Professional Digital Two-Way Radio System

MOTOTRBO™

IP Site Connect

System Integration Guide

MOTOROLA

1. Overview

In IP Site Connect mode, repeaters across dispersed locations exchange voice, data, and control packets over an IPv4-based back-end network. The potential applications for this mode include:

- **Connecting two or more dispersed locations for day-to-day communications.**
  For example, a customer's manufacturing facility and a distribution facility across towns can be connected using MOTOTRBO repeaters in IP Site Connect mode.
- **Building a larger or more effective RF coverage area.**
  For example, multiple repeaters installed in an amusement park or a high-rise building can be connected to provide a contiguous area of RF coverage. The need for multiple repeaters may stem from any combination of geography (distance or topographical interference problems) and in-building or cross-building RF penetration issues.
- **Broadcasting announcements to all sites.**
  This is useful in case of emergency or special events.
- **Connecting repeaters operating in different RF bands.**
  For example, repeaters operating in UHF (UHF-1 and UHF-2) or VHF frequencies can be combined so that voice or data from one system flows into another.

2. References

(1) MOTOTRBO System Planner (68007024085)

3. IP Site Connect Protocol

A repeater has three network interfaces: Ethernet, USB, and Over-The-Air. Repeaters use their Ethernet ports to communicate among themselves using IPv4/UDP. Since UDP does not support confirmation, an IP Site Connect system provides its own acknowledgement and retries mechanism for critical activities. Note that the Ethernet port is not a default IP gateway for a repeater, i.e. an IP datagram arrived from USB or Over-The-Air is not automatically routed to the Ethernet port.

It is not necessary to get a static IPv4 addresses for IP Site Connect devices (except for the Master). The IPv4 address of an IP Site Connect device can be dynamic. In this case, the IPv4 address is allocated by a DHCP server. The dynamic nature of the IPv4 address implies that the address may change every time it powers-on or even periodically (every few hours) while the IP Site Connect device is on. The dynamic address of a repeater is selected by selecting the DHCP option in the repeater CPS. It is recommended that the lease time of the IPv4 address from the DHCP should be kept as long as possible. Note that a change in the IPv4 address of an IP Site Connect device causes short disruption of service for the device. For a static IPv4 address, the DHCP option should not be selected and the CPS user should provide the static IPv4 address, and the gateway's IPv4 address and Netmask.

An IP Site Connect configuration uses a procedure called "Link Management" to keep an IP Site Connect device aware of the presence, the current IPv4 addresses, and UDP ports of other IP Site Connect devices. The Link Management requires only one of the repeaters (called a Master) to act as a broker of IPv4/UDP addresses. The Master gets a static IPv4 address from its ISP and the Master's IPv4/UDP address is configured into all the IP Site Connect devices.

The Master's IPv4/UDP address refers to its address as seen from the IP Network. Note that a firewall/NAT may translate the address in customer network into another address in the IP Network.

An IP Site Connect device registers its IPv4/UDP address during power-on and upon a change in its IPv4/UDP address with the Master. The Master notifies to all the IP Site Connect devices whenever the IPv4 address of an IP Site Connect device changes. An IP Site Connect device maintains a table of the latest IPv4 addresses of other IP Site Connect devices and it uses the table to send an IPv4/UDP message to another IP Site Connect device.

The IP Site Connect devices may be behind firewalls. For successful communication between two IP Site Connect devices (say R1 and R2), the firewall of R1 must be open for messages from R2 and vice versa. Since the IPv4/UDP address of an IP Site Connect device is dynamic, it is not possible to manually configure the firewalls. The Link Management procedure overcomes this problem by periodically, for example, setting the *Keep FW Open Time* to every 6 seconds, sending a dummy message from R1 to R2 and vice versa. On a receipt of an outbound message (say, from R1 to R2), the R1's firewall keeps itself open for a short duration of approximately 20 seconds for an inbound message from R2. An IP Site Connect device (say, R1) sends the dummy message to another IP Site Connect device (say, R2) only if R1 has not sent any message to R2 in last *Keep FW Open Time*. The value of *Keep FW Open Time* is customer-programmable and should be kept less than the duration for which the firewall remains open for inbound messages. Exchange of dummy messages between two IP Site Connect devices also acts as a "Keep Alive" messages. They are required, even if there is no firewall or the firewall is configured to keep itself open for any message destined to the IP Site Connect device.

An IP Site Connect system automatically discovers the presence of a new IP Site Connect device. The new IP Site Connect device is configured with the IPv4/UDP address of the Master. On power-on, the new IP Site Connect device informs its IPv4/UDP address to the Master and

the Master informs all the other IP Site Connect devices about the presence of a new IP Site Connect device. This allows adding an IP Site Connect device to a live IP Site Connect system. This simplifies the installation/addition of an IP Site Connect device as there is no need to take the system down and configure other IP Site Connect devices with the IPv4/UDP address of the new IP Site Connect device.

The periodic link management messages between an IP Site Connect device and the Master also act as “keep alive” messages. In absence of messages from an IP Site Connect device for one minute, the Master concludes that either the IP Site Connect device has failed or the failure is in the network in-between and the Master informs all the other IP Site Connect devices about the absence of the IP Site Connect device. An IP Site Connect device also maintains periodic link management messages with every other IP Site Connect device. In absence of messages from another IP Site Connect device for one minute, the IP Site Connect device concludes that either the other IP Site Connect device has failed or the failure is within the network in between. Thus, the link management messages allow an IP Site Connect system to reconfigure itself on failure of one or more IP Site Connect devices and the system continues to provide services with the available IP Site Connect devices. In case of network failure, it is possible that an IP Site Connect system becomes multiple IP Site Connect systems, where each system has a subset of original set of IP Site Connect devices. All the new systems continue to provide the services that are possible with their subset of IP Site Connect devices. Note that there will be only one system that has the Master. When the IP network recovers, the multiple systems automatically become one system. When an IP Site Connect system has only one repeater, then both the slots of the repeater repeat only locally (i.e. over-the-air) as per the MOTOTRBO Single Site specifications. A repeater operates in multiple modes such as disabled, locked, knocked down, enabled and analogue, enabled and digital with voice/data or control services, and single or multiple site operation for each slot. Note: all repeater channels which together constitute a given wide area channel must have the same slot number (in other words it is not possible to have both slot 1 and slot 2 channels on the same wide area channel). The repeater informs the Master whenever its mode of operation changes and the Master informs to all the other IP Site Connect devices. This allows the IP Site Connect system to adapt its operation when the mode changes. Note that only an enabled and digital repeaters (with a channel enabled for multiple site operation) participate in voice/data/control communication across multiple sites.

A disadvantage of link Management is that the Master becomes a single point of failure. But the consequence of failure of the Master is limited. The IP Site Connect system continues to function except that it is not possible to add an IP Site Connect device into the system. If an IP Site Connect device powers on, while the Master is in failed state, then it will not be able to join the IP Site Connect system. On failure of the Master, it is possible to switch a redundant IP Site Connect device to act as an Master. The static IPv4 address and the UDP port number of the redundant IP Site Connect device should be same as that of the failed Master; otherwise all the IP Site Connect devices will require to be reconfigured with the IPv4 address and the UDP port number of the new Master.

4. IP Network Requirements

1) The IP Network can be a dedicated network or an internet provided by an Internet Service Provider (ISP).
2) ISPs provide a range of technologies such as dial-up, DSL (typically ADSL), Cable modem, Broadband wireless access, Canopy, ISDN, Frame Relay, Satellite Internet access, etc. The IP Network cannot be based on dial-up connection (due to small bandwidth) or Satellite Internet access (due to large delay).
3) Sufficient bandwidth must be made available by the IP Network and the packet loss / latency must be within the limits documented in reference (1).
4) A static IP Address and UDP Port for Master repeater must be made available by the IP Network to all Peer devices on the IP Site Connect system.
5) When a Peer device registers with the Master repeater, the IP Network supplies the return IP Address and UDP Port of that Peer device to the Master repeater. This IP Address and UDP Port must then be made available by the IP Network to all other IP Site connect devices on the IP Site Connect System.
6) The IP Network must not use a Proxy server which directs all IP devices to a home (or logon) page before they are able to gain access to the WAN.

5. MOTOTRBO IP Addresses

The Radio and Accessory IP addresses (highlighted in blue in **Figure 5.1** below) are used when the repeater communicates with accessories and PC applications (such as the CPS) via the USB port, while the IP Site Connect IP Addresses (highlighted in red in **Figure 5.1** below) are used when the repeater communicates with other IP Site Connect devices via the Ethernet port.

When configuring an IP Site Connect system, it's important that these 2 types of IP address do not conflict, otherwise both the repeater's USB and Ethernet capabilities may be rendered inoperable. To avoid conflict, the Radio IP address should be left unmodified and the IP Site Connect IP Addresses should be placed on a completely different subnet.

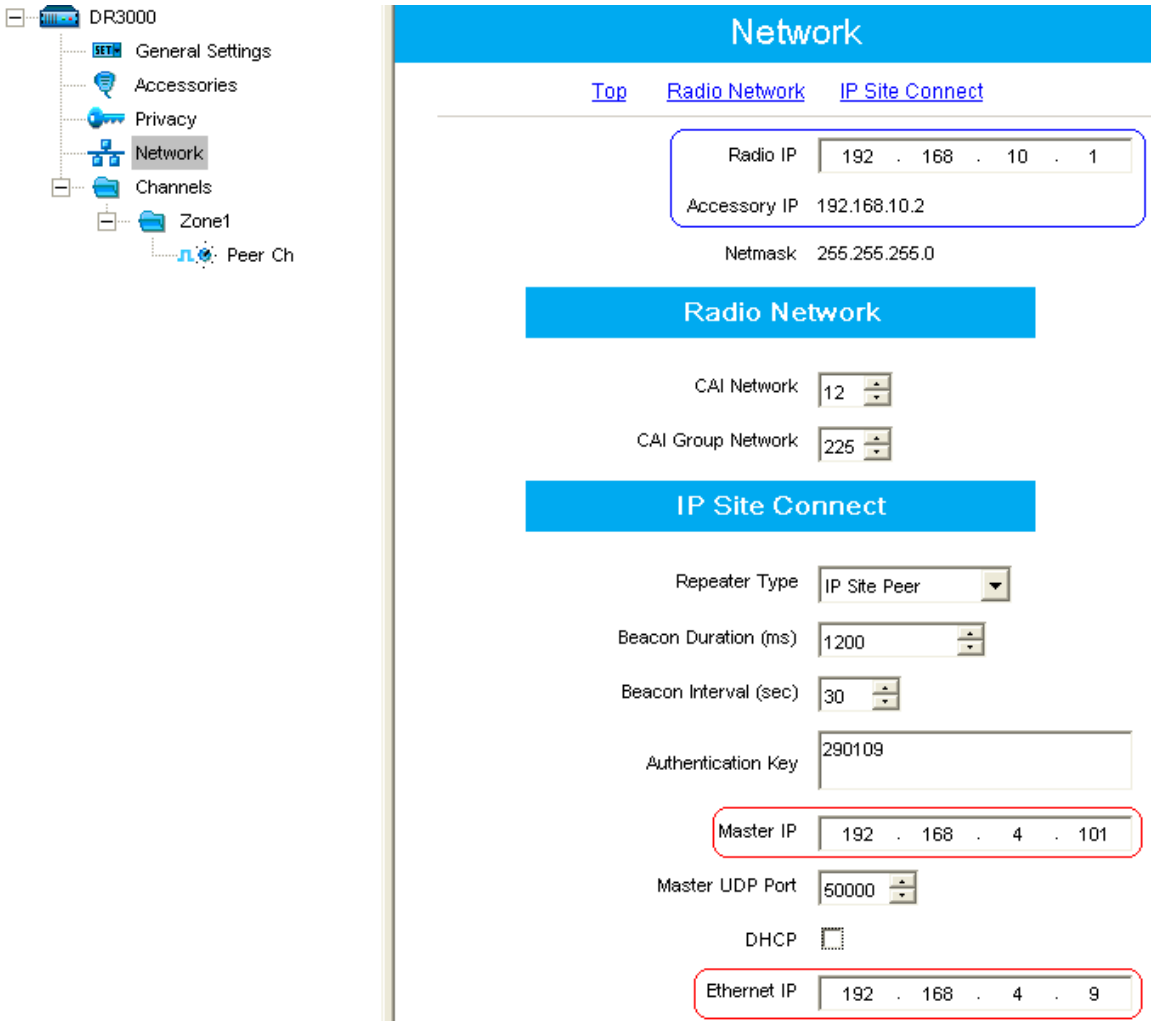


Figure 5.1

6. ‘Back to Back’ Repeaters

The simplest IP Site Connect system configuration may be achieved by connecting 2 repeaters ‘back to back’ (see **Figure 6.1** below). Since both repeaters are connected directly to each other, then a crossover Ethernet cable is required for this configuration.

This system configuration is useful for demonstrating the basic principles of IP Site Connect and is also useful where radios need to communicate across two bands (e.g. VHF and UHF).

Figure 6.1

Note: The procedures described in this section assume the repeaters and radios have already been successfully configured for single site operation.

The procedure for configuring the Master repeater for IP Site Connect is as follows:

1) Read the Master repeater using the CPS, navigate to the General Settings screen and enter a Radio ID. Each repeater in the system must contain a unique Radio ID, however since repeaters use Radio IDs differently to radios, then repeaters do NOT need to avoid using the same values already assigned to radios. For the example in **Figure 6.2** below, the Master repeater uses a Radio ID of 1.

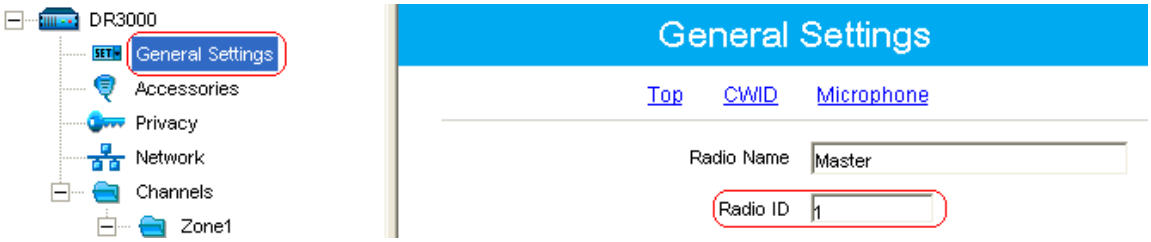


Figure 6.2

2) Navigate to the Network screen and set the Repeater Type to ‘IP Site Master’ (see **Figure 6.3** below).

3) For this simple system configuration radios are not required to automatically roam across the sites, so disable the beacon signal feature (see **Figure 6.3** below).

4) It is not physically possible for rouge repeaters to attach themselves to this simple system configuration, so disable the repeater authentication feature by leaving the Authentication Key field blank (see **Figure 6.3** below).

