

# **InterJak Technical Brief**

## **Wireless Broadband Applications**

**Filinet Corporation**  
757 N. Pastoria Avenue  
Sunnyvale, CA 94087  
408.331.2900

Filinet Europe ApS  
Herlev Hovedgade 82c, 1  
2730 Herlev, Denmark  
+45 44 50 37 70

[www.filinet.com](http://www.filinet.com)

## **InterJak 200 802.11b Wireless Broadband Applications**

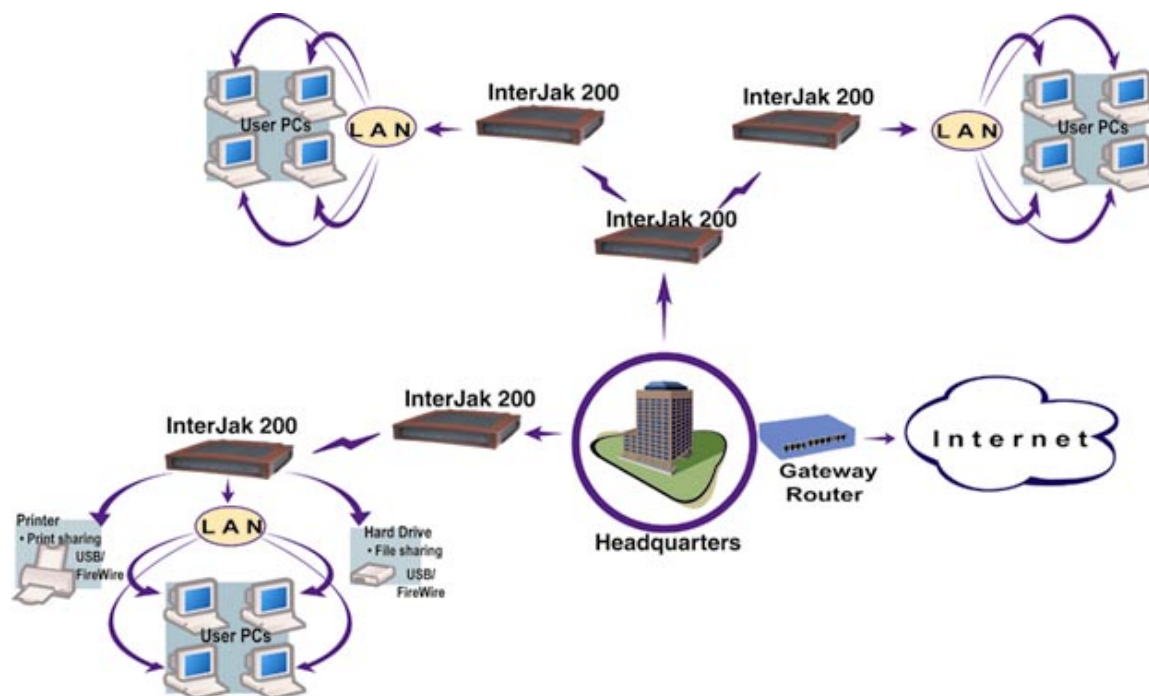
### **Introduction**

This technical brief provides information on wireless broadband applications available with the InterJak 200 802.11b (WAN) product and describes several example configurations for point-to-point and point-to-multipoint wireless links.

For general information on the InterJak Service Appliance product line and services available, please see the main Filanet web site at <http://www.filanet.com>. For access to the InterJak Technical Reference Manual and other application notes, please see the Filanet support section at <http://www.filanet.com/support>.

### **Wireless Applications**

The InterJak 200 802.11b contains a built-in 802.11b wireless interface that supports connection to a variety of specialized external antennas and amplifiers for use in long distance wireless links. It supports two routable Ethernet interfaces for connection to ISP infrastructure or end customer premises equipment. Depending upon the antennas used and a number of other factors, distances of more than 20 miles for point-to-point and point-to-multipoint links are possible.



**Figure 1: Example Wireless Broadband Application**

The InterJak 200 802.11b is based on the IEEE 802.11b 2.4 GHz high-rate wireless networking standard (11 Mbps, with adaptive rate control), and uses Direct Sequence Spread Spectrum (DSSS) CSMA/CA with ACK (and RTS/CTS) for signaling and collision avoidance. The InterJak supports BSS access point, BSS station, and IBSS ad-hoc modes of operation, for flexibility in creating point-to-point and point-to-multipoint wireless networks.

The InterJak can function either as an end node (BSS station) on the wireless network, providing a wireless WAN network connection to a set of local clients, or it can function as an interior wireless network router/concentrator (BSS access point), providing the interface between the wireless network end nodes and an interior wired network. The InterJak 200 802.11b can also serve as an effective wireless router for site-to-site or building-to-building high-speed wireless links.

The end node InterJak can provide any of its services to local clients, including DHCP server, NAT/NAPT, file server, print server, routing, web content filtering, traffic shaping, VPN, etc. The interior InterJak, through full support of static routing and RIP2, and two Ethernet interfaces, can provide robust routing between the wireless WAN and the backbone wired network. See Figure 1 for a simple diagram showing where the InterJak 200 802.11b may fit into wireless networks.

### Some Basic Wireless Terms

**Basic Service Set (BSS)** – A set of wireless stations that communicate with one another. The term BSS is often used to represent an infrastructure BSS, where all wireless stations communicate with a central Access Point (AP). For wireless broadband applications, combinations of BSS stations and BSS access points support both point-to-point and point-to-multipoint applications.

**BSS Access Point (AP)** – The Access Point serves as the central management agent for the BSS and will relay traffic between BSS stations if necessary (i.e. multipoint capability).

**BSS Station** – One or more stations will join a BSS created by the Access Point, and for wireless broadband applications will serve as the customer premises end-points for wireless point-to-point/multipoint links.

**Independent Basic Service Set (IBSS)** – In an Independent BSS, all stations communicate directly with one another (no central access point). For wireless broadband applications, this mode can support only point-to-point links, and is generally used only for special applications.

**Direct Sequence Spread Spectrum (DSSS)** – High Rate (HR) DSSS is specified in the IEEE 802.11b 2.4 GHz standard. The HR/DSSS PHY (physical interface) provides extended data rates of 5.5 Mbps and 11 Mbps, as well as a rate-shift mechanism to interoperate with older 802.11 DSSS equipment.

**Frequency Hopped Spread Spectrum (FHSS)** – This is an alternative PHY mechanism used by some wireless broadband equipment. A channel agility option allows FHSS 1 Mbps and 2 Mbps wireless networks to interoperate with HR/DSSS 11 Mbps wireless networks without interfering with each other. In North America channels 1, 6, and 11 are specified for non-overlapping networks.

**CSMA/CA** – CSMA/CA stands for carrier sense multiple access with collision avoidance. This is very similar to the mechanism used in IEEE 802.3, except that CSMA/CA uses additional mechanisms for collision avoidance (to aid in reducing the chance of wireless collisions).

**Request To Send/Clear To Send (RTS/CTS)** – This optional signaling may be enabled on BSS stations in heavily loaded point-to-multipoint applications. RTS/CTS adds some overhead to the wireless network, but offers the ability to reserve the wireless medium for short periods of time (in order to help reduce wireless collisions).

**Service Set Identity (SSID)** – The SSID represents a unique wireless “network name”, and is used so that stations can join a particular BSS. Each wireless network should use a unique SSID. On the InterJak 200 802.11b, the *Network name* is the same as the SSID, and both access points and stations in a particular wireless network should use the same name.

**Point-to-Point Wireless** – Consists of a single fixed wireless link between two sites. For example, this could be a dedicated long distance wireless link between an ISP’s infrastructure and an end customer site.

**Point-to-MultiPoint Wireless** – Consists of fixed wireless links between multiple end wireless stations and a single central wireless access point. The access point is responsible for repeating traffic between end wireless stations if necessary.

---

## Basic Services

In addition to basic wireless routing capabilities, the InterJak 200 802.11b supports a variety of standard networking services.

*Firewall:* Stateful, dynamic firewall with built-in URL filtering.

*File/Print Server:* USB and IEEE 1394 ports enable plug-n-play of hard disks and printers.

*DHCP:* Dynamic Host Configuration Protocol server and client capabilities manage and assign IP addresses and settings on LAN and WAN interfaces.

*Network Address Translation:* Network Address Port Translation (NAPT), and Multi-NAT map internal to external addresses.

*IP Routing:* Routing between Ethernet and wireless interfaces. Supports static routes, as well as RIP1 and RIP2.

*Management Services:* Complete set of management and monitoring tools for secure local and remote configuration, provisioning, and monitoring.

*DMZ Support:* Dedicated LAN segment supporting public hosts while private data is secured on a separate LAN segment.

---

## Optional Services

In addition to basic services, a number of optional value-add services are available for the InterJak 200 802.11b.

*VPN:* IPSec client-to-site and site-to-site, and PPTP server support securely and cost effectively connect remote offices and remote users over the Internet to resources on local networks. Also allows secure connections for remote trouble-shooting and configuration at the customer premises.

*Content Filtering:* Web Content Filtering to manage web usage for businesses and schools.

*Traffic Shaping:* Prioritize network traffic to ensure good response time for particular applications. Offers ability to bandwidth-limit wireless connections.

*Network Monitoring:* Provides statistics, status, and graphs of your network traffic. SNMP trap load thresholds can be configured.

*Email Server:* Full e-mail server relaying and receiving Internet e-mail. Able to fetch mail from other servers and provide central inbox.

*Service Provisioning Portal (SPP):* Provides a separate web-based management application supporting remote provisioning, management, and monitoring of large numbers of InterJak appliances.

---

## Security

The InterJak 200 802.11b supports several features to aid in securing wireless WAN links.

*Wireless Network Name (SSID):* Each wireless access point (generally used on the infrastructure side of a wireless link) must have a wireless network name and channel number assigned. By making the wireless network name unique (and enabling the “Closed Wireless Network” option), casual discovery and snooping is made much more difficult.

*Closed Wireless Network Option:* The Closed Wireless Network option prevents the InterJak 200 802.11b from broadcasting its wireless network name (SSID), and prevents wireless clients from probing the InterJak for this name.

*Firewall Rules:* Custom firewall rules can restrict access on a wireless link to particular network ports and can limit source and destination IP addresses or subnets.

*Optional VPN Service:* Support for IPSec and PPTP tunnels over a wireless link allows for secure authentication and encryption.

---

## **Remote Management and Monitoring**

Secure remote management is supported through the built-in Java applet encrypted Filanet Web Management Interface, through simple configuration file downloads, through a telnet CLI (Command Line Interface), or through the Service Provisioning Portal (SPP) service.

It is also possible to monitor the wireless configuration, status, and statistics of the InterJak 200 802.11b through the InterJak Web Management Interface, SNMP, or a telnet session.

**Web Management Interface:** You can connect to the InterJak locally or remotely (if enabled in the InterJak firewall settings), with all operations through the Web Management Interface encrypted via a Java applet (ensuring a secure connection). You can view current wireless configuration information on the wireless networking page, as well as open a pop-up web signal/link/noise window. Under the monitor web page you may view wireless transmit and receive statistics. With the network monitor service (optional service), you may view custom graphs of wireless load and performance as well as create SNMP trap thresholds.

**SNMP:** Using tools such as HP OpenView or SolarWinds you may view SNMP status/statistics of the InterJak wireless interface either locally or remotely (if SNMP is enabled on the InterJak).

