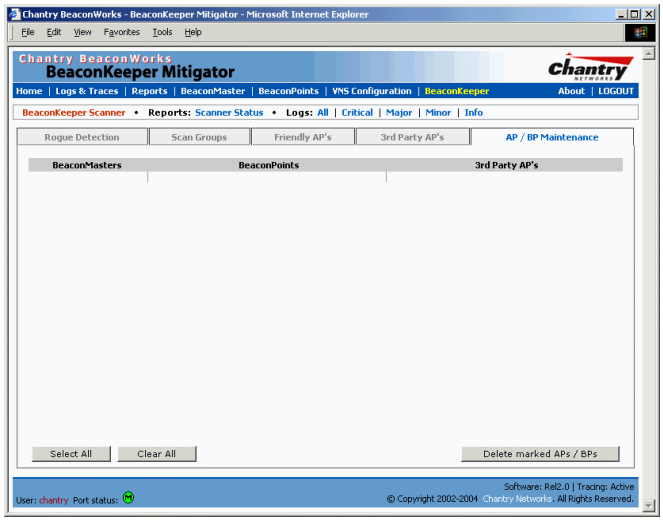


Screen 62: BeaconKeeper Mitigator Scanner – 3rd Party APs

Maintain the BeaconKeeper list of access points and BeaconPoints

When BeaconPoints or Third-Party Access Points are deleted in the BeaconWorks user interface on a BeaconMaster has its RFDC running and is in communication with the Analysis Engine, this information will also be displayed in the BeaconKeeper Mitigator's *AP / BP Maintenance* screen.

1. To view the *AP / BP Maintenance* screen, click on the **AP / BP Maintenance** tab..



Screen 63: BeaconKeeper Mitigator Scanner – AP / BP Maintenance

The deleted access points and BeaconPoints will be marked with a "Deleted" flag

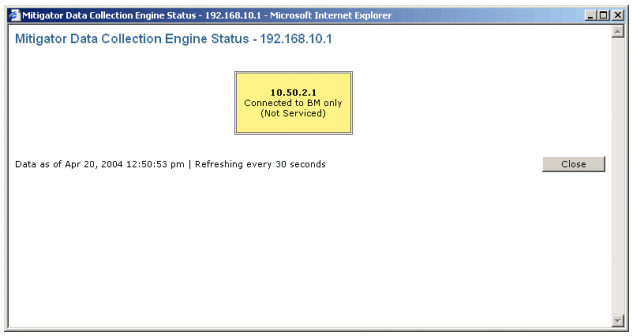
2. To delete the marked access points and BeaconPoints from the BeaconKeeper Mitigator's database, click on the **Delete marked AP / BPs** button.

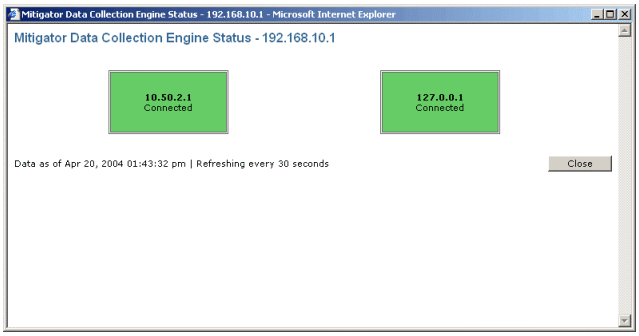
BeaconKeeper Mitigator: Viewing the Scanner Status Report

When the BeaconKeeper Mitigator is enabled, you can view a report on the connection status of the RF Data Collector Engines with the Analysis Engine.

View the BeaconKeeper scanner engine status display

1. Click the **BeaconKeeper** tab in any screen, and then click on the **Scanner Status** tab. Examples of the connection reports are shown below.





Screen 64: BeaconKeeper Mitigator – Scanner Status Report

The IP address of the RFDC engine is displayed, with its status:

- Connected (green box) – the Analysis Engine has connection with the RFDC on that BeaconMaster.
- Connected but not serviced (yellow box) – the Analysis Engine has connection with the RFDC but is not synchronized with it yet.
- Not connected (red box) – the Analysis Engine is aware of the RFDC and attempting connection.

Ongoing Operation: BeaconPoint Maintenance – Software

Periodically, the software used by the BeaconPoints is altered, either for reasons of upgrade or security. The new version of the software is installed from the BeaconMaster, using the *BeaconPoint Maintenance* area of the user interface.

You prepare the version of software for each BeaconPoint that will be uploaded to the BeaconPoint in one of time scenarios:

- the next time the BeaconPoint connects. Part of the BeaconPoint boot sequence is to seek and install its software from the BeaconMaster.
- an immediate upgrade and reboot.

BeaconPoint software: Dynamic reconfiguration (without reboot)

In Release 2.0, a number of the properties of each radio on a BeaconPoint can be modified (in the *BeaconPoint Configuration* screen) without requiring a reboot of the BeaconPoint. However, modifying the following properties does require a reboot:

- enabling or disabling either radio
- changing the radio channel between “Auto” and any fixed channel number.

In addition, the BeaconPoint must be rebooted after it has been added to a VNS, or the radio assignment in a VNS has been changed. Any changes to security also require a reboot of the BeaconPoint.

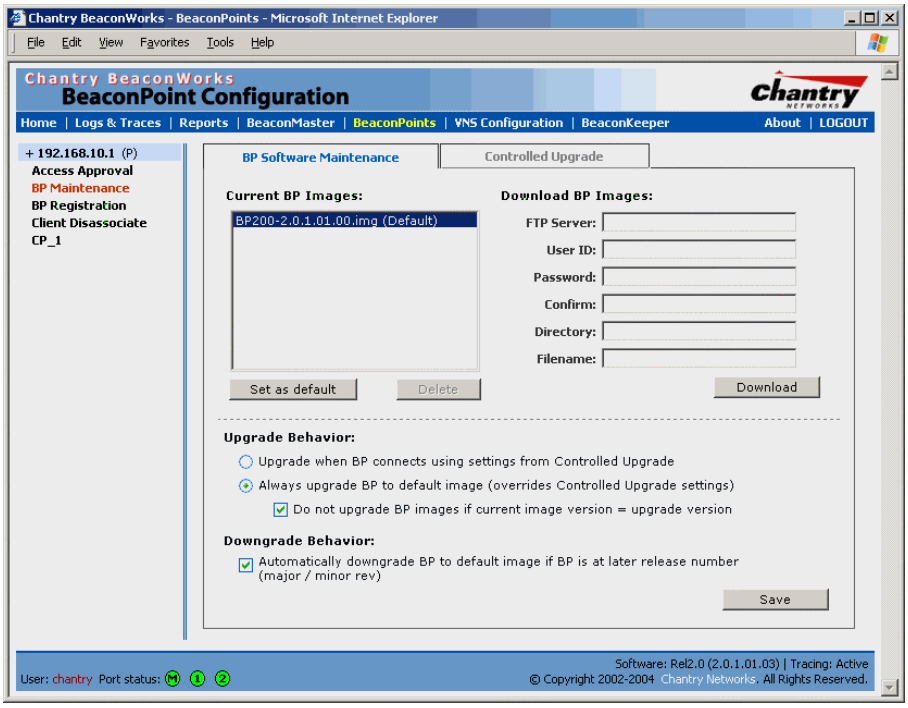
BeaconPoint software: Dual image backup

The BeaconPoint in Release 2.0 keeps a backup copy of its software image. When a software upgrade is sent to the BeaconPoint, the upgrade becomes the BeaconPoint’s current image and the previous image becomes the backup. In the event of failure of the current image, the BeaconPoint will run the backup image.

Maintain the list of current BeaconPoint software images

1. Select the **BeaconPoints** tab in any screen. The *BeaconPoint Configuration* screen appears. Click on the **BP Maintenance** option in the left-hand list.
2. To maintain the list of current BeaconPoint software images, click on the **BP Software Maintenance** tab. The *BP Software Maintenance* screen appears.

Chantry Networks Inc. Copyright 2004. All rights reserved.



Screen 65: BeaconPoint Configuration – BP Maintenance: Software Maintenance

The **Current BP Images** area displays the list of BP software versions that have been downloaded and are available. (This list appears in the drop-down list of available images in the *Controlled Upgrade* screen.)

3. To select an image as the default image to be used for software upgrade, highlight the image name in the list and click on the **Set as default** button.
4. To delete a software image from the list, highlight the version in the displayed list of **Current BP Images** and click on the **Delete** button.
5. To download a new image to be added to the list, fill in the fields in the **Download BP Images** area with parameters for FTP transfer: FTP server, User ID, Password, Confirm password, Directory, Filename.

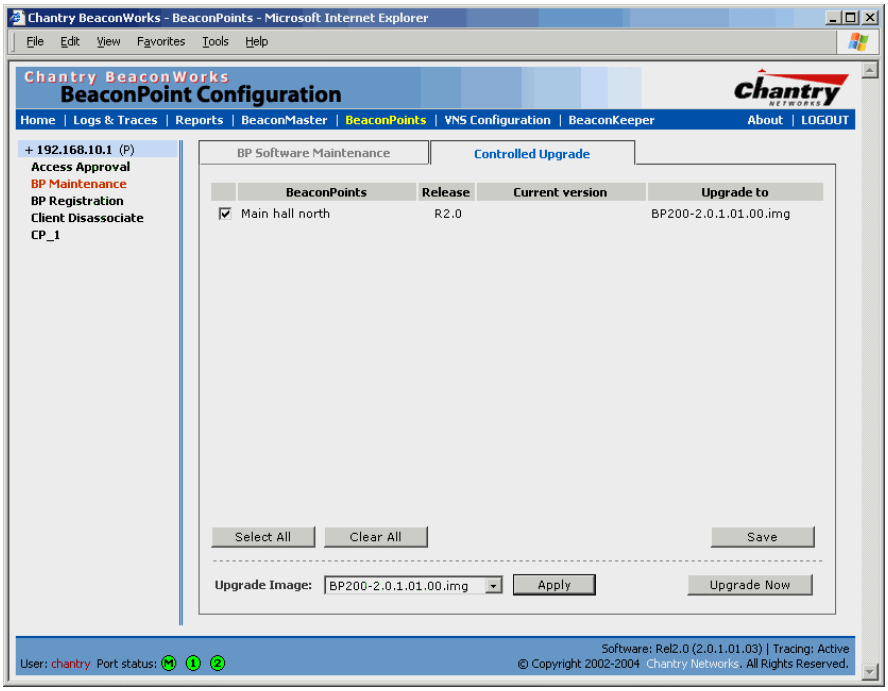
   Click on the **Download** button.
6. In the **Upgrade Behavior** area, select one of these radio buttons:
   - Upgrade when BP connects using setting from Controlled Upgrade
   - Always upgrade BP to default image (overrides Controlled Upgrade settings)

   For either choice, click the checkbox on to prevent an upgrade if current image version is the same as the upgrade version (this overrides Upgrade Now behavior)
7. In the **Upgrade Behavior** area, click the checkbox on to automatically downgrade BP to default image if BP is at later release number (major/minor rev)
8. To save these parameters, click on the **Save** button.