5) Since this is the Master repeater and there is no DHCP server, deselect the DHCP option and enter Static values for the Ethernet IP, Gateway IP and the Gateway Netmask. For this simple connection it does not matter what subnet the repeater is programmed for, however the subnet parameters must be consistent for both repeaters. For the example in **Figure 6.3** below, the Master repeater is programmed to operate on the subnet 192.168.4.X and the subnet parameters are programmed as follows:

- Ethernet IP (192.168.4.101): This defines the Master repeater's static address which must be unique within the system.
- Gateway IP (192.168.4.254): This defines an arbitrary gateway address. There is obviously no gateway for this system configuration, however an arbitrary address within the subnet still needs to be defined. The address itself must be unique within the system and it's strongly recommended that the last digit NOT be set to '0' (note: the lowest address for most subnets is usually reserved and unexpected behaviour may result if this address is used as the Gateway).
- Gateway Netmask (255.255.255.0): This mask defines the range of IP addresses within the subnet which in this example is 192.168.4.X (where x = 0 to 255).

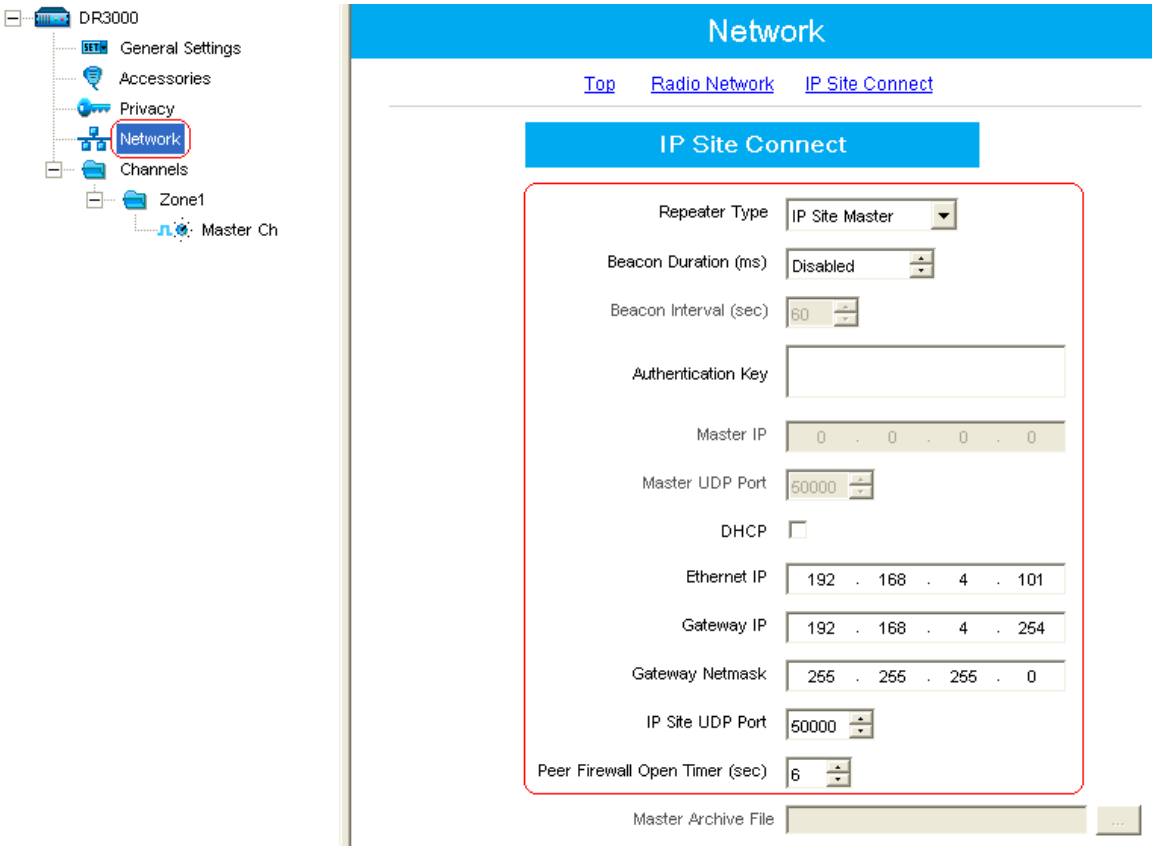


Figure 6.3

6) Leave the IP Site UDP Port and Peer Firewall Open timer at their default values of 50000 and 6 respectively (see Figure 6.3 above).

7) Navigate to each of the repeater channels where one or both of the slots are required to be 'Wide Area' and specify the IP Site Connect option. For the example shown in Figure 6.4 below, a single repeater channel is defined and both its slots are 'Wide Area'.

8) Leave the Messaging Delay at its default value of 'Normal' (see Figure 6.4 below).

9) If the Master repeater has a dedicated RF channel on which to operate (i.e. it is not sharing the channel with another system), then it's strongly recommended that the RSSI Threshold be increased from its default value of -115dBm to -90dBm (see Figure 6.4 below). For further details, refer to section 12.

10) Re-program the Master repeater using the CPS.

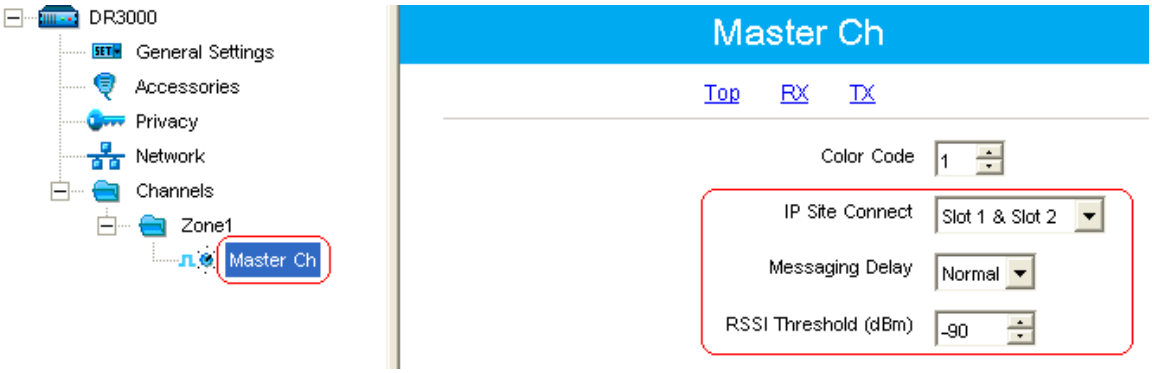


Figure 6.4

The procedure for configuring the Peer repeater for IP Site Connect is as follows:

1) Read the Peer repeater using the CPS, navigate to the General Settings screen and enter a Radio ID. Ensure that the Radio ID for the Peer repeater is NOT the same as the radio ID for the Master repeater. For the example in **Figure 6.5** below, the Peer repeater uses a Radio ID of 2.

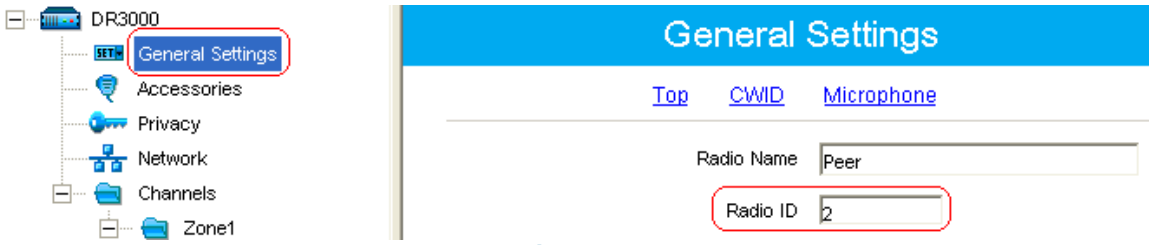


Figure 6.5

2) Navigate to the Network screen and set the Repeater Type to 'IP Site Peer' (see **Figure 6.6** below).

3) Disable the beacon signal and authentication features as per the Master repeater (see **Figure 6.6** below).

4) Set the Master IP and Master UDP Port to the same Ethernet IP address and IP Site UDP Port that were set for the Master repeater (see **Figure 6.6** below).

5) Deselect the DHCP option as per the Master repeater (see **Figure 6.6** below).

6) The Peer repeater must be configured to operate on the same subnet as the Master repeater, so deselect the DHCP option and enter appropriate Static values for the Ethernet IP, Gateway IP and the Gateway Netmask. For the example in **Figure 6.6** below, the Peer repeater is programmed to operate on the subnet 192.168.4.X (as per the Master repeater) and the subnet parameters are programmed as follows:
   - Ethernet IP (192.168.4.9): This defines the Peer repeater's static address which must be unique within the system.
   - Gateway IP (192.168.4.254): Configured as per the Master repeater.
   - Gateway Netmask (255.255.255.0): Configured as per the Master repeater.

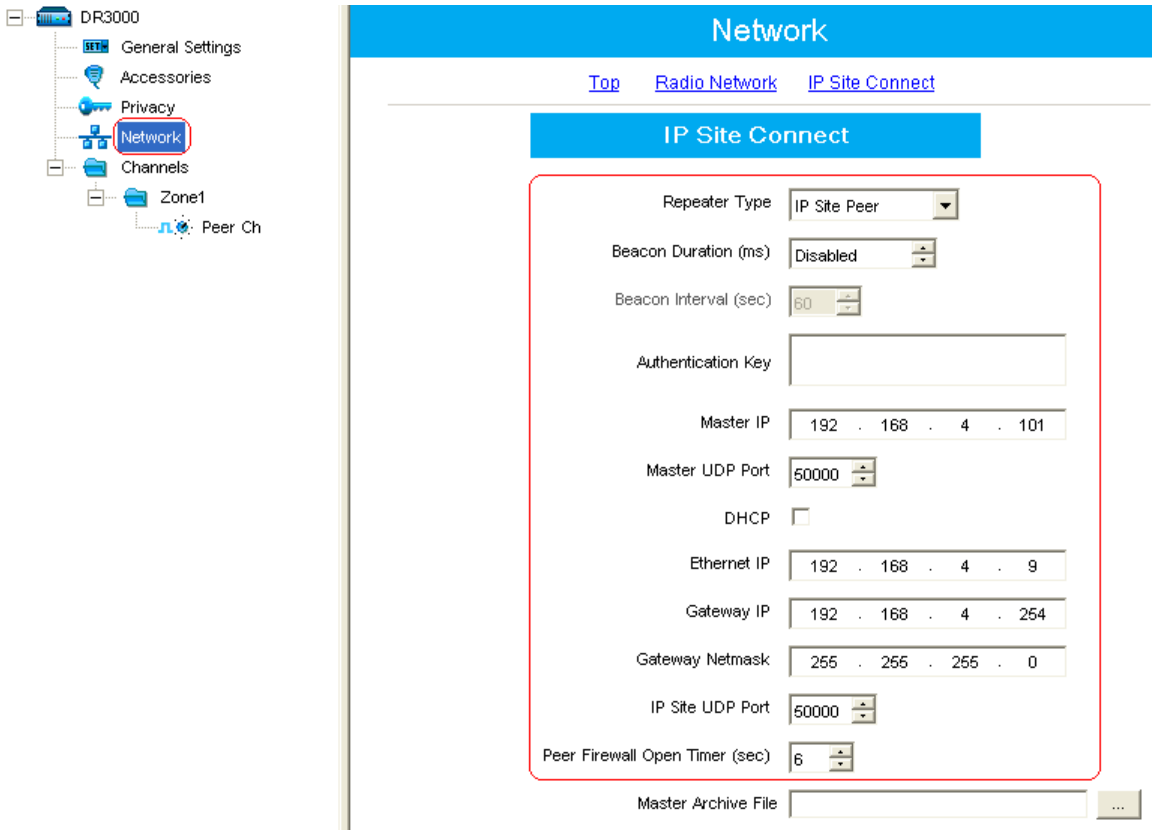


Figure 6.6

7) Leave the IP Site UDP Port and Peer Firewall Open timer at their default values of 50000 and 6 respectively (see **Figure 6.6** above).

8) Navigate to each of the repeater channels where one or both of the slots are required to be 'Wide Area' and specify the IP Site Connect option. For the example shown in **Figure 6.7** below, a single repeater channel is defined and both its slots are 'Wide Area'.

9) Leave the Messaging Delay at its default value of 'Normal' (see **Figure 6.7** below).

10) If the Peer repeater has a dedicated RF channel on which to operate (i.e. it is not sharing the channel with another system), then it's strongly recommended that the RSSI Threshold be increased from its default value of -115dBm to -90dBm (see **Figure 6.7** below). For further details, refer to section 12.

11) Re-program the Peer repeater using the CPS.

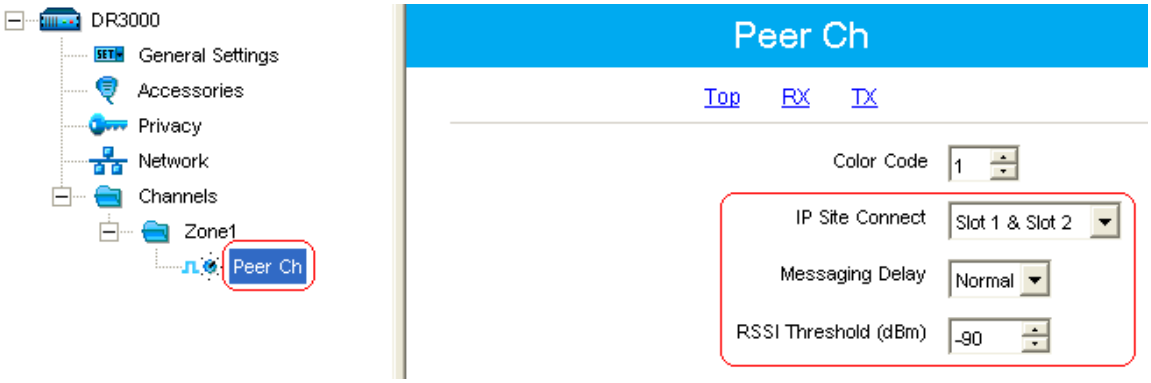


Figure 6.7

The procedure for configuring a radio to operate on this IP Site Connect system is as follows:

1) Read the radio using the CPS and navigate to each of the radio's 'Wide Area' channels. Select the IP Site Connection option and a messaging Delay of 60 ms (see **Figure 6.8** below).

2) For this simple system configuration radios are not required to automatically roam across the sites, so the Site/Roam List option can either be set to 'None' or a Scan list can be specified as per the example in **Figure 6.8** below.