**Telnet:** You can connect to the InterJak locally or remotely (if enabled in the InterJak firewall settings) by doing a telnet CLI (command line interface) session to the IP address of the InterJak. The “wlan” CLI command displays the current settings and statistics of the wireless interface on the InterJak. Note: All information sent over the telnet session is clear text. For a more secure remote telnet CLI session, run telnet over a VPN/PPTP tunnel to the InterJak (optional service).

---

## **Automated InterJak Configuration**

It is possible to automate and pre-configure the InterJak 200 802.11b for customer installation. From the InterJak web management interface, under *System:Maintenance*, it is possible to download the current InterJak configuration, upload new configurations, or configure the InterJak to automatically poll for new configuration settings from an external server.

For larger deployments, Filanet’s Service Provider Portal (SPP) can support configuration, provisioning, and management of many InterJak appliances. This can be used in conjunction with a custom InterJak CD-ROM based installation program to fully automate deployment of the InterJak 200 802.11b. Please contact Filanet for additional information on SPP and custom CD-ROM installation options.

Please see the Filanet InterJak Technical Reference Manual for more information on automating and pre-configuring the installation of the InterJak product line.

---

## **Traffic Shaping**

The InterJak traffic shaping optional service allows for traffic prioritization, traffic overload protection, and maximum bandwidth limits for wireless and wired connections. For wireless links, this is

particularly useful for supporting bandwidth service agreements, preventing overload of wireless links, and balancing point-to-multipoint configurations.

Please see the traffic shaping example towards the end of this technical brief. For more information, please refer to the InterJak web management on-line help and Technical Reference Manual.

---

## Performance

The InterJak 200 802.11b supports the full 11 Mbps 802.11b standard. In end customer long distance links, performance of up to 6 Mbps has been measured, with typical performance of 3 to 4 Mbps (over links of up to 20 miles).

Overall performance will vary somewhat, depending upon a number of factors:

- Quality and gain of external antenna equipment
- Alignment and tuning of directional antennas
- Length of cable feeds and loss in connectors
- Interference from other 2.4 GHz sources
- Use of external amplifiers

---

## Equipment

The InterJak 200 802.11b allows for simple connection to cable feeds, external antennas, and amplifiers. The InterJak will either come with an included pigtail (to N-type male), a MMCX connector, or a RP SMA connector for third-party standard N-type pigtail cables.

**Note:** An optional rack-mount kit is available for the InterJak 200 802.11b.

A popular source for pigtail cables, cable feeds, external antennas, and amplifiers is HyperLinkTech ([www.hyperlinktech.com](http://www.hyperlinktech.com)). A typical set of equipment needed for each side of a wireless link includes:

- *Pigtail cable:* Either a pigtail to N-type male will be included, or a MMCX (or RP SMA) to N-type pigtail cable can be purchased.
- *Cable feed:* LMR-400 cable or similar is recommended, with better performance (less cable loss) resulting from shorter cable runs. A typical cable feed will be terminated with N-type connectors.
- *External antenna:* An external 2.4 GHz antenna is necessary for outdoor installations (usually terminated with an N-type connector). Depending upon the installation, antenna choices include parabolic grid, yagi, omni-directional, path, or grid antennas. Please refer to technical references on antenna applications for more information on antenna selection, installation, and alignment.
- *Optional lightning protector:* Depending upon the installation, a lightning protector may be necessary.
- *Optional bi-directional signal amplifier:* Depending upon the wireless link distance, loss in cable feeds, and type of antennas, an external bi-directional signal amplifier may be needed. For most wireless links, an external signal amplifier is not necessary.

---

## Installation

For installation of the InterJak 200 802.11b, it is best to refer to technical sources for advice on antenna alignment and installation. Some general recommendations for installations include:

- Ensure a clear line-of-site from the infrastructure site to the customer premises. Anything obstructing a clear-line of site will affect distance and performance.
- Keep the wireless cable feed as short as possible. It is much better to run a longer CAT5 Ethernet cable and ensure a short wireless cable feed.
- Protect the InterJak 200 802.11b from environmental elements. The InterJak is a solid-state device, and can withstand wide environmental conditions, but the InterJak must be protected from outdoor elements.
- Install and provision the InterJak 200 802.11b (and antenna) on the infrastructure side of a wireless link before installing at the customer premises. The InterJak on the infrastructure side may be configured in “Infrastructure Access Point” mode, along with a Network Name and Channel Number. Also networking and routing should be properly configured on this InterJak before installing at the customer premises.
- Install the InterJak 200 802.11b (and antenna) on the customer premises side of a wireless link next. This InterJak will be configured as an “Infrastructure Station”. By setting the wireless Network Name to that configured on the infrastructure-side InterJak, the station InterJak will automatically attempt to scan channels and associate with the access point InterJak. A pop-up “Signal Quality” web page is available on the station (showing Link, Signal, and Noise graphs) to aid in aligning antennas.
- The installation may be checked from the customer premises side via a laptop connected to an InterJak Ethernet port. First ping the IP address of the local InterJak Ethernet port, followed by the local InterJak wireless port, then the remote InterJak wireless port and remote InterJak Ethernet port.
- If basic networking settings are configured properly on both InterJaks (including routes if necessary), and the station has associated with the access point, it is then possible to perform additional web based configuration of either InterJak by typing the IP address of each InterJak into a standard web browser.

---

## FCC Regulations

The InterJak 200 802.11b itself has been tested for FCC certification. This does not guarantee that a complete configuration of InterJak, cable feed, optional external amplifier, and directional antenna will meet FCC requirements. It is the responsibility of the party using the InterJak to ensure FCC compliance. Please refer to specific FCC (or other certification agency) requirements for details on limits.

In general, the InterJak 200 802.11b may be used with most third-party external antennas without issues, as long as an external amplifier is not used. Use of an external amplifier requires careful selection of amplifier and external antenna gain, and cabling.

A couple of web links describing practical FCC and antenna selection information:

[http://www.ins.com/papers/FCCPart15\\_and\\_the\\_ISM\\_2.4G\\_Band.index](http://www.ins.com/papers/FCCPart15_and_the_ISM_2.4G_Band.index)  
<http://www.ins.com/papers/BAWUG-antenna101/img0.htm>

---

## Equipment Compatibility

The InterJak 200 802.11b follows the IEEE 802.11b high-rate standard (2.4 GHz, HR/DSSS, 11 Mbps). It supports both IBSS (ad-hoc) and BSS (access point and station) modes of operation, allowing operation with all devices following the 802.11b standard.

The InterJak 200 802.11b can interoperate with other wireless broadband equipment that follows the 802.11b standard (and operate in standard IBSS ad-hoc, BSS station, or BSS access point modes of operation). Please contact Filanet for specific questions related to equipment interoperability.

---

## Configuration Examples

The following sections illustrate basic example wireless network configurations supporting point-to-point and point-to-multipoint links between InterJak 200 802.11b devices.

First, basic wireless configuration settings are explained, and an example wireless point-to-point test configuration is described. Next, more representative configurations describing point-to-point and point-to-multipoint routed wireless connections are illustrated and explained.

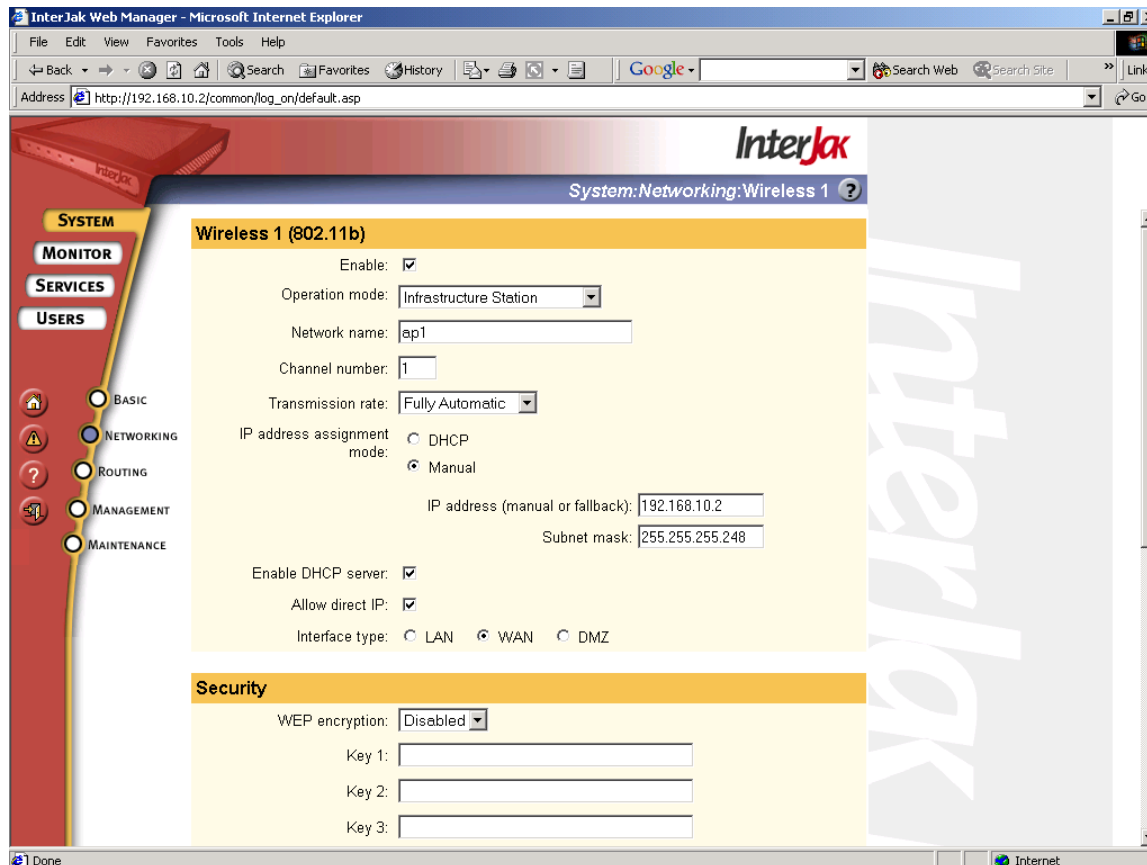
---

## Basic Wireless Settings

This section introduces the basic wireless settings available on the InterJak 200 802.11b. There are a number of other settings that must be configured on the InterJak 200 802.11b in order to create a wireless link between two networks. The detailed steps described for each wireless configuration illustrated in following sections will cover these settings. Please also refer to the Filanet Technical Reference Manual (included with the InterJak 200 802.11b) for detailed information on the services supported by the InterJak product line.

Figure 2 below is a screen shot of the upper section of the InterJak 200 802.11b wireless configuration screen. This is a screen from the web based management interface of the InterJak 200 802.11b. The login page for this web management interface may be loaded by running the Filanet Administrator's Client and double-clicking on the InterJak listed, or by typing the IP address of the InterJak into a web browser.

After logging into the InterJak web management interface, InterJak wireless specific settings are available under *System:Networking:Wireless 1*. **Note:** The InterJak Quick Setup will configure some of the InterJak wireless settings, but for wireless point-to-point and point-to-multipoint installations, it is necessary to go to the *Wireless 1* management page to fully configure the wireless interface.