Define the parameters for a BeaconPoint software upgrade

1. Select the **BeaconPoints** tab in any screen. The *BeaconPoint Configuration* screen appears. Click on the **BP Maintenance** option in the left-hand list.

2. To set the software upgrade parameters, click on the **Controlled Upgrade** tab. The *Controlled Upgrade* screen appears.



Screen 66: BeaconPoint Configuration – BP Maintenance: Controlled Upgrade

The top portion of the screen displays a list of the registered BeaconPoints and the current software image on each one.

3. Select a BeaconPoint for software upgrade by clicking its checkbox on. Use the **Select All** or **Clear All** buttons to modify your selections.

   To save the BeaconPoint selections, click on **Save** button.

4. In the **Upgrade Image** field, from the drop-down list, select the software version you wish to use for the upgrade. (This list is maintained in the *BP Software Maintenance* screen, described above.) Click on **Apply** button.

   The selected image now appears in the **Upgrade To** column beside the selected BeaconPoint.

5. To run the software upgrade **immediately**, click on the **Upgrade Now** button. This will force the selected BeaconPoint to reboot, during which the new software version will be loaded.

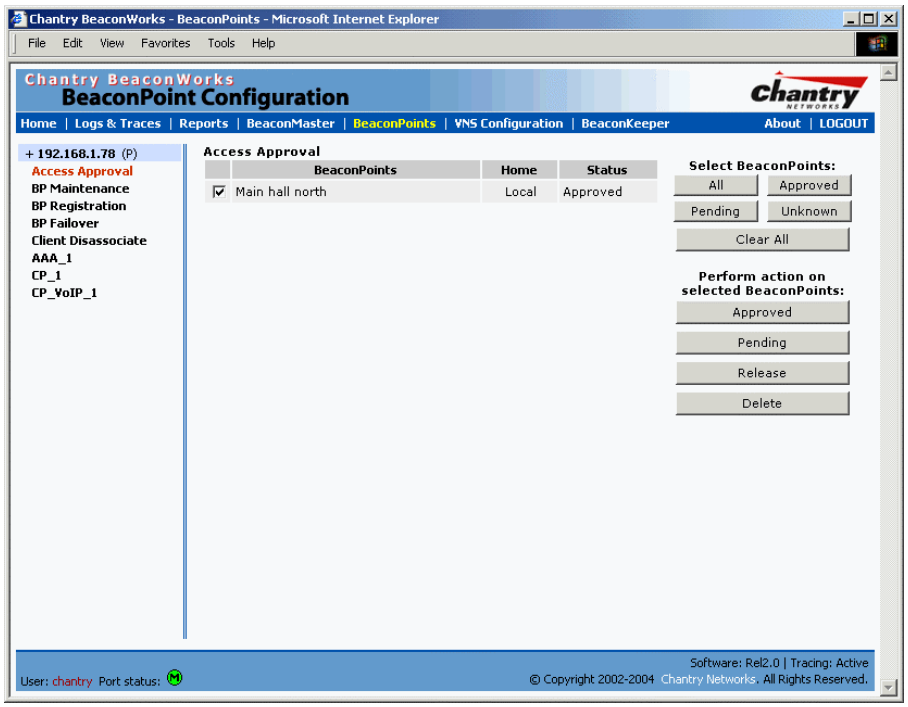
Note: Some of the settings defined in the *BP Software Maintenance* screen will override the **Upgrade Now** function. See previous screen.

Ongoing Operation: BeaconPoint Access Approval

You can also view and modify the status of registered BeaconPoints. Use this function to modify the status of a BeaconPoint from "Pending" to "Approved" for a manual registration.

Modify a BeaconPoint's registration status (approve access)

1. Select the **BeaconPoints** tab in any screen. The *BeaconPoint Configuration* screen appears. Click on the **Access Approval** option in the left-hand list. The *Access Approval* screen appears.



Screen 67: BeaconPoint Configuration – Access Approval

The screen displays the current registered BeaconPoints and their current registration status.

The **Home** field displays "Local" (this BeaconMaster) or "Foreign" (other BeaconMaster), if you have set up two BeaconMasters in Paired Mode, as described in the *BeaconMaster Configuration: Availability* topic.

2. Select the BeaconPoints for status change, either by:
   - clicking the checkbox on to select a specific BeaconPoint, or
   - using one of the **Select BeaconPoints** buttons to select by category.
3. To perform an action on the selected BeaconPoints, click on one of the **Action** buttons: Approved, Pending, Release, Delete.

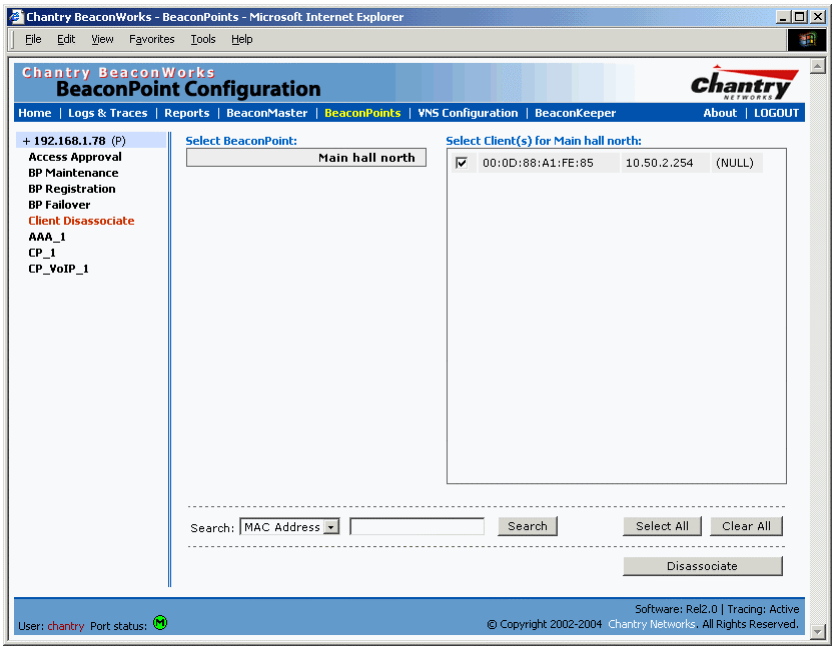
Note: A typical use of this function is to change a BeaconPoint's status from "Pending" to "Approved", if the BeaconMaster was set to register only approved BeaconPoints, in the *BeaconPoint Configuration: BP Registration* screen.
Use the "Release" function to release "foreign" BeaconPoints after recovery from a Failover, as described in the *BeaconMaster Configuration: Availability* topic.

Ongoing Operation: BeaconPoint Disassociate a Client

There are times when you want to cut the connection with a particular wireless device, for service reasons or to deal with a security issue. Using the BeaconMaster user interface, you can *disassociate* any wireless device from its BeaconPoint.

Disassociate a Wireless Device Client

1. Select the **BeaconPoints** tab in any screen. The *BeaconPoint Configuration* screen appears.
2. Click on the **Client Disassociate** option in the left-hand portion the *BeaconPoint Configuration* screen. The *Wireless Unit Disassociate* screen appears.



Screen 68: BeaconPoint Configuration – Wireless Unit (Client) Disassociate

The *Client Disassociate* screen displays the current active sessions, the wireless devices that are currently active for each BeaconPoint.

3. Click on the checkbox to select the wireless device to be disassociated.
4. To search for a client by MAC Address, IP Address or User ID, select one and then key in the parameters and click on the **Search** button.
5. Click on the **Disassociate** button to terminate the client's session immediately.

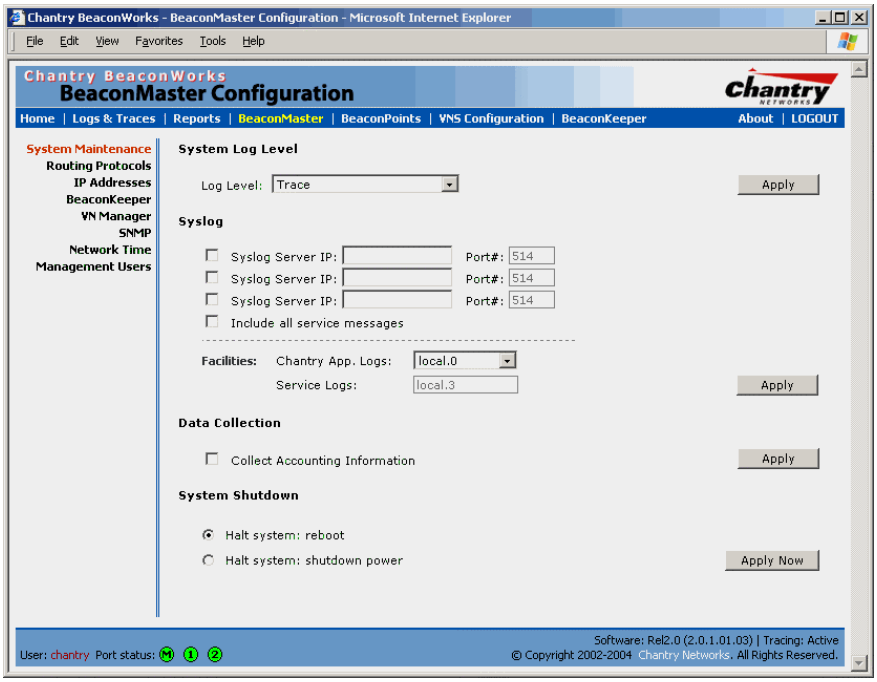
Ongoing Operation: BeaconMaster System Maintenance

Use the *System Maintenance* screen to perform various maintenance tasks, including:

- change the log level
- enable and define parameters for Syslog event reporting (see next topic)
- enable or disable the collecting of accounting information
- force an immediate system shutdown, with or without reboot.

Performing BeaconMaster maintenance functions

1. Click on the **BeaconMaster** tab in any screen. The *BeaconMaster Configuration* screen appears. In the left-hand portion of the screen, click on the **System Maintenance** option. The *System Maintenance* screen appears. .



Screen 69: BeaconMaster Configuration – System Maintenance

Change the System Log Level

2. From the drop-down list, select the desired log level (Trace, Info, Minor, Major, Critical). Click on the **Apply** button.