3) Re-program the radio using the CPS

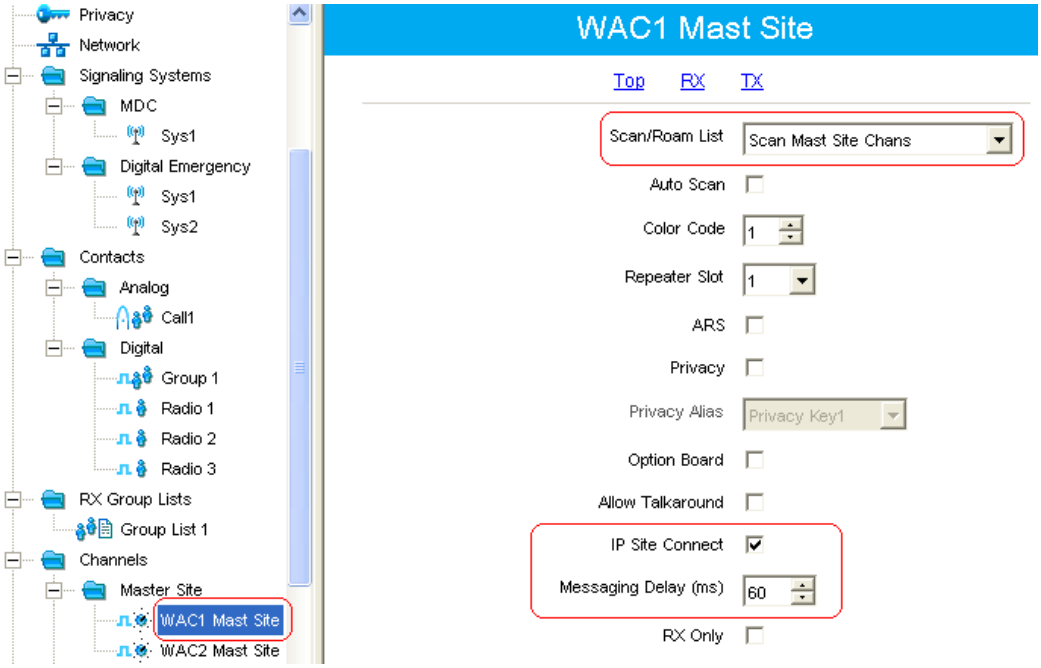


Figure 6.8

7. Local Area Network (LAN)

Building on the 'Back to Back' configuration, the next level of IP Site Connect system involves the addition of a Local Area Network (see **Figure 7.1** below). The simplest way to implement a LAN is to use an IP Switch. Since the IP Site Connect devices (i.e. repeaters and RDAC application) are not connected directly to each other, then straight Ethernet cables are required for this configuration.

The main advantage of this system configuration over the 'Back to Back' configuration is that the LAN (e.g. IP Switch) introduces additional ports which enable additional repeaters and 'Repeater Diagnostic and Control' (RDAC) applications to be added to the system. This system configuration is useful for demonstrating the basic principles of IP Site Connect in conjunction with the RDAC application. Additionally, this configuration is also useful for system topologies containing local overlapping sites (e.g. campus-wide or high-rise configurations) and for where radios need to communicate across two bands (e.g. VHF and UHF).

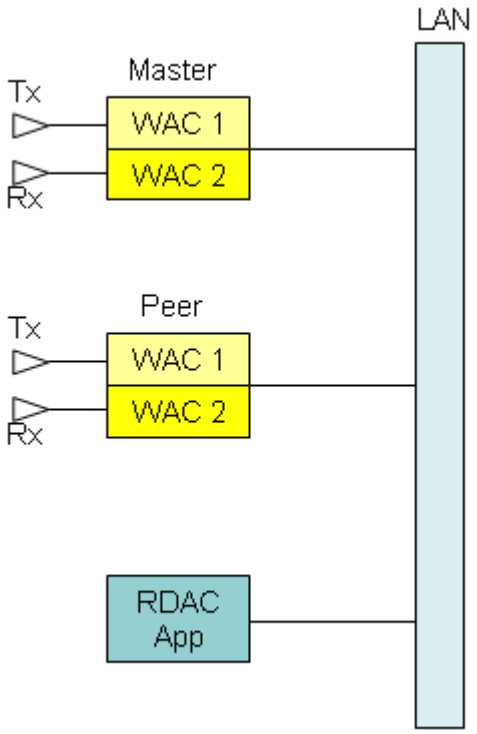


Figure 7.1

Note: The procedures described in this section build upon the configuration described in section 6.

As with the 'Back to Back' configuration, there is no DHCP server or Gateway for this LAN configuration and so the way in which the repeaters and radios are programmed is essentially the same as for the 'Back to Back' configuration. However, there are a few additional considerations for this system configuration as described below.

If radios are required to automatically roam across the sites, the beacon signal feature may need to be enabled (note: beacon signals facilitate radios roaming across sites where there may be too little user activity on the system for the radios' roaming algorithms to otherwise operate efficiently). The procedure for enabling the beacon signal feature is as follows:

1) The Beacon Duration and Beacon Interval fields both need specifying. These beacon parameters should be the same for all repeaters in the system and the Beacon Interval should also be the same as the Beacon Interval programmed into the radios.

2) To set the repeater beacon parameters, navigate to the Network screen for each of the repeaters in the system and set the Beacon Duration and the Beacon Interval. In the example shown in **Figure 7.2** below, the Beacon Duration is set to 1.2 seconds and the Beacon Interval is set to 30 seconds. For details on how to identify optimal beacon parameters, please refer to reference (1).

Figure 7.2

3) To set the radio beacon parameter, navigate to the Network screen for each of the radios in the system which are required to automatically roam and set the Beacon Duration. In the example shown in **Figure 7.3** below, the Beacon Duration is set to 1.2 seconds (as per the repeaters).

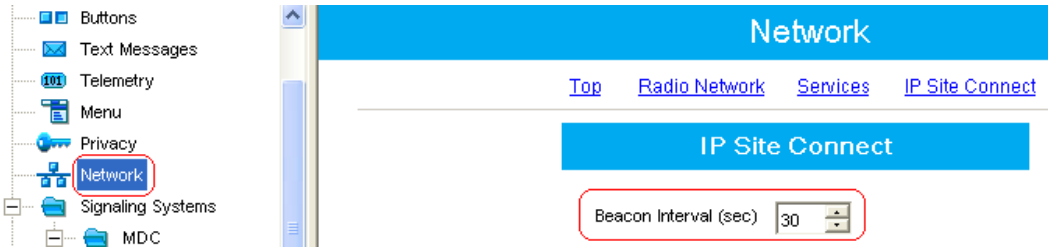


Figure 7.3

If there are concerns about rouge repeaters (or RDAC applications) attaching themselves to this system, the authentication feature should be enabled which forces IP Site Connect devices to carry out an authentication procedure before they attach themselves to the system. The procedure fore enabling the authentication feature is as follows:

1) The same Authentication Key needs to be specified for all repeaters and RDAC applications in the system.

2) To specify the repeater Authentication Key, navigate to the Network screen for each of the repeaters in the system and specify the Authentication Key as a hexadecimal number. In the example shown in **Figure 7.4** below, the Authentication Key is set to 290109 (note: any repeater or RDAC application not containing this key will be unable to attach itself to this system).

Figure 7.4

If the IP Site Connect devices are being added to an existing LAN, then the Static values for the Ethernet IP, Gateway IP and the Gateway Netmask must be consistent with other devices already operational on the subnet (i.e. no conflicting IP Addresses etc.). If however the IP Site Connect devices are being added to a new and dedicated LAN (e.g. IP Switch), then the same Static values from section 6 can be re-used.

The example shown in this section contains a single Peer repeater, however additional Peer repeaters may be added (note: IP Site Connect can support up to 15 devices in total). Each additional Peer repeater should be configured for IP Site Connect in the same way as the first Peer repeater with the exception that the Radio ID and Ethernet IP fields for each additional Peer repeater must be unique within the system.

If radios are required to automatically roam across the sites, the roaming characteristics need configuring into the radio personality as follows:

1) To make the radio operation more intuitive to the user, it is recommended that the channels from the different sites be grouped into radio zones as shown in **Figure 7.5** below. For this example there are 2 radio zones (i.e. 'Mast Site' and 'Peer Site').

2) Where there are revert channels (both Emergency and GPS), it is recommended that these channels are all grouped together into a zone by themselves as shown in **Figure 7.5** below.

3) It is also recommended that the channels from the different sites which together constitute a given wide area channel be duplicated from each other and that the following (site specific) parameters be modified accordingly for each channel:
   - Channel Name
   - RX Frequency
   - TX Frequency
   - Colour Code
   - Repeater Slot
   - Emergency System (if Emergency Revert is employed).

4) Ideally all other channel parameters should remain common across all channels which constitute a wide area channel. If alternative configurations are required (e.g. the radio needs to belong to different talkgroups), then it is recommended that additional wide area channels are defined in the radio personality. For the example in **Figure 7.5** below there are 2 wide area channels (i.e. WAC1 and WAC2).

Note: By following the above recommendations, the user shall be able to select the wide area channel using the rotary (i.e. position 1 = wide area channel 1, position 2 = wide area channel 2, position 3 = wide area channel 3 etc.), the radio shall be able to automatically roam across the site channels which constitute the selected wide area channel and the radio behaviour shall be consistent across the entire wide area channel.

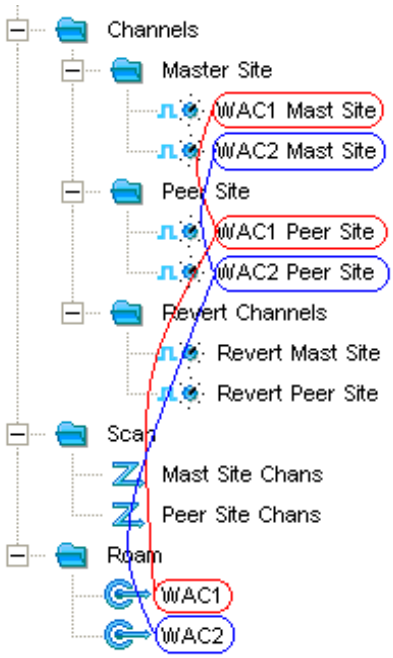


Figure 7.5

5) In order for the radio to link together the individual channels which constitute the wide area channels, it requires a roam list to be defined for each wide area channel. For this example, there are 2 Roam lists; one for WAC1 and another for WAC2. Figure 7.6 below shows the Roam list for WAC1.

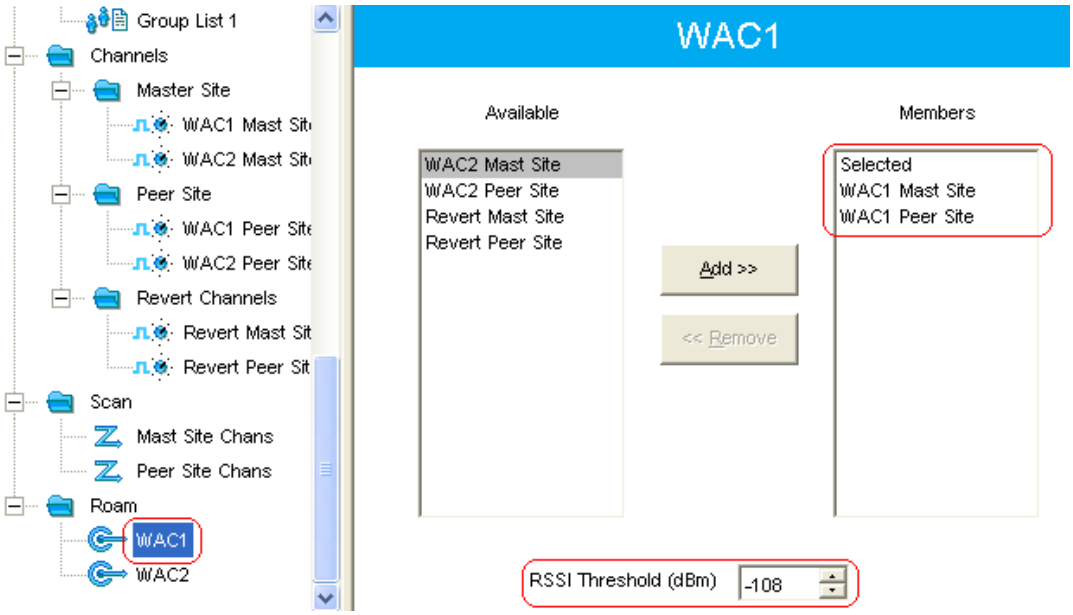


Figure 7.6

6) For each roam list, select the channels from the different sites which together constitute the given wide area channel and also specify the RSSI Threshold (note: this RSSI Threshold is used by the radio to determine when to start searching for another site using the Passive Site Search).

7) For each site channel belonging to a wide area channel, select the given Roam List. **Figure 7.7** below show the Roam List selection for 'WAC1 Mast Site'. For this example, 'WAC1 Peer Site' also uses the WAC1 Roam List, while 'WAC2 Mast Site' and 'WAC3 Peer Site' use the WAC2 Roam List.

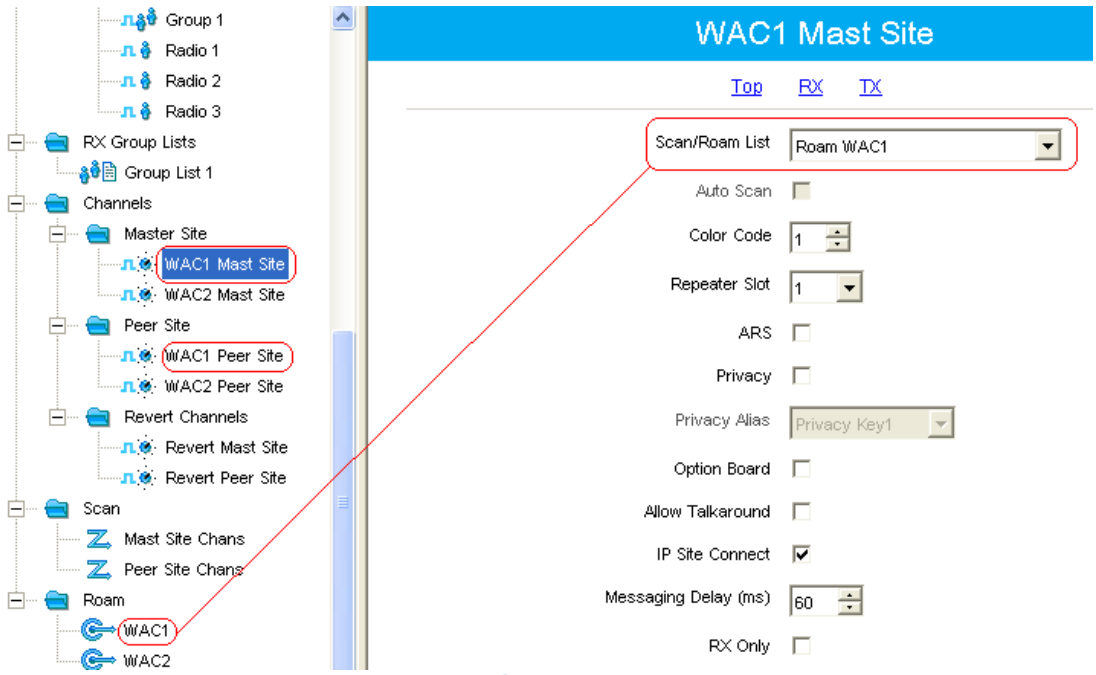


Figure 7.7

The procedure for configuring the RDAC application is as follows:

1) Since there is no DHCP server, the LAN connection for the RDAC PC needs to be statically configured to operate on the same subnet as the other IP Site Connect devices. To do this, open up the Local Area Connection Properties on the PC, select the 'Internet Protocol (TCP/IP)' item and click on 'Properties'.