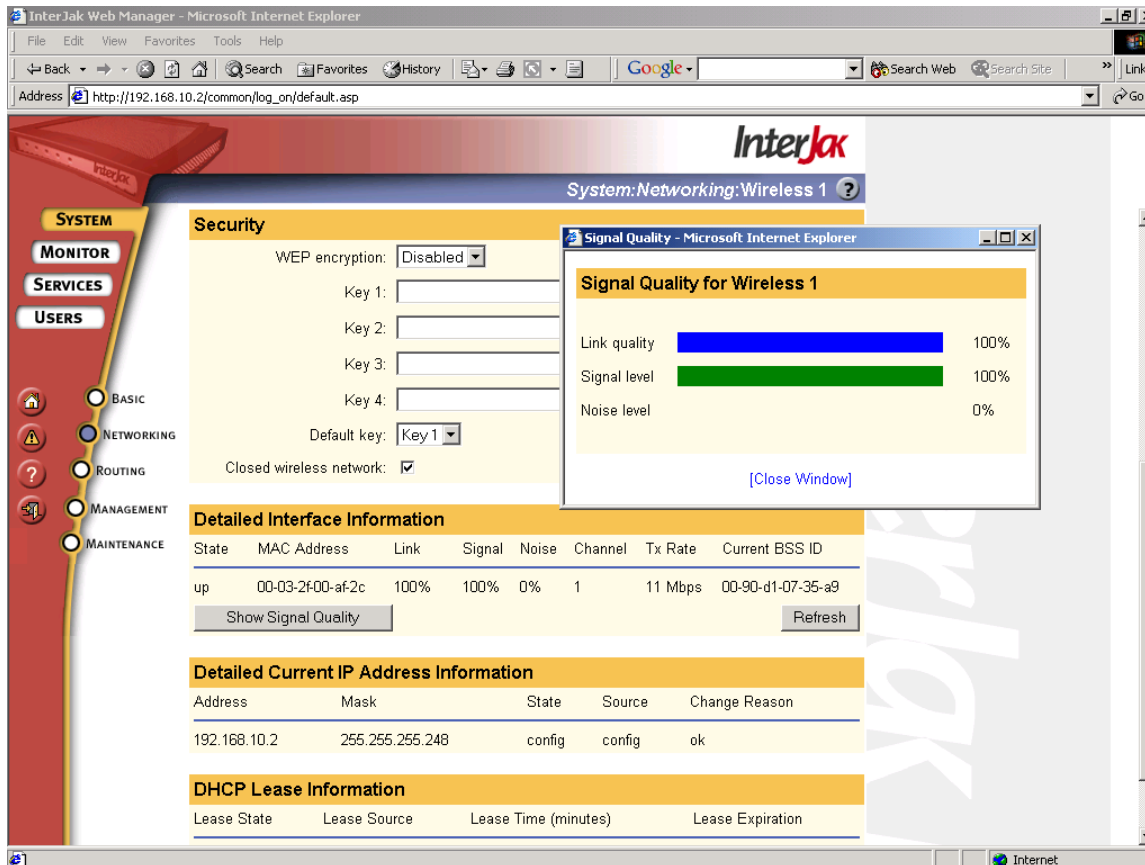


**Figure 2: Wireless Web Management Page (basic settings)**

### Basic Wireless Settings

- **Enable:** Turns the 802.11b interface ON or OFF.
- **Operation Mode:** This selects the wireless network mode or type. For a wireless broadband link, the InterJak 200 802.11b on the infrastructure (interior) side of a connection would normally be configured in Infrastructure Access Point operation mode. The InterJak 200 802.11b on the customer premises would normally be configured in Infrastructure Station mode.
- **Network Name:** This is the group name of the wireless network – in 802.11b terms, it is the SSID. All wireless stations communicating with each other must be configured with the same name. Note that the network name is case sensitive, and must be unique if running several collocated wireless networks.
- **Transmission Rate:** Select the transmission rate. This should be 'Fully Automatic' unless there are some special requirements to set a specific rate.
- **Channel Number:** This is the radio channel number (i.e. the radio frequency) that will be used for wireless transmissions. Choose a value from 1 to 11. If collocating several wireless networks, try for separation of three or four channels.
- **IP Address Assignment Mode:** Select either DHCP or manual addressing. In a wireless WAN configuration, you will most likely specify a manual IP address for an interior InterJak's wireless interface, but could get the address via DHCP if the InterJak is functioning as an end node.
- **IP Address and Subnet mask:** Specifies the IP address and subnet mask, used as the manual IP address (if manual IP addressing is selected) or the fallback IP address (if DHCP addressing is selected).

- *Enable DHCP server*: If checked, the InterJak will act as a DHCP server on the wireless interface. In a wireless WAN application, it is likely that IP addresses will be manually assigned, so the DHCP server will not be enabled.
- *Allow Direct IP*: If checked, this allows an Administrator Client, connecting via the wireless interface, to force the InterJak to a specific IP address on this interface, so that the administrator can communicate with the InterJak during initial installation. See “Forcing an IP Address with Direct IP” in the InterJak Technical Reference Manual. This will typically not be used in a wireless WAN application.
- *Interface Type*: This selects the firewall and network address translation (NAT/NAPT) rules to use for the wireless segment.



**Figure 3: Wireless Web Management Page (security, detailed interface information, signal quality)**

The *System:Networking:Wireless 1* screen (figure 3) also contains settings for the 802.11b security features:

### Security

- *Enable*: Turns WEP encryption ON or OFF for the wireless interface. This is normally not used for point-to-point and point-to-multipoint connections.
- *Closed wireless network*: Prevents the InterJak from broadcasting its network name, making it more difficult to scan for the network (helping prevent outside intrusion).

**Note:** Additional security is available through use of firewall rules and the optional VPN service.

The *System:Networking:Wireless 1* screen displays information on the interface status and current IP settings:

### Detailed Interface Information

- *State*: up/down/pending (pending DHCP results)
- *MAC Address*: The MAC address of the InterJak's wireless interface.
- *Link*: Indicates the current wireless link quality, as a value from 0 to 100%; a low value indicates a large number of bad packets are being detected at the radio level, possibly caused by radio interference or reflections. This value is not displayed when in Access Point mode.
- *Signal*: Indicates the current radio signal strength, as a value from 0 to 100%. This value is not displayed when in Access Point mode.
- *Channel*: The current radio channel number. When in Access Point mode, this will reflect the manually configured setting. When in Station mode, this will reflect the channel number configured on the InterJak access point it has associated with.
- *TxRate*: The transmission rate. This value is not displayed for an Access Point, which may be communicating with multiple stations at various speeds.
- *Current BSS ID*: This is the MAC address of the Access Point in an infrastructure mode network.

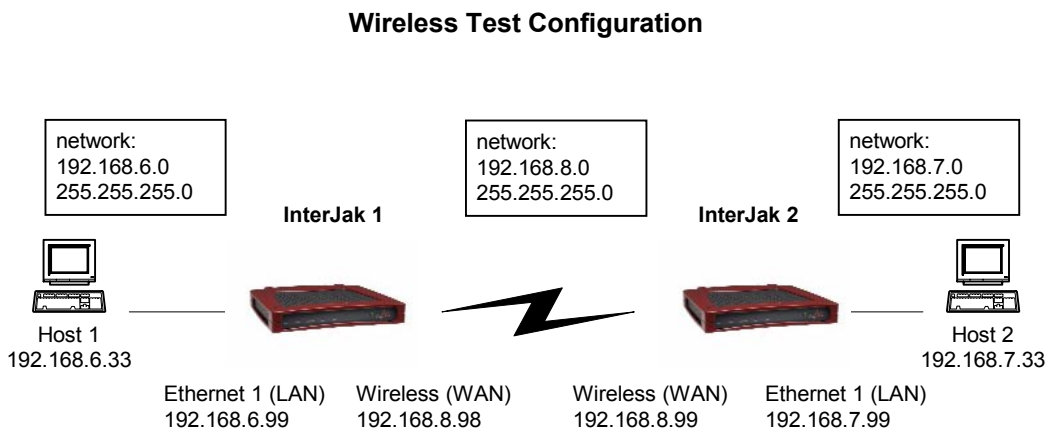
### Detailed Current IP Address Information

- *Address*: The current IP address of the wireless interface.
- *Mask*: The current subnet mask on the wireless interface.
- *State*: Current state of IP address (down/dhcp/config/forced)
- *Source*: How the IP address was assigned (dhcp/config/forced)
- *DHCP Lease Information*: This shows the status of any DHCP leases on this interface.

---

### Basic Wireless Test Configuration

A simple controlled configuration for testing and provisioning is shown in figure 4. The two InterJak 200 802.11b products may be set up together in a lab or office (using the included simple omnidirectional antenna), or may be connected to external directional antennas for testing over longer distances.



**Figure 4: Basic Wireless Test Configuration**

## Equipment

- Two Windows PC hosts, with Ethernet interfaces (Host 1, Host 2)
- Two InterJak 200 802.11b products (InterJak 1, InterJak 2)
- Included simple omni-directional antennas, or external antenna equipment
- Two Ethernet crossover cables for direct connect between PCs and InterJaks

### 1) Configure IP settings on two Windows PC hosts.

- PC Host 1 IP address of 192.168.6.33, subnet of 255.255.255.0, and default gateway of 192.168.6.99.
- PC Host 2 IP address of 192.168.7.33, subnet of 255.255.255.0, and default gateway of 192.168.7.99

### 2) Connect PC Hosts to InterJaks

- Connect Ethernet crossover between Host 1 and InterJak 1 (Ethernet 1 port)
- Connect Ethernet crossover between Host 2 and InterJak 2 (Ethernet 1 port)
- Power-on both InterJaks

### 3) Configure InterJak 1

- Run Filanet Windows Administrator's Client on PC Host 1 to discover InterJak 1, and then double-click on listed InterJak to force useable IP address.
- Log into InterJak (following Quick Setup instructions). After running through Quick Setup (if it comes up), ensure the following steps are performed.
- Under *System*, under *System Information*, click on the *Edit* button, and enter information here such as *Windows workgroup* of wireless, *Server name* of InterJak1, etc.
- Under *Services:Firewall*, click on *Edit* and deselect the *Enable firewall* checkbox, and click *Apply*. This disables the firewall so that all traffic can pass through the WAN interface (custom firewall rules can be added later to further secure the wireless link).
- Under *Services:Address Translation (NAT/NAPT)*, click on *Edit* and deselect both *Enable NAPT* options at the top of the page, and click *Apply*. This disables NAPT between LAN and WAN, allowing standard routing.
- Under *Services:Networking:Ethernet 1*, choose the following settings and then click *Apply*:

*Enable* button selected

*IP address assignment* of Manual

*IP address* of 192.168.6.99

*Subnet mask* of 255.255.255.0

*Enable DHCP server* deselected

*Allow direct IP* selected

- Under *Services:Networking:Wireless 1*, choose the following settings and then click *Apply*:

*Enable* button selected

*Operation Mode* of Infrastructure Access Point

*Network name* of InterJakTest (or any other unique text)

*Channel number* of 6 (or any other unused wireless channel number)

*IP address assignment* of Manual

*IP address* of 192.168.8.98

*Subnet mask* of 255.255.255.0

*Enable DHCP server* deselected

*Allow direct IP* selected

*Interface Type* of WAN

- Under *System:Routing*, under *Default Gateway*, click on *Edit*, and enter the *Gateway address* of 192.168.8.99 (wireless interface of InterJak 2).

**Note:** Alternatively, leave the *Default Gateway* blank, click on the *Add Route* button, enter *Destination subnet address* of 192.168.7.0, *Destination subnet mask* of 255.255.255.0, *Interface of Gateway*, and *Gateway address* of 192.168.8.99.