Enable Data Collection for Accounting

3. Click the checkbox on to enable the collecting of accounting data. Click on the **Apply** button.

Perform a System Shutdown

4. To shut down the BeaconWorks system, with its BeaconPoints, click on the appropriate radio button:
   - Halt system, reboot
   - Halt system, shutdown power

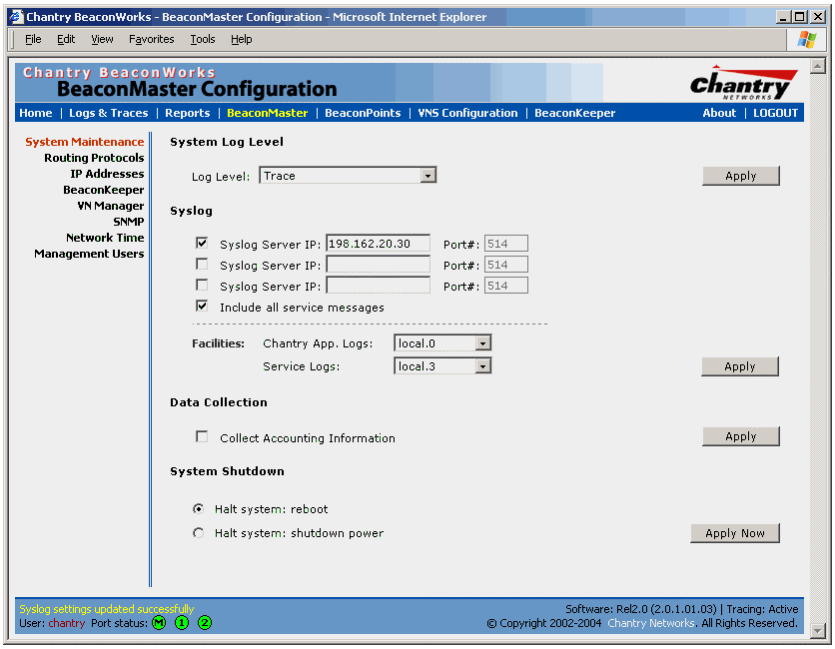
   Click on the **Apply Now** button.

Event Messages relayed to a Syslog server

In addition to viewing BeaconWorks events generated by its internal event server in the *Reports and Displays* area of the user interface, you can also relay those messages to a centralized event server on your enterprise network.

The relay is done using the *syslog protocol*, a protocol used for the transmission of event notification messages across networks. In the protocol a device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

Use the *System Maintenance* screen, *Syslog* area, to enable the syslog function and to define the location of one or more centralized Event Servers (syslog servers).



Screen 70: BeaconMaster Configuration – System Maintenance: Syslog enabled

1. Click the checkbox on to enable the **Syslog** function for up to three syslog servers.
2. For each enabled syslog server, key in a valid IP address for the server on the network. The default port for syslog is 514.
3. In the **Facilities** area, in the **Chantry App. Logs** drop-down list, select the log level ("local.0" to "local.6") to be sent to the syslog server. (This will apply to all three servers.)
4. To include additional system messages as well as the standard component messages, click the **Include all service messages** checkbox on. If the box is left unchecked, only BeaconWorks component messages (logs and traces) are relayed. (This will apply to all three servers.)

   The system messages that can be included in Release 2.0 are:

   - DHCP messages reporting users receiving IP addresses
   - Startup Manager Task messages reporting component startup and failure.

If you clicked the **Include all service messages** checkbox on, the **Facilities** drop-down list for **Service Logs** become selectable. Select a log level from the list.

5. To activate the above settings, click on the **Apply** button.

The log level mapping between syslog and BeaconWorks event logging is shown below:

Syslog	*BeaconWorks*
LOG_CRIT	Critical
LOG_ERR	Major
LOG_WARNING	Minor
LOG_INFO	Information
LOG_DEBUG	Trace

Note: The syslog daemon must be running on both the BeaconMaster and on the remote syslog server before the logs can be synchronized. If you change the log level on the BeaconMaster, you must also modify the appropriate setting in the syslog configuration on remote syslog server.

Chantry Networks Inc. Copyright 2004. All rights reserved.

Ongoing Operation: BeaconWorks Logs and Traces

BeaconWorks Log and Data Files

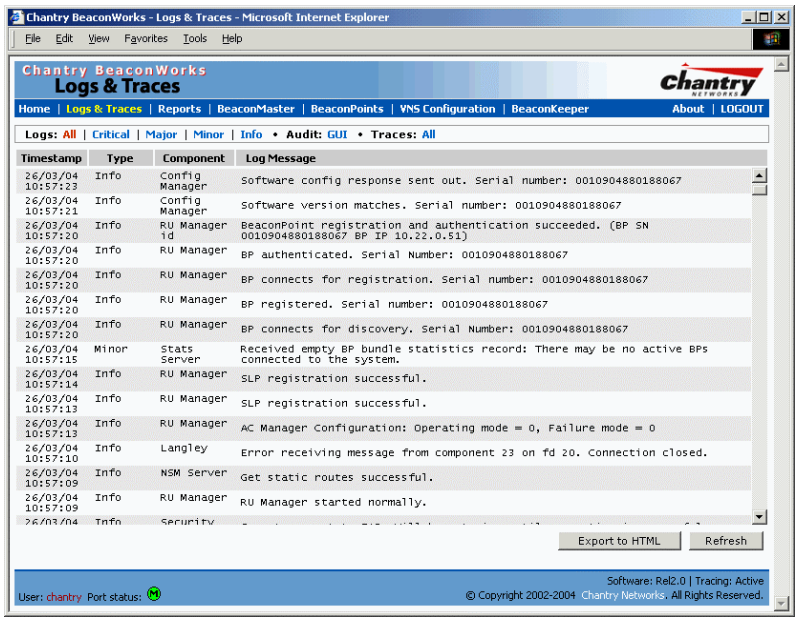
The Chantry BeaconWorks system stores configuration data and log files in flat files. These files include:

- event and alarm logs (triggered by events, described below)
- trace logs (triggered by component activity, described below)
- accounting files (created on a half-hourly basis, up to six files).

The files are stored in the operating system and have a maximum size of 1 GB.

The accounting files are stored in a directory that is created every day. Eight directories are maintained in a circular buffer (when all are full, the most recent replaces the earliest).

The BeaconMaster generates three types of messages (Logs, Traces and Audits). To view these, select the **Logs & Traces** tab in any screen.



Screen 71: Logs & Traces: Log Display – All

The details for each type of message are described below.

Logs and Alarms

Log messages are triggered by events. The log messages contain the time of event, severity, source component and any details generated by the source component. The messages are classified at four levels of severity:

- Informational, the activity of normal operation
- Minor (alarm)
- Major (alarm)
- Critical (alarm)

The alarm messages (*minor*, *major* or *critical* log messages) are triggered by activities that meet certain conditions that should be known and dealt with.

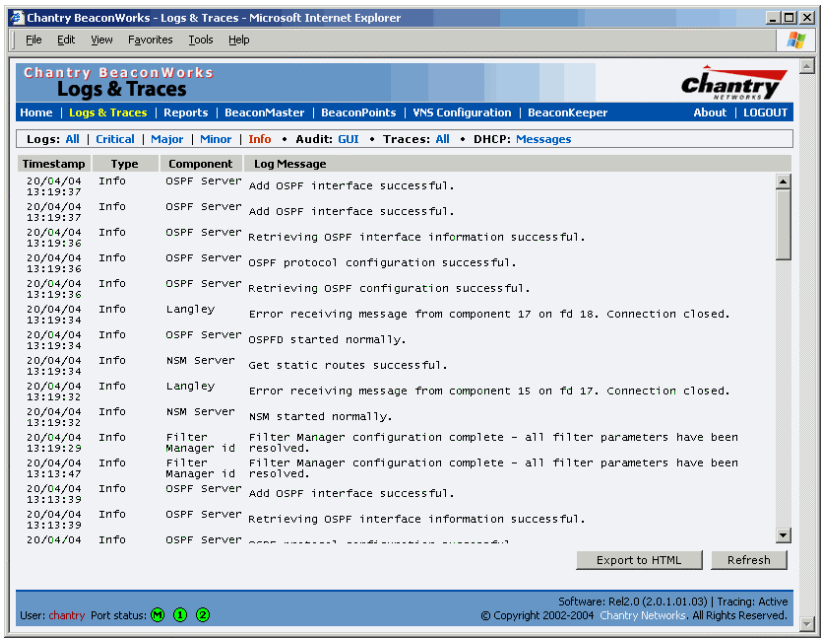
On the BeaconMaster, conditions such as the following generate an alarm message:

- Reboot due to failure
- Software upgrade failure on the BeaconMaster
- Software upgrade failure on the BeaconPoint
- Detection of rogue access point activity without valid ID

If SNMP is enabled on the BeaconMaster, alarm conditions will trigger a trap in SNMP (Simple Network Management Protocol). An SNMP trap is an event notification sent by the managed agent (a network device) to the management system to identify the occurrence of conditions. (See *BeaconMaster Configuration: Setting up SNMP* for more information on enabling this function on the BeaconMaster.)

View the Logs

1. Select the **Logs & Traces** tab in any screen. In the Navigation bar, to view all logs, click on one of the **Log** tabs. The *Log* screen appears (**Info** shown below).



Screen 72: Logs & Traces: Log Display – Info

   The events are displayed in chronological order, sorted by the **Timestamp** column.
2. To sort the display by **Type** or **Component**, click on the column heading.
3. To filter the logs by severity, in order to display only **Info**, **Minor**, **Major** or **Critical** logs, click on the appropriate Log tab at the top of the screen.
4. To refresh the information in any display, click on the **Refresh** button.
5. To export the displayed information from any display as an HTML file, click on the button.

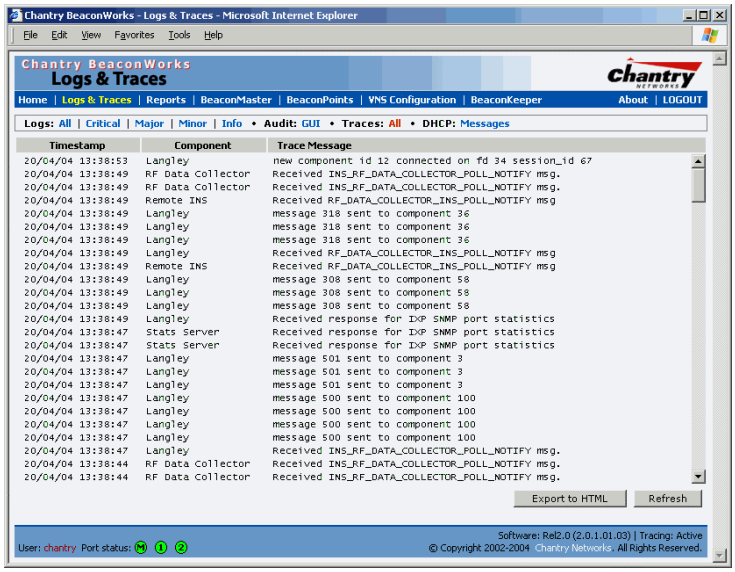
Note: The component called "Langley" is Chantry's term for the inter-process messaging infrastructure on the BeaconMaster.