2) In the resulting Internet Protocol (TCP/IP) Properties window that opens up, select 'Use the following IP address', specify the IP address parameters and click 'OK'. For the example in **Figure 7.8** below, the IP address parameters are configured as follows:
   - IP address (192.168.4.12): This defines the PC's static address which must be unique within the system.
   - Subnet mask (255.255.255.0): Configured as per the Gateway Netmask setting for the other IP Site Connect devices.
   - Default gateway IP 192.168.4.254): Configured as per the Gateway IP setting for the other IP Site Connect devices.

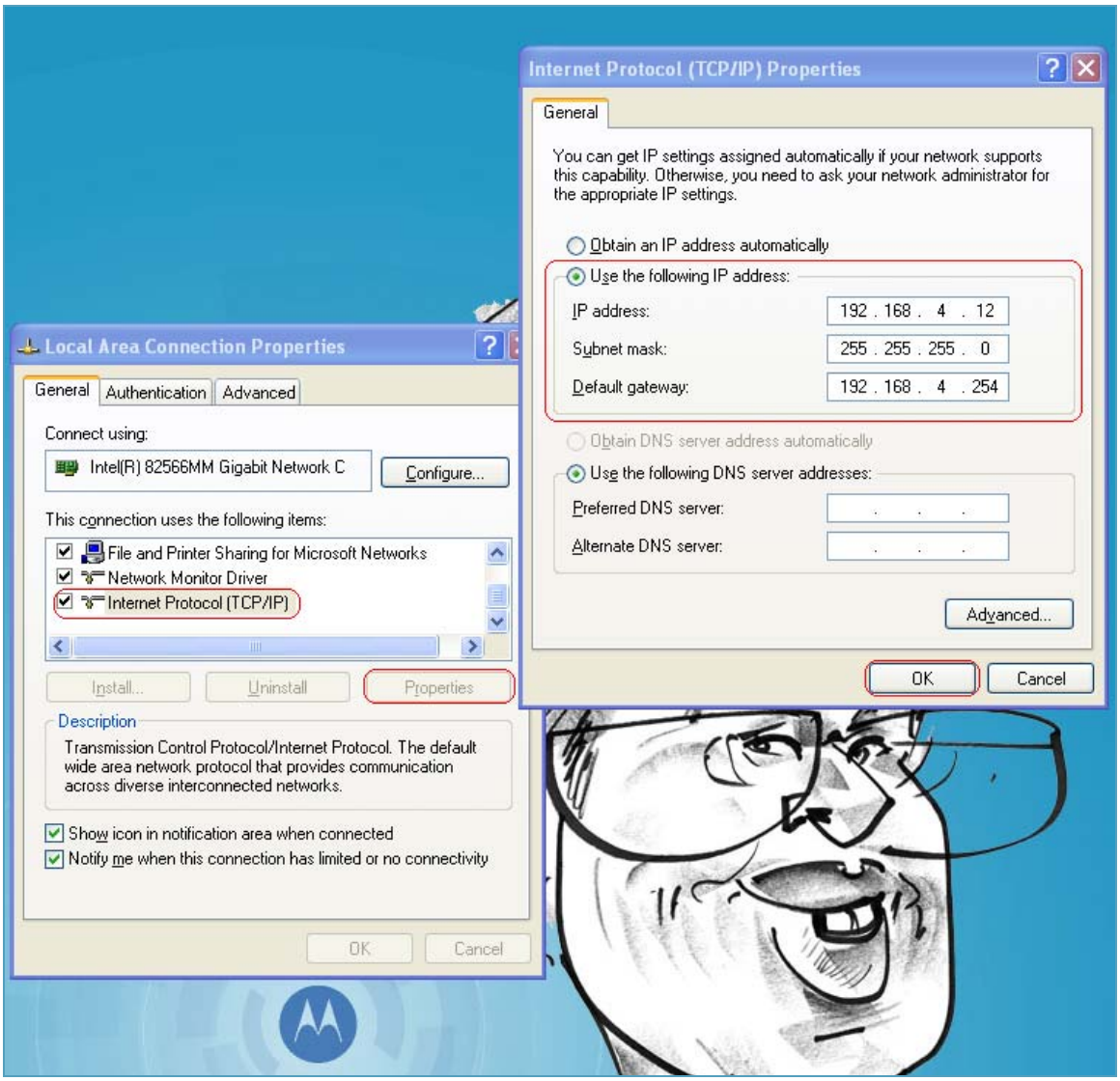


Figure 7.8

3) Invoke the RDAC application and configure the system parameters by clicking on the System option (see **Figure 7.9** below).

4) In the System window that opens up, select the 'IP Site Mode' option and specify the IP Site Settings. For the example in **Figure 7.9** below, the IP Site Settings are configured as follows:
   - Master IP Address (192.168.4.101): Set to the Master repeater's Ethernet IP address.
   - Master UDP Port (50000): Set to the Master repeater's IP Site UDP Port.
   - RDAC ID (3): Set to a unique value within the system (i.e. one which does not conflict with the Radio IDs for the Master or any of the Peer repeaters).
   - RDAC UDP Port (50000): Left as the default value.
   - Authentication Key (290109): Set to the same value as all the other IP Site Connect devices in the system.
   - Firewall Open Timer (6): Left as the default value.
   - Master Retry Timer (200): Left as the default value.

5) Click OK in the System window and then click on the Connect option (note: there will be a short delay while the RDAC application establishes a connection with the Master repeater and each of the Peer repeaters).

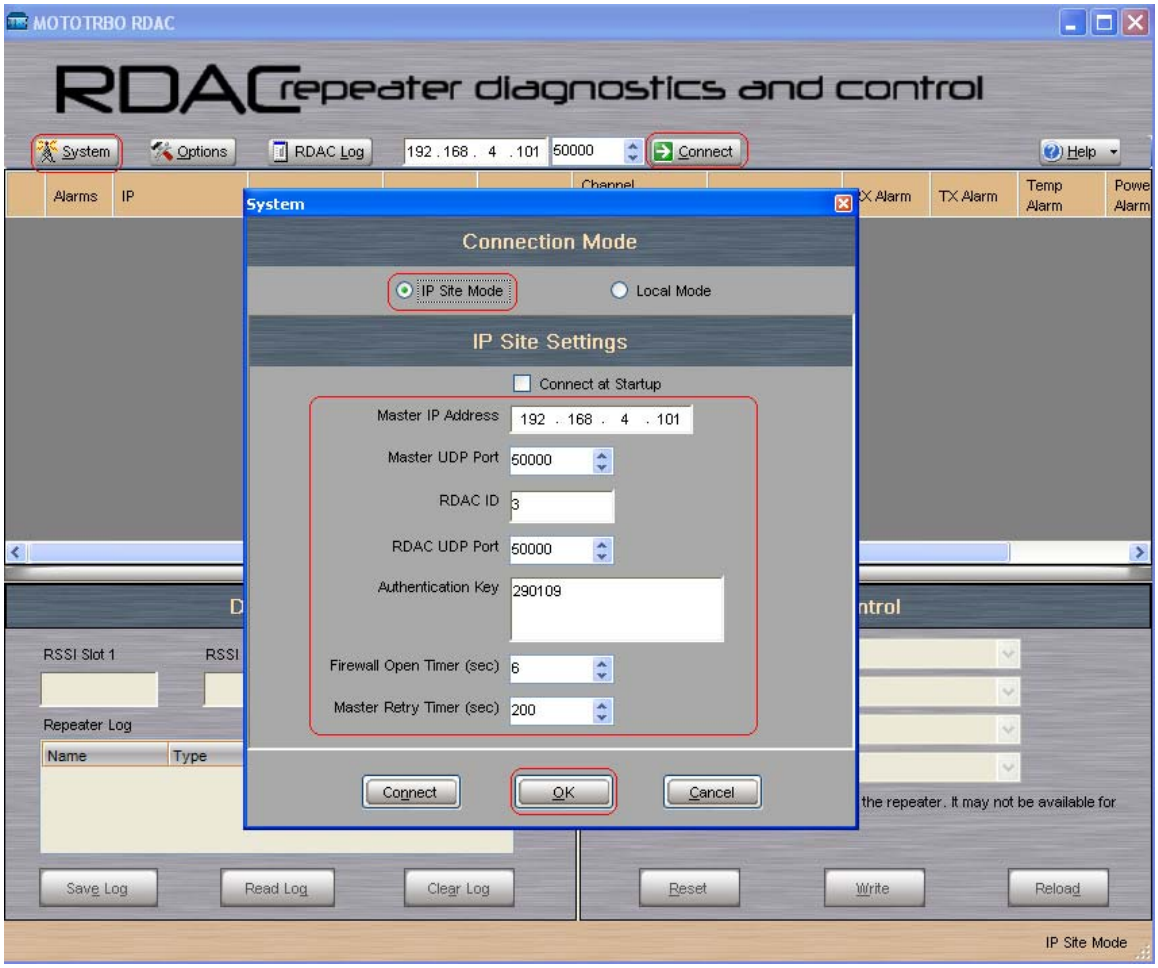


Figure 7.9

8. Local Area Network with DHCP Server

Building on the Local Area Network configuration, the next level of IP Site Connect system involves the addition of a DHCP server to the LAN (see **Figure 8.1** below). Since the IP Site Connect devices (i.e. repeaters and RDAC application) are not connected directly to each other, then straight Ethernet cables are required for this configuration.

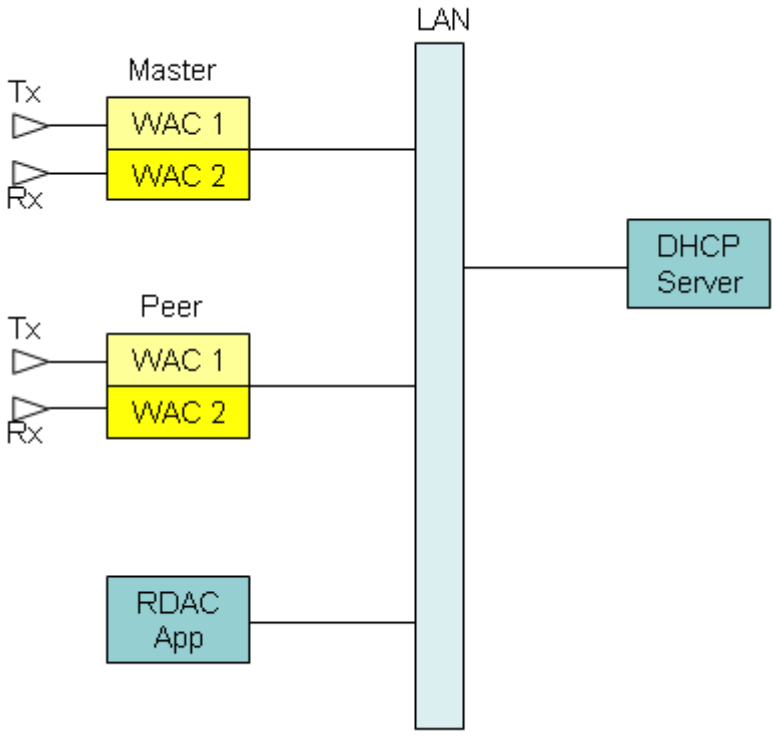


Figure 8.1

Note: The procedures described in this section build upon the configuration described in section 7.

The way in which the IP Site Connect devices are programmed for this configuration is essentially the same as in section 7. However, there are a few additional considerations for this system configuration as described below.

1) The IP address for the Master repeater must remain statically assigned, however the IP addresses for any or all of the Peer Repeaters and RDAC applications may be dynamically assigned by the DHCP server.

2) Any static IP addresses assigned to IP Site Connect devices must be outside the range of dynamic IP addresses assigned by the DHCP Server, but within the range of IP addresses for the subnet (as defined by the Gateway Netmasks for the devices on the LAN).

3) To enable the IP address of a Peer repeater to be dynamically assigned, navigate to the Network screen for the repeater and select the DHCP option as shown in **Figure 8.2** below.

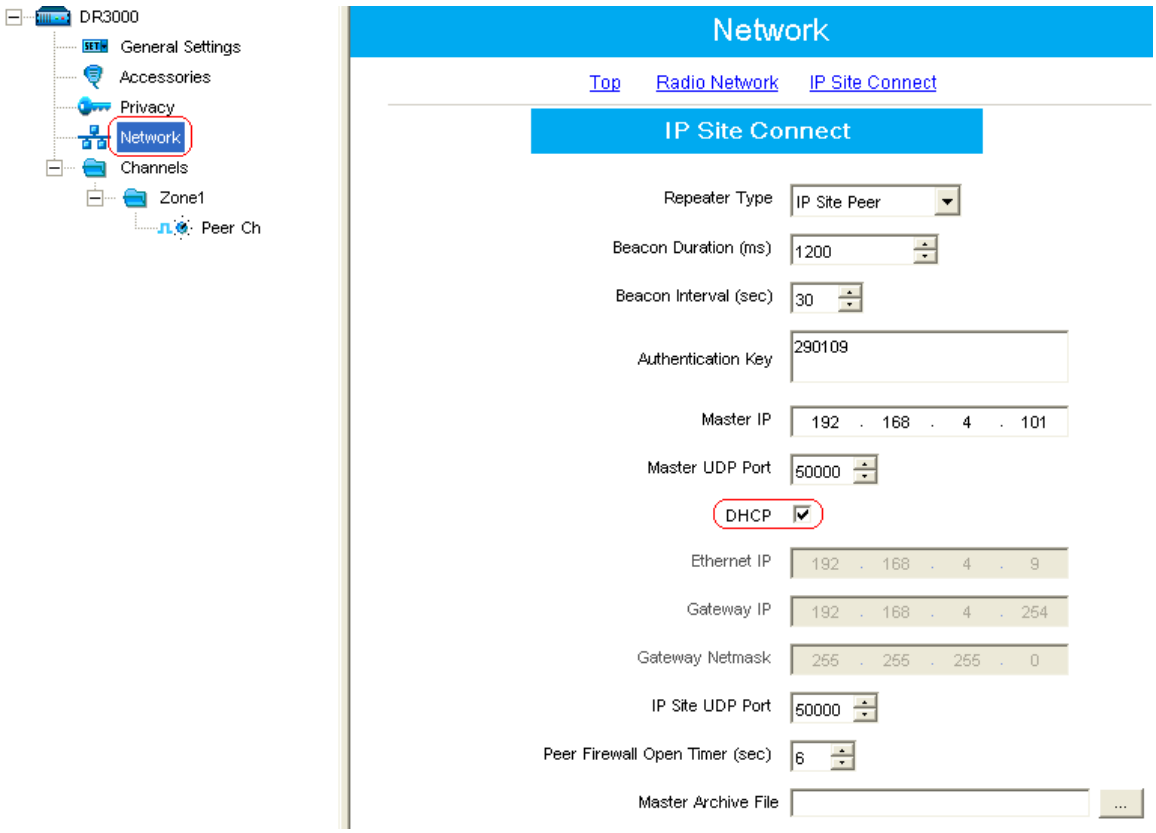


Figure 8.2

4) To enable the IP address of an RDAC application to be dynamically assigned, open up the Local Area Connection Properties on the PC, select the 'Internet Protocol (TCP/IP)' item and click on 'Properties'. In the resulting Internet Protocol (TCP/IP) Properties window that opens up, select 'Use the following IP address' and select the 'Obtain an IP address automatically' as shown in **Figure 8.3** below.