#### 4) Configure InterJak 2

- Run Filanet Windows Administrator's Client on PC Host 2 to discover InterJak 2, and then double-click on listed InterJak to force useable IP address.
- Log into InterJak (following Quick Setup instructions). After running through Quick Setup (if it comes up), ensure the following steps are performed.
- Under *System*, under *System Information*, click on the *Edit* button, and enter information here such as *Windows workgroup* of wireless, *Server name* of InterJak2, etc.
- Under *Services:Firewall*, click on *Edit* and deselect the *Enable firewall* checkbox, and click *Apply*. This disables the firewall so that all traffic can pass through the WAN interface (custom firewall rules can be added later to further secure the wireless link).
- Under *Services:Address Translation (NAT/NAPT)*, click on *Edit* and deselect both *Enable NAPT* options at the top of the page, and click *Apply*. This disables NAPT between LAN and WAN, allowing standard routing.
- Under *Services:Networking:Ethernet 1*, choose the following settings and then click *Apply*:

<i>Enable</i> button selected
-------------------------------

<i>IP address assignment</i> of Manual
--

<i>IP address</i> of 192.168.7.99
-----------------------------------

<i>Subnet mask</i> of 255.255.255.0
-------------------------------------

<i>Enable DHCP server</i> deselected
--------------------------------------

<i>Allow direct IP</i> selected
---------------------------------

- Under *Services:Networking:Wireless 1*, choose the following settings and then click *Apply*:

<i>Enable</i> button selected
-------------------------------

<i>Operation Mode</i> of Infrastructure Station
---

<i>Network name</i> of InterJakTest (same name configured for InterJak 1)
---

<i>Channel number</i> of 6 (for station mode, does not matter, as the channel will be automatically picked up from the InterJak access point)
---

<i>IP address assignment</i> of Manual
--

<i>IP address</i> of 192.168.8.99
-----------------------------------

<i>Subnet mask</i> of 255.255.255.0
-------------------------------------

<i>Enable DHCP server</i> deselected
--------------------------------------

<i>Allow direct IP</i> selected
---------------------------------

<i>Interface Type</i> of WAN
------------------------------

- Under *System:Routing*, under *Default Gateway*, click on *Edit*, and enter the *Gateway address* of 192.168.8.98 (wireless interface of InterJak 1).

**Note:** Alternatively, leave the *Default Gateway* blank, click on the *Add Route* button, enter *Destination subnet address* of 192.168.6.0, *Destination subnet mask* of 255.255.255.0, *Interface of Gateway*, and *Gateway address* of 192.168.8.98.

#### Testing the Wireless Network

- From PC Host 2, log into InterJak 2, and go to *System:Networking:Wireless 1*. Under *Detailed Interface Information*, *State* should show up, values under *Link*, *Signal*, *Noise*, *Channel*, *Tx Rate*, and *Current BSSID* should look valid. Click on *Show Signal Quality* button to view a dynamic web pop-up window showing current Signal/Link/Noise values.

**Note:** Under InterJak 1, since it is configured as the Access Point, it will not show values under *Link*, *Signal*, *Noise*, or *Tx Rate*, so it is much better to use the InterJak configured as Station to check/tune the wireless link.

- From PC Host 1, open a command prompt, and perform the following commands:
  - ping 192.168.6.99** (address of InterJak 1 Ethernet interface)
  - ping 192.168.8.98** (address of InterJak 1 wireless interface)
  - ping 192.168.8.99** (address of InterJak 2 wireless interface)
  - ping 192.168.7.99** (address of InterJak 1 Ethernet interface)
  - ping 192.168.7.33** (address of PC Host 2)
  - tracert -d 192.168.7.33** (address of PC Host 2)

If any of these fail, check to make sure the firewall and NAT/NAPT is disabled on both InterJaks, routes or default gateways are configured properly on both InterJaks, the wireless interfaces are configured properly, and the end PC Hosts are configured properly.

## Remote Management

- To locally manage and monitor InterJak 1 from Host 1, perform one of the following:
  - Web Management Interface:** Type 192.168.6.99 into a web browser
  - Telnet CLI (Command Line Interface):** At a command prompt, type “telnet 192.168.6.99”
  - Telnet Syslog:** At a command prompt, type “telnet 192.168.6.99 24”
- To remotely manage and monitor InterJak 2 from Host 1, perform one of the following:
  - Web Management Interface:** Type 192.168.8.99 into a web browser
  - Telnet CLI (Command Line Interface):** At a command prompt, type “telnet 192.168.8.99”
  - Telnet Syslog:** At a command prompt, type “telnet 192.168.8.99 24”

**Note:** All data passed over the InterJak Web Management Interface is encrypted via a Java applet, while all data passed over the telnet sessions are clear text. Use the optional InterJak VPN/PPTP service to support secure remote telnet sessions.

---

## Fully Routed Wireless Configuration

An example point-to-multipoint routed configuration is shown in figure 5. One InterJak 200 802.11b serves as an access point at the wired infrastructure. Two additional InterJak stations provide wireless connections to the customer premises. In this example configuration, a small pool of public IP addresses are provided to the customer premises, while private IP addresses are used for the wireless link.

### Equipment

- Three InterJak 200 802.11b products (InterJak 1, InterJak 2, InterJak 3)
- External antenna equipment for wireless links
- Infrastructure networking equipment, including Internet router
- Customer premises networking hosts

#### 1) **Configure Internet router (on wired infrastructure)**

- Route to net 216.35.139.64, subnet 255.255.255.248, and gateway 216.35.139.1 (InterJak 1).

#### 2) **Connect InterJak 1 to infrastructure and antenna**

- Connect InterJak Ethernet 1 interface to wired infrastructure
- Connect InterJak wireless interface to antenna equipment (via pigtail cable)
- Power-on InterJak 1

### Example Configuration (Fully Routed)

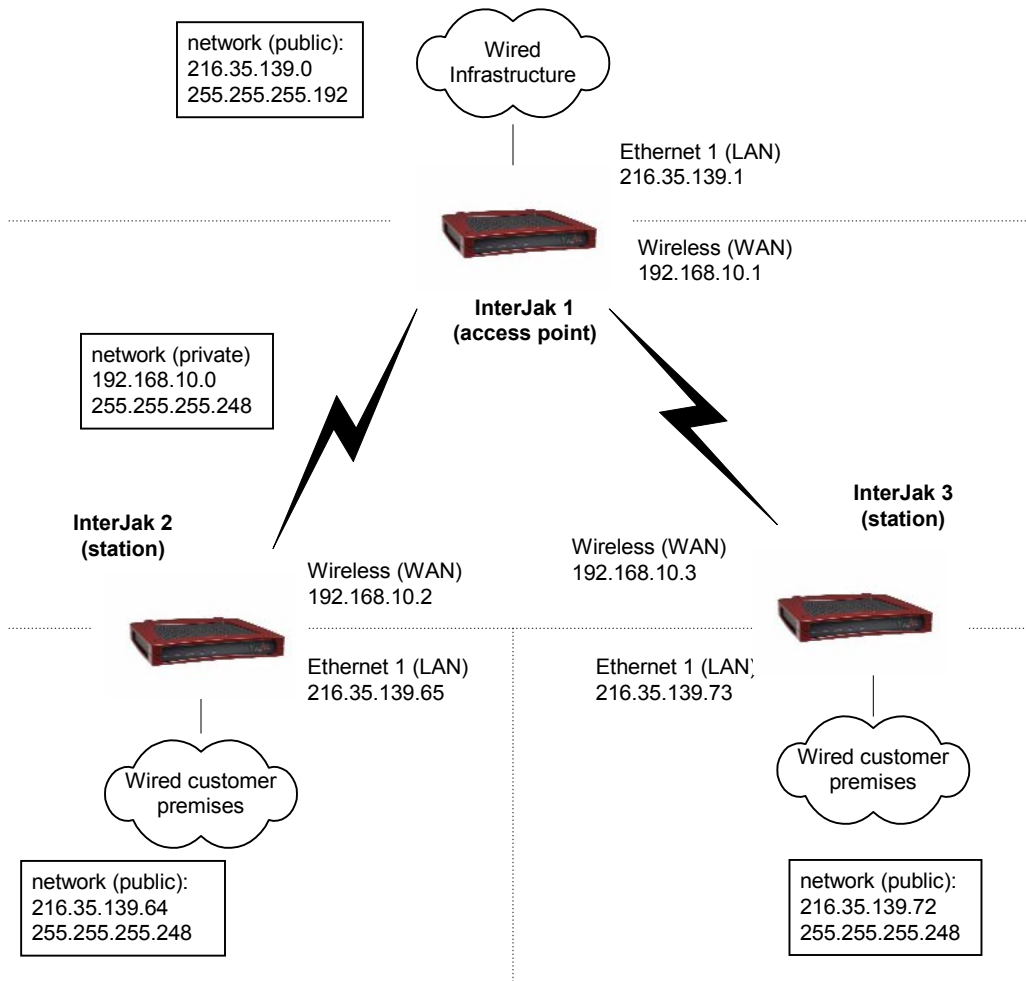


Figure 5:

### Example Routed Wireless Test Configuration

#### 3) Configure InterJak 1

- Under *System*, under *System Information*, click on the *Edit* button, and enter information here such as *Windows workgroup* of wireless, *Server name* of InterJak1, etc.
- Under *Services:Firewall*, click on *Edit* and deselect the *Enable firewall* checkbox, and click *Apply*. This disables the firewall so that all traffic can pass through the WAN interface (custom firewall rules can be added later to further secure the wireless link).
- Under *Services:Address Translation (NAT/NAPT)*, click on *Edit* and deselect both *Enable NAPT* options at the top of the page, and click *Apply*. This disables NAPT between LAN and WAN, allowing standard routing.
- Under *Services:Networking:Ethernet 1*, choose the following settings and then click *Apply*:

<i>Enable</i> button selected
<i>IP address assignment</i> of Manual
<i>IP address</i> of 216.35.139.1
<i>Subnet mask</i> of 255.255.255.192 (net of 64)

- |                                      |
|--------------------------------------|
| <i>Enable DHCP server</i> deselected |
| <i>Allow direct IP</i> selected      |
- Under *Services:Networking:Wireless 1*, choose the following settings and then click *Apply*:
 

<i>Enable</i> button selected
<i>Operation Mode</i> of Infrastructure Access Point
<i>Network name</i> of InterJakRouted (or any other unique text)
<i>Channel number</i> of 6 (or any other unused wireless channel number)
<i>IP address assignment</i> of Manual
<i>IP address</i> of 192.168.10.1
<i>Subnet mask</i> of 255.255.255.248 (net of 8)
<i>Enable DHCP server</i> deselected
<i>Allow direct IP</i> selected
<i>Interface Type</i> of WAN
  - Under *System:Routing*, under *Default Gateway*, click on *Edit*, and enter the *Gateway address* of the wired infrastructure Internet router.
  - Under *System:Routing*, click on the *Add Route* button, enter *Destination subnet address* of 216.35.139.64, *Destination subnet mask* of 255.255.255.248, *Interface* of Gateway, and *Gateway address* of 192.168.10.2. This adds a route to the public net at InterJak 2.
  - Under *System:Routing*, click on the *Add Route* button, enter *Destination subnet address* of 216.35.139.72, *Destination subnet mask* of 255.255.255.248, *Interface* of Gateway, and *Gateway address* of 192.168.10.3. This adds a route to the public net at InterJak 3.
- 4) **Install InterJak 2**
- Connect InterJak Ethernet 1 interface to customer network (e.g. switch on wired network)
  - Connect InterJak wireless interface to antenna equipment (via pigtail cable)
  - Power-on InterJak 2
- 5) **Configure PC hosts**
- Configure customer PC hosts with static IP addresses in range 216.35.139.66-71, subnet address of 255.255.255.248, gateway of 216.35.139.65, and proper external DNS servers.  
**Note:** It is possible to use DHCP server capability on InterJak 2 to automatically supply IP addresses, gateway, and DNS servers.
- 6) **Configure InterJak 2**
- Under *System*, under *System Information*, click on the *Edit* button, and enter information here such as *Windows workgroup* of wireless, *Server name* of InterJak2, etc.
  - Under *Services:Firewall*, click on *Edit* and deselect the *Enable firewall* checkbox, and click *Apply*. This disables the firewall so that all traffic can pass through the WAN interface (firewall may be enabled later to protect customer premises).
  - Under *Services:Address Translation (NAT/NAPT)*, click on *Edit* and deselect both *Enable NAPT* options at the top of the page, and click *Apply*. This disables NAPT between LAN and WAN, allowing standard routing.
  - Under *Services:Networking:Ethernet 1*, choose the following settings and then click *Apply*:
 