Traces

Trace messages display activity by component. These can be used for system debugging, troubleshooting and internal monitoring of software.

View the Traces

1. To view the list of **Traces**, messages by component, click on its tab.



Screen 73: Logs & Traces: Trace Messages

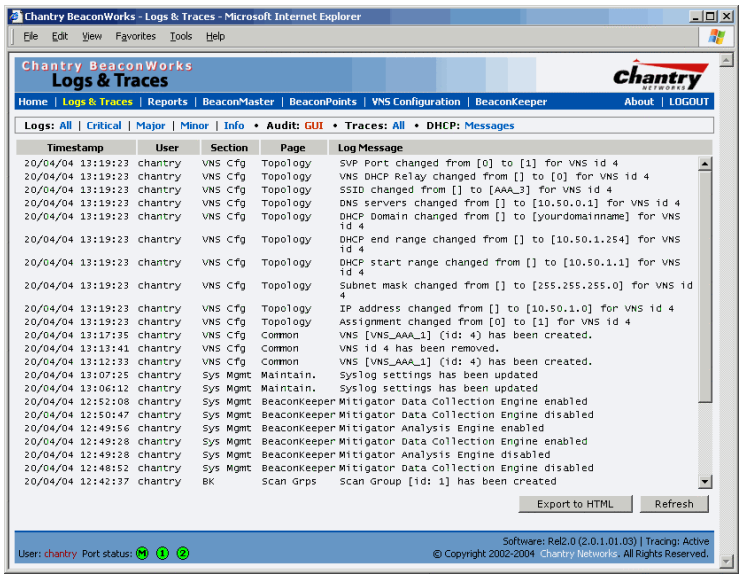
You can sort, refresh and export the Trace information, as described for Log displays.

Audits

Audit files record administrative changes made to the system. For example, the GUI Audit displays changes to the Graphical User Interface on the BeaconMaster.

View the Audits

1. To view the **GUI Audit** display, click on the **GUI Audit** tab.

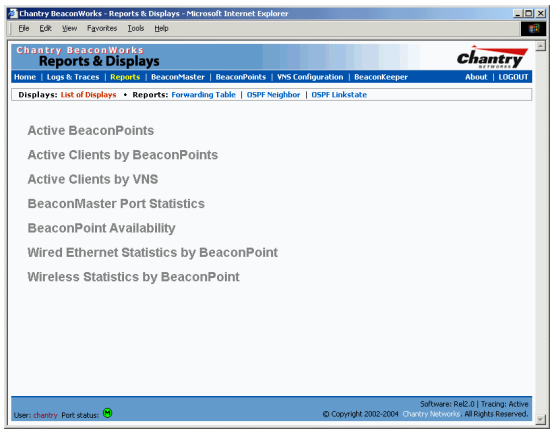


Screen 74: Logs & Traces: GUI Audit

Ongoing Operation: BeaconWorks Reports and Displays

View Displays

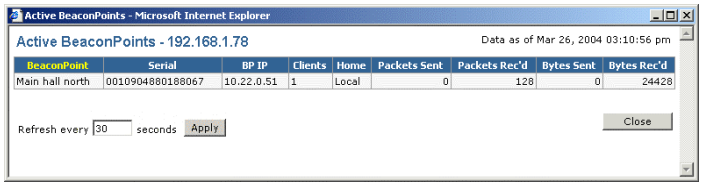
To view BeaconWorks reports and displays, click on the **Reports** tab in any screen. The *List of Displays* screen appears, with a menu of available displays. The navigation bar across the top of the screen shows the available **Reports**.



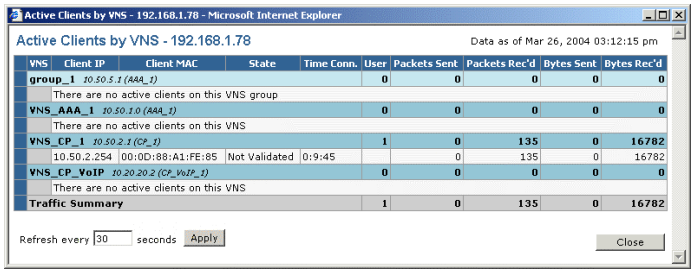
Screen 75: Reports and Displays – List of Displays

Note: If a BeaconMaster has been configured as a VN Manager, three additional reports are available in the *List of Displays* screen. (See the VN Manager topic.)

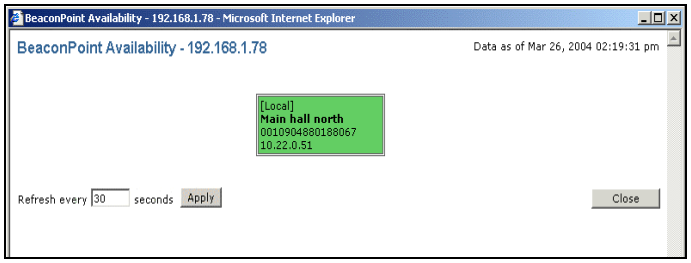
Click on an option in the menu to view its display screen, with current information about BeaconMaster and BeaconPoint activity. Some examples are illustrated below.



Screen 76: Displays – Active BeaconPoints



Screen 77: Displays – Active Clients by VNS



Screen 78: Displays – BeaconPoint Availability

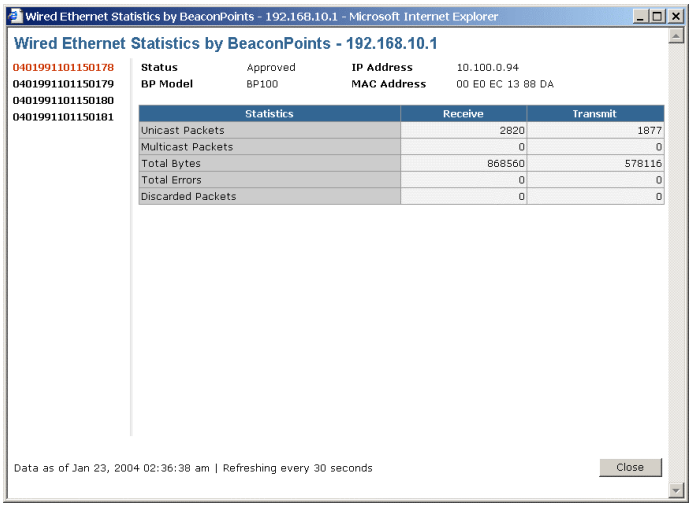
View Statistics for BeaconPoints

Two displays show information about activity on a selected BeaconPoint:

- Wired Ethernet Statistics by BeaconPoints
- Wireless Statistics by BeaconPoints

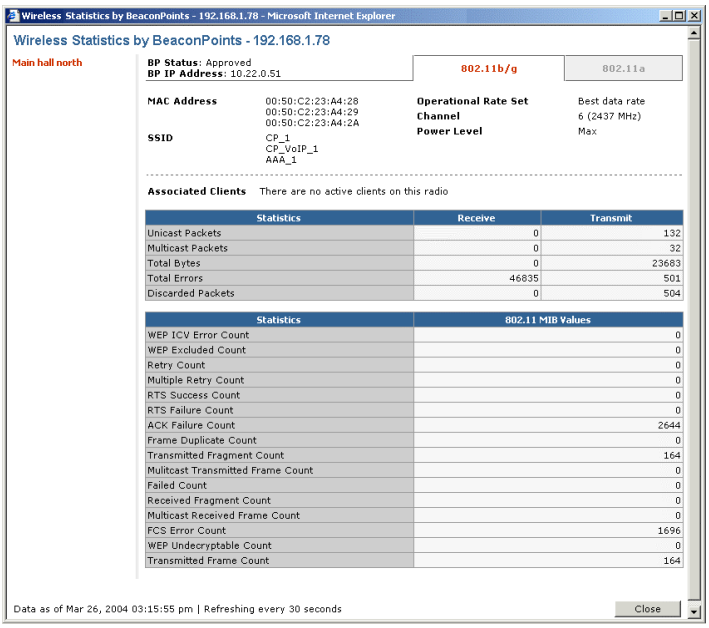
These displays are snapshots of the BeaconPoint activity at that point in time. The statistics displayed are those defined in the 802.11 MIB, defined in the IEEE 802.11 standard (in Section 11.4 and Annex D).

To view the **Wired Ethernet Statistics by BeaconPoints** display, click on its option in the **List of Displays** menu. The displays lists the registered BeaconPoints in the left-hand list. Click on the selected BeaconPoint to display its information.



Screen 79: Display – Wired Ethernet Statistics by BeaconPoints

To view the **Wireless Statistics by BeaconPoints** display, click on its option in the **List of Displays** menu.



Screen 80: Display – Wireless Statistics by BeaconPoints

The displays lists the registered BeaconPoints in the left-hand list. Click on the selected BeaconPoint. Then click on the appropriate tab to display information for each radio on the BeaconPoint

If there are associated clients on this radio, you can view information on a selected client. Click on the **View Client** button. The Associated Clients popup window appears.

Associated Clients - BP 0010904880188067, Radio 802.11b/g - 192.168.1.78

Client	Received				Transmitted				Counts				
MAC Addr	RSSI	Rate	Frames	Errors	RSSI	Rate	Frames	Errors	Auth.	Deauth.	Assoc.	Deassoc.	Reassoc.
00:90:7A:01:2F:44	5949	3	406	0	46	835177	272	0	68	68	136	67	0

Screen 81: Display – Wireless Statistics by BeaconPoints: Clients

View Reports

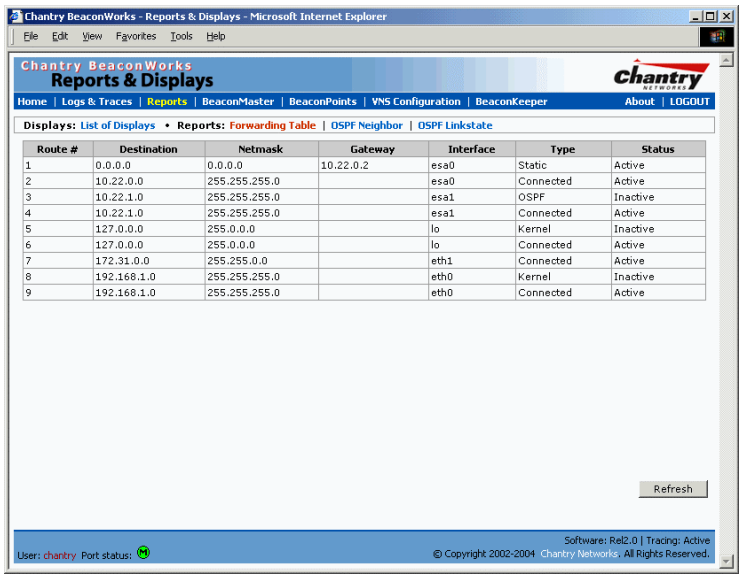
To view BeaconWorks reports and displays, click on the **Reports** tab in any screen. The *List of Displays* screen appears, with a menu of available displays.