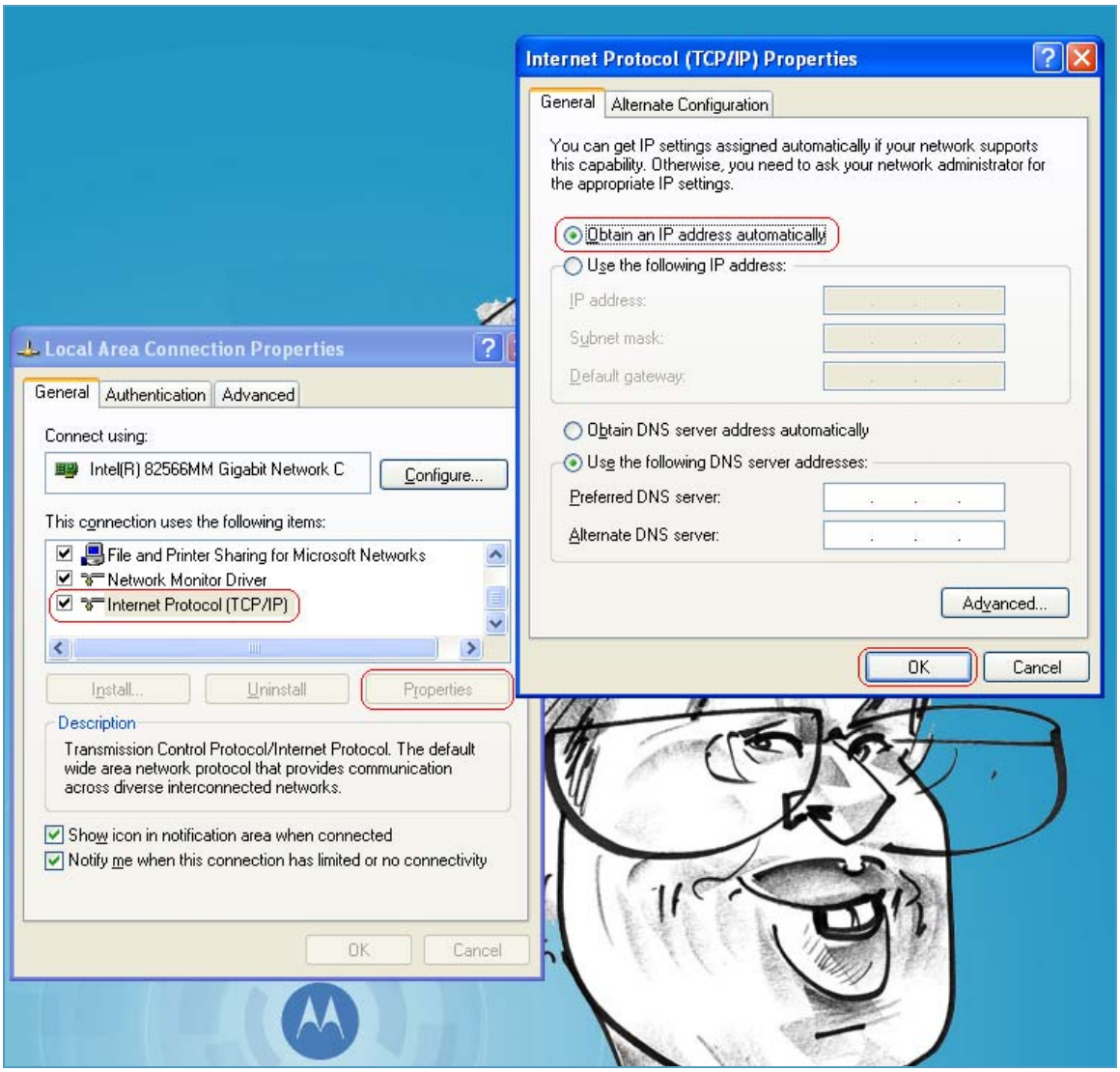

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel
Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Intel(R) 82566MM Gigabit Network C
Configure...
This connection uses the following items:
File and Printer Sharing for Microsoft Networks
Network Monitor Driver
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK
Cancel

Figure 8.3

9. Wide Area Network (WAN)

In reality, many IP Site Connect systems will contain multiple Local Area Networks linked together by routers and a Wide Area network (see **Figure 9.1** below). An example of a WAN might typically be the public Internet, while an example of the interfaces linking the various LANs to the WAN might typically be ADSL connections to respective Internet Service Providers. Since the IP Site Connect devices (i.e. repeaters and RDAC application) are not connected directly to each other, then straight Ethernet cables are required for interfacing to the IP Site Connect devices for this configuration.

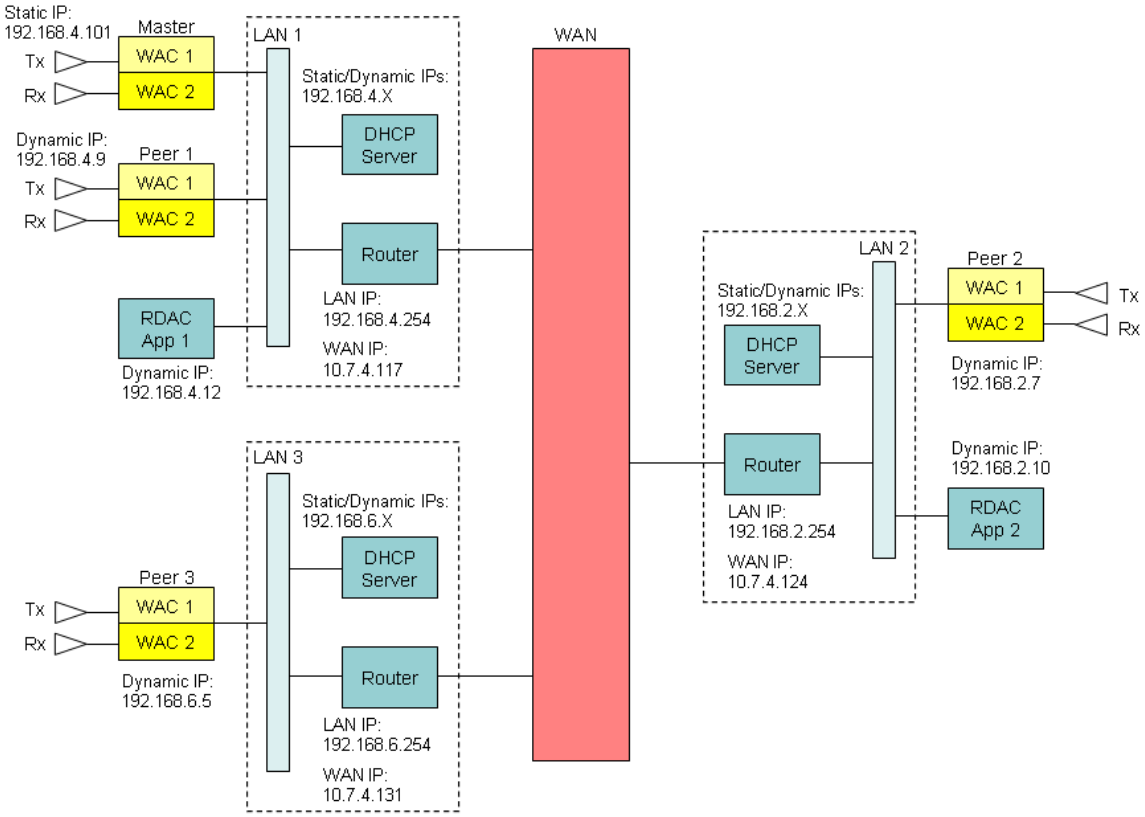


Figure 9.1

Note: The procedures described in this section build upon the configuration described in section 8.

For the above system configuration, the Master repeater is statically configured to operate on LAN 1 as shown in **Figure 9.2** below.

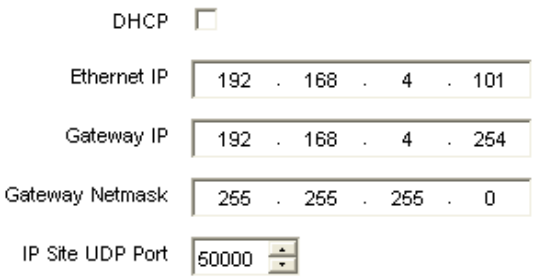


Figure 9.2

The Ethernet IP (i.e. the Master repeater's IP address) is outside the range of dynamic IP addresses assigned by the DHCP Server, but within the range of IP addresses for the subnet (as defined by the Gateway Netmasks for the devices on the LAN). Also, the Gateway IP corresponds to the LAN IP address of the router for LAN 1.

For the above system configuration, all Peer repeaters are configured to dynamically operate on their respective LANs as shown in **Figure 9.3** below and the LAN connections for all RDAC PCs are also configured to dynamically operate on their respective LANs. The IP addresses for all the Peer repeaters and RDAC applications are therefore dynamically assigned by their respective LAN DHCP servers.

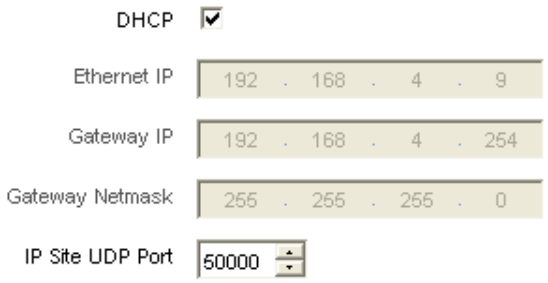


Figure 9.3

For the above system configuration, all Peer repeaters and RDAC applications must address the Master repeater using the WAN address of the LAN 1 router (i.e. 10.7.4.117) as shown in **Figure 9.4** below rather than the static IP address of the Master repeater itself (i.e. 192.168.4.101).

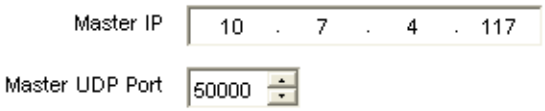


Figure 9.4

The reason why all Peer repeaters and RDAC applications need to address the Master repeater using the WAN address of the LAN 1 router is because the IP addresses of all devices behind all of the routers in the above system configuration are local to their respective LANs and are not therefore available over the WAN. For this to work however, the LAN 1 router must be configured for 'Port Forwarding' such that all incoming packets addressed to the router's WAN address and a specified external UDP port get forwarded directly to the Master repeater. For this particular system configuration, the external UDP port is the same as the Master repeater's UDP port (i.e. 50000). However, if the LAN 1 router was configured to forward packets to the Master repeater using a different external UDP port, then the Peer repeaters and RDAC applications would have to address the Master repeater using this alternative UDP Port instead.

Some additional points to note with the above system configuration are as follows:

1) 'Port Forwarding' does not need to be configured for any of the Peer repeaters or RDAC applications. The reason for this is that incoming packets addressed to these devices only ever occur after these devices have already transmitted outgoing packets on the WAN, and publicly addressable IP addresses and ports have subsequently been made available by their respective LAN routers.

2) The publicly addressable IP addresses and ports for all Peer repeaters and RDAC applications are made known to all other IP Site Connect devices via the Master repeater (which acts as a broker of IP addresses).

3) The devices on a given LAN do not need to be configured with unique port numbers since the routers will ensure that the publicly addressable ports assigned to each device are unique.

4) A publicly addressable IP address and port which have been assigned to a given Peer device will remain open only for a limited time if there is no activity to/from that device. For this reason all Peer repeaters and RDAC applications are able to transmit 'keep alive' messages while there is no other activity present. The frequency of these 'keep alive' messages can be configured via the 'Peer Firewall Open Timer' field. When selecting a value, ensure that it is shorter than the time which the publicly addressable IP address and port remain open while there is no other activity. The default value for this timer is 6 seconds as shown in **Figure 9.5** below.

Figure 9.5

5) Even though the Peer repeaters and RDAC applications on the Master repeater's LAN are theoretically able to address the Master Repeater using the Master repeater's static IP address (because they are all on the same LAN), they must still use the WAN address of the LAN 1 router. If they do not do this, then they themselves will not be addressable by IP Site Connect devices on other LANs and as such will be cut off from the rest of the IP Site Connect system.

6) For the above system configuration, LAN 1 and LAN 2 both contain multiple IP Site Connect devices. For this configuration to work, the LAN 1 and LAN 2 routers MUST support 'Hairpinning', which means these routers must loop back any packets addressed from one IP Site Connect device on a given LAN to another IP Site Connect device on the same LAN. If these routers do not support 'Hairpinning', then such packets will be lost because the routers will see these packets being addressed to WAN addresses (i.e. their own WAN addresses) and will therefore route them to the WAN. In summary, routers that do not support 'Hairpinning' may only support a single IP Site Connect device on their LANs.

7) Some routers support partial 'Hairpinning' in that they loop back any packets addressed from one IP Site Connect device on a given LAN to another IP Site Connect device on the same LAN, however in doing so they erroneously use the local address of the IP Site Connect device initiating the packets rather than its publicly addressable IP address and port. This causes problems where there are Peer repeaters and RDAC applications on the same LAN as the Master repeater because they end up registering local IP addresses with the Master repeater which are not addressable by IP Site Connect devices on other LANs. In summary, routers that support partial 'Hairpinning' may not support Peer repeaters or RDAC applications where there is a Master repeater on the LAN and IP Site Connect devices on other LANs. However, such routers can still support multiple Peer repeaters and RDAC applications where there is no Master repeater on the LAN.