<i>Enable</i> button selected
<i>IP address assignment</i> of Manual
<i>IP address</i> of 216.35.139.65
<i>Subnet mask</i> of 255.255.255.248 (net of 8)
<i>Enable DHCP server</i> deselected
<i>Allow direct IP</i> selected
- Note:** DHCP server may be enabled, along with custom DHCP server address pool, to automatically provide IP addresses to customer premises PC hosts (see DHCP Service)
- Under *Services:Networking:Wireless 1*, choose the following settings and then click *Apply*:
 

<i>Enable</i> button selected
-------------------------------

<i>Operation Mode</i> of Infrastructure Station
<i>Network name</i> of InterJakRouted (same name configured for InterJak 1)
<i>Channel number</i> of 6 (for station mode, does not matter, as the channel will be automatically picked up from the InterJak access point)
<i>IP address assignment</i> of Manual
<i>IP address</i> of 192.168.10.2
<i>Subnet mask</i> of 255.255.255.248 (net of 8)
<i>Enable DHCP server</i> deselected
<i>Allow direct IP</i> selected
<i>Interface Type</i> of WAN

- Under *System:Routing*, under *Default Gateway*, click on *Edit*, and enter the *Gateway address* of 192.168.10.1 (wireless interface of InterJak 1).
- **Optional:** Under *System:Routing*, click on the *Add Route* button, enter *Destination subnet address* of 216.35.139.72, *Destination subnet mask* of 255.255.255.0, *Interface* of Gateway, and *Gateway address* of 192.168.10.3 (InterJak 3 wireless interface). Necessary only for point-to-multipoint operation (access to 216.35.139.72 net from 216.35.139.64 net).

#### 7) **Configure InterJak 3**

Repeat steps described in 4), 5), and 6) for InterJak 3 (using wireless IP address of 192.168.10.3, and Ethernet IP address of 216.35.139.73). Also add a route back to 216.35.139.64 net if desired.

### Testing the Wireless Network

- From PC host on wired customer premises at InterJak 2, log into InterJak 2, and go to *System:Networking:Wireless 1*. Under *Detailed Interface Information*, *State* should show up, values under *Link*, *Signal*, *Noise*, *Channel*, *Tx Rate*, and *Current BSSID* should look valid. Click on *Show Signal Quality* button to view a dynamic web pop-up window showing current Signal/Link/Noise values.
- From PC host on wired customer premises at InterJak 2, open a command prompt, and perform the following commands:  
**ping 216.35.139.65** (address of InterJak 2 Ethernet interface)  
**ping 192.168.10.2** (address of InterJak 2 wireless interface)  
**ping 192.168.10.1** (address of InterJak 1 wireless interface)  
**ping 216.35.139.1** (address of InterJak 1 Ethernet interface)  
**ping** address of Internet router on wired infrastructure  
**ping 192.168.10.3** (address of InterJak 3 wireless interface)  
**ping 216.35.139.73** (address of InterJak 3 Ethernet interface), to check multi-point

If any of these fail, check to make sure the firewall and NAT/NAPT is disabled on both InterJaks, routes or default gateways are configured properly on all InterJaks, the wireless Interfaces are configured properly, and the end PC Hosts are configured properly.

### Remote Management

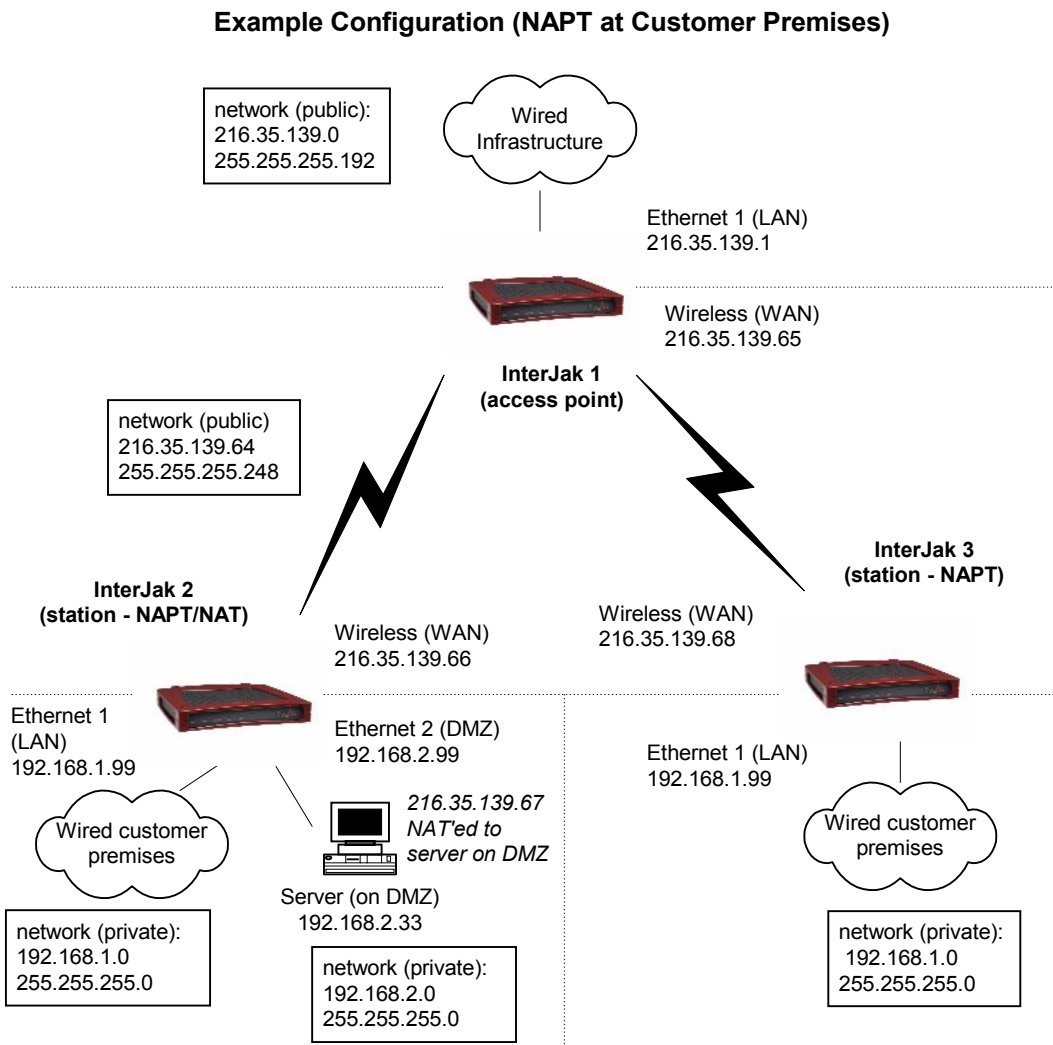
- To locally manage and monitor InterJak 1 from the wired infrastructure, perform one of the following:  
**Web Management Interface:** Type 216.35.139.1 into a web browser  
**Telnet CLI (Command Line Interface):** At a command prompt, type "telnet 216.35.139.1"  
**Telnet Syslog:** At a command prompt, type "telnet 216.35.139.1 24"
- To remotely manage and monitor InterJak 2 from the wired infrastructure, perform one of the following:  
**Web Management Interface:** Type 216.35.139.65 into a web browser

**Telnet CLI (Command Line Interface):** At a command prompt, type “telnet 216.35.139.65”  
**Telnet Syslog:** At a command prompt, type “telnet 216.35.139.65 24”

**Note:** All data passed over the InterJak Web Management Interface is encrypted via a Java applet, while all data passed over the telnet sessions are clear text. Use the optional InterJak VPN/PPTP service to support secure remote telnet sessions.

### Routed Wireless Configuration with NAPT/NAT (at Customer Premises)

An example point-to-multipoint configuration (with network address translation at customer premises) is shown in figure 6. One InterJak 200 802.11b serves as an access point at the wired infrastructure. Two additional InterJak stations provide wireless connections to the customer premises (and network address translation). In this example configuration, pools of private IP addresses are provided at the customer premises, while a small pool of public IP addresses are used for the wireless links.



**Figure 6: Example Routed Wireless Test Configuration (with NAPT/NAT at customer premises)**

## Equipment

- Three InterJak 200 802.11b products (InterJak 1, InterJak 2, InterJak 3)
- External antenna equipment for wireless links
- Infrastructure networking equipment, including Internet router
- Customer premises networking hosts

### 1) Configure Internet router (on wired infrastructure)

- Route to net 216.35.139.64, subnet 255.255.255.248, and gateway 216.35.139.1 (InterJak 1).

### 2) Connect InterJak 1 to infrastructure and antenna

- Connect InterJak Ethernet 1 interface to wired infrastructure
- Connect InterJak wireless interface to antenna equipment (via pigtail cable)
- Power-on InterJak 1

### 3) Configure InterJak 1

- Under *System*, under *System Information*, click on the *Edit* button, and enter information here such as *Windows workgroup* of wireless, *Server name* of InterJak1, etc.
- Under *Services:Firewall*, click on *Edit* and deselect the *Enable firewall* checkbox, and click *Apply*. This disables the firewall so that all traffic can pass through the WAN interface (custom firewall rules can be added later to further secure the wireless link).
- Under *Services:Address Translation (NAT/NAPT)*, click on *Edit* and deselect both *Enable NAPT* options at the top of the page, and click *Apply*. This disables NAPT between LAN and WAN, allowing standard routing.
- Under *Services:Networking:Ethernet 1*, choose the following settings and then click *Apply*:

*Enable* button selected

*IP address assignment* of Manual

*IP address* of 216.35.139.1

*Subnet mask* of 255.255.255.192 (net of 64)

*Enable DHCP server* deselected

*Allow direct IP* selected

- Under *Services:Networking:Wireless 1*, choose the following settings and then click *Apply*:

*Enable* button selected

*Operation Mode* of Infrastructure Access Point

*Network name* of InterJakNapt (or any other unique text)

*Channel number* of 6 (or any other unused wireless channel number)

*IP address assignment* of Manual

*IP address* of 192.168.10.1

*Subnet mask* of 255.255.255.248 (net of 8)

*Enable DHCP server* deselected

*Allow direct IP* selected

*Interface Type* of WAN

- Under *System:Routing*, under *Default Gateway*, click on *Edit*, and enter the *Gateway address* of the wired infrastructure Internet router.

### 4) Install InterJak 2

- Connect InterJak Ethernet 1 interface to customer premises network (e.g. switch on wired network)
- Connect InterJak Ethernet 2 interface to customer premises server (server on DMZ segment)
- Connect InterJak wireless interface to antenna equipment (via pigtail cable)
- Power-on InterJak 2

## 5) Configure PC hosts

- Configure customer premises PC hosts (at InterJak 2 net) to use DHCP for IP address, gateway, and DNS servers.
- Configure customer premises server (at InterJak 2 net) to use DHCP for IP address, gateway, and DNS servers.