To access a **Report**, click on one of the options in the navigation bar across the top of the screen. The following reports are currently available in BeaconWorks:

To access a **Report**, click on one of the options in the navigation bar across the top of the screen. The following reports are currently available in BeaconWorks:

- Forwarding Table (routes defined in the *BeaconMaster Routing Protocols* screen)
- OSPF Neighbor (available is OSPF is enabled in the *BeaconMaster Routing Protocols* screen)
- OSPF Linkstate (available is OSPF is enabled in the *BeaconMaster Routing Protocols* screen)

For example, to view the routing table report, click on **Forwarding Table** tab.



Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	10.22.0.2	esa0	Static	Active
2	10.22.0.0	255.255.255.0		esa0	Connected	Active
3	10.22.1.0	255.255.255.0		esa1	OSPF	Inactive
4	10.22.1.0	255.255.255.0		esa1	Connected	Active
5	127.0.0.0	255.0.0.0		lo	Kernel	Inactive
6	127.0.0.0	255.0.0.0		lo	Connected	Active
7	172.31.0.0	255.255.0.0		eth1	Connected	Active
8	192.168.1.0	255.255.255.0		eth0	Kernel	Inactive
9	192.168.1.0	255.255.255.0		eth0	Connected	Active

Screen 82: Forwarding Table Report

BeaconMaster Configuration: Setting up SNMP

SNMP: Background

The Chantry BeaconWorks system supports Simple Network Management Protocol (SNMP), Version 1 and 2c, for retrieving BeaconMaster statistics and configuration information.

Simple Network Management Protocol, a set of protocols for managing complex networks, sends messages, called protocol data units (PDUs), to different parts of a network. Devices on the network that are SNMP-compliant, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

The Chantry system accepts SNMP "Set", "Get" and "Trap" commands. In Release 2.0 support is provided for retrieving information from the router MIB-II (SNMP_GET) as well as SNMP traps. Release 2.0 supports the retrieval of wireless information (802.11 MIB).

In BeaconWorks Release 2.0, the MIB support includes:

1. MIB-II (RFC1213), for the following groups for the router characteristics of the BeaconMaster:
   - System Group
   - Interfaces Group
   - Address Translation Group
   - IP Group
   - ICMP Group
   - TCP Group
   - UDP Group

Note: Because of limitations in data captured in the control / data planes, MIB II compliance is incomplete. For example, esa/IXP ports can only provide the interface statistics.

2. The Chantry Enterprise MIB, which includes:
   - 802.11 MIB (IEEE 802.11 standard)
   - IANAif Type-MIB
   - IF-MIB
   - INET-ADDRESS-MIB
   - IP-FORWARD-MIB
   - SNMPv2-MIB
   - SNMPv2-SMI
   - SNMPv2-TC

   The Chantry MIB also includes:
   - CHANTRY-AC-MIB

Chantry Networks Inc. Copyright 2004. All rights reserved.

- CHANTRY-PRODUCTS-MIB
- CHANTRY-SMI
- CHANTRY-VNS-MIB

The MIB is provided for compilation into an external NMS.

No support has been provided for automatic device discovery by an external NMS.

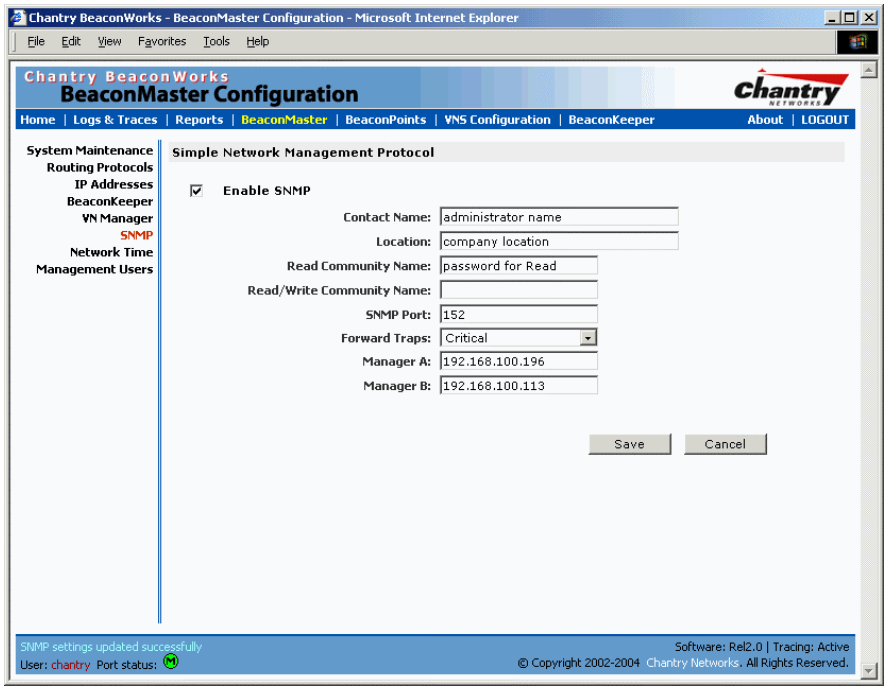
The BeaconMaster is the only point of SNMP access for the entire system. In effect, the BeaconMaster will proxy sets and gets and alarms from the associated BeaconPoints.

SNMP: Enabling on the BeaconMaster

The Chantry BeaconWorks system also supports the Simple Network Management Protocol (SNMP), version 1 and 2c, standard, for system monitoring and alarm reporting. If your enterprise network uses SNMP, you can enable SNMP on the BeaconMaster and define where the BeaconMaster should send the SNMP messages.

Setting SNMP Parameters

1. Click on the **BeaconMaster** tab in any screen. The *BeaconMaster Configuration* screen appears.
2. In the left-hand portion of the screen, click on the **SNMP** option. The *Simple Network Management Protocol* screen appears.



Screen 83: BeaconMaster Configuration – SNMP Setup

3. Key in:

Contact Name	The name of SNMP administrator.
Location	Location of the SNMP administration machine (descriptive).
Read Community Name	Key in the password for Read activity.
Read/Write Community Name	Key in the password for Read/Write activity.
SNMP Port:	Key in the destination port for SNMP traps. The industry standard is 162. [If left blank, no traps are generated.]
Forward Traps	From the drop-down list, select the severity level of the traps to be forwarded: Informational, Minor, Major, Critical.
Manager A:	The IP address of the specific machine on the network where the SNMP traps are monitored.
Manager B:	The IP address of a second specific machine on the network where the SNMP traps are monitored, if Manager A is not available.

To enable SNMP traps, ensure that the following three fields are defined:

- SNMP port
- Read Community
- Manager A and/or Manager B

The list of SNMP traps supported can be found in the Chantry MIB.

Chantry Networks Inc. Copyright 2004. All rights reserved.

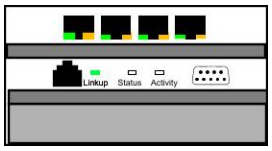
Appendix 1: BeaconWorks System States and LEDs

BeaconMaster System States and LEDs

The BeaconMaster has the two system states:

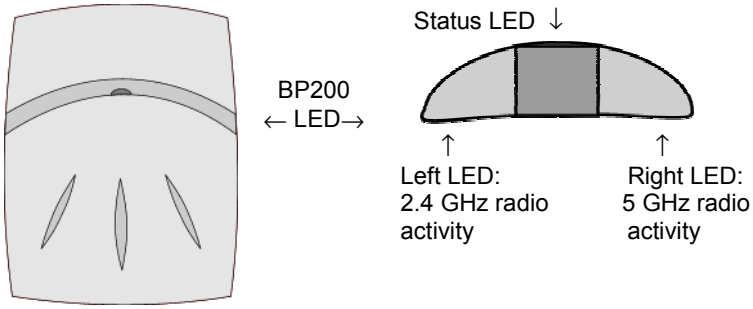
- Enters "**Standby**" when shut down in the *BeaconMaster Configuration – System Maintenance* screen. The BeaconMaster:
  - sends control message to BeaconPoint to enter "Standby" state
  - will not handle any wireless traffic or sessions
  - disables DHCP, Policy Manager, Security Manager, BeaconPoint Manager, Redirector.
  - remains on the wired network.
- Enters "**Active**" state on startup in the user interface. The BeaconMaster can now respond to the BeaconPoint's "discover" message by returning a message that the BeaconPoint can enter the "active" state.

The activity and traffic on the BeaconMaster can be monitored via three LEDs on the back of the BeaconMaster.



BeaconPoint BP200 System States

For the BP200 the Status LED in the centre also indicates power The Status LED is dark when unit is off and is green (solid) when the BP has completed discovery and is operational.



The chart below shows states and corresponding Status LED displays on the BP200:

State / Process	Description	LEDs
Power	BeaconPoint not powered.	off
Power	Start up: Power On Self Test (POST)	steady green (briefly)
Power	Power On Self Test (POST) successful	off (briefly)
Discovery	If he POST self test is successful, the BP begins "Discovery" process. BeaconPoint is powered on and searching for an active BeaconMaster. It sends a "discover" message and waits for a response.	orange (steady)
Fail to find DHCP	BeaconPoint failed to find DHCP (will stay in this state until a route appears)	red-orange (alternate blink)
Failed discovery	If there are SLP issues in failed discovery, the LED display changes.	green-orange (alternate blink)

Chantry Networks Inc. Copyright 2004. All rights reserved.