8) The repeaters and radios in an IP Site Connect system need to take account of the messaging delays introduced by the IP network. Where the maximum IP network delay (due to propagation, serialisation and handling) is less than 60ms, the Messaging Delay for the repeater channel(s) should be set to 'Normal' as shown in **Figure 9.6** below. Where however the maximum IP network delay is between 60 and 90ms, the Messaging Delay for the repeater channel(s) should be set to 'High'.

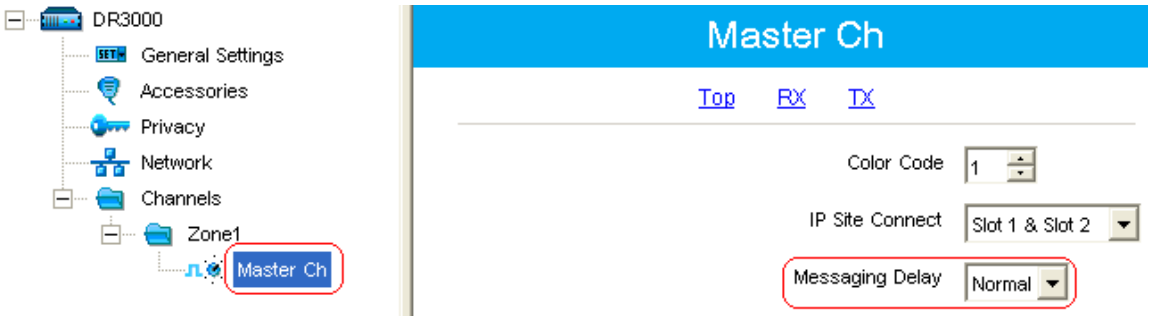


Figure 9.6

Similarly, where the maximum IP network delay is less than 60ms, the Messaging Delay for the radio channel(s) should be set to 60ms as shown in **Figure 9.7** below and where the maximum IP network delay is between 60 and 90ms, the Messaging Delay for the radio channel(s) should be set to 90ms (note: radio messaging delays greater than 90ms should only be configured where MOTOTRBO radios are being used on non-Motorola infrastructure requiring such long delays).

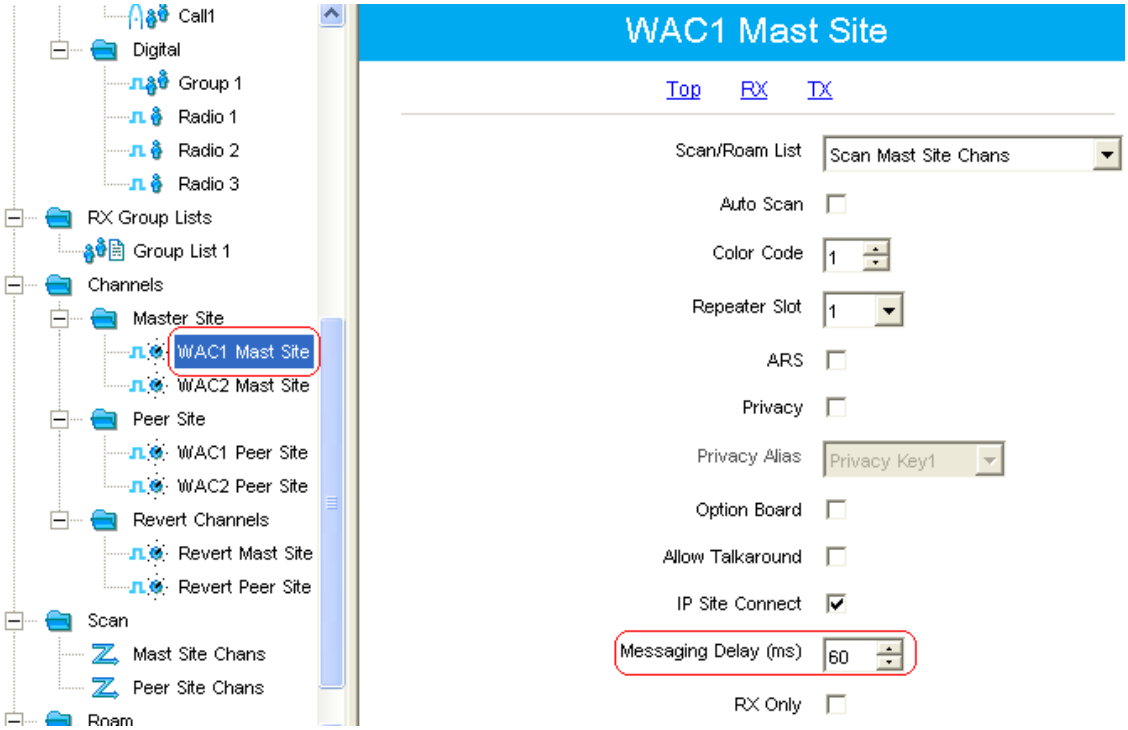


Figure 9.7

9) For this system configuration, since all Peer repeaters and RDAC applications address the Master repeater using the WAN address of the LAN 1 router (i.e. 10.7.4.117) rather than the Master IP address (i.e. 192.168.4.101), then for certain routers it may be possible for the Master repeater to be configured with a dynamic IP address as shown in **Figure 9.8** below. The Master Ethernet IP, Gateway IP and Gateway Netmask will then be assigned by the DHCP server and it will be the responsibility of the WAN 1 router to ensure that all incoming packets for the Master repeater get forwarded to the Master repeater's dynamic IP address. Note: not all routers are able to support 'Port Forwarding' to dynamic IP addresses, and even where this is possible, this is not a configuration which is recommended.

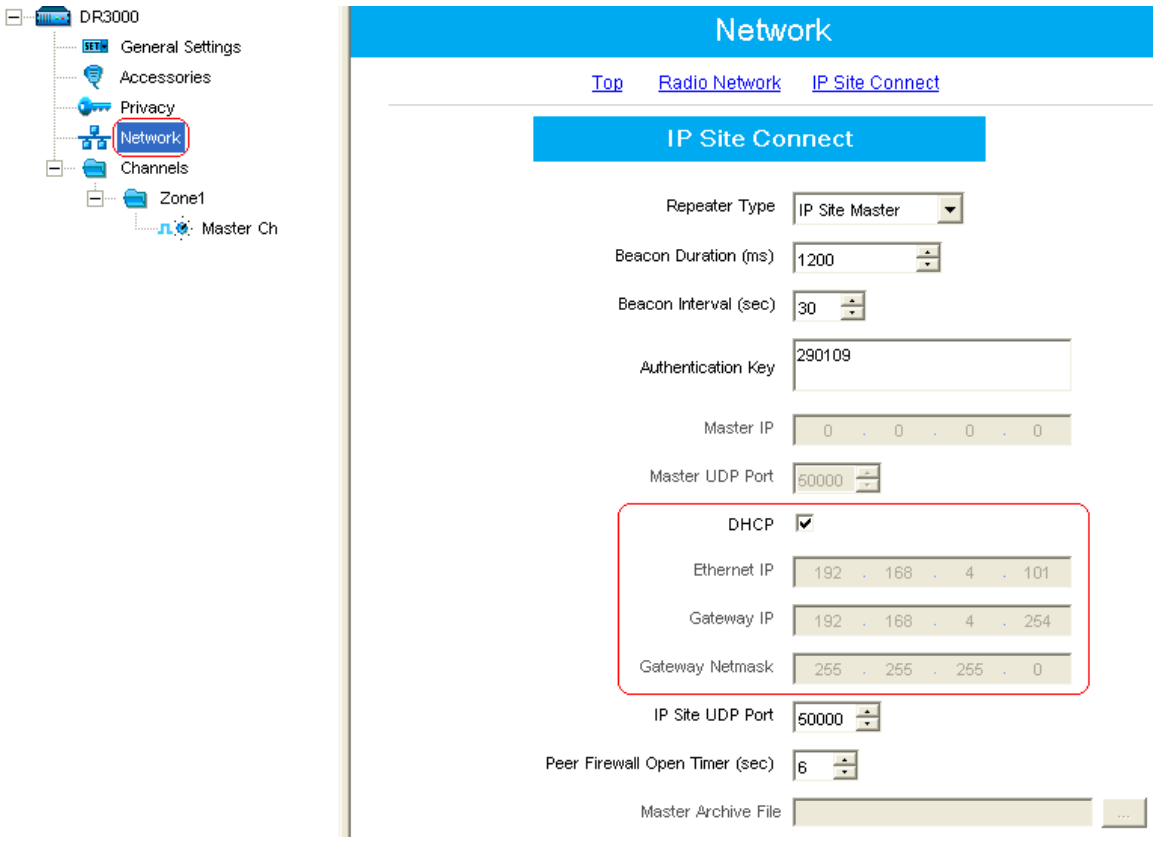


Figure 9.8

10) Some proprietary WANs (e.g. corporate Intranets) provide all devices on the network with the ability to address all other devices on the network by their IP address. When a device is connected to such a network, the DHCP server assigns the device an IP address, and the mapping tables for the appropriate network routers are automatically updated to ensure the correct routing of packets to the device. However, since the Master repeater needs a static IP address, then a network administrator will need to assign a static IP address for the Master repeater and manually configure the mapping tables for the appropriate network routers in advance to ensure the correct routing of packets to the Master repeater.

11) The easiest and most secure method of interfacing an IP Site Connect system to a WAN is to use secure modems containing a VPN. All IP Site Connect addressing can then be local and the management of all IP Site Connect packets across the WAN can be automatically handled by the VPN.

10. Motorola Wireless Broadband

Motorola provides a number of different Wireless Broadband solutions which can be used as Wireless Ethernet connectivity for IP links in the IP Site Connect system configurations.

The following tables provide a high level summary of Motorola's Wireless Broadband portfolio:

Point to Point		Point to Multipoint	
• Establish communications to facilities that may not be reached cost-effectively with wired connections • Establish cost-effective network redundancy or extend network reach without trenching new fiber – ROI 4-8 months • Establish connectivity in previously inaccessible or high-interference locations • Easy to Plan & Install – web based link planning tool		• Formerly known as Canopy • Fast, Simple Installation • Industry Leading Interference Tolerance • Scalable as Subscriber Base Grows - Access Points and Subscriber Modules can be deployed in hours, reducing the cost and delay of service • Attractive Total Cost of Ownership – ROI 18-24 months • Lower cost point than 'Point to Point'.	
Model	**Comments**	**Model**	**Comments**
PTP 100	• Line of Sight (LoS) operation • Same hardware platform as PMP 100/200	PMP 100	• Line of sight (LoS) operation • Same hardware platform as PTP 100 and PMP 200
PTP 200	• Near Line of Sight (nLoS) & LoS operation • Same hardware platform as PMP 400	PMP 200	• LoS operation • Same hardware platform as PTP 100 and PMP 100
PTP 300	• Non Line of Sight (NLoS) plus nLoS & LoS operation	-	-
-	-	PMP 400	• Near Line of Sight & LoS operation • Same hardware platform as PTP200
PTP 500	• Non Line of Sight (NLoS) plus nLoS & LoS operation	PMP 500	• Non Line of Sight (NLoS) plus nLoS & LoS operation • Licensed only solution at 3.5 GHz
PTP 600	• Non Line of Sight (NLoS) plus nLoS & LoS operation	-	-

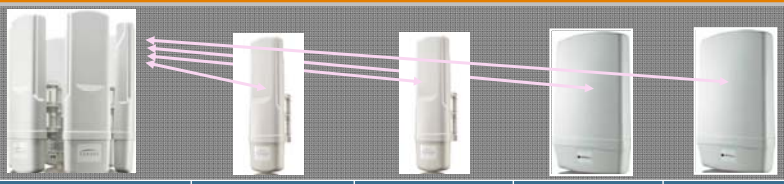
Point to Point Performance - Comparison

Features	PTP100	PTP200	PTP300	PTP500	PTP600
Unlicensed spectrum	Y	Y	Y	Y	Y
Ethernet throughput (max)	14 Mbps	21 Mbps	25 Mbps	105 Mbps	300 Mbps
Line of Site range (max)	10 mi / 15km	5 mi /8 km	155 mi / 250 km	155 mi /250km	124 mi / 200km
Near Line of Site range (max)		5 mi /8 km	20 mi / 32km	20 mi / 32km	20 mi/ 32km
None Line of Site range (max)			5 mi / 8 km	5 mi / 8 km	5 mi / 8 km
Security	Y	Y	Y	Y	Y

* Note – Distances reflect full power. EU regulations typically results in 25% of the products achievable distances

MOTOROLA WIRELESS BROADBAND 17

Point to Multipoint Performance Comparison



Features	PMP100	PMP200	PMP400	PMP500
Spectrum	2.4, 5.1, 5.2, 5.4, 5.8, 5.9Ghz	2.4, 5.1, 5.2, 5.4, 5.8, 5.9Ghz	5.4Ghz	3.5Ghz
Ethernet throughput (max)	7 Mbps	14 Mbps	21 Mbps	14 Mbps
Line of Site range (max)	x mi / 4km	x mi / 4km	5 mi / 8km	12 mi / 20km
Near Line of Site range (max)	No	No	tba	tba
Security	Y	Y	Y	Y

MOTOROLA WIRELESS BROADBAND 20

To configure the above Wireless Broadband solutions, refer to the appropriate Wireless Broadband ‘Quick Start’ and ‘Installation’ manuals.

Once a Wireless Broadband product has been configured, it can be used in place of any ‘wired’ IP link in any system configuration contained in this System Integration Guide. To facilitate the integration of IP Site Connect, a number of ‘tested’ IP Site Connect and wireless broadband system configurations are documented below.

Since the IP Site Connect devices (i.e. repeaters and RDAC application) are not connected directly to each other, then straight Ethernet cables are required for interfacing to the IP Site Connect devices for these wireless broadband configurations.

1) Point to Point (PTP) and ‘Back to Back’ Repeaters

The configuration shown in **Figure 10.1** below has been tested with the following products: PTP 100, PTP 200, PTP 300, PTP 500 and PTP 600.

Note: For the IP Site Connect device configuration details refer to section 6.

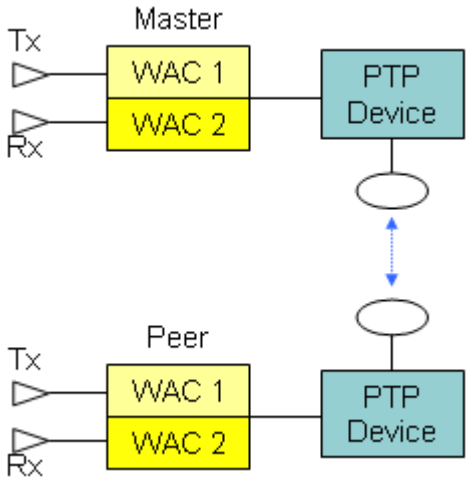


Figure 10.1

2) Point to Point (PTP) and Local Area Network (LAN)

The configuration shown in **Figure 10.2** below has been tested with the following products: PTP 100, PTP 200, PTP 300, PTP 500 and PTP 600.

Note: For the IP Site Connect device configuration details refer to section 7.