## 6) Configure InterJak 2

- Under *System*, under *System Information*, click on the *Edit* button, and enter information here such as *Windows workgroup* of wireless, *Server name* of InterJak2, etc.
- Under *Services:Address Translation (NAT/NAPT)*, click on *Edit* and ensure that both NAPT options are enabled (NAPT to LAN, and NAPT to DMZ).
- Under *Services:Networking:Ethernet 1*, choose the following settings and then click *Apply*:

*Enable* button selected

*IP address assignment* of Manual

*IP address* of 192.168.1.99

*Subnet mask* of 255.255.255.0

*Enable DHCP server* selected

*Allow direct IP* selected

- Under *Services:Networking:Ethernet 2*, choose the following settings and then click *Apply*:

*Enable* button selected

*IP address assignment* of Manual

*IP address* of 192.168.2.99

*Subnet mask* of 255.255.255.0

*Enable DHCP server* selected

*Allow direct IP* selected

*Interface Type* of DMZ

- Under *Services:Networking:Wireless 1*, choose the following settings and then click *Apply*:

*Enable* button selected

*Operation Mode* of Infrastructure Station

*Network name* of InterJakNapt (same name configured for InterJak 1)

*Channel number* of 6 (for station mode, does not matter, as the channel will be automatically picked up from the InterJak access point)

*IP address assignment* of Manual

*IP address* of 216.35.139.66

*Subnet mask* of 255.255.255.248 (net of 8)

*Enable DHCP server* deselected

*Allow direct IP* selected

*Interface Type* of WAN

- Under *System:Routing*, under *Default Gateway*, click on *Edit*, and enter the *Gateway address* of 216.35.139.65 (wireless interface of InterJak 1).
- Under *System:Basic*, under *Domain Name System*, click on *Edit* and enter external DNS servers to be handed (via DHCP) to customer premises PC hosts.
- Under *Services:DHCP Server*, click on *Edit* to assign a static IP address to the customer premises server on InterJak Ethernet 2 port. Under *Static entries*, click on the *Add* button, enter an *IP address* of 192.168.2.33, *MAC address* of the server, *Host name* of the server, and click the *Add* button. This will ensure that the customer premises server will always receive 192.168.2.33 as its IP address from the InterJak DHCP server.
- Under *Services:Address Translation (NAT/NAPT)*, add a rule to NAT the public IP address of 216.35.139.67 to the customer premises server attached to InterJak Ethernet 2 port (private

address of 192.168.2.33). Under *Network Address Translation (NAT) Rules*, click on *Add NAT Rule* button, click on the *Enable* checkbox, enter *Public address* of 216.35.139.67, *Private address* of 192.168.2.33, and adjust settings under *Firewall* as necessary (e.g. *Enable web browsing (HTTP)* checkbox). When complete, hit the *Apply* button. This will translate the public address of 216.35.139.67 to private address of 192.168.2.33 on the DMZ.

**Note:** It is also possible to export services from the customer premises server to the InterJak public address of 216.35.139.66, via NAPT. Please see on-line web help pages and the InterJak Technical Reference Manual for more information on NAPT and NAT rules.

## 7) Configure InterJak 3

Repeat steps described in 4), 5), and 6) for InterJak 3 (using wireless IP address of 216.35.139.68, and Ethernet IP address of 192.168.1.99).

## Testing the Wireless Network

- From PC host on wired customer premises at InterJak 2, log into InterJak 2, and go to *System:Networking:Wireless 1*. Under *Detailed Interface Information*, *State* should show up, values under *Link*, *Signal*, *Noise*, *Channel*, *Tx Rate*, and *Current BSSID* should look valid. Click on *Show Signal Quality* button to view a dynamic web pop-up window showing current *Signal/Link/Noise* values.
- From PC host on wired customer premises, open a command prompt, and perform the following commands:
  - ping 192.168.1.99** (address of InterJak 2 Ethernet interface)
  - ping 216.35.139.66** (address of InterJak 2 wireless interface)
  - ping 216.35.139.65** (address of InterJak 1 wireless interface)
  - ping 216.35.139.1** (address of InterJak 1 Ethernet interface)
  - ping** address of Internet router on wired infrastructure

## Remote Management

- To locally manage and monitor InterJak 1 from the wired infrastructure, perform one of the following:
  - Web Management Interface:** Type 216.35.139.1 into a web browser
  - Telnet CLI (Command Line Interface):** At a command prompt, type "telnet 216.35.139.1"
  - Telnet Syslog:** At a command prompt, type "telnet 216.35.139.1 24"
- To remotely manage and monitor InterJak 2 from the wired infrastructure, perform one of the following:
  - Web Management Interface:** Type 216.35.139.66 into a web browser
  - Telnet CLI (Command Line Interface):** At a command prompt, type "telnet 216.35.139.66"
  - Telnet Syslog:** At a command prompt, type "telnet 216.35.139.66 24"

**Note:** All data passed over the InterJak Web Management Interface is encrypted via a Java applet, while all data passed over the telnet sessions are clear text. Use the optional InterJak VPN/PPTP service to support secure remote telnet sessions.

---

## Routed Wireless Configuration with NAPT (at ISP infrastructure)

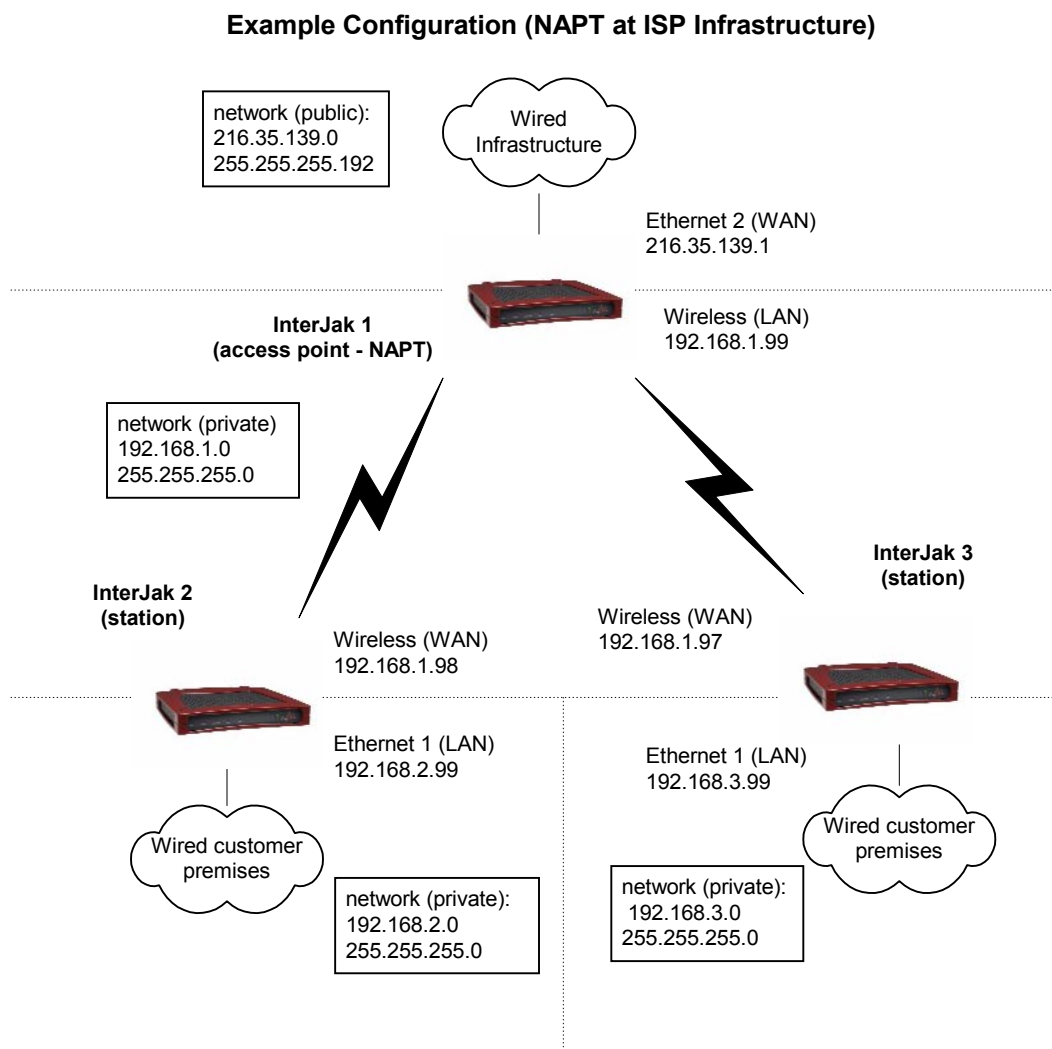
An example point-to-multipoint configuration (with network address translation at the wired infrastructure) is shown in figure 7. One InterJak 200 802.11b serves as an access point at the wired infrastructure (and provides network address translation). Two additional InterJak stations provide wireless connections to the customer premises. In this example configuration, pools of private IP addresses are provided for both the customer premises and the wireless links.

## Equipment

- Three InterJak 200 802.11b products (InterJak 1, InterJak 2, InterJak 3)
- External antenna equipment for wireless links
- Infrastructure networking equipment, including Internet router
- Customer premises networking hosts

### 1) Connect InterJak 1 to infrastructure and antenna

- Connect InterJak Ethernet 2 interface to wired infrastructure
- Connect InterJak wireless interface to antenna equipment (via pigtail cable)
- Power-on InterJak 1



**Figure 7: Example Routed Wireless Test Configuration (with NAPT/NAT at infrastructure)**

### 2) Configure InterJak 1

- Under *System*, under *System Information*, click on the *Edit* button, and enter information here such as *Windows workgroup* of wireless, *Server name* of InterJak1, etc.

- Under *Services:Firewall*, click on *Edit* and deselect the *Enable firewall* checkbox, and click *Apply*. This disables the firewall so that all traffic can pass through the WAN interface.
- Under *Services:Address Translation (NAT/NAPT)*, click on *Edit* and ensure that both NAPT options are enabled (NAPT to LAN, and NAPT to DMZ).
- Under *Services:Networking:Ethernet 2*, choose the following settings and then click *Apply*:

<i>Enable</i> button selected
<i>IP address assignment</i> of Manual
<i>IP address</i> of 216.35.139.1
<i>Subnet mask</i> of 255.255.255.192 (net of 64)
<i>Enable DHCP server</i> deselected
<i>Allow direct IP</i> selected
<i>Interface Type</i> of WAN

- Under *Services:Networking:Wireless 1*, choose the following settings and then click *Apply*:

<i>Enable</i> button selected
<i>Operation Mode</i> of Infrastructure Access Point
<i>Network name</i> of InterJakNapt (or any other unique text)
<i>Channel number</i> of 6 (or any other unused wireless channel number)
<i>IP address assignment</i> of Manual
<i>IP address</i> of 192.168.1.99
<i>Subnet mask</i> of 255.255.255.0
<i>Enable DHCP server</i> deselected
<i>Allow direct IP</i> selected
<i>Interface Type</i> of LAN

- Under *System:Routing*, under *Default Gateway*, click on *Edit*, and enter the *Gateway address* of the wired infrastructure Internet router.
- Under *System:Routing*, click on the *Add Route* button, enter *Destination subnet address* of 192.168.2.0, *Destination subnet mask* of 255.255.255.0, *Interface* of Gateway, and *Gateway address* of 192.168.1.98. This adds a route to the private net at InterJak 2 customer premises.
- Under *System:Routing*, click on the *Add Route* button, enter *Destination subnet address* of 192.168.3.0, *Destination subnet mask* of 255.255.255.0, *Interface* of Gateway, and *Gateway address* of 192.168.1.97. This adds a route to the private net at InterJak 3 customer premises.