Registration	BeaconPoint learns the BeaconMaster's IP address, and can begin the Registration process	orange (blink)
Failed Registration	BeaconPoint fails to learn the BeaconMaster's IP address.	red (blink)
Standby	1. BeaconPoint enters this state from "Discovery" when it encounters an active BeaconMaster and completes the Registration process. 2. BeaconPoint enters this state from "Active" when it receives a control message from the BeaconMaster to enter this state. If the BeaconPoint has any wireless device traffic, it will drop the traffic.	green (blink)
	BeaconPoint fails to register. It will wait 5 seconds and try again.	red (slow blink)
	Firmware download from the BeaconMaster is in progress	orange + green (blink)
Active (Ready)	BeaconPoint has received a control message from an active BeaconMaster to enter "active" or "ready" state. It is ready to receive wireless traffic. **Note**: The two Traffic LEDs on either side of the Status LED display a green (blink) if there is active wireless traffic. The left LED is for the 2.4 GHz radio. The right LED is for the 5 GHz radio.	green (steady)

Appendix 2: Glossary of Terms and Acronyms

TERM	Explanation
AAA	Authentication, Authorization and Accounting. A system in IP-based networking to control what computer resources users have access to and to keep track of the activity of users over a network.
Access Point (AP)	A wireless LAN transceiver or “base station” that can connect a wired LAN to one or many wireless devices.
Ad-hoc mode	An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). (Compare Infrastructure Mode)
AES	Advanced Encryption Standard (AES) is an algorithm for encryption that works at multiple network layers simultaneously
ARP	Address Resolution Protocol. A protocol used to obtain the physical addresses (such as MAC addresses) of hardware units in a network environment. A host obtains such a physical address by broadcasting an ARP request, which contains the IP address of the target hardware unit. If the request finds a unit with that IP address, the unit replies with its physical hardware address.
Association	A connection between a wireless device and an Access Point.
asynchronous	Asynchronous transmission mode (ATM). A start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.
BSS	Basic Service Set. A wireless topology consisting of one Access Point connected to a wired network and a set of wireless devices. Also called an infrastructure network. *See also IBSS.*
Captive Portal	A browser-based authentication mechanism that forces unauthenticated users to a web page. Sometimes called a “reverse firewall”.
CHAP	Challenge-Handshake Authentication Protocol. One of the two main authentication protocols used to verify a user’s name and password for PPP Internet connections. CHAP is more secure than PAP because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.
CLI	Command Line Interface.
Collision	Two Ethernet packets attempting to use the medium simultaneously. Ethernet is a shared media, so there are rules for sending packets of data to avoid conflicts and protect data integrity. When two nodes at different locations attempt to send data at the same time, a collision will result. Segmenting the network with bridges or switches is one way of reducing collisions in an overcrowded network.
Datagram	A datagram is “a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.” (RFC1594). The term has been generally replaced by the term *packet*. Datagrams or packets are the message units that the Internet Protocol deals with and that the Internet transports.
Decapsulation	See *tunnelling*.
Device Server	A specialized, network-based hardware device designed to perform a single or specialized set of server functions. Print servers, terminal servers, remote access servers and network time servers are examples of device servers.
DHCP	Dynamic Host Configuration Protocol. A protocol for assigning dynamic IP addresses

TERM	Explanation
	to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. (Compliant with IETF RFC1531.)
Directory Agent (DA)	A component of Service Location Protocol (SLP) (RFC 2608) that stores and maintains a cache of service advertisements that are sent by the Service Agent (SA). When deployed, the DA resolves User Agent (UA) service requests.
Diversity antenna and receiver	Diversity wireless systems are those with two antennas and receivers. A diversity receiver can choose the strongest signal and therefore can avoid signal conflicts such as a partial phase cancellation (multipath) or a total phase cancellation (drop-out) from a transmitter with two microphones.
DSSS	Direct-Sequence Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare FHSS)
DTIM	DTIM delivery traffic indication message (in 802.11 standard)
EAP-TLS EAP-TTLS	EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. IEEE 802.1x specifies how EAP should be encapsulated in LAN frames. In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication. EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys. EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates. (*See also PEAP*)
ELA (OPSEC)	Event Logging API (Application Program Interface) for OPSEC, a module in Check Point used to enable third-party applications to log events into the Check Point VPN-1/FireWall-1 management system.
Encapsulation	See *tunnelling*.
ESS	Extended Service Set (ESS). Several Basic Service Sets (BSSs) can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS. (See BSS and SSID.)
FHSS	Frequency-Hopping Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that "hops" in a random but predictable sequence from

TERM	Explanation
	frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare DSSS)
FQDN	Fully Qualified Domain Name. A “friendly” designation of a computer, of the general form *computer.[subnetwork.].organization.domain*. The FQDN names must be translated into an IP address in order for the resource to be found on a network, usually performed by a Domain Name Server.
FTM	Forwarding Table Manager.
FTP	File Transfer Protocol.
Gateway	In the wireless world, an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.
Gigabit Ethernet	The high data rate of the Ethernet standard, supporting data rates of 1 gigabit (1,000 megabits) per second.
GUI	Graphical User Interface
Heartbeat message	A heartbeat message is a UDP data packet used to monitor a data connection, polling to see if the connection is still alive. In general terms, a heartbeat is a signal emitted at regular intervals by software to demonstrate that it is still alive. In networking, a heartbeat is the signal emitted by a Level 2 Ethernet transceiver at the end of every packet to show that the collision-detection circuit is still connected.
Host	(1) A computer (usually containing data) that is accessed by a user working on a remote terminal, connected by modems and telephone lines. (2) A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.
HTTP	Hypertext Transfer Protocol is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. A Web browser makes use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. (RFC2616: Hypertext Transfer Protocol -- HTTP/1.1)
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL, is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS uses Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.
IBSS	Independent Basic Service Set, see BSS. An IBSS is the 802.11 term for an adhoc network. See adhoc network.
ICMP	Internet Control Message Protocol, an extension to the Internet Protocol (IP) defined by RFC792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.
ICV	ICV (Integrity Check Value) is a 4-byte code appended in standard WEP to the 802.11 message. Enhanced WPA inserts an 8-byte MIC just before the ICV. (See WPA and MIC)
IE	Internet Explorer.
IEEE	Institute of Electrical and Electronics Engineers, a technical professional association, involved in standards activities.
IETF	Internet Engineering Task Force, the main standards organization for the Internet.

TERM	Explanation
Infrastructure Mode	An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. (See *ad-hoc mode* and BSS.)
Internet or IP telephony	IP or Internet telephony are communications, such as voice, facsimile, voice-messaging applications, that are transported over the Internet, rather than the public switched telephone network (PSTN). IP telephony is the two-way transmission of audio over a packet-switched IP network (TCP/IP network). An Internet telephone call has two steps: (1) converting the analog voice signal to digital format, (2) translating the signal into Internet protocol (IP) packets for transmission over the Internet. At the receiving end, the steps are reversed. Over the public Internet, voice quality varies considerably. Protocols that support quality of service (QoS) are being implemented to improve this.
IP	Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (host) on the Internet has at least one IP address that uniquely identifies it. Internet Protocol specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.
IPC	Interprocess Communication. A capability supported by some operating systems that allows one process to communicate with another process. The processes can be running on the same computer or on different computers connected through a network.
IPsec IPsec-ESP IPsec-AH	Internet Protocol security (IPSec), Internet Protocol security Encapsulating Security Payload (IPsec-ESP). The encapsulating security payload (ESP) encapsulates its data, enabling it to protect data that follows in the datagram. Internet Protocol security Authentication Header (IPsec-AH). AH protects the parts of the IP datagram that can be predicted by the sender as it will be received by the receiver. IPsec is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet. For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as *Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley)*, which allows the receiver to obtain a public key and authenticate the sender using digital certificates.
isochronous	Isochronous data is data (such as voice or video) that requires a constant transmission rate, where data must be delivered within certain time constraints. For example, multimedia streams require an isochronous transport mechanism to ensure that data is delivered as fast as it is displayed and to ensure that the audio is synchronized with the video. Compare: asynchronous processes in which data streams can be broken by random intervals, and synchronous processes, in which data streams can be delivered only at specific intervals.
ISP	Internet Service Provider.
IV	IV (Initialization Vector), part of the standard WEP encryption mechanism that concatenates a shared secret key with a randomly-generated 24-bit initialization vector. WPA with TKIP uses 48-bit IVs, an enhancement that significantly increases

TERM	Explanation
	the difficulty in cracking the encryption. (See WPA and TKIP)
LAN	Local Area Network.
LSA	Link State Advertisements received by the currently running OSPF process. The LSAs describe the local state of a router or network, including the state of the router's interfaces and adjacencies. *See also OSPF.*
MAC	Media Access Control layer. One of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel.
MAC address	Media Access Control address. A hardware address that uniquely identifies each node of a network.
MIB	Management Information Base is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP. A MIB is a collection of definitions defining the properties of a managed object within a device. Every managed device keeps a database of values for each of the definitions written in the MIB. Definition of the MIB conforms to RFC1155 (Structure of Management Information).
MIC	Message Integrity Check or Code (MIC), also called "Michael", is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte integrity check value (ICV) that is appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks. Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with. (See WPA, TKIP and ICV).
MTU	Maximum Transmission Unit. The largest packet size, measured in bytes, that a network interface is configured to accept. Any messages larger than the MTU are divided into smaller packets before being sent.
MU	Mobile Unit, a wireless device such as a PC laptop.
multicast, broadcast, unicast	Multicast: transmitting a single message to a select group of recipients. Broadcast: sending a message to everyone connected to a network. Unicast: communication over a network between a single sender and a single receiver.
NAS	Network Access Server, a server responsible for passing information to designated RADIUS Servers and then acting on the response returned. A NAS-Identifier is a RADIUS attribute identifying the NAS server. (RFC2138)
NAT	Network Address Translator. A network capability that enables a group of computers to dynamically share a single incoming IP address. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.
Netmask	In administering Internet sites, a netmask is a string of 0's and 1's that mask or screen out the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the "255.255.255.0" netmask allows the specific host computer address to be visible.
NIC	Network Interface Card. An expansion board in a computer that connects the computer to a network.
NMS	Network Management System. The system responsible for managing a network or a portion of a network. The NMS talks to network management agents, which reside in the managed nodes.
NTP	Network Time Protocol, an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Based on UTC, NTP synchronizes client workstation clocks to the U.S. Naval Observatory Master Clocks in Washington, DC and Colorado Springs

TERM	Explanation
	CO. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock. (RFC1305)
OFDM	Orthogonal frequency-division multiplexing, a method of digital modulation in which a signal is split into several narrowband channels at different frequencies. OFDM is similar to conventional frequency-division multiplexing (FDM). The difference lies in the way in which the signals are modulated and demodulated. Priority is given to minimizing the interference, or crosstalk, among the channels and symbols comprising the data stream. Less importance is placed on perfecting individual channels. OFDM is used in European digital audio broadcast services. It is also used in wireless local area networks.
OID	Object Identifier.
OPSEC	OPSEC (Open Platform for Security) is a security alliance program created by Check Point to enable an open industry-wide framework for interoperability of security products and applications. Products carrying the "Secured by Check Point" seal have been tested to guarantee integration and interoperability.
OS	Operating system.
OSI	Open System Interconnection. An ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, down through the presentation, session, transport, network, data link layer to the physical layer at the bottom, over the channel to the next station and back up the hierarchy.
OSI Layer 3	The Network layer (OSI Layer 3) provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.
OSPF	Open Shortest Path First, an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure (topography). Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information. The host using OSPF sends only the part that has changed, and only when a change has taken place. (RFC2328)
OUI	Organizationally Unique Identifier (used in MAC addressing).
Packet	The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into packets. Each packet is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).
PAP	Password Authentication Protocol is the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. (See *CHAP*).
PDU	Protocol Data Unit. A data object exchanged by protocol machines (such as management stations, SMUX peers, and SNMP agents) and consisting of both