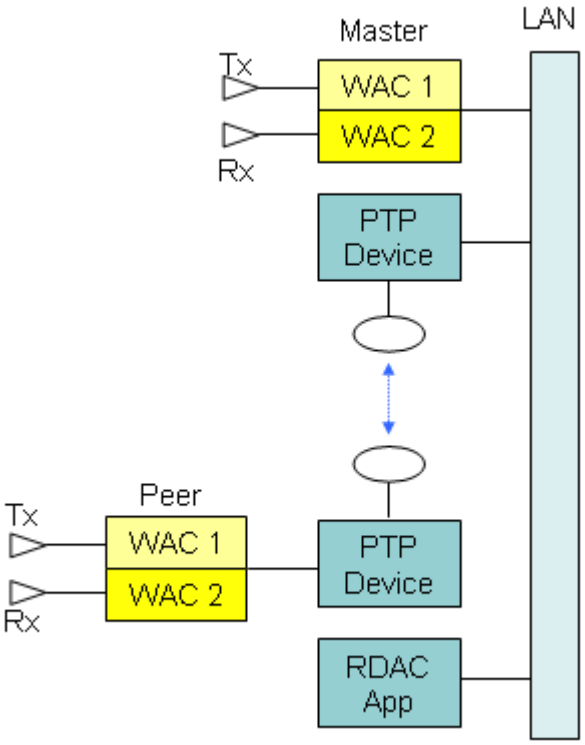


Figure 10.2

3) Point to Point (PTP) Cluster and Local Area Network (LAN)

The configuration shown in **Figure 10.3** below has been tested with the following products: PTP 100, PTP 200, PTP 300, PTP 500 and PTP 600.

Note: For the IP Site Connect device configuration details refer to section 7.

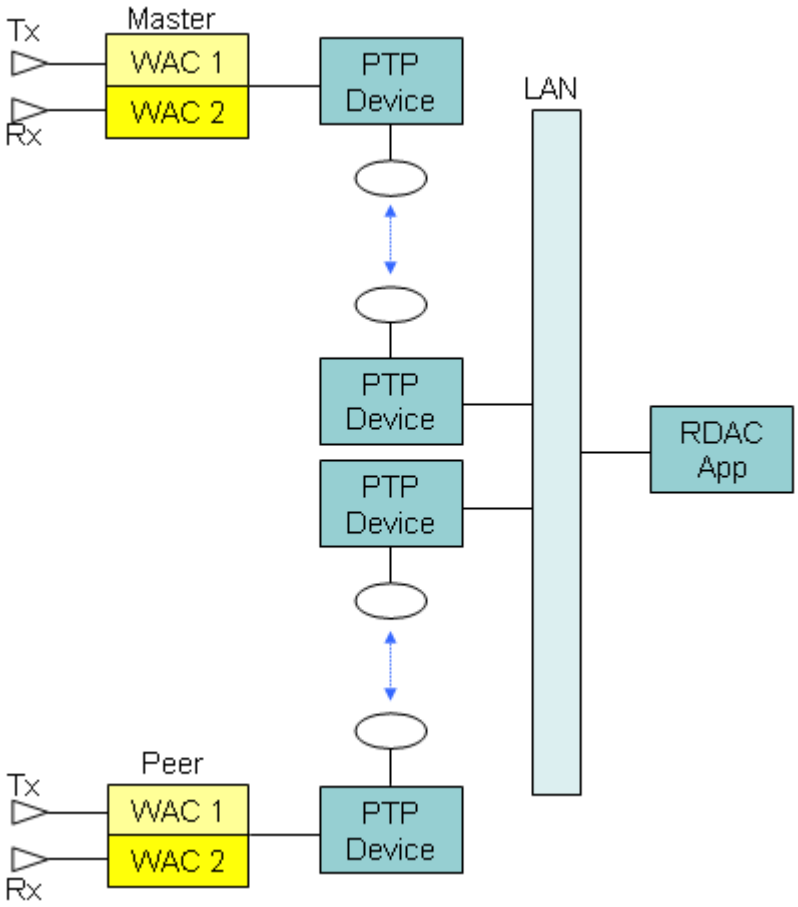


Figure 10.3

4) Point to Point (PTP) and Wide Area Network (WAN)

The configuration shown in **Figure 10.4** below has been tested with the following products: PTP 100, PTP 200, PTP 300, PTP 500 and PTP 600.

Note: For the IP Site Connect device configuration details refer to section 9.

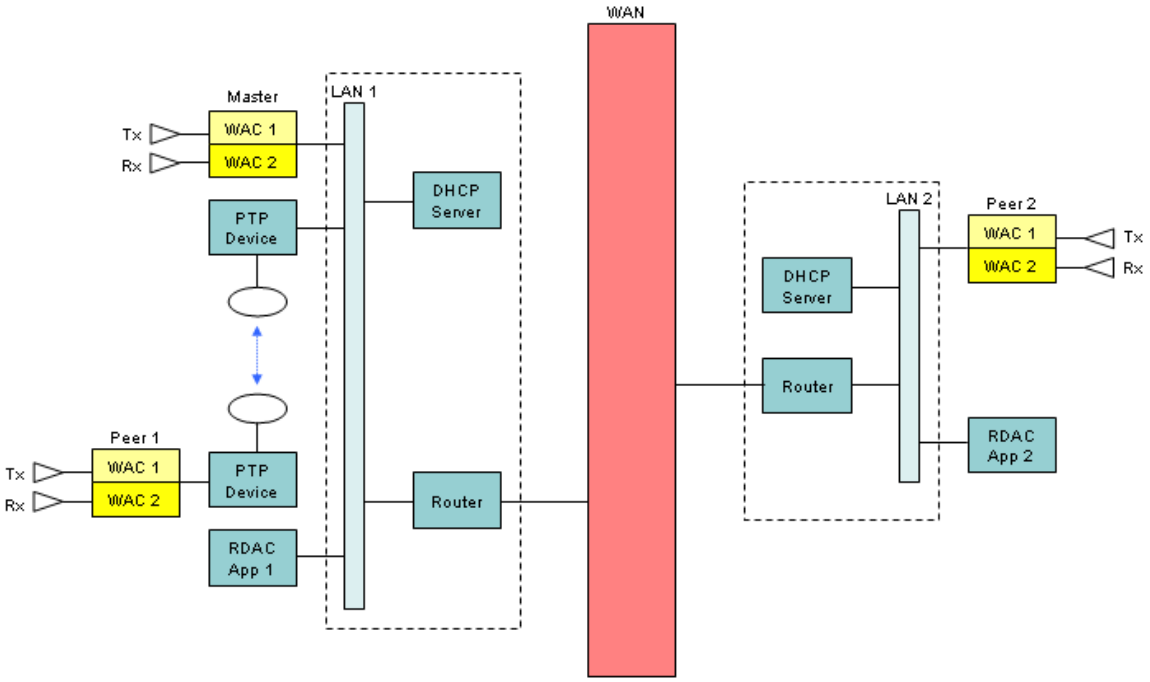


Figure 10.4

5) Point to Multi-Point (PMP) and Wide Area Network (WAN)

The configuration shown in **Figure 10.5** below has been tested with the following products: PMP 100 and PMP 200.

PMP (Point to Multipoint) devices have wider RF beams than the PTP (Point to Point) devices which enable them to support multiple wireless IP links. Additionally they also contain internal IP Switches to facilitate the routing of packets between the different devices linked together by the multiple wireless IP links. In **Figure 10.5** below the Internal IP Switch for the PMP AP device is disabled such that the routing of packets between the Master and Peer 1 repeaters is managed by the LAN 1 Router (note: if the Internal IP Switch was enabled, the routing of these packets would be managed directly by the PMP AP device).

Note: For the IP Site Connect device configuration details refer to section 9.

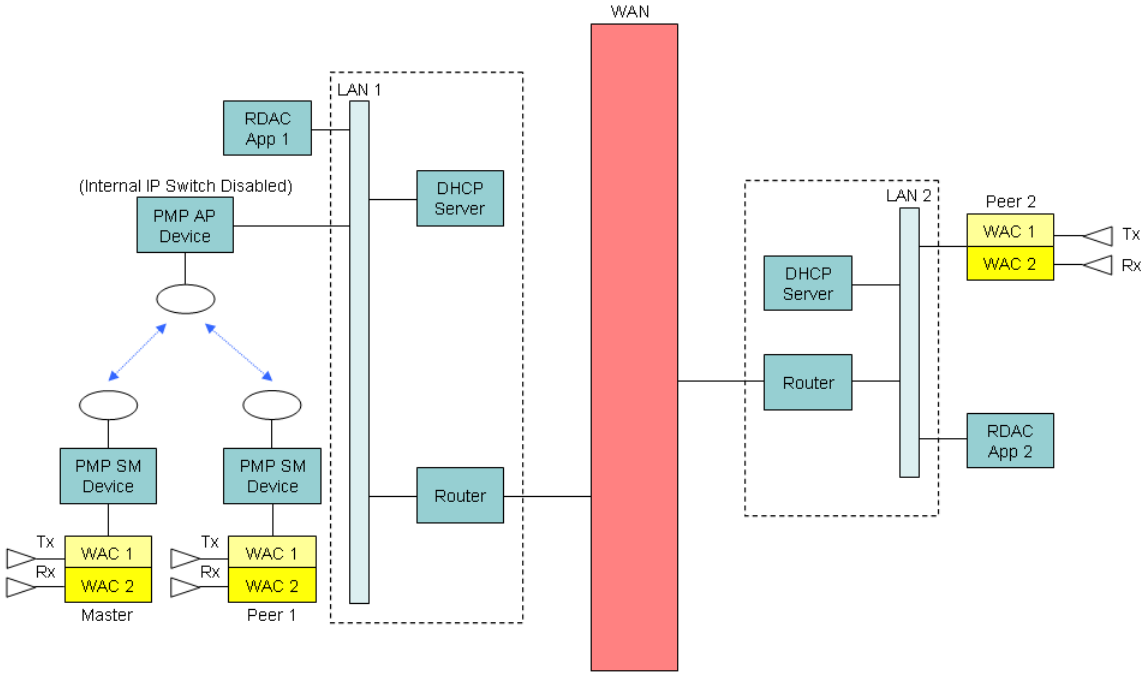


Figure 10.5

6) Point to Multi-Point (PMP) Cluster and Local Area Network (LAN)

The configuration shown in **Figure 10.6** below has been tested with the following products: PMP 100 and PMP 200.

In **Figure 10.6** below the Internal IP Switches for the PMP AP devices are enabled such that the routing of packets between the IP Site Connect devices attached to the PMP SM devices is managed by the respective PMP AP devices (note: if the Internal IP Switches were disabled then these packets would be lost because there is no router to in **Figure 10.6** to manage them).

Note: For the IP Site Connect device configuration details refer to section 7.

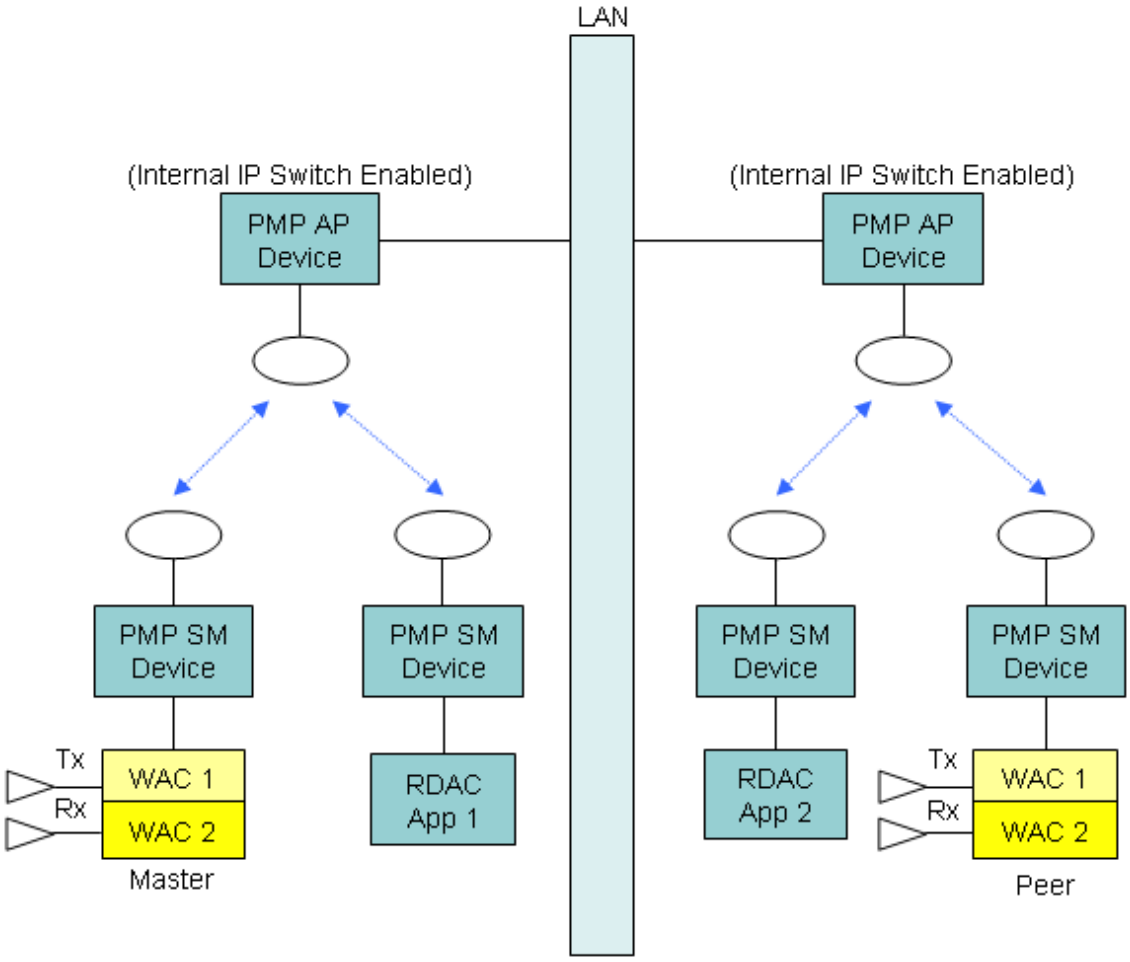


Figure 10.6

7) Point to Multi-Point (PMP) Cluster and Wide Area Network (WAN)

The configuration shown in **Figure 10.7** below has been tested with the following products: PMP 100 and PMP 200.

In **Figure 10.7** below the Internal IP Switches for the PMP AP devices are disabled such that the routing of packets between the IP Site Connect devices attached to the PMP SM devices is managed by the LAN 1 Router (note: if the Internal IP Switches were enabled, the routing of these packets would be managed directly by the PMP AP devices).

Note: For the IP Site Connect device configuration details refer to section 9.