### 3) Install InterJak 2

- Connect InterJak Ethernet 1 interface to customer premises network (e.g. switch on wired network)
- Connect InterJak wireless interface to antenna equipment (via pigtail cable)
- Power-on InterJak 2

### 4) Configure PC hosts

- Configure customer premises PC hosts (at InterJak 2 net) to use DHCP for IP address, gateway, and DNS servers.

### 5) Configure InterJak 2

- Under *System*, under *System Information*, click on the *Edit* button, and enter information here such as *Windows workgroup* of wireless, *Server name* of InterJak2, etc.
- Under *Services:Firewall*, click on *Edit* and deselect the *Enable firewall* checkbox, and click *Apply*. This disables the firewall so that all traffic can pass through the WAN interface (firewall may be enabled later to protect customer premises).
- Under *Services:Address Translation (NAT/NAPT)*, click on *Edit* and deselect both *Enable NAPT* options at the top of the page, and click *Apply*. This disables NAPT between LAN and WAN, allowing standard routing.

- Under *Services:Networking:Ethernet 1*, choose the following settings and then click *Apply*:

<i>Enable</i> button selected
<i>IP address assignment</i> of Manual
<i>IP address</i> of 192.168.2.99
<i>Subnet mask</i> of 255.255.255.0
<i>Enable DHCP server</i> selected
<i>Allow direct IP</i> selected

- Under *Services:Networking:Wireless 1*, choose the following settings and then click *Apply*:

<i>Enable</i> button selected
<i>Operation Mode</i> of Infrastructure Station
<i>Network name</i> of InterJakNapt (same name configured for InterJak 1)
<i>Channel number</i> of 6 (for station mode, does not matter, as the channel will be automatically picked up from the InterJak access point)
<i>IP address assignment</i> of Manual
<i>IP address</i> of 192.168.1.98
<i>Subnet mask</i> of 255.255.255.0
<i>Enable DHCP server</i> deselected
<i>Allow direct IP</i> selected
<i>Interface Type</i> of WAN

- Under *System:Routing*, under *Default Gateway*, click on *Edit*, and enter the *Gateway address* of 192.168.1.99 (wireless interface of InterJak 1).
- Under *System:Basic*, under *Domain Name System*, click on *Edit* and enter external DNS servers to be handed (via DHCP) to customer premises PC hosts.

## 6) Configure InterJak 3

Repeat steps described in 3), 4), and 5) for InterJak 3 (using wireless IP address of 192.168.1.97, and Ethernet IP address of 192.168.3.99).

## Testing the Wireless Network

- From PC host on wired customer premises at InterJak 2, log into InterJak 2, and go to *System:Networking:Wireless 1*. Under *Detailed Interface Information*, *State* should show up, values under *Link*, *Signal*, *Noise*, *Channel*, *Tx Rate*, and *Current BSSID* should look valid. Click on *Show Signal Quality* button to view a dynamic web pop-up window showing current Signal/Link/Noise values.
- From PC host on wired customer premises at InterJak 2, open a command prompt, and perform the following commands:  
**ping 192.168.2.99** (address of InterJak 2 Ethernet interface)  
**ping 192.168.1.98** (address of InterJak 2 wireless interface)  
**ping 192.168.1.99** (address of InterJak 1 wireless interface)  
**ping 216.35.139.1** (address of InterJak 1 Ethernet interface)  
**ping** address of Internet router on wired infrastructure

## Remote Management

- To locally manage and monitor InterJak 1 from the wired infrastructure, perform one of the following:  
**Web Management Interface:** Type 216.35.139.1 into a web browser  
**Telnet CLI (Command Line Interface):** At a command prompt, type "telnet 216.35.139.1"  
**Telnet Syslog:** At a command prompt, type "telnet 216.35.139.1 24"

- To remotely manage and monitor InterJak 2 from the wired infrastructure, additional steps must be performed, since InterJak 1 is NAPTing from the wireless segment to the wired infrastructure. There are two possible ways to allow remote management of InterJak 2 or InterJak 3 from the wired infrastructure:

Create NAT rules to map a public IP address at the wired infrastructure (e.g. 216.35.139.2) to the private IP address on InterJak 2 or InterJak 3 (e.g. 192.168.1.98). This can be done under *Services:Address Translation:Network Address Translation (NAT) Rules*, clicking on *Add NAT Rule*, typing in the proper IP addresses, and selecting *Enable web browsing (HTTP)* and *Enable Telnet*. It is then possible to use this NATed public IP address to manage the remote InterJak.

Connect a PC host or separate private network directly to the Ethernet 1 port on InterJak 1 from the wired infrastructure. Configure the Ethernet 1 port as another LAN interface with private network (e.g. 192.168.10.0), and add a route to the wireless private net (192.168.1.0). It will then be possible to remotely manage InterJak 2 or InterJak 3 by using the private wireless IP address of each system.

**Note:** All data passed over the InterJak Web Management Interface is encrypted via a Java applet, while all data passed over the telnet sessions are clear text. Use the optional InterJak VPN/PPTP service to support secure remote telnet sessions.

---

## Other Wireless Configurations

A large number of additional wireless configurations are possible through use of the InterJak routing (static, RIP1, RIP2), NAPT, and multi-NAT capabilities. NAPT (Network Address and Port Translation) and NAT (Network Address Translation) are described in detail within the InterJak Technical Reference Manual.

The support of two independent Fast Ethernet interfaces on the InterJak 200 802.11b allows for protected DMZ segments, and additional combinations of routing, NAPT, and NAT functions. For example, at the end customer premises, one Ethernet port may be used to route a small public subnet for use with local servers, while the second Ethernet port may be used with NAPT to share a single public IP address among a large number of workstations.

Some possible routing, NAPT, and NAT configurations might include:

**Pure Routing:** InterJak at ISP infrastructure running as router, InterJak at end customer premises running as router, with either public or private subnet covering wireless links.

**ISP side routing, customer side NAPT/NAT:** InterJak at ISP infrastructure running as router, InterJak at end customer premises performing NAPT of wireless public IP address to customer private IP addresses. InterJak at end customer premises may also perform NAT of additional addresses to end customer private IP addresses (for local servers).

**ISP side NAPT, customer side routing:** InterJak at ISP infrastructure performing NAPT of public IP address to private wireless subnet, InterJak at end customer premises running as router between private wireless subnet and private end customer subnet.

**ISP side NAPT, customer side NAPT:** InterJak at ISP infrastructure performing NAPT of public IP address to private wireless subnet, InterJak at end customer premises performing NAPT of private address on wireless subnet to private end customer subnet.

**ISP side NAT, customer side NAPT/NAT:** InterJak at ISP infrastructure performing NAT of public IP addresses to private addresses on wireless subnet, InterJak at end customer premises performing NAPT of each address to private end customer subnet. InterJak at end customer premises may also perform NAT of additional addresses to end customer private IP addresses (for local servers).

### Traffic Shaping Configuration

An example point-to-multipoint routed configuration is shown in figure 8. With the optional Filanet traffic shaping service, it is possible to prioritize and shape traffic. It is also possible to set simple bandwidth limits on wireless links to prevent overloading of a wireless link, to enforce service level agreements, or to balance traffic flow in point-to-multipoint configurations.

Following is an example configuration demonstrating how to set simple upstream and downstream bandwidth limits for each wireless link. For more information on the traffic shaping service, please see the InterJak web management interface on-line help and InterJak Technical Reference Manual.

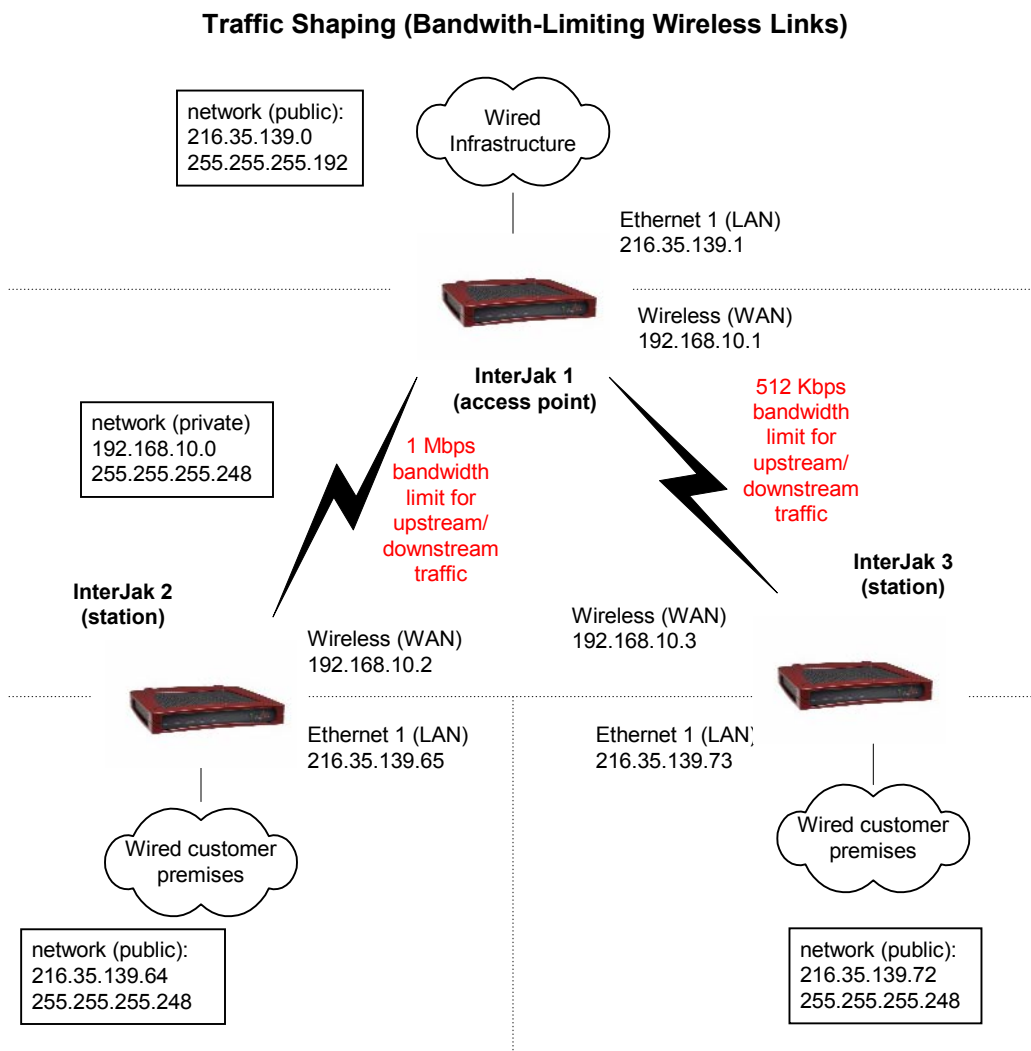


Figure 8:

### Traffic Shaping Test Configuration

### Traffic Shaping Requirements (for this example configuration)

- Total tested bandwidth of wireless links is 4 Mbps (will vary depending upon installation)
- Wireless link between InterJak 1 (at ISP infrastructure) and InterJak 2 (at customer premises) to be bandwidth limited to 1 Mbps (service level agreement).
- Wireless link between InterJak 1 (at ISP infrastructure) and InterJak 3 (at customer premises) to be bandwidth limited to 512 Kbps (service level agreement).
- All upstream and downstream traffic of all types (TCP, UDP, ICMP) is to be bandwidth limited.