TERM	Explanation
	protocol control information and user data. PDU is sometimes used as a synonym for ``packet''.
PEAP	PEAP (Protected Extensible Authentication Protocol) is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (*See also EAP-TLS*)
PHP server	Hypertext Preprocessor.
PKI	Public Key Infrastructure
PoE	Power over Ethernet. The Power over Ethernet standard (802.3af) defines how power can be provided to network devices over existing Ethernet connection, eliminating the need for additional external power supplies.
POST	Power On Self Test, a diagnostic testing sequence performed by a computer to determine if its hardware elements are present and powered on. If so, the computer begins its boot sequence.
push-to-talk (PTT)	The push-to-talk (PTT) is feature on wireless telephones that allows them to operate like a walkie-talkie in a group, instead of standard telephone operation. The PTT feature requires that the network be configured to allow multicast traffic. A PTT call is initiated by selecting a channel and pressing the “talk” key on the wireless telephone. All wireless telephones on the same network that are monitoring the channel will hear the transmission. On a PTT call you hold the button to talk and release it to listen.
QoS	Quality of Service. A term for a number of techniques that intelligently match the needs of specific applications to the network resources available, using such technologies as Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks. QoS features provide better network service by supporting dedicated bandwidth, improving loss characteristics, avoiding and managing network congestion, shaping network traffic, setting traffic priorities across the network. Quality-of-Service (QoS): A set of service requirements to be met by the network while transporting a flow. (RFC2386)
RADIUS	Remote Authentication Dial-In User Service. An authentication and accounting system that checks UserName and Password and authorizes access to a network. The RADIUS specification is maintained by a working group of the IETF (RFC2865, RFC2866.)
RFC	Request for Comments, a series of notes about the Internet, submitted to the IETF and designated by an RFCnumber, that may evolve into an Internet standard.
Roaming	In 802.11, roaming occurs when a wireless device (a station) moves from one Access Point to another (or BSS to another) in the same Extended Service Set (ESS) – identified by its SSID.
RP-SMA	Reverse Polarity-Subminiature version A, a type of connector used with wireless antennas
RSN	Robust Security Network. A new standard within IEEE 802.11 to provide security and privacy mechanisms. The RSN (and related TSN) both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).
RSSI	RSSI received signal strength indication (in 802.11 standard)
RTS / CTS	RTS request to send, CTS clear to send (in 802.11 standard)

TERM	Explanation
Segment	In ethernet networks, a section of a network that is bounded by bridges, routers or switches. Dividing a LAN segment into multiple smaller segments is one of the most common ways of increasing available bandwidth on the LAN.
SLP	Service Location Protocol. A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices. (From RFC2165)
SMI	Structure of Management Information. A hierarchical tree structure for information that underlies Management Information Bases (MIBs), and is used by the SNMP protocol. Defined in RFC1155 and RFC1442 (SNMPv2).
SMT (802.11)	Station ManagemenT. The object class in the 802.11 MIB that provides the necessary support at the station to manage the processes in the station such that the station may work cooperatively as a part of an IEEE 802.11 network. The four branches of the 802.11 MIB are: • dot11smt - objects related to station management and local configuration • dot11mac - objects that report/configure on the status of various MAC parameters • dot11res – Objects that describe available resources • dot11phy – Objects that report on various physical items.
SNMP	Simple Network Management Protocol. A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters. SNMP includes a limited set of management commands and responses. The management system issues Get, GetNext and Set messages to retrieve single or multiple object variables or to establish the value of a single variable. The managed agent sends a Response message to complete the Get, GetNext or Set.
SNMP trap	An event notification sent by the SNMP managed agent to the management system to identify the occurrence of conditions (such as a threshold that exceeds a predetermined value).
SSH	Secure Shell, sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer. SSH is a suite of three utilities - slogin, ssh, and scp - secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. With SSH commands, both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.
SSID	Service Set Identifier. A 32-character unique identifier attached to the header of packets sent over a Wireless LAN that acts as a password when a wireless device tries to connect to the Basic Service Set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS. In 802.11 networks, each Access Point advertises its presence several times per second by broadcasting beacon frames that carry the ESS name (SSID). Stations discover APs by listening for beacons, or by sending probe frames to search for an AP with a desired SSID. When the station locates an appropriately-named Access Point, it sends an *associate request frame* containing the desired SSID. The AP replies with an *associate response frame*, also containing the SSID. Some APs can be configured to send a zero-length broadcast SSID in beacon frames instead of sending their actual SSID. The AP must return its actual SSID in the probe response.

TERM	Explanation
SSL	Secure Sockets Layer. A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. URL's that require an SSL connection start with *https:* instead of *http*. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.
Subnet mask	(See "netmask")
Subnets	Portions of networks that share the same common address format. A subnet in a TCP/IP network uses the same first three sets of numbers (such as 198.63.45.xxx), leaving the fourth set to identify devices on the subnet. A subnet can be used to increase the bandwidth on the network by breaking the network up into *segments*.
SVP	SpectraLink Voice Protocol, a protocol developed by SpectraLink to be implemented on access points in order to facilitate voice prioritization over an 802.11 wireless LAN that will carry voice packets from SpectraLink wireless telephones.
Switch	In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.
syslog	A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them. Syslog uses the user datagram protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC3164)
TCP / IP	Transmission Control Protocol. TCP, together with IP (Internet Protocol), is the basic communication language or protocol of the Internet. Transmission Control Protocol manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. Internet Protocol handles the address part of each packet so that it gets to the right destination. TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network.
TFTP	Trivial File Transfer Protocol. An Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP). TFTP is described formally in Request for Comments (RFC) 1350.
Thin AP (Lightweight AP)	A thin AP architecture uses two components: an access point that is essentially a stripped-down radio and a centralized management controller that handles the other WLAN system functions. Wired network switches are also required. A fat (or thick) AP architecture concentrates all the WLAN intelligence in the access

TERM	Explanation
	point. The AP handles the radio frequency (RF) communication, as well as authenticating users, encrypting communications, secure roaming, WLAN management, and in some cases, network routing.
TKIP	Temporal Key Integrity Protocol (TKIP) is an enhancement to the WEP encryption technique that uses a set of algorithms that rotates the session keys. TKIP's enhanced encryption includes a per-packet key mixing function, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. The encryption keys are changed (rekeyed) automatically and authenticated between devices after the rekey interval (either a specified period of time, or after a specified number of packets has been transmitted).
TLS	Transport Layer Security. (See *EAP*, Extensible Authentication Protocol)
ToS	Type of Service. An attribute used in Quality of Service (QoS).
TSN	Transition Security Network. A subset of Robust Security Network (RSN), which provides an enhanced security solution for legacy hardware. The Wi-Fi Alliance has adopted a solution called Wireless Protected Access (WPA), based on TSN. RSN and TSN both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).
Tunnelling	Tunnelling (or *encapsulation*) is a technology that enables one network to send its data via another network's connections. Tunnelling works by encapsulating packets of a network protocol within packets carried by the second network. The receiving device then *decapsulates* the packets and forwards them in their original format.
UDP	User Datagram Protocol. A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive packets over an IP network. It is used primarily for broadcasting messages over a network.
U-NII	Unlicensed National Information Infrastructure. Designated to provide short-range, high-speed wireless networking communication at low cost, U-NII consists of three frequency bands of 100 MHz each in the 5 GHz band: 5.15-5.25GHz (for indoor use only), 5.25-5.35 GHz and 5.725-5.825GHz. The three frequency bands were set aside by the FCC in 1997 initially to help schools connect to the Internet without the need for hard wiring. U-NII devices do not require licensing.
VLAN	Virtual Local Area Network. A network of computers that behave as if they are connected to the same wire when they may be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. When a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration. The standard is defined in IEEE 802.1Q - Virtual LANs, which states that "IEEE 802 Local Area Networks (LANs) of all types may be connected together with Media Access Control (MAC) Bridges, as specified in ISO/IEC 15802-3. This standard defines the operation of Virtual LAN (VLAN) Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure."
VNS	Virtual Network Services (VNS). A Chantry-specific technique that provides a means of mapping wireless networks to a wired topology.
VoIP	Voice Over Internet Protocol. An internet telephony technique. With VoIP, a voice transmission is cut into multiple packets, takes the most efficient path along the Internet and is reassembled when it reaches the destination.
VPN	Virtual Private Network. A private network that is constructed by using public wires to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
Walled Garden	A restricted subset of network content that wireless devices can access.

TERM	Explanation
WEP	Wired Equivalent Privacy. A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.
Wi-Fi	Wireless fidelity. A term referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. Used in reference to the Wi-Fi Alliance, a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification.
WINS	Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer, called *name resolution*. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. WINS supports dynamic addressing (DHCP) by maintaining a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one. DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.
WLAN	Wireless Local Area Network.
WPA	Wireless Protected Access, or Wi-Fi Protected Access is a security solution adopted by the Wi-Fi Alliance that adds authentication to WEP's basic encryption. For authentication, WPA specifies IEEE 802.1x authentication with Extensible Authentication Protocol (EAP). For encryption, WPA uses the Temporal Key Integrity Protocol (TKIP) mechanism, which shares a starting key between devices, and then changes their encryption key for every packet. Certificate Authentication (CA) can also be used. Also part of the encryption mechanism are 802.1X for dynamic key distribution and Message Integrity Check (MIC) a.k.a. "Michael" WPA requires that all computers and devices have WPA software.
WPA-PSK	Wi-Fi Protected Access with Pre-Shared Key, a special mode of WPA for users without an enterprise authentication server. Instead, for authentication, a Pre-Shared Key is used. The PSK is a shared secret (passphrase) that must be entered in both the wireless access point or router and the WPA clients. This preshared key should be a random sequence of characters at least 20 characters long or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. After the initial shared secret, the Temporal Key Integrity Protocol (TKIP) handles the encryption and automatic rekeying.