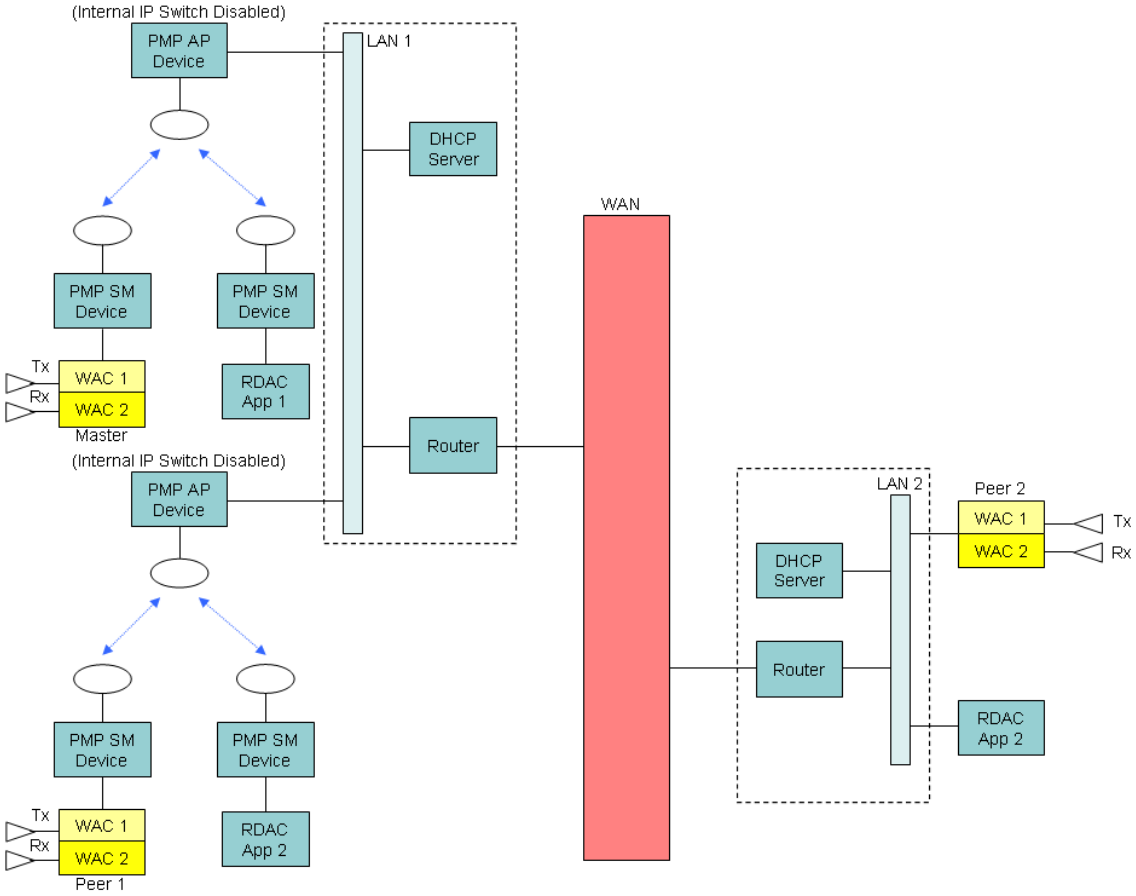


Figure 10.7

11. Analogue to Digital Migration

Where there is a customer requirement to gradually migrate analogue fleets on a legacy analogue radio system to digital fleets on a digital IP Site Connect system, while at the same time provide a degree of communication between the two types of fleet, there are two basic strategies available as described below.

Firstly, it is possible to configure MOTOTRBO radios so they can work both in digital mode on the IP Site Connect system and in analogue mode on the legacy analogue radio system. In analogue mode, MOTOTRBO radios are able to support the following features:

- Carrier squelch operation
- TPL/DPL signalling
- Select 5 signalling (via an option board)

Additionally it is also possible for MOTOTRBO radios to support dual mode scan such that they can automatically switch between digital an analogue mode. However, MOTOTRBO radios can not support both channel scan and site roam on the same channel, so if automatic switching between analogue and digital mode (via means of dual mode scan) is required, then the user needs to be able to switch to a channel where site roaming is not enabled.

The second analogue to digital migration strategy is to use an 'Analogue to Digital (A/D) Bridge' as shown in **Figure 11.1** below.

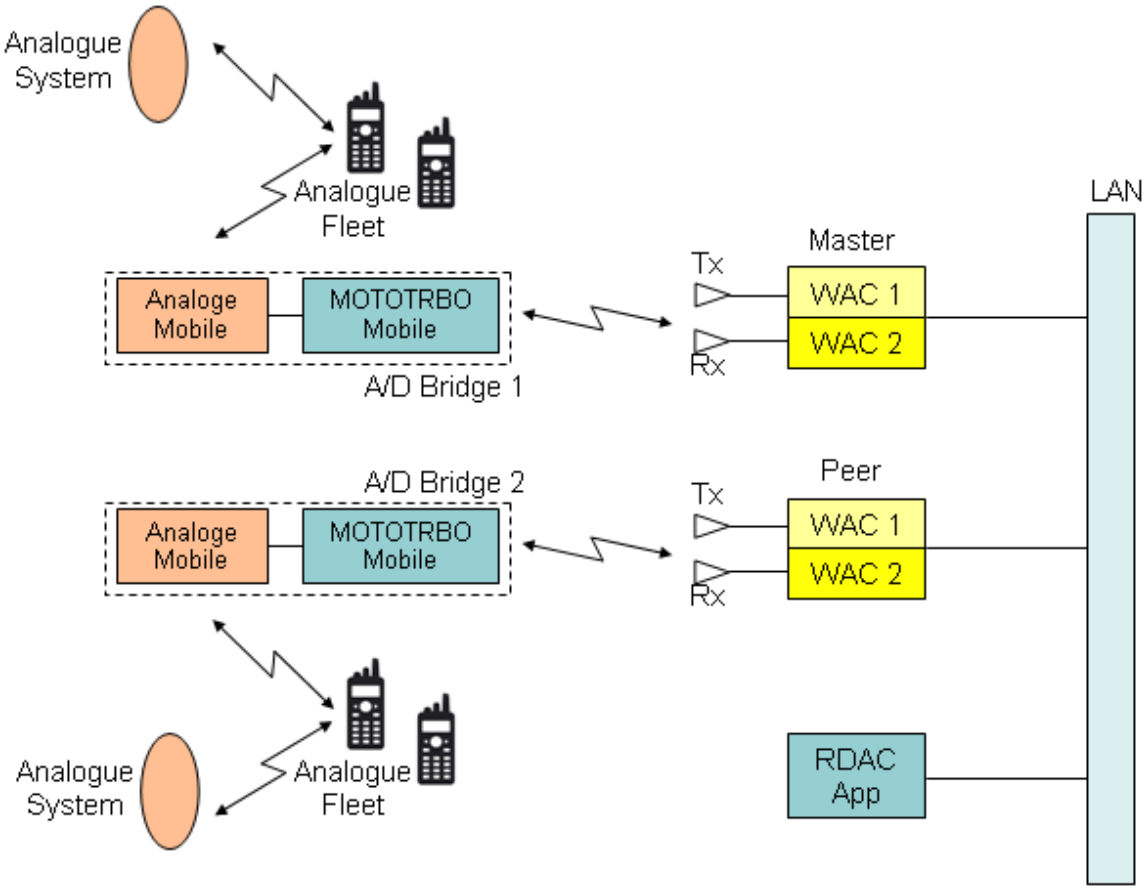


Figure 11.1

An ‘A/D Bridge’ consists of an analogue mobile (or MOTOTRBO mobile in analogue mode) connected via an appropriate lead to a MOTOTRBO mobile in digital mode. The lead itself needs to connect the ‘Rx Audio’ on each mobile to the ‘Tx Audio’ on the other mobile. Additionally, the lead also needs to connect the ’PL/Talkgroup Detect’ on each mobile to the ‘PTT Input’ on the other mobile (note: the MOTOTRBO mobile needs to be configured to make the ‘PL/Talkgroup Detect’ output available on one of the GPIO pins).

For the solution shown in **Figure 11.1**, analogue voice is converted to digital voice by the ‘A/D Bridge’ for transporting over the IP Site Connect system. At the other end, digital voice transported over the IP Site Connect system is converted back to analogue voice by the ‘A/D Bridge’.

There are several ways in which the ‘A/D Bridge’ mobiles can be configured as follows:

- ***Analogue Receive***: the analogue mobiles can be configured to un-mute for carrier, a specified TPL/DPL tone or (one of more) specified select five tone sequences.
- ***Digital Transmit***: the MOTOTRBO mobiles can be configured to transmit a Group Call, Private Call or All Call.
- ***Digital Receive***: the MOTOTRBO mobiles can be configured to un-mute for a Group Call, Private Call or All Call.
- ***Analogue Transmit***: the analogue mobiles can be configured to transmit carrier, a specified TPL/DPL tone or a specified select five tone sequence.

The above configurations enable the required interoperability between the analogue and digital fleets to be defined. Additionally, the IP Site Connect system can be used simply as a backbone by those analogue fleets wishing to communicate among themselves without involving any digital radios. However, it should be remembered that the IP Site Connect system is unable to convey baseband analogue signalling. So for example, once an analogue call has been setup, select five signalling or DTMF live dial digits can not be conveyed over the IP Site Connect system from one ‘A/D Bridge’ device to another.

12. Shared and Dedicated Channel Usage

For single site operation a radio determines if it is permitted to transmit on a given channel based on its configured 'Admit Criteria' and any activity which may already be present on the channel originating either from the radio's own system or (in the case where the channel is a 'shared channel') or from another radio system.

For wide area channel operation (on an IP Site Connect system) a radio is still able to determine if it is permitted to transmit on a given channel based on its configured 'Admit Criteria' and any activity which may already be present on the channel originating from the radio's own system. However, the radio is not able to detect activity originating from other radio systems across the entire wide area channel (which by its nature covers multiple sites). For this reason, when a radio transmits on a wide area channel, any repeater on that wide area channel will refrain from transmitting if it detects an interfering signal from another radio system. Once the interfering signal has disappeared however, the repeater will then commence transmitting.

The threshold at which a repeater determines an interfering signal to be present is configurable using the 'RSSI Threshold' parameter shown in **Figure 12.1** below.

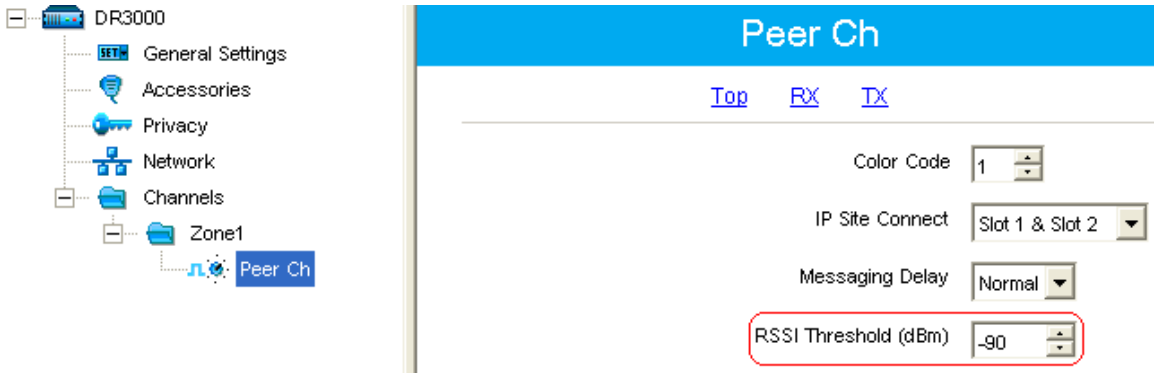


Figure 12.1

If the given repeater is able to operate on a dedicated RF channel (i.e. it is not required to share the channel with another system), then it's strongly recommended that the RSSI Threshold be increased from its default value of -115dBm to -90dBm. This will ensure that interference originating from a number of different sources does not prevent the repeater from transmitting.

If the given repeater is required to operate on a shared RF channel (i.e. it required to share the channel with another system), then consultation with the spectrum regulator is required to determine the optimal threshold.

13. Troubleshooting

If there is no communication between all or some of the IP Site Connect devices, carry out the following checks:

1) Wait for a few minutes in case the IP Site Connect devices are still in the process of trying to establish the link.
2) Try Pinging the Master repeater with a PC from each Peer IP network access point. If this does not work then there is either a problem with the IP network or the Master repeater configuration.
3) For each IP Site Connect device, check that the Radio ID is unique.
4) For each repeater, if the DHCP option is not selected check that the 'Radio IP' and 'IP Site Connect' IP addresses are on different subnets.
5) For the Master repeater, check that the repeater type is set to 'IP Site Master'.
6) For each Peer repeater, check that the repeater type is set to 'IP Site Peer'.
7) For all IP Site Connect devices, check that the Authentication Keys (if enabled) are all the same.
8) For the Master repeater, check that a valid Ethernet IP address is defined and that all Peer devices reference either this IP Address or (where the Master repeater is behind a router) the WAN address of the Master repeater's router.
9) For the Master repeater, check that a valid Gateway IP and Gateway Netmask are defined.
10) For the Master repeater, check that a valid IP Site UDP Port number is defined and that all Peer devices reference this Master UDP Port number.
11) For each Peer device, if the DHCP option is selected check that there is a DHCP Server on the subnet.
12) For each Peer device, if the DHCP option is not selected check that a valid Ethernet address, Gateway IP and Gateway Netmask are defined.
13) For each Peer device, check that a valid IP Site UDP Port number is defined.
14) For each repeater channel, ensure that the 'IP Site Connect' option reflects which slots are required to be part of a wide area channel.
15) For each repeater channel, ensure that the 'Messaging Delay' option reflects the maximum IP network delay (due to propagation, serialisation and handling).
16) For each repeater channel, ensure that the 'RSSI Threshold' is not set so low that interfering signals are causing the repeater to refrain from keying up.

Some typical IP Network issues which may cause problems for IP Site Connect are as follows:

1) Poor audio quality will be experienced if insufficient bandwidth is made available by the IP Network or if there is excessive packet loss / latency. For further details, refer to reference (1).
2) The IP Site Connect system will fail to operate correctly if a static IP Address and UDP Port for the Master repeater are not made available by the IP Network to all Peer devices on the IP Site Connect system.
3) When a Peer device registers with the Master repeater, the IP Network supplies the return IP Address and UDP Port of that Peer device to the Master repeater. The IP Site Connect system will fail to operate correctly if this IP Address and UDP Port are not then made available by the IP Network to all other IP Site connect devices on the IP Site Connect System.
4) If there is a Proxy server which directs all IP devices on a given LAN to a home (or logon) page before they are able to gain access to the WAN, then any repeater on that LAN will be unable to communicate over the WAN (note: repeaters do not support HTML).