## Important Notes

- Traffic shaping only affects traffic transmitted (not received). This means that traffic shaping should be enabled on both the InterJak at the ISP infrastructure and the InterJak at the customer premises.
- You should have a feel for the overall bandwidth supported by a particular wireless link before setting bandwidth limits.
- Queues, classifiers, and firewall rules are used to allow complete flexibility in shaping or bandwidth limiting particular types of traffic, source of traffic, and destination of traffic.
- A Traffic Shaping Interface must be enabled, at least one Queue must be defined, and at least one associated Classifier must be added for traffic shaping or bandwidth limiting to occur.

### 1) Configure InterJak 1 at ISP infrastructure

- Under *Services*, click on *Enter Service Key* button if needed to enable optional traffic shaping service.
- Under *Services:Traffic Shaping*, click on *Edit* button under *Traffic Shaping Interface 1* to enable traffic shaping.
- Click on *Enable* checkbox, select the *Wireless 1* interface, set *Bandwidth* to 4 Mbps, and click on *Apply*.
- Click on *Queue 1* under *Traffic Shaping Interface 1*, click on *Enable* checkbox, set *Bandwidth* to 1 Mbps (Maximum Bandwidth Allowed), and click on *Apply*. **Note:** Queue 1 will be used for downstream traffic shaping to InterJak 2 at the customer premises.
- Click on *Queue 2* under *Traffic Shaping Interface 1*, click on *Enable* checkbox, set *Bandwidth* to 512 Kbps (Maximum Bandwidth Allowed), and click on *Apply*. **Note:** Queue 2 will be used for downstream traffic shaping to InterJak 3 at the customer premises.
- At the bottom of the *Traffic Shaping* page, click on the *Firewall Services* button. This will allow the creation of a specific Firewall Service to bandwidth limit all traffic. **Note:** Firewall Services are used to classify the types of traffic to shape.
- Under *Firewall Services*, click on the *Add Firewall Service* button. Under *Add Service*, enter a *Name* of "All traffic" (no quotes), click on the *Enable* checkbox under *First Traffic Definition*, and select *Protocol* of *All*. Leave all other fields empty and click on *Apply*.
- At the bottom of the *Traffic Shaping* page, under *Classifiers*, click on the *Add Classifier* button. This is used to associate a traffic classifier with one of the Queues created above, so that the Queue can bandwidth limit based on type, source, and destination of traffic.
- Under *Add Traffic Classifier*, select the *Firewall service* of *All traffic* (the one created earlier), set the *Source IP address/mask* to 0.0.0.0/0.0.0.0, *Destination IP address/mask* to 216.35.139.64/255.255.255.248, *Traffic queue* to *Queue 1*, and click on *Apply*. **Note:** This associates all traffic destined to the wired customer premises network at InterJak 2 with Traffic Queue 1 (which is bandwidth limited to 1 Mbps).
- Under *Add Traffic Classifier*, select the *Firewall service* of *All traffic* (the one created earlier), set the *Source IP address/mask* to 0.0.0.0/0.0.0.0, *Destination IP address/mask* to 216.35.139.72/255.255.255.248, *Traffic queue* to *Queue 2*, and click on *Apply*. **Note:** This associates all traffic destined to the wired customer premises network at InterJak 3 with Traffic Queue 2 (which is bandwidth limited to 512 Kbps).

- 2) **Configure InterJak 2 at customer premises** (Note: This may be done remotely by entering 216.35.139.65 into a web browser)
  - Under *Services*, click on *Enter Service Key* button if needed to enable optional traffic shaping service.
  - Under *Services:Traffic Shaping*, click on *Edit* button under *Traffic Shaping Interface 1* to enable traffic shaping.
  - Click on *Enable* checkbox, select the *Wireless 1* interface, set *Bandwidth* to 4 Mbps, and click on *Apply*.
  - Click on *Queue 1* under *Traffic Shaping Interface 1*, click on *Enable* checkbox, set *Bandwidth* to 1 Mbps (Maximum Bandwidth Allowed), and click on *Apply*. **Note:** Queue 1 will be used for upstream traffic shaping to InterJak 1 at the ISP infrastructure.
  - At the bottom of the *Traffic Shaping* page, click on the *Firewall Services* button.
  - Under *Firewall Services*, click on the *Add Firewall Service* button. Under *Add Service*, enter a *Name* of "All traffic" (no quotes), click on the *Enable* checkbox under *First Traffic Definition*, and select *Protocol* of *All*. Leave all other fields empty and click on *Apply*.
  - At the bottom of the *Traffic Shaping* page, under *Classifiers*, click on the *Add Classifier* button.
  - Under *Add Traffic Classifier*, select the *Firewall service* of *All traffic* (the one created earlier), set the *Source IP address/mask* to 216.35.139.64/255.255.255.248, *Destination IP address/mask* to 0.0.0.0/0.0.0.0, *Traffic queue* to *Queue 1*, and click on *Apply*. **Note:** This associates all traffic sent from the customer premises across the wireless link with Traffic Queue 1 (which is bandwidth limited to 1 Mbps).

Traffic Queue 2 (which is bandwidth limited to 512 Kbps).
- 3) **Configure InterJak 3 at customer premises** (Note: This may be done remotely by entering 216.35.139.73 into a web browser)
  - Repeat step described above in 2) for InterJak 3 (using *Bandwidth* of 512 Kbps and *Source IP address/mask* of 216.35.139.72/255.255.255.248). This will bandwidth-limit upstream traffic to 512 Kbps.

---

## Basic Firewall Configuration

The InterJak 200 802.11b product's built-in stateful firewall may be used to help protect both the ISP infrastructure and the end customer premises from intruders. This, in conjunction with unique Wireless Network Names (SSIDs), the Closed Wireless Network Option, and optional VPN service, can help ensure protection of both the wireless link itself and the wired networks on either side of the link.

Following are some basic firewall settings to support a simple routed wireless network (see Figure 8 for reference). For detailed information on the InterJak firewall service, please refer to the InterJak Technical Reference Manual.

### Firewall Requirements (for the example configuration shown in Figure 8)

- Basic firewall support on InterJak at customer premises to protect customer's internal wired network.
- Firewall support on InterJak at ISP infrastructure to only accept wireless traffic originating from customer premises network.

## Important Notes

- Very sophisticated and flexible firewall rules are possible with the InterJak 200 802.11b. Please refer to the InterJak Technical Reference Manual for detailed information on the InterJak firewall service.
  - When changing firewall rules on an InterJak remotely, it is possible to lock yourself out of the remote web management interface (via the firewall). When changing firewall settings, please take advantage of the InterJak “Test Configuration Mode” support (*System:Maintenance:Test Configuration Mode*). This allows new configuration changes to be safely tested before fully committing the changes. If the remote connection is lost due to the new changes, the test configuration mode will time-out and you will be able to re-connect after the time-out period. Please see the on-line help under *System:Maintenance:Test Configuration Mode* for details.
- 1) **Enable Firewall on InterJaks 2 and 3 at Customer Premises** (Note: These changes may be made remotely by typing the IP address of the remote InterJak into a web browser).
    - On InterJak 2, under *Services:Firewall*, under *Firewall Setup*, click on the *Edit* button.
    - Select the *Allow WAN access to web management*, in order to allow remote web management from the ISP infrastructure. Select *Log firewall violation attempts* if desired (these can be logged locally, to a syslog server, or to a system admin via an e-mail message). Select other firewall checkbox options as necessary (see on-line help for details).
    - Click on the *Apply* button. The firewall will now protect the customer premises wired LAN from the wireless WAN.
    - Perform the above steps on InterJak 3.
  - 2) **Enable Firewall on InterJak 1 at ISP Infrastructure**
    - On InterJak 1, under *Services:Firewall*, under *Firewall Services*, click on the *Add Firewall Service* button. Under *Add Service*, enter a *Name* of “All traffic” (no quotes), click on the *Enable* checkbox under *First Traffic Definition*, and select *Protocol* of *All*. Leave all other fields empty and click on *Apply*. This creates a firewall definition supporting all traffic, and will be used to open a hole in the firewall for the customer premises wired network.
    - Under *Firewall Services*, click on the *Add Rule* button, under *Firewall service* select “All traffic”, under *Source IP address/mask* enter 216.168.139.64 and 255.255.255.248 (customer network at InterJak 2). Under *Destination IP address/mask* enter 0.0.0.0 and 0.0.0.0 (for all addresses). Under *Action* select *ACCEPT*, under *Chain* select *ALL*. Click on the *Apply* button. This opens a hole in the firewall allowing all traffic originating from the 216.168.139.64 network.
    - Under *Firewall Services*, click on the *Add Rule* button, under *Firewall service* select “All traffic”, under *Source IP address/mask* enter 216.168.139.72 and 255.255.255.248 (customer network at InterJak 3). Under *Destination IP address/mask* enter 0.0.0.0 and 0.0.0.0 (for all addresses). Under *Action* select *ACCEPT*, under *Chain* select *ALL*. Click on the *Apply* button. This opens a hole in the firewall allowing all traffic originating from the 216.168.139.72 network.

---

## Advanced: RTS/CTS and Fragmentation Thresholds

For advanced tuning of heavily loaded point-to-multipoint wireless links, it is possible to reduce the number of wireless collisions through use of RTS/CTS (request to send/clear to send) signaling. This feature is only necessary on point-to-multipoint wireless links where there are heavy traffic loads sent from several stations to an access point (e.g. upstream traffic). Downstream traffic from the access point to one or more stations is not normally affected by loads and does not benefit from RTS/CTS signaling.

Support for RTS/CTS signaling may be enabled through the InterJak Command Line Interface (CLI), Service Provisioning Portal (SPP), or by updating the InterJak Configuration File. Please see the InterJak Technical Reference Manual for details on using the InterJak Command Line Interface (CLI) or editing the InterJak Configuration File.

Following is an example demonstrating how to enable RTS/CTS signaling for packets larger than 500 bytes. Please note that RTS/CTS should only be enabled on an end station InterJak (normally those at the customer premises).

Changing RTS/CTS Threshold via CLI (enable signaling for packets larger than 500 bytes):

- Telnet to the InterJak, and enter your administrator name and password.
- Type **help** to see the list of all CLI commands, and **wlan** for status on the wireless interface.
- Type the following at the CLI interface to change the current RTS/CTS threshold to 500 bytes (from default value of 2347).  
**config**  
**[:wlan0]**  
**rts threshold=500**  
**end**
- The RTS/CTS threshold change will be merged into the InterJak Configuration File. You will have to restart the InterJak for this change to take effect. To change the RTS/CTS threshold back to its original value (disabled), perform the above steps but set “rts threshold” to 2347.

Wireless fragmentation threshold settings may be changed in this way as well, and may help in environments where there is heavy interference or packet loss. Normally it will not be necessary to change the default fragmentation threshold (disabled), but if necessary a fragmentation threshold may be set on InterJak stations and access points.

Changing Fragmentation Threshold via CLI (enable wireless packet fragmentation for packets larger than 500 bytes):

- Telnet to the InterJak, and enter your administrator name and password.
- Type the following at the CLI interface to change the current fragmentation threshold to 500 bytes (from default value of 2346).  
**config**  
**[:wlan0]**  
**fragmentation threshold=500**  
**end**
- The fragmentation threshold change will be merged into the InterJak Configuration File. You will have to restart the InterJak for this change to take effect. To change the fragmentation threshold back to its original value (disabled), perform the above steps but set “fragmentation threshold” to 2346.

---

## For Further Information

For general information on the InterJak Service Appliance product line, and services available, please see the main Filanet web site at <http://www.filanet.com>. For access to the InterJak Technical Reference Manual and other application notes, please see the Filanet support section at <http://www.filanet.com/support>.