Appendix 3: Index of Procedures, Screens and Figures

List of Procedures:

Installing the BeaconMaster 16
Changing the Management Port IP address web browser, ethernet port method 17
Add the BeaconMaster to your enterprise network 19
To run the Graphical User interface 20
Configuring the data ports on the BeaconMaster 23
Setting up a Static Route on the BeaconMaster 26
Viewing the Routing Table on the BeaconMaster 27
Setting up OSPF Routing on the BeaconMaster 28
Define the Security Mode for registering BeaconPoints 33
View and modify properties of registered BeaconPoints 36
View and modify the radio settings of registered BeaconPoints 38
Add and register a BeaconPoint manually 40
Set up a BeaconPoint with static configuration 42
Create a subnet (VNS) 48
Configure the new VNS (overview of basic steps) 49
Create an SSID for Captive Portal VNS 50
Identify the BeaconPoint radios that will be assigned to this VNS 51
Enable Management Traffic on this VNS 51
Enable Third Party Access Points on this VNS 51
Enable QoS Policy for voice-over-internet traffic on this VNS 51
Set the IP address for the VNS (for the DHCP server on the BeaconMaster) 51
Set time limits for IP assignments 52
Set the name server configuration 52
Use DHCP Relay for the VNS 52
Save the new VNS 53
Set up authentication by Captive Portal 53
Define how the BeaconMaster will access the RADIUS server 54
Define the RADIUS server priority for RADIUS Redundancy 55
Define the Filter ID Values on this VNS. 56
Configure the appearance of the Captive Portal page 56
Define filtering rules for a Non-Authenticated Filter 57
Set up a Static WEP key for a selected VNS 59
Set up a VNS with no authentication 61
Set up a VNS for voice traffic 63
Configure the BeaconPoint radio for a voice traffic VNS 64
Create an AAA topology 66
Identify the BeaconPoint radios that will be assigned to this VNS 66
Enable Management Traffic on this VNS 66
Set the IP address for the VNS (for the DHCP server on the BeaconMaster) 67
Set time limits for IP assignments 67
Set the name server configuration 67
Use DHCP Relay for the VNS 68
Save the new VNS for AAA 68
Set up authentication by AAA (802.1x) method 68
Define how the BeaconMaster will access the RADIUS Server. 69
Define the RADIUS server priority for RADIUS Redundancy 70
Define the Filter ID Values on this VNS. 70
Set up an AAA Group 71
Configure the VNS Topology for an AAA Group 71
Define filtering rules for a Filter ID group 72
Define the filtering rules for a Default Filter 74
Set up static WEP privacy for a selected AAA VNS 76
Set up dynamic WEP privacy for a selected AAA VNS 77
Set up Wi-Fi Protected Access privacy (WPA) for an AAA VNS 78

Specify a re-key interval for WPA Privacy 78
Enable WPA in PSK mode if there is no authentication server 79
Save the privacy parameters for this VNS 79
Prepare for setting up the Availability feature 80
Set up two BeaconMasters as a pair, for availability 81
Modifying BP Failover selections for availability 82
View the BeaconPoint Availability Report 82
View the SLP activity with the “slpdump tool” 83
Events and actions during a Failover 84
Set up a BeaconMaster as a VN Manager 86
View displays when VN Managers is enabled 86
Designate BeaconMaster management users 88
Set Network Time parameters 89
Set up third-party access points on the BeaconMaster 90
Enable and configure the BeaconKeeper Mitigator Analysis Engine 94
Define the BeaconKeeper Mitigator RF Data Collector Engines 94
Set up and run the BeaconKeeper Mitigator scan task mechanism: 95
View the BeaconKeeper scan results and build list of Friendly APs 97
View the BeaconKeeper list of Third-Party APs 99
Maintain the BeaconKeeper list of access points and BeaconPoints 99
View the BeaconKeeper scanner engine status display 100
Maintain the list of current BeaconPoint software images 101
Define the parameters for a BeaconPoint software upgrade 102
Modify a BeaconPoint’s registration status (approve access) 104
Disassociate a Wireless Device Client 105
Performing BeaconMaster maintenance functions 106
Change the System Log Level 106
Enable Data Collection for Accounting 106
Perform a System Shutdown 106
View the Logs 110
View the Traces 111
View the Audits 111
Setting SNMP Parameters 116

List of Screens:

Screen 1: Chantry BeaconWorks User Interface Login 17
Screen 2: Chantry BeaconWorks User Interface Main Menu 17
Screen 3: BeaconMaster Configuration – IP Addresses – Management Port 18
Screen 4: Modify Management Port Settings (System Port Configuration) 18
Screen 5: Chantry BeaconWorks User Interface Login 20
Screen 6: Change Password popup 20
Screen 7: Chantry BeaconWorks Main Menu 21
Screen 8: BeaconMaster Configuration – IP Addresses / Interfaces 23
Screen 9: BeaconMaster Configuration – Static Routes 26
Screen 10: Report – Forwarding Table 27
Screen 11: BeaconMaster Configuration – Routing, OSPF tab 28
Screen 12: Reports – OSPF Neighbor and Linkstate 29
Screen 13: BeaconPoint Configuration – BP Registration Mode 33
Screen 14: BeaconPoint Configuration: Message R1.1 version of BP software 36
Screen 15: BeaconPoint Configuration – Properties 37
Screen 16: BeaconPoint Configuration – Properties (after modifications) 38
Screen 17: BeaconPoint Configuration – Radio 802.11a (5 GHz) 38
Screen 18: BeaconPoint Configuration – Radio 802.11b/g (2.4 GHz) 39
Screen 19: BeaconPoint Configuration – Add BeaconPoint 41
Screen 20: BeaconPoint Configuration: Static Configuration 42
Screen 21: Virtual Network Configuration: Before any VNS definitions 48

Chantry Networks Inc. Copyright 2004. All rights reserved.

Screen 22: Virtual Network Configuration: Topology for a new VNS Subnet 49
Screen 23: Virtual Network Configuration – Topology – SSID Assignment 50
Screen 24: Virtual Network Configuration – Exclusions subscreen 52
Screen 25: Virtual Network Configuration – Topology – DHCP Relay 53
Screen 26: Virtual Network Configuration – Authentication – Captive Portal 54
Screen 27: Virtual Network Configuration – Authentication CP – Add RADIUS Server... 54
Screen 28: Captive Portal login configuration..... 56
Screen 29: Virtual Network Configuration – Non-Authenticated Filter for Captive Portal 58
Screen 30: Virtual Network Configuration – Privacy – Captive Portal VNS 60
Screen 31: Virtual Network Configuration – Authentication – None 61
Screen 32: Virtual Network Configuration: Topology – QoS for Voice Traffic 63
Screen 33: BeaconPoint Configuration for QoS VNS (need screen with correct settings) 64
Screen 34: Virtual Network Configuration – Topology – AAA Assignment 66
Screen 35: Virtual Network Configuration – Exclusions subscreen 67
Screen 36: Virtual Network Configuration – Authentication – AAA 69
Screen 37: Virtual Network Configuration – Authentication AAA – RADIUS Server Configuration 69
Screen 38: Virtual Network Configuration – Topology – AAA Group 71
Screen 39: Virtual Network Configuration –Filter ID Value filtering rules 73
Screen 40: Virtual Network Configuration – Default Filter 74
Screen 41: Virtual Network Configuration – Filtering – AAA Group 75
Screen 42: Virtual Network Configuration – Privacy – AAA VNS: Static Keys 76
Screen 43: Virtual Network Configuration – Privacy – AAA VNS: WPA..... 78
Screen 44: BeaconPoint Configuration – Paired BeaconMasters for Availability..... 81
Screen 45: BeaconPoint Configuration – BP Failover for Paired BM..... 82
Screen 46: Report – BeaconPoint Availability 83
Screen 47: BeaconPoint configuration – View SLP Registration 83
Screen 48: BeaconMaster Configuration – VN Manager 86
Screen 49: Reports and Displays for a VN Manager: Menu..... 87
Screen 50: Reports and Displays for a VN Manager: Examples..... 87
Screen 51: Reports and Displays for a VN Manager: BM Tunnel Traffic 87
Screen 52: BeaconMaster Configuration – Management Users 88
Screen 53: BeaconMaster Configuration – Network Time 89
Screen 54: BeaconMaster Configuration – IP Addresses / Interfaces 90
Screen 55: Virtual Network Configuration – Topology for Third-Party APs..... 91
Screen 56: BeaconKeeper Mitigator – Rogue Summary Report..... 93
Screen 57: BeaconMaster Configuration – BeaconKeeper Mitigator Configuration 94
Screen 58: BeaconMaster Configuration – BeaconKeeper Mitigator: Collection Engines95
Screen 59: BeaconKeeper Mitigator Scanner – Scan Groups 95
Screen 60: BeaconKeeper Mitigator Scanner – Rogue Detection 98
Screen 61: BeaconKeeper Mitigator Scanner – Friendly APs..... 98
Screen 62: BeaconKeeper Mitigator Scanner – 3rd Party APs 99
Screen 63: BeaconKeeper Mitigator Scanner – AP / BP Maintenance..... 99
Screen 64: BeaconKeeper Mitigator – Scanner Status Report 100
Screen 65: BeaconPoint Configuration – BP Maintenance: Software Maintenance..... 102
Screen 66: BeaconPoint Configuration – BP Maintenance: Controlled Upgrade..... 103
Screen 67: BeaconPoint Configuration – Access Approval..... 104
Screen 68: BeaconPoint Configuration – Wireless Unit (Client) Disassociate 105
Screen 69: BeaconMaster Configuration – System Maintenance 106
Screen 70: BeaconMaster Configuration – System Maintenance: Syslog enabled 107
Screen 71: Logs & Traces: Log Display – All 109
Screen 72: Logs & Traces: Log Display – Info 110
Screen 73: Logs & Traces: Trace Messages 111
Screen 74: Logs & Traces: GUI Audit..... 111
Screen 75: Reports and Displays – List of Displays 112
Screen 76: Displays – Active BeaconPoints..... 112
Screen 77: Displays – Active Clients by VNS..... 112

Screen 78: Displays – BeaconPoint Availability 112
Screen 79: Display – Wired Ethernet Statistics by BeaconPoints 113
Screen 80: Display – Wireless Statistics by BeaconPoints 113
Screen 81: Display – Wireless Statistics by BeaconPoints: Clients 114
Screen 82: Forwarding Table Report 114
Screen 83: BeaconMaster Configuration – SNMP Setup 116

List of Figures:

Figure 1: Standard wireless network solution 5
Figure 2: Chantry BeaconWorks Solution 6
Figure 3: BeaconWorks Traffic Flow diagram 8
Figure 4: The Chantry BeaconMaster 15
Figure 5: The Chantry BeaconMaster – back view diagram 16
Figure 6: The Chantry BeaconPoint 30

Chantry Networks Inc. Copyright 2004. All rights reserved.